PTO/SB/14 (11-08)
Approved for use through 09/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	9400.004.02
	Application Number	
Title of Invention	METHODS AND APPARATUS FOR DEALING WITH MALWARE	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Applicant Information:

Applicant 1 Remove

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Melvyn		Morris	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Belper	Country Of Residence[i]	GB

Citizenship under 37 CFR 1.41(b)[i] GB

Mailing Address of Applicant:

Address 1	Webroot Inc.		
Address 2	385 Interlocken Crescent, Suite 800		
City	Broomfield	State/Province	CO
Postal Code	80021	Country[i]	US

Applicant 2 Remove

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Joseph		Jaroch	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Elk Grove Village	State/Province	IL	Country of Residence[i]	US

Citizenship under 37 CFR 1.41(b)[i] US

Mailing Address of Applicant:

Address 1	Webroot Inc.		
Address 2	385 Interlocken Crescent, Suite 800		
City	Broomfield	State/Province	CO
Postal Code	80021	Country[i]	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

PTO/SB/14 (11-08)
Approved for use through 09/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	9400.004.02
	Application Number	
Title of Invention	METHODS AND APPARATUS FOR DEALING WITH MALWARE	

Customer Number	61529		
Email Address	sean@nodiplaw.com	Add Email	Remove Email

Application Information:

Title of the Invention	METHODS AND APPARATUS FOR DEALING WITH MALWARE		
Attorney Docket Number	9400.004.02	Small Entity Status Claimed	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		Sub Class (if any)	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)		Suggested Figure for Publication (if any)	

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S. C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	61529		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Prior Application Status			Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61443095	2011-02-15

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

PTO/SB/14 (11-08)
Approved for use through 09/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	9400.004.02
	Application Number	
Title of Invention	METHODS AND APPARATUS FOR DEALING WITH MALWARE	

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).

Remove

Application Number	Country [i]	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
			(•) Yes ( ) No

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Assignee Information:

Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office.

Assignee 1 Remove

If the Assignee is an Organization check here. [X]

Organization Name	Webroot Inc.		
Mailing Address Information:			
Address 1	385 Interlocken Crescent		
Address 2	Suite 800		
City	Broomfield	**State/Province**	CO
Country [i]	US	Postal Code	80021
Phone Number		Fax Number	
Email Address			

Additional Assignee Data may be generated within this form by selecting the **Add** button. Add

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/Sean R. O'Dowd/			Date (YYYY-MM-DD)	2012-02-13
First Name	Sean R.	Last Name	O'Dowd	Registration Number	53403

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

METHODS AND APPARATUS FOR DEALING WITH MALWARE

Claim of Priority under 35 U.S.C. §119

[0001] The present Application for Patent claims priority to Provisional Application No. 61/443,095 entitled "METHODS AND APPARATUS FOR DEALING WITH MALWARE" filed February 15, 2011, and assigned to the assignee hereof and hereby expressly incorporated by reference herein.

Reference to Co-Pending Applications for Patent

[0002] The present Application for Patent is related to the following co-pending U.S. Patent Applications: "METHODS AND APPARATUS FOR MALWARE THREAT RESEARCH," having Attorney Docket No. 9400.004.03, filed concurrently herewith, assigned to the assignee hereof, and expressly incorporated by reference herein; and "METHODS AND APPARATUS FOR AGENT-BASED MALWARE MANAGEMENT" having Attorney Docket No. 9400.004.04, filed concurrently herewith, assigned to the assignee hereof, and expressly incorporated by reference herein.

BACKGROUND

Field

[0003] The present invention relates generally to methods and apparatus for dealing with malware. And more specifically, systems and methods for protection against malware.

Background

[0004] The term "malware" is used herein to refer generally to any executable computer file or, more generally "object", that is or contains malicious code, and thus includes viruses, Trojans, worms, spyware, adware, etc. and the like.

[0005] A typical anti-malware product, such as virus scanning software, scans objects or the results of an algorithm applied to the object or part thereof to look for signatures in the object that are known to be indicative of the presence of malware. Generally, the method of dealing with malware is that when new types of malware are released, for example via the Internet, these are eventually detected. Once new items of malware

have been detected, then the service providers in the field generate signatures that attempt to deal with these and these signatures are then released as updates to their anti-malware programs. Heuristic methods have also been employed.

[0006] These systems work well for protecting against known malicious objects. However, since they rely on signature files being generated and/or updated, there is inevitably a delay between a new piece of malware coming into existence or being released and the signatures for identifying that malware being generated or updated and supplied to users. Thus, users are at risk from new malware for a certain period of time which might be up to a week or even more.

[0007] More recently, so-called "cloud" based techniques have been developed for fighting malware/viruses. In these techniques, protection is provided by signatures that are stored in the cloud, i.e. in a central server to which the remote computers are connected. Thus, a remote computer can be given protection as soon as a new malware object is spotted and its signature stored in the central server, so that the remote computer is protected from it without the need to wait for the latest signatures to be downloaded and installed on the remote computer. This technique can also give the advantage of moving the processing burden from the remote computer to the central server. However, this technique is limited by sending only signature information or very basic information about an object to the central server. Therefore, in order to analyse whether or not an unknown object is malware, a copy of that object is normally sent to the central server where it is investigated by a human analyst. This is a time consuming and laborious task introducing considerable delay in classifying malware as safe or unsafe. Also, given the considerable volume of new objects that can be seen daily across a community, it is unrealistic to have a skilled human analyst investigate each new object thoroughly. Accordingly, malevolent objects may escape investigation and detection for considerable periods of time during which time they can carry out their malevolent activity in the community.

[0008] We refer in the following to our previous application US-A-2007/0016953, published 18th January 2007, entitled "METHODS AND APPARATUS FOR DEALING WITH MALWARE," the entire contents of which are hereby incorporated by reference. In this document, various new and advantageous cloud-based strategies for fighting malware are disclosed. In particular a cloud-based approach is outlined where the central server receives information about objects and their behaviour on

remote computers throughout the community and builds a picture of objects and their behaviour seen throughout the community. This information is used to make comparisons with this data across the community in developing and applying various heuristics and or rules to determine whether a newly seen object is malevolent or not.

[0009] This approach to fighting malware involves communicating, storing and managing vast amounts of data at the central server, which is a challenging problem in itself. It is also challenging to develop new schemes for more accurately and more efficiently detecting malware given the vast amount of data collected about objects seen in the community and the constantly evolving strategies used by malware writers to evade detection. It is also desirable to improve the processes for analysing the data to make the best use of the time and specialised skills of the human malware analysts.

[0010] Malware is also becoming increasingly adept at self-defence by interfering with the operation of security programs installed on a computer. This is another problem that security software must contend with.

SUMMARY

[0011] According to a first aspect of the present invention, there is provided a method of classifying a computer object as malware, the method includes:

at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored and or processed;

wherein the base computer comprises plural threat servers arranged to receive the data from the plural remote computers and apply rules and or heuristics against that data in real time to determine whether or not the object is malware and to communicate the determination to the remote computers;

the base computer further comprising at least one central server in communication with the threat servers and arranged to receive the data about objects from the threat servers to maintain a master database of data received about objects from all of the threat servers.

[0012] According to another aspect, an apparatus is provided for classifying a computer object as malware, the apparatus includes a base computer arranged to receive data about a computer object from each of plural remote computers on which the object or similar objects are stored or processed. The base computer includes plural threat servers arranged to receive the data from the plural remote computers and apply rules or

heuristics against that data in real time to determine whether or not the object is malware and to communicate the determination to the remote computers. The the base computer also includes at least one central server in communication with the threat servers and arranged to receive the data about objects from the servers to maintain a master database of data received about objects from all threat servers.

[0013] According to yet another aspect, a method is provided for connecting a remote computer to one of a plurality of servers. The method includes installing an agent program on the remote computer, the agent program having an algorithm for allocating the remote computer to a server determined by the time when the agent program was installed; and connecting the agent program to the allocated server.

[0014] As will become apparent in view of the following disclosure, the various aspects and embodiments of the invention can be combined.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] Figure 1 shows schematically apparatus in which an embodiment of the present invention may be implemented;

[0016] Figure 2 is a flowchart showing schematically the operation of an example of a method according to an embodiment of the present invention;

[0017] Figure 3 shows a more detailed view of an example of a base computer 3 according to an embodiment of the present invention;

[0018] Figure 4 shows an example where web servers are located in different geographical locations;

[0019] Figure 5 shows schematically the apparatus of Figure 3 in more detail and in particular the way in which data can be moved from the FX layer to the ENZO layer in an embodiment;

[0020] Figure 6 shows schematically an example in which a new instance of an ENZO server is created in accordance with an embodiment of the invention;

[0021] Figure 7 shows schematically an example of apparatus by which an ENZO server shares out its workload between plural servers in accordance with an embodiment of the invention;

[0022] Figure 8 is a chart showing an example of a scheme for analysing data about objects according to an embodiment of the present invention;

[0023] Figure 9 show shows schematically an example of a scheme for processing data about objects according to an embodiment of the invention;

[0024] Figures 10 to 13 show graphical user interfaces of an example of a computer program for researching objects according to an embodiment of the present invention;

[0025] Figure 14 shows an example of an agent program on a remote computer according to an embodiment of the present invention; and

[0026] Figure 15 shows the hierarchy on a computer system.

DETAILED DESCRIPTION

[0027] **OVERVIEW**

[0028] Referring to Figure 1, a computer network is generally shown as being based around a distributed network such as the Internet 1. Embodiments of the present invention may however be implemented across or use other types of network, such as a LAN. Plural local or "remote" computers 2 are connected via the Internet 1 to a "central" or "base" computer 3. The computers 2 may each be variously a personal

computer, a server of any type, a PDA, mobile phone, an interactive television, or any other device capable of loading and operating computer objects. An object in this sense may be a computer file, part of a file or a sub-program, macro, web page or any other piece of code to be operated by or on the computer, or any other event whether executed, emulated, simulated or interpreted. An object 4 is shown schematically in the figure and may for example be downloaded to a remote computer 2 via the Internet 1 as shown by lines 5 or applied directly as shown by line 6. The object 4 may reside in computer RAM, on the hard disk drive of the computer, on removable storage connected to the computer, such as a USB pen drive, an email attachment, etc.

[0029] In one exemplary embodiment, the base computer 3 is in communication with a database 7 with which the remote computers 2 can interact when the remote computers 2 run an object 4 to determine whether the object 4 is safe or unsafe. The community database 7 is populated, over time, with information relating to each object run on all of the connected remote computers 2. As will be discussed further below, data representative of each object 4 may take the form of a so-called signature or key relating to the object, its attributes and behaviour.

[0030] Referring now to Figure 2, at the start point 21, a computer object 4 such as a process is run at a remote computer 2. At step 22, by operation of a local "agent" program or software running on the remote computer 2, the operation of the process is hooked so that the agent program can search a local database stored at the remote computer 2 to search for a signature or key representing that particular process, its related objects and/or the event. If the local signature is present, it will indicate either that the process is considered to be safe or will indicate that that process is considered unsafe. An unsafe process might be one that has been found to be malware or to have unforeseen or known unsafe or malevolent results arising from its running. If the signature indicates that the process is safe, then that process or event is allowed by the local agent program on the remote computer 2 to run at step 23. If the signature indicates that the process is not safe, then the process or event is stopped at step 24.

[0031] It will be understood that there may be more than two states than "safe" or "not-safe" and choices may be given to the user. For example, if an object is considered locally to be not safe, the user may be presented with an option to allow the related process to run nevertheless. It is also possible for different states to be presented to each

remote computer 2. The state can be varied by the base computer to take account of the location, status or ownership of the remote computer or timeframe.

[0032] Furthermore, the agent software at the remote computer 2 may be arranged to receive rules or heuristics from the base computer 3 for classifying objects as safe or unsafe. If the object is unknown locally, the agent software may apply the rules or heuristics to the details of the object to try to classify the object as safe or unsafe. If a classification is made, details of the object and classification are passed to the base computer 3 to be stored in the community database 7. This means that the agent software is capable of providing protection against previously unseen objects even if it is "offline", e.g. it is unable to connect to the base computer for any reason. This mechanism is described in more detail later in the disclosure.

[0033] If the object is still not classified locally, then details of the object are passed over the Internet 1 or other network to the base computer 3 for storing in the community database 7 and for further analysis at the base computer 3. In that case, the community database 7 is then searched at step 25 for a signature for that object that has already been stored in the community database 7. The community database 7 is supplied with signatures representative of objects, such as programs or processes, run by each monitored remote computer 2. In a typical implementation in the field, there may be several thousands or even millions of remote computers 2 connected or connectable to the base computer 3 and so any objects that are newly released upon the Internet 1 or that otherwise are found on any of these remote computers 2 will soon be found and signatures created and sent to the base computer 3 by the respective remote computers 2.

[0034] When the community database 7 is searched for the signature of the object that was not previously known at the remote computer 2 concerned, then if the signature is found and indicates that that object is safe, then a copy of the signature or at least a message that the object is safe is sent to the local database of the remote computer 2 concerned at step 26 to populate the local database. In this way, the remote computer 2 has this information immediately to hand the next time the object 4 is encountered. A separate message is also passed back to the remote computer 2 to allow the object to run in the current instance.

[0035] If the signature is found in the community database 7 and this indicates for some reason that the object is unsafe, then again the signature is copied back to the local

database and marked "unsafe" at step 27, and/or a message is sent to the remote computer 2 so that running of the object is stopped (or it is not allowed to run) and/or the user given an informed choice whether to run it or not.

[0036] If after the entire community database 7 has been searched the object is still unknown, then it is assumed that this is an entirely new object which has never been seen before in the field. A signature is therefore created representative of the object at step 28, or a signature sent by the remote computer 2 is used for this purpose.

[0037] At this point, rules or heuristics may be applied by the base computer 3 to the details of the object to try to classify the object as safe or unsafe. If a classification is made, the signature is marked as safe or unsafe accordingly in the community database 7. The signature is copied to the local database of the remote computer 2 that first ran the object. This mechanism is described in more detail later in the disclosure.

[0038] If the object is still not classified, the signature may be initially marked as bad or unsafe in the community database 7 at step 29. The signature is copied to the local database of the remote computer 2 that first ran the object at step 30. A message may then be passed to the remote computer 2 to instruct the remote computer 2 not to run the object or alternatively the user may be given informed consent as to whether to allow the object to run or not. In addition, a copy of the object itself may be requested at step 31 by the community database 7 from the remote computer 2.

[0039] If the user at the remote computer 2 chooses to run a process that is considered unsafe because it is too new, then that process may be monitored by the remote computer 2 and/or community database 7 and, if no ill effect occurs or is exhibited after a period of time of n days for example, it may then be considered to be safe. Alternatively, the community database 7 may keep a log of each instance of the process which is found by the many remote computers 2 forming part of the network and after a particular number of instances have been recorded, possibly with another particular number of instances or the process being allowed to run and running safely, the signature in the community database 7 may then be marked as safe rather than unsafe. Many other variations of monitoring safety may be done within this concept.

[0040] The database 7 may further include a behaviour mask for the object 4 that sets out the parameters of the object's performance and operation. If an object is allowed to run on a remote computer 2, even if the initial signature search 22 indicates that the object is safe, then operation of that object may be monitored within the parameters of

the mask. Any behaviour that extends beyond that permitted by the mask is identified and can be used to continually assess whether the object continues to be safe or not.

[0041] The details of an object 4 that are passed to the base computer 3 may be in the form of a signature or "key" that uniquely identifies the object 4. This is mainly to keep the data storage and transmission requirements as minimal as possible. This key may be formed by a hashing function operating on the object at the remote computer 2.

[0042] The key in the exemplary embodiment is specially arranged to have at least three severable components, a first of the components representing executable instructions contained within or constituted by the object, a second of the components representing data about the object, and a third of the components representing the physical size of the object. The data about the object in the second component may be any or all of the other forms of identity such as the file's name, its physical and folder location on disk, its original file name, its creation and modification dates, resource information such as vendor, product and version, and any other information stored within the object, its file header or header held by the remote computer 2 about it; and, events initiated by or involving the object when the object is created, configured or runs on the respective remote computers. In general, the information provided in the key may include at least one of these elements or any two or more of these elements in any combination.

[0043] In one embodiment, a checksum is created for all executable files, such as (but not limited to) .exe and .dll files, which are of the type PE (Portable Executable file as defined by Microsoft). Three types of checksums are generated depending on the nature of the file:

[0044] Type 1: five different sections of the file are check summed. These include the import table, a section at the beginning and a section at the end of the code section, and a section at the beginning and a section at the end of the entire file. This type applies to the vast majority of files that are analysed;

[0045] Type 2: for old DOS or 16 bit executable files, the entire file is check summed;

[0046] Type 3: for files over a certain predefined size, the file is sampled into chunks which are then check summed. For files less than a certain predefined size, the whole file is check summed.

[0047] For the check summing process, in principle any technique is possible. The MD5 (Message-Digest algorithm 5) is a widely-used cryptographic hash function that may be used for this purpose.

[0048] This allows a core checksum to be generated by viewing only the executable elements of the checksum and making a comparison between two executables that share common executable code.

[0049] For the type 1 checksum mentioned above, three signature processes may be used. The first defines the entire file and will change with almost any change to the file's content. In particular, the first defines a representative sampling of the contents of the program in that if any fundamental change is made to the program, the checksum will change, but trivial changes can be identified as such, allowing correlation back to the original program body. The second attempts to define only the processing instructions of the process, which changes much less. The third utilises the file's size, which massively reduces the potential of collisions for objects of differing sizes. By tracking the occurrences of all signatures individually appearing with different counterparts, it is possible to identify processes that have been changed or have been created from a common point but that have been edited to perform new, possibly malevolent functionality.

[0050] As well as checksum data, in many embodiments metadata about the object is captured and sent to the base computer 3. Amongst other types, the types of metadata captured and sent to the base computer 3 might be:

[0051] "Events": these define the actions or behaviours of an object acting upon another object or some other entity. The event may include three principal components: the key of the object performing the act (the "Actor"), the act being performed (the "Event Type"), and the key of the object or identity of another entity upon which the act is being performed (the "Victim"). For example, the event data might capture the identity, e.g. the IP address or URL, of a network entity with which an object is communicating, another program acting on the object or being acted on by the object, a database or IP registry entry being written to by the object, etc. While simple, this structure allows a limitless series of behaviours and relationships to be defined. Examples of the three components of an event might be:

Actor	Event Type	Victim
Object 1	Creates Program	Object 2
Object 1	Sends data	IP Address 3
Object 1	Deletes Program	Object 4
Object 1	Executes	Object 2

Object 2 Creates registry key Object 4

[0052] "Identities:" these define the attributes of an object. They include items such as the file's name, its physical location on the disk or in memory, its logical location on the disk within the file system (its path), the file's header details which include when the file was created, when it was last accessed, when it was last modified, the information stored as the vendor, the product it is part of and the version number of the file and it contents, its original file name, and its file size.

[0053] "Genesisactor": the key of an object that is not the direct Actor of an event but which is the ultimate parent of the event being performed. For example in the case of a software installation, this would be the key of the object that the user or system first executed and that initiated the software installation process, e.g. Setup.exe.

[0054] "Ancillary data": many events may require ancillary data, for example an event such as that used to record the creation of a registry run key. In this situation the "event" would identify the Actor object creating the registry run key, the event type itself (e.g. "regrunkey"), and the Victim or subject of the registry run key. The ancillary data in this case would define the run key entry itself; the Hive, Key name and Value.

[0055] "Event Checksums": because the event data can be quite large extending to several hundred bytes of information for a single event, its identities for the Actor and Victim and any ancillary data, the system allows for this data itself to be summarised by the Event Checksums. Two event checksums are used utilising a variety of algorithms, such as CRC and Adler. The checksums are of the core data for an event. This allows the remote computer 2 to send the checksums of the data to the central computer 3 which may already have the data relating to those checksums stored. In this case, it does not require further information from the remote computer 2. Only if the central computer 3 has never received the checksums will it request the associated data from the remote computer 2. This affords a considerable improvement in performance for both the remote and central computers 2,3 allowing much more effective scaling.

[0056] Thus, the metadata derived from the remote computers 2 can be used at the community database 7 to define the behaviour of a process across the community. As mentioned, the data may include at least one of the elements mentioned above (file size, location, etc.) or two or three or four or five or six or all seven (or more elements not specifically mentioned here). The data stored in the community database 7 provides an extensive corollary of an object's creation, configuration, execution, behaviour,

identities and relationships to other objects or entities that either act upon it or are acted upon by it. This may be used accordingly to model, test and create new automated rules and heuristics for use in the community database 7 and as rules that may be added to those held and used in the local database of the remote computers 2 to identify and determine the response of the remote computers 2 to new or unknown processes and process activity.

[0057] Moreover, it is possible to monitor a process along with any optional sub-processes as a homogenous entity and then compare the activities of the top level process throughout the community and deduce that certain, potentially malevolent practices only occur when one or more specific sub-processes are also loaded. This allows effective monitoring (without unnecessary blocking) of programs, such as Internet Explorer or other browsers, whose functionality may be easily altered by downloadable optional code that users acquire from the Internet, which is of course the principal source of malevolent code today.

[0058] **DISTRIBUTED ARCHITECTURE**

[0059] The system as described so far is generally as described in our previous application US-A-2007/0016953. There now follows a description of new, advantageous schemes in operating such a system. It will be appreciated that in the description in relation to Figures 1 and 2 the central computer and the community database are presented for convenience as single entities. As will be apparent from the following discussion, the base computer 3 can be comprised of multiple computers and servers, etc. and the community database 7 can be made up multiple databases and storage distributed around this central system.

[0060] Figure 3 shows an example of an arrangement for the base computer 3. The remote computer 2 has an agent program 10, which generally includes the same functionality as the agent program described above in relation to Figures 1 and 2. In short, the agent program 10 the monitors objects on that computer 2 and their behaviour and communicates with the base computer 3 to send details of new objects and behaviour found on the remote computer 2 and to receive determinations of whether the objects are safe or not. The agent program 10 optionally communicates with a local database 11, which holds a local copy of signatures relating to the objects found on the remote computer 2.

[0061] The agent program 10 can be comparatively small compared with other commercially available anti-malware software. The download size for the agent program 10 can be less than 1 MB and occupy about 3 MB of memory when running, using more memory only to temporarily hold an image of a file(s) being scanned. In comparison, other anti-malware packages will typically have a download of 50 MB and occupy 50 MB to 200 MB of computer memory whilst scanning files. Thus, the exemplary architecture can occupy less that 2% of system resources compared with other products.

[0062] This is achieved primarily by the exmplary agent program 10 being developed in a low-level language, having direct access to system resources such as the video display, disk, memory, the network(s), and without the incorporation of many standard code or dynamic linked libraries to perform these functions. Memory usage is optimised by storing data in the local database structure that provides the ability to refer to objects by a unique identifier rather than requiring full filenames or signatures. All unnecessary dynamic link libraries are unloaded from the process immediately as they are identified as no longer being used, and background threads are merged to reduce CPU usage. A small, efficient agent can be deployed more quickly and can used alongside other programs, including other security programs, with less load on or impact on the computer's performance. This approach also has the advantage of having less surface area for attack by malware making it inherently more secure.

[0063] The agent program 10 communicates with the base computer 3 over the Internet 1 via the Internet's Domain Name Resolution System (DNS) 50.

[0064] The base computer 3 has a first layer comprising one or more servers 61, which in this example are web servers. In the present disclosure, the web servers 61 are referred to as "FX servers" or "threat servers" and the first layer is referred to as the "FX layer". However, it will be appreciated that any type of suitable server may be used according to need. The remote computers 2 are allocated to one of the web servers 61 as explained in more detail below.

[0065] The FX layer 60 makes real time decisions as to whether or not an object is benign or malevolent based on the details of that object sent from the remote computer 2. Each web server 61 of the FX layer 60 is connected to a database 62 which contains entries for all of the objects known to the base computer 3 and a classification of whether the object is safe or unsafe. The database 62 also stores rules for deciding

whether unknown objects are safe or unsafe based on the information received from the remote computer 2. The web server 61 first searches the database 62 for matching signatures to determine if the object is safe or unsafe or unknown. As described above, the signature can be a function of the hashes (checksum data) derived from file itself, event data involving the object and or metadata about the object in any combination. If the object is unknown, the web server 61 then determines if any of the rules classify the object as unsafe. The web server 61 then communicates back to the remote computer 2 whether the object is safe and can be allowed to run, unsafe and is to be prevented from running, or unknown in which case the object can be allowed to run or not according to user preference.

[0066] Thus, the FX layer 60 reacts in real time to threats to determine whether or not malware should be allowed to run on a remote computer 2.

[0067] Sitting behind the FX layer 60 is a second layer (called the "ENZO layer" 70 herein). Information about objects received by the FX layer 60 from the remote computers 2 is sent to the ENZO layer 70 such that a master record is maintained at the ENZO layer 70 of all data received from all remote computers 2. This process is described in more detail below.

[0068] The ENZO layer 70 has one or more servers 74 (referred to as “central servers” or “ENZO servers” in this disclosure) connected to one or more "master" databases which aggregate all of the information received from all web servers 61 from all remote computers 2. The databases may comprise any combination of the following three databases and in one exemplary embodiment has all three.

[0069] 1) An object database 71, which has entries containing object signatures (e.g. their MD5 checksums) and including metadata received about objects, e.g. file name, file location, or any other metadata collected by the system as described above.

[0070] 2) A behaviour database 72 for capturing details of the behaviour of objects observed on a remote computer 2. This database 72 is populated by the event data sent from the remote computers 2 and allows a picture to be built up of the behaviour and relationships an object has across the community.

[0071] 3) A computer-object database 73 which associates remote computers 2 in the community with objects observed on those remote computers 2 by associating objects with identification codes sent from the remote computer 2 during object detail transmission. The computer may be identified by at least the following three identifiers

sent from the remote computer: one which relates to the physical system, one which relates to the operating system instance and one which relates to the logged on user.

[0072] As will be appreciated, in a community having for example 10 million or more remote computers 2, each having on average hundreds to thousands of objects, each having a large number of behaviours and associations with other objects, the amount of data held in the databases 71,72,73 is enormous.

[0073] The ENZO servers 74 can query the databases 71,72,73 and are operable, either by automation or by input from a human analyst or both, in monitoring object behaviour across the community and in investigating objects and developing rules for spotting malware. These rules are fed back to the FX layer 60 and or the agent program 10 running on remote computers 10 and, as discussed elsewhere in this document, are used by the web servers 61 or the agent program 10 in real time to stop malware from running on remote computers 2. The performance of those rules in accurately stopping malware on the remote computers 2 is fed back to the ENZO layer 70 and can be used to refine the rules. The techniques used are described further in the following disclosure.

[0074] In an exemplary embodiment, some or all of the servers 61,74 and databases 62,71,72,73 of the FX and ENZO layers 60,70 are implemented using cloud computing. Cloud computing is a means of providing location-independent computing, whereby shared servers provide resources, software, and data to computers and other devices on demand. Generally, cloud computing customers do not own the physical infrastructure, instead avoiding capital expenditure by renting usage from a third-party provider. Cloud computing users avoid capital expenditure on hardware, software, and services when they pay a provider only for what they use. New resources can quickly be put on line. This provides a large degree of flexibility for the user.

[0075] An example of cloud computing is the Amazon Elastic Compute Cloud (EC2), which is a central part of the Amazon.com cloud computing platform, Amazon Web Services (AWS). Another example is the Windows Azure Platform, which is a Microsoft cloud platform that enables customers to deploy applications and data into the cloud. EC2 is used in the present example to provide cloud computing. Nonetheless, it will be appreciated that, in principle, any suitable cloud architecture could be used to implement the base computer 3. Alternatively conventional data centres could be used

to implement the base computer 3, or a mixture of conventional data centres and cloud-based architecture could be used.

[0076] EC2 allows users to rent virtual computers on which to run their own computer applications. EC2 allows scalable deployment of applications by providing a web service through which a user can boot an Amazon Machine Image to create a virtual machine, which Amazon calls an "instance," containing any software desired.

[0077] A user can create, launch, and terminate server instances as needed, paying by the hour for active servers, allowing the provision of "elastic" computing. EC2 provides users with control over the geographical location of instances, which allows for latency optimization and high levels of redundancy. For example, to minimize downtime, a user can set up server instances in multiple zones which are insulated from each other for most causes of failure such that one backs up the other. In this way, the cloud provides complete control of a user's computing resources and its configuration, i.e. the operating system and software packages installed on the resource. Amazon EC2 allows the user to select a configuration of memory, CPU, instance storage, and the boot partition size that is optimal for the operating system and application. EC2 reduces the time required to obtain and boot new server instances to minutes, allowing the user to quickly scale capacity, both up and down, their computing requirements change.

[0078] EC2 maintains a number of data centres in different geographical regions, including: US East Coast, US West Coast, EU (Ireland), and Asia Pacific (APAC) (Singapore). As shown by Figure 4, in an exemplary embodiment, the servers and databases of the base computer 3 are implemented in plural of these geographical locations 80.

[0079] The important question therefore arises of how to allocate remote computers 2 to a particular instance of web server 61 in the FX layer 60. Important considerations in this decision are to minimise latency and to share the load evenly across the web servers. Ideally, the load on resources would be shared approximately equally across all instances of web servers in order to avoid web servers being under utilised and to minimise the number of web servers required. It is also desirable to implement a simple solution which does not add significantly to the speed or size of the agent program 10 on the remote computers, or place an overhead on the base computer 3.

[0080] 1) In an exemplary embodiment, the agent program 10 uses the geographical location of the remote computer 2 in allocating the remote computer 2 to a web server

61, i.e. based on its proximity to a geographical region 80 of the cloud. The location of the remote computer can be determined by any convenient means, such as examining the IP address of the remote computer 2 against a database of known location ranges, or performing a network route analysis to determine the number of "hops" required to reach the destination server. This functionality can be performed by the agent program 10 running on the remote computer 2 when it is first installed on the computer 2. And by allocating based on location, latency can be minimised.

[0081] 2) In an exemplary embodiment, the agent program 10 generates a random number based on the date and time of its installation seeded with unique identifiers of the remote computer to decide to which web server 61 it should be mapped. This provides a simple, pseudo random way of mapping remote computers 2 to web servers 61, which shares the load evenly between web servers 61 even if several thousand remote computers are being installed simultaneously.

[0082] 3) The DNS distribution layer then maps the URL to the physical data centre. The Domain Name System (DNS) is a hierarchical naming system built on a distributed database for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. The DNS distribution network 50 allows load balancing to plural servers 61 making up the FX layer 60.

[0083] Any combination of these techniques can be used by the agent program 10 to allocate a remote computer 2 to a web server 61. And all three may be used in combination.

[0084] The agent program may also utilize a secondary algorithm to re-map the remote computer 2 to different URL in case the primary URL is unavailable for any reason, e.g. if the servers go down. Also, in the event that malware has been able to disable the DNS mechanism then the agent program 10 can make direct contact with the FX servers 61 by referring directly to a series of direct IP addresses reserved for this purpose.

[0085] Optionally, the agent program 10 is arranged so that it can reassign the remote computer 2 to a different server 61 by receiving feedback/instruction from the server 61 the computer is already connected to. This can be used to add central control to the allocation of agent program 10 to servers 61, which adds more flexibility to the system.

[0086] Thus, this scheme allows a simple, agent managed way of dynamically load balancing between servers and providing resiliency, whilst dealing with geographical

location. In known prior art arrangements, specialised hardware load balancers are employed in the network to divide load to other servers, or else agents are manually allocated to web servers 61 when the agent program 10 is installed.

[0087] Using a cloud-based distributed architecture for the base computer 3 presents challenges in trying to maintain integrity of data across the servers and in managing the update of data across the many servers. As will be clear from the foregoing, the web servers 61 in a typical implementation will be dealing with huge amounts of data. There will be large amounts of commonality in the data, which can be used for determining rules on what objects are malware. However, it is impractical to store all data on all web servers 61 on all regions. This presents a problem in determining whether or not the data is common in real time.

[0088] To address these issues, an exemplary embodiment adopts the following scheme. Each web server 61 in the FX layer 60 examines an incoming packet of data from a remote computer 2 about an object seen on that remote computer 2. The agent program 10 generates a checksum of the data packet and sends it to the web server 61. The web server 61 has a database 62 of objects that have previously been seen and which have already been sent to the ENZO server 74. The web server 61 checks its database 62 for the checksum of the incoming data. If the checksum is found, then the data has already been seen by the ENZO server 74. In this case, the web server 61 just increases the count associated with that checksum in its database of the number of times that data has been seen to assist in determining the popularity of a piece of software or the frequency of the occurrence of a specific event. This information can then be forwarded to the ENZO server 74. If the checksum is not found in the FX database 62, then the web server requests the full data packet from the remote computer and then forwards this to the ENZO server 74. The ENZO server 74 then stores this data in the appropriate databases 71,72,73. Thus, the ENZO layer 70 keeps a master list in the object database 71 of all data objects, their metadata and behaviour seen on all of the remote computers 2. This master list is propagated back to all of the web servers 61 in all of the geographical locations 80. Thus, all web servers 61 are updated with information about which objects have been seen by the community.

[0089] This scheme has been found to reduce workload and traffic in the network by a factor of about 50 compared with a conventional scheme where typically each piece of

data on being received by a web server would immediately be propagated to all other servers in the system.

[0090] It is desirable that the data held in the master databases 71,72,73 in the ENZO layer 70 provide scalability, accessibility and resilience to the data for users. It will be appreciated that if just one live ENZO server 74 is used, then if that server becomes inaccessible, all live data is lost. For this reason, in many embodiments at least one ENZO server 74 resides in each region 80 of the cloud to provide redundancy. This means that the web servers 61 are not all directly linked to the same ENZO server 74, but rather the web servers 61 are only linked to the ENZO server 74 in their own region 80. This creates a need for an extensible method of providing data to multiple database servers.

[0091] Figure 5 shows schematically a scheme of updating data from a web server 61 to an ENZO server 74. Each web server 61 has two temporary databases 63a, 63b linked to it. At an initial starting point, one database 63a is part full 63b (active) and the other is empty (inactive). As information about objects is received from a remote computer 2 by the web server 61, it posts the information into the active database 63a. This information will be checksum information received from the remote computers 2 about objects or events seen on the remote computer. If the checksum is previously unseen at the web server, the associated data about that object or event is posted to the database along with its checksum.

[0092] Once the active database 63a reaches a predetermined size or some other predetermined criteria is met, the contents of the active database 63a are put into long term storage 66 together with a time stamp of the point in time when this happens. While this is occurring, the inactive database 63b is made active and starts to fill with new data as it arrives, and the formerly active database 63a is cleared and made inactive. Again, when this database is full, then the process of time stamping and moving the contents of the database to long term storage is repeated and the databases are swapped over. In some embodiments, the FX layer 60 has a S3 sub-layer 65, which is responsible for managing input/output to the long term storage 66. S3 (Simple Storage Service) is an online storage web service offered by Amazon Web Services. S3 is an Amazon service for the storage of high volume data in a secure and non-volatile environment through a simple web services interface. S3 is used to store the history of the FX server data being sent from the FX servers to the ENZO servers. When a block

of data is put into long term storage 66, the S3 layer 66 also forwards this data to the ENZO server 74 or servers so that the ENZO server can update its databases. All FX servers feed all ENZO servers via the S3 storage service.

[0093] The databases 63a,63b may be emptied into long term storage 66 for example every few minutes or even every few seconds. However, as will be appreciated, the actual time period used can be selected according to the load and size of the databases and may be chosen dynamically based on for example the load on the database or the size of the data. Thus, the S3 layer 65 holds all of the data received by all of the web servers 61 in the community. This has a number of advantages as illustrated by Figure 6.

[0094] Firstly, this can be used to allow the master ENZO databases 71,72,73 to be rebuilt for example in the event that an ENZO server 74 develops a problem. Also, if the data held by an ENZO server 74 is corrupted somehow, for example by a problem in a software upgrade on the ENZO server 74, it is possible to roll back the databases at the ENZO server 74 to a point before the corruption occurred. By using the timestamps associated with the blocks of data in the S3 layer 65, the ENZO server 74 can request the data blocks in long term storage 66 at the S3 layer 65 to be resent to the ENZO server 74 so the server's databases 71,72,73 can be brought up to date.

[0095] Furthermore, using this scheme, the ENZO servers 74 in multiple regions 80 can create backup databases of the ENZO databases by receiving the data from the S3 layer. This can be done without affecting the live ENZO databases 74, so these can carry on functioning seamlessly.

[0096] The alternative would be to post to databases at a single ENZO server which is designated the master server and to propagate the data from the master server to other servers in the community. However, this in effect creates one “live” server and one or more backups. The live server therefore does most of the work, e.g. pre-processing data received from the agents, updating the databases and analysing the data for threats, whilst the backup servers are under utilised. Thus, the live server must be more powerful than the backup servers. This tends to be wasteful and inefficient of resources. In comparison, the exemplary embodiment, shares the workload around the servers equally.

[0097] It is also desirable for operators, human malware analysts, etc., to have a copy of the data from a live server for research, etc. Image servers may be created in the same

way as the live servers and the backup servers. The user of the system can take the image server offline when he needs to take an image for offline use. Once the image is taken, the image database can be brought up to date using the blocks of data from the S3 layer.

[0098] Cloud computing can recreate instances of web servers very quickly, e.g., in a matter of minutes. Cloud computing is therefore advantageous in implementations where the volume of transactions grows (or shrinks). In this situation, a new server instance can be quickly created to handle the new load. However, it is necessary to take an image of a live server to create the image. This is disruptive to the processes running on that instance during imaging. It is therefore clearly not acceptable to take a live server out of commission for this period. Therefore, in many embodiments, a special dedicated image server is maintained behind the ENZO server, which is updated in a similar way to the live and backup servers. In this case, the image server is taken off-line and imaged. This process might take for example 30 minutes. During this time, the image server is not receiving updates from the S3 server and therefore becomes out of date. However, since the exact time when the server went off line is known, it can be updated by requesting data blocks from the S3 server with a timestamp later than when it went off line. Thus, an image can be taken of an updated server for offline use etc. and brought back up to date without affecting the running of the system.

[0099] It is also desirable to be able to scale out the architecture of the ENZO layer 70. For example, a live server 74 may be running out of processing power due to the increase in traffic it is seeing from web servers 61 or agents 10. For example, more remote computers 2 may be connected to the system, or a common software package may be updated leading to a large volume of new data being sent to the ENZO layer 70. In this situation, a second or further live server instance can be created in the ENZO layer 70 in order to scale out horizontally (as opposed to adding more CPU/RAM to an existing server). As described above, it is relatively straightforward to create an image of an ENZO server 74 in a cloud-computing environment. As can be seen from Figure 7, the data on each server 74 is divided into a plurality of sections. In this case the data on the server 74 is divided into eight sections 0-7. Each section does a share of the processing on that server. When the server is divided, various sections are allocated to each server. So, for example, in the example of Figure 7, the original server L1 processes data 0-3, and the newly created server L2 processes data 4-7. Each server

then handles pre-processing and storing its own data. For the purposes of analysing the data, in many embodiments the data from these multiple severs is aggregated so that the human analyst is working on the complete set of data when investigating malware (as described in more detail below). Of course, the data can be divided in different ways among the servers according to need.

[00100] So, instead of holding a single database and then having to dissect it if it is required to distribute the load across multiple servers, in many embodiments the database is already dissected making it is much easier to make a transition to further distribution of the database workload across multiple servers.

[00101] The number of data sections may be selected to be eight, because this is enough to give reasonable flexibility and ability to expand. However, it is rare that a business needs to expand by more than 800% at any time. Nonetheless, other plural numbers of data sections can be used as appropriate.

[00102] This architecture allows vast amounts of data to be managed across multiple locations and servers. The architecture can be scaled and servers copied without incurring extra work or affecting the running of the system. The data can be exchanged across servers that can change dynamically.

[00103] **USING TREND DATA**

[00104] Malware evolves at a significant pace. Historically, malware used a single infection (module or program) to infect many computers. As this allowed malware researchers to quickly become aware of the infection, signatures could be quickly deployed to identify and block the threat. In the last decade, malware authors have made their threats contain many varied modules, which shared a common purpose. To detect and block these new threats is a much greater challenge for malware research and to creating and distributing signatures to identify and block all of the variations, any one of which could infect one or more computers. Due to the varied and distributed nature of these modern threats malware researchers are often late in identifying that a threat even exists.

[00105] By collecting hashes, signatures and statistics of new programs and modules correlated by path and file details, and aggregating this information at a central location, it is possible to use a method of analysis that will allow faster identification of new threats.

[00106] On any given day the amount of new commercial programs and modules that are created can be considered almost constant. This data can be measured against any of the metadata or event data collected about the object. In one example, the data is measured against the Path (Folder) location of new files created. The data can also be measured against their filenames, and file types (e.g. .exe, .dll, .drv, etc.) along with details such as vendor, product and version information, registry keys, or any other system derived data forwarded to base computer. Any combination of these factors is possible. In whichever way it is chosen to group the data, by establishing a baseline for the pattern and distribution of this data across the groups it is possible to quickly identify outliers.

[00107] Figure 8 shows an example of collected data over a time period grouped according to folders in the file system compared with the established normal distribution (base line). If the number of new programs in the windows system32 subfolder is normally x in any given time period t (e.g., in a given day) and in a particular time period $t1$ under consideration it is $1.4x$ (or exceeds some other predetermined ratio) then it indicates an abnormal increase in the number of new files which signifies possible malware activity. This identification allows greater focus to be placed on researching these outliers. Processes can be readily developed that can use this outlier information to automatically group, identify or prioritise research effort and even make malware determinations. Where automated rules are used to identify malware, this information can be used to automatically heighten sensitivity of these rules when applied to objects in the group that has been identified as an outlier.

[00108] Another example of this technique is to focus on a filename and compare the number of new objects (as represented by its hash) that utilize that name, or the number of new objects all of which have new names. This is contrary to the general principles of most commercial software, which needs consistency to enable manageability of their products. Most commercial applications have only a few names and each file name has only a few variants as each new release is made available. In contrast, some malware has thousands of variants using the same, similar or similarly structured name and which are observed by the community utilising the related names within a very short window of time (e.g., seconds-weeks).

[00109] In principle, any length of time for the window can be selected. In practice, this is likely to be of the order of every 15 minutes, or every few hours, or a day, rather than longer periods like every week.

[00110] In some embodiments, techniques are provided to provide context for researchers. In detecting malware, human analysts and computer automated analysis have different strengths and are often used together to some degree to harness the capabilities of both. Computers are good at applying rules to and processing large amounts of data. In the present application, the amount of data received from agent program 10 running on remote computers 2 is vast and therefore suited to being processed by computer. It would be impractical to have human operators to look at all of this data to determine malware. On the other hand, experienced human analysts are highly adept at spotting malware given the appropriately focussed data about that object and similar objects and their context. Often a human analyst can "intuitively" spot malware, in a way that is difficult to reduce to a set of rules and teach to a machine. For example, kernel32.dll is a file associated with the Windows (RTM) operating system. A malware program may be called something similar, e.g. kernel64.dll, which would immediately be apparent to a user as being suspicious, but which it would be difficult to teach a machine to spot.

[00111] The pattern may be obvious in retrospect when an analyst is presented with the relevant data. However, this is a rear view mirror approach. The problem is finding the relevant data in the vast amount of data being received at the base computer 3 so that the analyst can focus his/her time on the important data. As illustrated by Figure 9, what is needed is some what of distilling the raw data 100 into groups of related data 101 to provide a focussed starting point for a malware researcher to investigate and take necessary action 102 to flag objects bad or safe 103 accordingly.

[00112] As will be appreciated, a single object on a remote computer 2 across the community can have a high degree of associations with other objects on remote computers 2. Some tools currently exist which can map links between entities to create a network of associations. However, when used for a malware object and its associations with other objects, these will result in a diagram that is so dense and complicated that it is practically useless for the purpose of allowing a human analyst to identify malware. The problem is sifting this data so useful features are extracted for the analyst so that he can quickly focus on the likely candidates for being malware.

[00113] An exemplary embodiment, illustrated by Figures 10 to 13, provides a software program running on the ENZO server 74 and giving the user a visual based tool for running queries against the databases. A query language such as TSQL may be used for example to query the database based on the user's input. As mentioned in the foregoing, the ENZO layer 70 has a complete record of the properties and activities of all objects seen on all remote computers 2 in their databases. Figure 10 shows an example of an on-screen display and user interface including a table 105 in which the rows represent the objects (determined by their signatures) that match the results of the current query. The user interface provides tools for creating new queries 106, for displaying current and recent queries 107 and for sorting the data displayed in the table for the current query 108. Clearly there may be more results than will fit on one screen. There may therefore be more than one page of results to which the user can navigate through appropriate controls 109 provided by the user interface.

[00114] The table 105 has a plurality of columns of data representing information about the objects. The information may include any of the data collected about an object, its metadata or its behaviour, sent to the base computer 3 by the remote computers 2. This may include any of the following for example: the name of the file, and the location (path) of the file, the country where the object was first encountered, the identity of the remote computer that encountered the object, its operating system and version number, details of the web browser and any other security products installed on the computer, the creator of the file, the icon associated with the file, etc. The information may include metadata about the file, such as the author or the size of the object or information relating to executable instructions in the object. The data may contain "actor" and "victim" information and details of its registry key. The information may include information about whether or not the object has been identified as safe or unsafe at the remote computer 2 or at the FX server 61.

[00115] The information displayed may contain counts of how often a particular attribute is present among all the objects returned by the query or across the community. In addition, the information may contain less easily understood information. As discussed above, the information collected about an object can include checksums of parts of the executable, e.g. the first 500 bytes of the executable part of the file. In many cases, the actual value of the checksum or other data is of little or no interest to the user. Therefore, in many implementations some or all of this information is presented to the

user in a graphical way, utilising colour, shape and or different symbols, which makes spotting patterns in the data more intuitive and speedy for the user.

[00116] In some embodiments, at least one column of data is presented according to the following scheme:

[00117] 1) if the value is unique in that column between the rows of data representing objects then the numeral "1" is presented.

[00118] 2) if the value is replicated between the rows of data on the screen, or between all the rows of data matching that query, then a coloured symbol (e.g. a green triangle or a red letter "P" in a blue square, etc.) is allocated for that value and displayed in that column for all rows that share that value. Thus, without needing to know what the symbols represent, the user can see at a glance which rows on the screen have commonality of an attribute.

[00119] This provides a starting point for running further queries. For example, the user can quickly see commonality between objects, which look interesting. As explained elsewhere in this document, a typical trait of malware is that the objects use a large number of file names, file locations, similar file sizes, similar code portions, etc. The program allows a user to refine a query by for example clicking on columns in the table and using the query creating tools 106 to add a particular attribute value to the predicate of the query, or to start a new query with this column value in the predicate, etc.

[00120] The ultimate aim of this process is for the user to find a query that returns the maximum number of rows with commonality. By this process, the user identifies a set of criteria made up of hashes and other metadata definitions that can be used to accurately identify similar objects that share criteria. For example, Figure 11 shows a user query that returns rows with a high degree of commonality representing objects that have commonality. The software also in many implementations allows the user to bring up a screen of statistics for the objects that have been returned from the query. In particular, as shown by Figure 12, the interface can display to the user the number of objects returned by the query that are known to the database as being malware, the number known as being not malware, and the number where it is not yet known whether or not the object is malware (represented in Figure 12 by differently shaded/coloured bars). Other data about the results of a query or objects having a certain attribute selected by the user can be shown in graphical form, e.g. a bar graph, or a pie diagram as shown in Figure 13. The user can take this information into account as well as

information shown in the table 105 when deciding whether or not the results of the query determine malware. The user can then take the appropriate action, such as tagging the objects returned by the query as malware, not malware, or suspicious and requiring further investigation. Thus, by being able to query and analyse the collective view of an object, i.e. its metadata and behaviours, across all agents 10 that have seen it, a more informed view can be derived, whether by human or computer, of the object. In addition it is possible to cross-group objects based on any of their criteria, i.e. metadata and behaviour.

[00121] To take an example, it might be a previously identified trait of certain types of malware that the malevolent object is located in the "recycle bin" of the operating system. This gives a starting point for the user to run a query to find all objects, or all objects encountered during a user specified time frame, that are located in the recycle bin by looking at their "path" attribute. This would display rows to the user corresponding to the different objects found (e.g. each row corresponding to a different MD5 signature). The user can then drill down through the rows by selecting interesting attributes by clicking on a value in a column. For example, the user may choose objects whose attributes show that the object's icon is the same as the icon used the "Notepad" program (which comes with Microsoft Windows (RTM) operating systems), but which are not Microsoft originating programs. In many implementations the system allows the user to apply Boolean operators in refining the query. The system allows the user to bring up statistics of how well the query cover objects that are known by the system to be malevolent or benign to give the user more information about useful the query is in classifying objects.

[00122] The users employed in grouping objects according to this scheme need not be highly skilled malware analysts. The users need only basic training in use of the tool and in grouping objects by running queries and looking for commonality. The final analysis of objects covered by the query can be taken by a skilled malware analyst. The advantage of this system is that the computer is doing the work in processing the raw data which is too large of a task to be practical for a human operator to complete. The human operators grouping the data need not be skilled, which reduces costs for the business. This reduces costs and leaves the skilled malware analysts to concentrate on queries that are found to be good candidates for further investigation. Thus, the skill of

these operators is most effectively deployed in using their experience to identify malware.

[00123] Referring to Figure 9, if at stage 103 the user decides that a query (Q5) is deterministic in classifying the objects returned by a query as safe or unsafe, then the rule can be passed back to the web servers 61 and or the agent program 10 at the remote computers 2 and used in real time in deciding whether new objects seen at the web servers 61 or remote computer 2 are safe or unsafe.

[00124] If a new object that has not been seen before by the community is received by a remote computer 2 or a web server 61 and is deemed by one of the rules run by the remote computer 2 or web server 61 to be unsafe, the object can be stopped from running on the remote computer 2 in real time, or the user of the remote computer 2 can be warned and given the option of continuing or not. Furthermore, the remote computer 2 (via the web server 61 to which it is assigned) or the web server 61 can report to the ENZO server 74 that a new object has been determined to be safe or unsafe by the rule. The ENZO server 74 can update its master database with this finding and this finding can be communicated to other remote computers 2 and or web servers 61 and used to update their databases that objects with that signature are unsafe and should be blocked in the future, or safe and should be allowed to run.

[00125] Alternatively, the rule can be used by human analyst at the ENZO layer to monitor suspicious objects. Objects covered by the rule can be displayed to a human analyst and the analyst can then decide for each object in turn whether it is malevolent or benign, and mark the object accordingly. These determinations for each object are sent back to the web servers 62 and or agent software 10 and used to decide whether or not the object is allowed to run when encountered at the remote computers in real time. This method does not react as quickly to new threats, compared with applying the rules in real time at the web servers 62 and or agent software 10. However, it may be preferred in cases where it is desired to keep the number of "false positives" low, and or where a rule is found to be good at identifying suspicious objects which need further investigation before a firm determination can be made that they are malware.

[00126] Furthermore, this action can be semi automated. The application can monitor the groupings along with any and all actions taken such as groups being determined as malicious or as benign. By tracking these actions it is possible for the ENZO server 74 to learn from human analysts how to identify and determine objects automatically. The

application can remember queries that have been run by users. If the same query is being run repeatedly by a user and returning malware objects, or if a researcher consistently takes the action of determining the objects to be malware, then the system can automatically identify this condition and create a rule of the criteria and the action to determined matching objects as malicious. This rule can be sent to the FX server layer 60 to enable real time actions to be made to catch objects that match the rule and determine them as malicious. The identity of these rules and of malware grouping applied by the rules can then be fed back to both the agent and the ENZO server 74. In this way the FX server 61 is performing an action sanctioned and distributed by the ENZO server 74, on its behalf. Similarly, these same processes can be applied to benign groups of objects resulting in rules that determine such objects as "good" which can be propagated back to the FX layer 60 in the same way for the rules for "bad" objects. Thus, the ENZO layer 70 allows the user to easily identify these groupings. The ENZO layer can then monitor the groupings along with any and all actions taken such as groups being determined as malicious or as benign. By tracking these actions it is possible for the ENZO layer 70 to learn from humans how to identify and determine objects automatically.

[00127] The ENZO layer 70 can also monitor trends and bring information to the human analysts' attention, such as the evolution in the behaviour of a previously known good program. For example, a legitimate version of the game Solitaire will be observed by the ENZO servers to have a particular behaviour profile from the actions performed by that program on remote computers over a period of time. If after a period of time that program starts exhibiting new, suspicious behaviour, such as trying to install a driver or accessing a web server in another country, this can be flagged for investigation.

[00128] Furthermore, an exemplary embodiment of the agent program 10 at the remote computer provides an interface that allows the user to report “false positives” to the system, i.e. where an object has been flagged as malware, which the user believes to be legitimate software. The system is arranged to feedback this information to the ENZO server 74. At this point, the system can determine that the rule is no longer reliably deterministic in finding malware and can disable the rule. Alternatively the system can flag the rule for manual review and or modification by a human analyst. Alternatively, it can be decided that the rule is generally useful despite the false positive and that the

false positive is an outlier. The conflicting benign object can then be specifically excluded from the rule at the FX layer 70 by placing it on a white list.

[00129] It should be noted that rules can be prioritised (applied in order by priority) and can be established to only apply against objects having a specific determination, location, popularity, age or any other criteria known by or derived by the database. For example, if a first rule determines the object originates from Microsoft, then it may be decided not to apply any further rules. In contrast, if a first rule determines that an object is suspicious, then it may be decided to apply further rules as appropriate.

[00130] Thus, many embodiments of the software application running on an ENZO server 74 provide powerful object behaviour monitoring and assessment. The software allows the user to obtain a thorough understanding of an object's behaviour on a remote computer and the contextual environment in which it is observed, in part through providing powerful data visualisation techniques. The software enables large research teams to work collaboratively and incrementally and leverages human research skills and experience through expert system automation.

[00131] **CONFIGURABLE FIREWALL**

[00132] It is desirable to stop malware before a computer becomes infected, e.g., when the infected file is received by email, downloaded, or when it is installed or run for the first time.

[00133] A well known example of a malware program is the "Zeus" Trojan. This program runs in the background on an infected computer and steals login details as they are entered on screen by a user by monitoring the user's keystrokes. This information is then sent to the criminal's servers where it can be used to take control of the infected computer. An instant message is sent to the criminal over the network when the malware program detects logon information being entered on an online banking website, so the criminal receives this information in near real time. The Trojan can then take remote control of the user's computer using the Virtual Network Connection protocol, a protocol that allows a remote user to access and take control of a computer remotely. The criminal can then steal money from the victim's bank account.

[00134] While most anti-malware software attempts to stop the malware from infecting a host computer or stopping communications with the malware as soon as possible, not much attention has been shown to finding and prosecuting the criminals responsible. One difficulty is that it is illegal for the anti-malware or even the police to hack into the

criminal's servers to find the criminal's data. Indeed, it a known ruse for the criminals to use so-called "botnets", which are "zombie networks" of legitimate users' computers which have been infected by malware and are thereby under the control of the criminals.

[00135] An exemplary embodiment illustrated by Figure 14 implements a firewall 95 with the agent program 10 at the remote computer 2. A firewall per se is well known. However, normally firewalls are configured by rules input by the user to govern what programs have permission to access the network for incoming/outgoing traffic. The exemplary embodiment additionally takes rules from the base computer 3 to limit, which objects on the remote computer 2 can communicate across the firewall and with which entities 96,97 on the network. For example, information can be sent from the base computer 3 to the firewall 95 that known active URLs of Zeus servers 97 are blocked from exchanging messages from all objects on the remote computer 2. Thus, the firewall 95 can implement a rule blocking communications with the criminal's servers.

[00136] This provides a valuable second line of defence against malware. It is generally desirable to stop malware at the point of infection by preventing the malware from infecting a computer. The next line of defence is to stop the malware from communicating. The configurable firewall 95 can therefore leverage the rules and knowledge developed about malevolent objects and network URLs held at the base computer 3 to provide a next line of defence in fighting malware.

[00137] Furthermore, in one embodiment, the agent program 10 can be used to contact the authorities 98, e.g., a law enforcement agency, if malevolent Internet traffic is detected. The IP traffic between the infected computer 2 and the criminal's server 97 can be intercepted by the firewall 95, stored and sent to the authorities' server 98, so the authorities can see what information the criminals were stealing through the malware. This information can be sent to the authorities' servers 98 in encrypted form for added security. In the exemplary embodiment, checksums are made and stored of the data that sent to the authorities' servers 98, as there are very strict processes in place for forensic data handling and evidence retention that should be observed.

[00138] Legal constraints will mean in most instances it is necessary to obtain permission from the user of the infected computer 2 before this information is captured and sent to a third party. In this situation, the agent program 10 will open a dialogue with the user to obtain permission before proceeding. In some instances, the user may

be happy to give blanket permission for data to be sent whenever a malware program or a particular class of malware program is detected on his computer 2, so it will not be necessary to obtain specific permission every time malevolent objects or communication is detected.

[00139] SELF DEFENCE

[00140] Malware has evolved to the state where it will attack, disable or otherwise destroy security products installed on a computer. There are two principle vectors, which need to be considered.

[00141] A first approach is to target the methods used by malware to identify security products. In this specific case the malware will use behaviour monitoring of processes running on the remote computer that view, observe, record, examine or otherwise interfere any aspect of the malware code. Examples might be a malware entity watching for processes or tasks which look at the registry keys the malware has used to configure, control or record its operation. As will be appreciated, malware is by its nature surreptitious. From the malware's point of view, no processes on the remote computer should be monitoring or interacting with the malware object, since the existence of the malware object on the local computer should be unknown. If any processes are monitoring the malware, it is therefore likely to be security software or a system monitoring tool or a system tool being used by the user of the computer 2 to rid the computer 2 of the infection.

[00142] Thus, by finding processes that are doing this, the malware process can find the identity of the process and its location or locations on disk. This identification then allows it the ability to delete, disable or interfere with the process or processes it has identified as potential threats. In most cases these will indeed be security programs or system monitoring tools, both which it might consider threats.

[00143] Many embodiments guard against this possible interference by malware programs by preventing the behavioural detection of a security program when examining the malware. This is achieved by hiding behind, masquerading as, and/or leveraging core operating system components to examine the malware's state and components. In particular, the agent program 10 performs operations by impersonating the system's context when it is necessary to rely on standard system calls, or circumventing any system calls by accessing data at the raw level as it is stored on disk. For example, the agent program 10 can directly impersonate the kernel of the operating

system when calling the ZwTerminateProcess function to terminate a malevolent process. In doing so, the malware cannot trace the call back to the agent program. The malware considers this behaviour as normal, as it expects the operating system to interact with it (e.g. it is necessary for the operating system to be able to terminate the process when the computer is shut down), and so the malware does not attempt to terminate the agent program process. Furthermore, the malware cannot react by killing the process as the process is only identifiable as the operating system itself. To kill the operating system would also prevent the malware from operating.

[00144] Figure 15 shows a hierarchy of control on a computer system 2 going from the kernel level 92 at the lowest level, the operating system level 91, and a web browser running 92 on the operating system 91. A second consideration is that, for malware to assert maximum control over the operation of the computer, it will often attempt to install a driver, possibly a kernel mode driver, which has complete control over processes and actions performed. A type of malware commonly known as a "rootkit" operates in this way and can, among other things, be used to conceal other malware, notably password-stealing key loggers and computer viruses. In certain cases the malware will load a malicious driver and use this to disable security applications and drivers from starting when Windows starts. In particular, the malware may have a list of drivers or program components that it knows correspond to security products.

[00145] To prevent malware from using this approach to disabling security applications the agent program 10 dynamically creates a second or backup driver or component 94 which loads as a backup of main component 93 during installation or bootup in the event that the main components 93 are inaccessible (as shown by Figure 14). It would have identical functionality but would be modified so as to appear different by name and form. This can be randomised, so that the malware cannot learn to identify the security program. In this scenario should the primary component fail to load, most likely due to being killed by malware, the second driver 94 would be loaded to perform its function. If the primary component 93 loads successfully, the secondary component 94 would simply terminate to avoid conflict by identifying the presence of the primary component 93. By randomising the filenames and checksums of the installed objects comprising the agent program 10, the agent program 10 is able to evade heuristic detection by active threats that would attempt to terminate or remove critical agent components.

[00146] Later versions of Microsoft's Windows operating system provide enhanced security by requiring system and low level drivers to be signed. This policy, called the kernel mode code signing policy, disallows any unauthorized or malicious driver to be loaded. Some malware creations modify the master boot record to nullify driver certification checks. The malware executed by an infected master boot record bypasses driver signing policy by changing the boot options of Microsoft boot programs that will allow an unsigned driver to load.

[00147] So, in these conditions the secondary driver or component could remove its own digital signature to evade detection by the malware. This means it would fail to load unless the master boot record had been modified to disable driver verification. So it represents no threat to an uninfected system and would never load unless the system was infected and the master boot record was modified.

[00148] Embodiments of the present invention have been described with particular reference to the examples illustrated. However, it will be appreciated that variations and modifications may be made to the examples described within the scope of the present invention.

[00149] Those of skill in the art would understand that information and signals may be represented using any of a variety of different technologies and techniques. For example, data, instructions, commands, information, signals, bits, symbols, and chips that may be referenced throughout the above description may be represented by voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, or any combination thereof.

[00150] Those of skill would further appreciate that the various illustrative logical blocks, modules, circuits, and algorithm steps described in connection with the embodiments disclosed herein may be implemented as electronic hardware, computer software, or combinations of both. To clearly illustrate this interchangeability of hardware and software, various illustrative components, blocks, modules, circuits, and steps have been described above generally in terms of their functionality. Whether such functionality is implemented as hardware or software depends upon the particular application and design constraints imposed on the overall system. Skilled artisans may implement the described functionality in varying ways for each particular application, but such implementation decisions should not be interpreted as causing a departure from the scope of the present invention.

[00151] One of ordinary skill in the art will appreciate that the various illustrative logical blocks, modules, and circuits described in connection with the embodiments disclosed herein may be implemented or performed with a general purpose processor, a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general purpose processor may be a microprocessor, but in the alternative, the processor may be any conventional processor, controller, microcontroller, or state machine. A processor may also be implemented as a combination of computing devices, e.g., a combination of a DSP and a microprocessor, a plurality of microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration.

[00152] The steps of a method or algorithm described in connection with the embodiments disclosed herein may be embodied directly in hardware, in a software module executed by a processor, or in a combination of the two. A software module may reside in RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, hard disk, a removable disk, a CD-ROM, or any other form of storage medium known in the art. An exemplary storage medium is coupled to the processor such the processor can read information from, and write information to, the storage medium. In the alternative, the storage medium may be integral to the processor. The processor and the storage medium may reside in an ASIC. The ASIC may reside in a user terminal. In the alternative, the processor and the storage medium may reside as discrete components in a user terminal.

[00153] The previous description of the disclosed embodiments is provided to enable any person skilled in the art to make or use the present invention. Various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments without departing from the spirit or scope of the invention. Thus, the present invention is not intended to be limited to the embodiments shown herein but is to be accorded the widest scope consistent with the principles and novel features disclosed herein.

WHAT IS CLAIMED IS:

CLAIMS

1. A method of classifying a computer object as malware, the method comprising:

at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored or processed;

wherein the base computer comprises plural threat servers arranged to receive the data from the plural remote computers and apply rules or heuristics against the data in real time to determine whether or not the object is malware and to communicate the determination to the remote computers;

the base computer further comprising at least one central server in communication with the threat servers and arranged to receive the data about objects from the threat servers to maintain a master database of data received about objects from all threat servers.

2. The method according to claim 1, wherein at least one threat server comprises at least one database for holding information received from remote computers to which it is attached, the method comprising:

storing the data in at least one database at the threat server; and

at intervals, storing the contents of the database in storage together with a timestamp and clearing the database.

3. The method according to claim 2, comprising creating a backup central server by receiving at a central server all of the time-stamped blocks of data and incorporating them into its database.

4. The method according to claim 2, comprising:

taking a central server off-line for a period of time such that it does not receive updates of data from the threat servers during that period of time;

after the period of time has elapsed, updating the database of the central server with time-stamped blocks of data from the storage that have a timestamp later than the time when the central server went off-line; and

bringing the central server back on line.

5. The method according to claim 2, comprising:

rolling back the database of a central server to a point of time in the past;

updating the database of the central server with time-stamped blocks of data from storage that have a timestamp later than the past point of time; and

bringing the central server back on line.

6. The method according to claim 2, wherein the central server has databases including at least one of:

a) object signatures and metadata about that object;

b) object behavior; and

c) information about what objects are present on what remote computers.

7. The method according to claim 6, wherein the threat and central servers are implemented using cloud computing.

8. The method according to claim 1, comprising:

maintaining at a threat server, a list of objects previously seen at the threat server and forwarded to the central server; and

if an object has not been seen before, sending the data about that object to the central server,

and if an object has been seen before, increasing the count for that object instead of sending the data.

9. An apparatus for classifying a computer object as malware, the apparatus comprising:

a base computer arranged to receive data about a computer object from each of plural remote computers on which the object or similar objects are stored or processed;

wherein the base computer comprises plural threat servers arranged to receive the data from the plural remote computers and apply rules or heuristics against that data in real time to determine whether or not the object is malware and to communicate the determination to the remote computers;

the base computer further comprising at least one central server in communication with the threat servers and arranged to receive the data about objects from the servers to maintain a master database of data received about objects from all threat servers.

10. The apparatus according to claim 9, comprising:

at least one database, the threat servers being arranged to store the data information received from remote computer in the database; and

storage, the threat servers being arranged to, at intervals, store the contents of the database in the storage together with a timestamp and clearing the database.

11. The apparatus according to claim 10, comprising:

a backup central server having a database, the database of the backup central server being populated by receiving at the backup central server all of the time-stamped blocks of data from the storage and incorporating them into the database.

12. The apparatus according to claim 10, wherein, in the event that a central server is taken off-line for a period of time such that it does not receive updates of data from the threat servers during that period of time, the central server is arranged to, after the period of time has elapsed, update its database with time-stamped blocks of data from the storage that have a timestamp later than the time when the central server went off-line.

13. The apparatus according to claim 10, wherein, in the event that the database of a central server is rolled back to a point of time in the past, the central server is arranged to update its database with time-stamped blocks of data from storage that have a timestamp later than the past point of time.

14. The apparatus according to claim 9, wherein the central server has databases including at least one of:

a) object signatures and metadata about that object;

b) object behavior; and

c) information about what objects are present on what remote computers.

15. The apparatus according to claim 14, wherein the threat and central servers are implemented using cloud computing.

16. The apparatus according to claim 9, wherein a threat server is arranged to maintain a list of objects previously seen at that threat server and forwarded to the central server; and,

if an object has not been seen before, the threat server is arranged to send the data about that object to the central server,

and if an object has been seen before, the threat server is arranged to increase the count for that object instead of sending the data.

17. A method of connecting a remote computer to one of a plurality of servers, the method comprising:

installing an agent program on the remote computer, the agent program having an algorithm for allocating the remote computer to a server determined by the time when the agent program was installed; and

connecting the agent program to the allocated server.

18. The method according to claim 17, wherein the algorithm allocates the remote computer to a server determined also by the proximity of the remote computer to the servers.

19. The method according to claim 17, comprising connecting the remote computer to a different server in accordance with information received by the agent program from the originally allocated server.

20. The method according to claim 17, wherein the agent program has a secondary algorithm to determine a secondary server for the remote computer in case the originally allocated server is inaccessible.

21. A non-transitory, tangible processor readable storage medium, encoded with processor readable instructions to perform a method for connecting a remote computer to one of a plurality of servers, the method comprising:

installing an agent program on the remote computer;

allocating the remote computer to one of the plurality of servers based upon a time when the agent program was installed on the remote computer; and

connecting the agent program to the allocated server.

22. The non-transitory, tangible processor readable storage medium of claim 21, wherein allocating the remote computer to one of the plurality of servers is also determined by the proximity of the remote computer to the servers.

23. The non-transitory, tangible processor readable storage medium of claim 21, the method including: connecting the remote computer to a different server in accordance with information received by the agent program from the originally allocated server.

24. The non-transitory, tangible processor readable storage medium of claim 21, the method including determining a secondary server for the remote computer to connect to in case the originally assigned remote computer is inaccessible.

METHODS AND APPARATUS FOR DEALING WITH MALWARE

ABSTRACT

Methods for classifying computer objects as malware and the associated apparatus are disclosed. An exemplary method includes, at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored or processed wherein the base computer comprises plural threat servers arranged to receive the data from the plural remote computers and apply rules or heuristics against the data in real time to determine whether or not the object is malware and to communicate the determination to the remote computers. The base computer includes at least one central server in communication with the threat servers and arranged to receive the data about objects from the threat servers to maintain a master database of data received about objects from all threat servers.

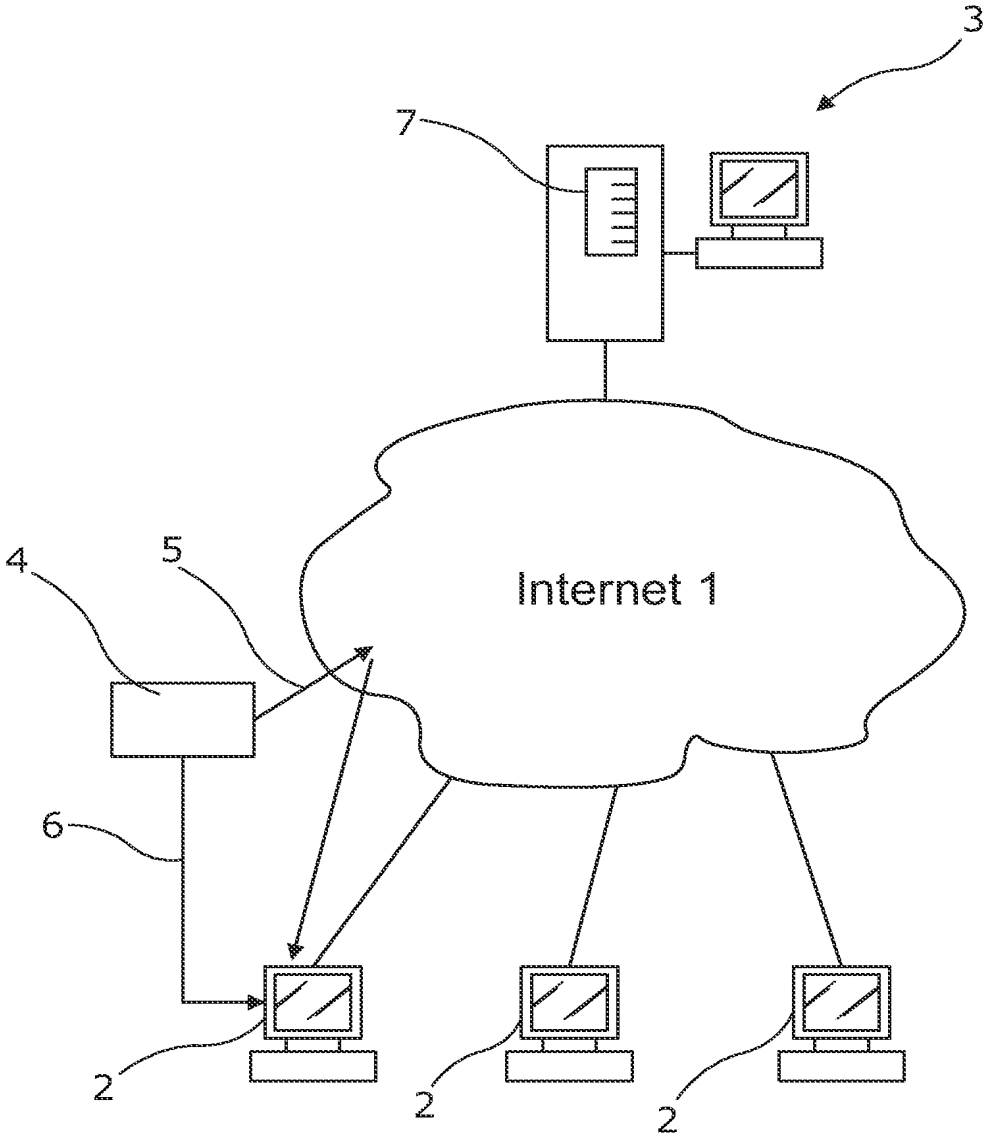


Fig. 1
(Prior Art)

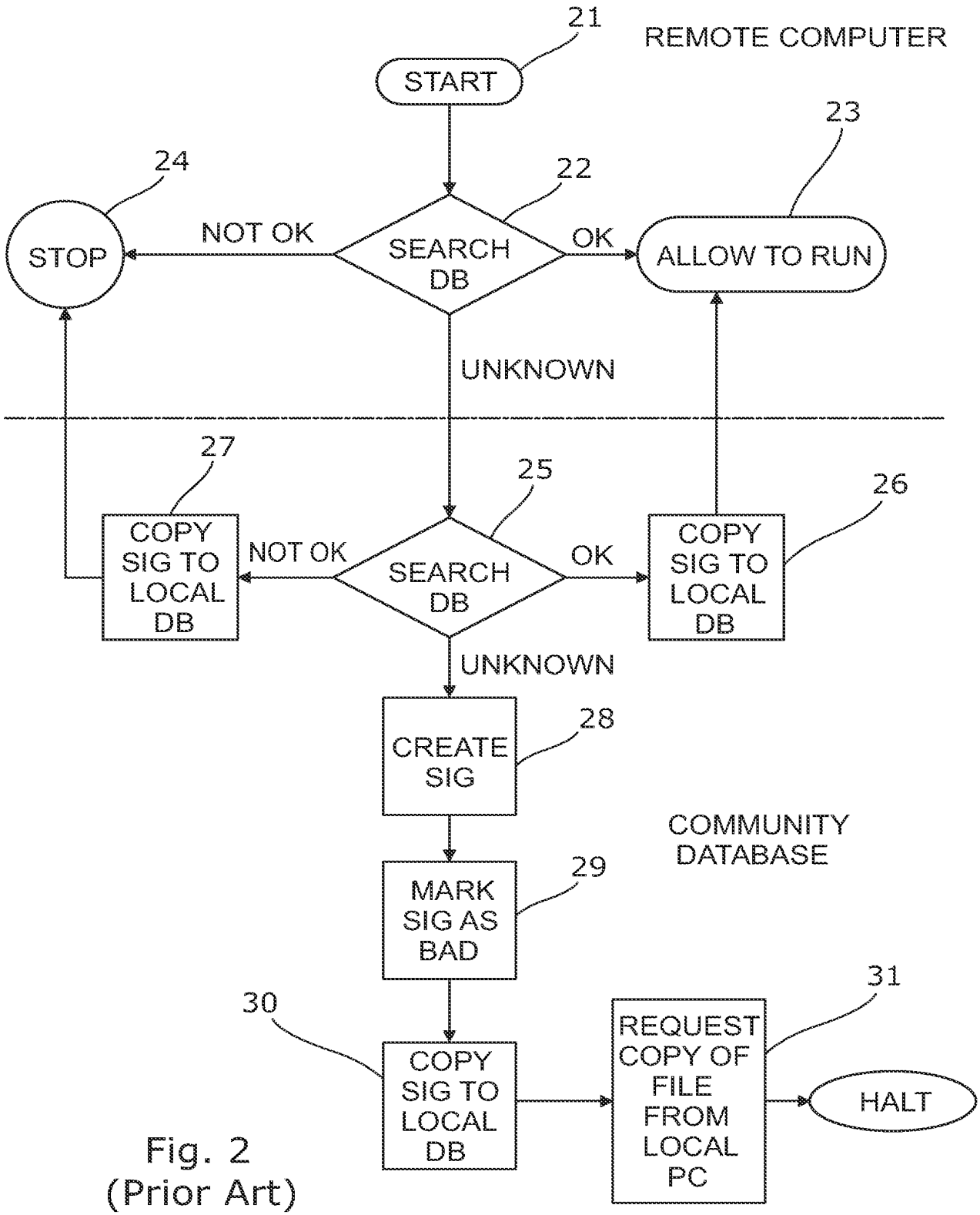


Fig. 2
(Prior Art)

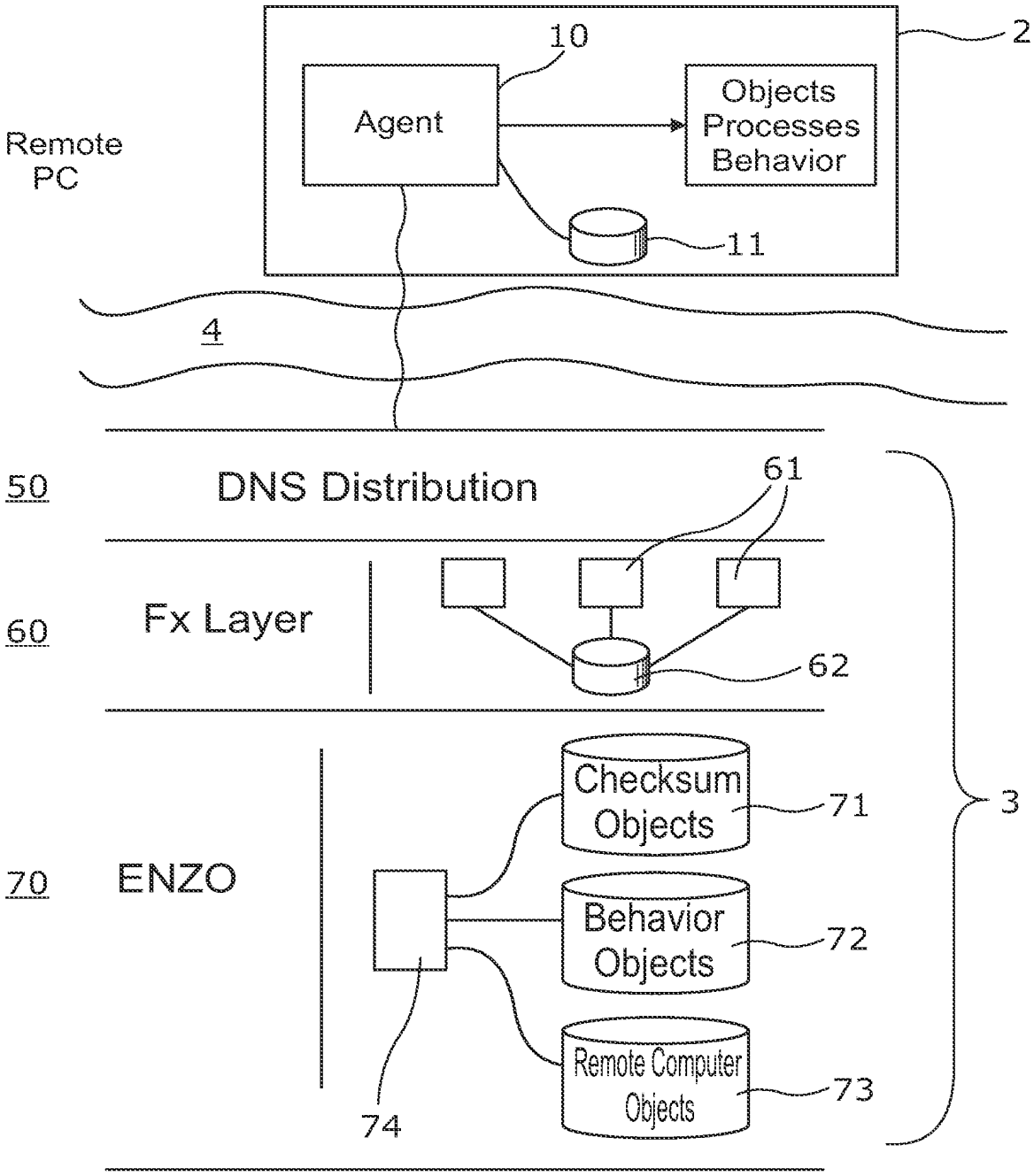

Remote PC
10
2
Agent
Objects Processes Behavior
11
4
50
DNS Distribution
61
60
Fx Layer
62
70
ENZO
Checksum Objects
71
Behavior Objects
72
Remote Computer Objects
73
74
3

Fig. 3

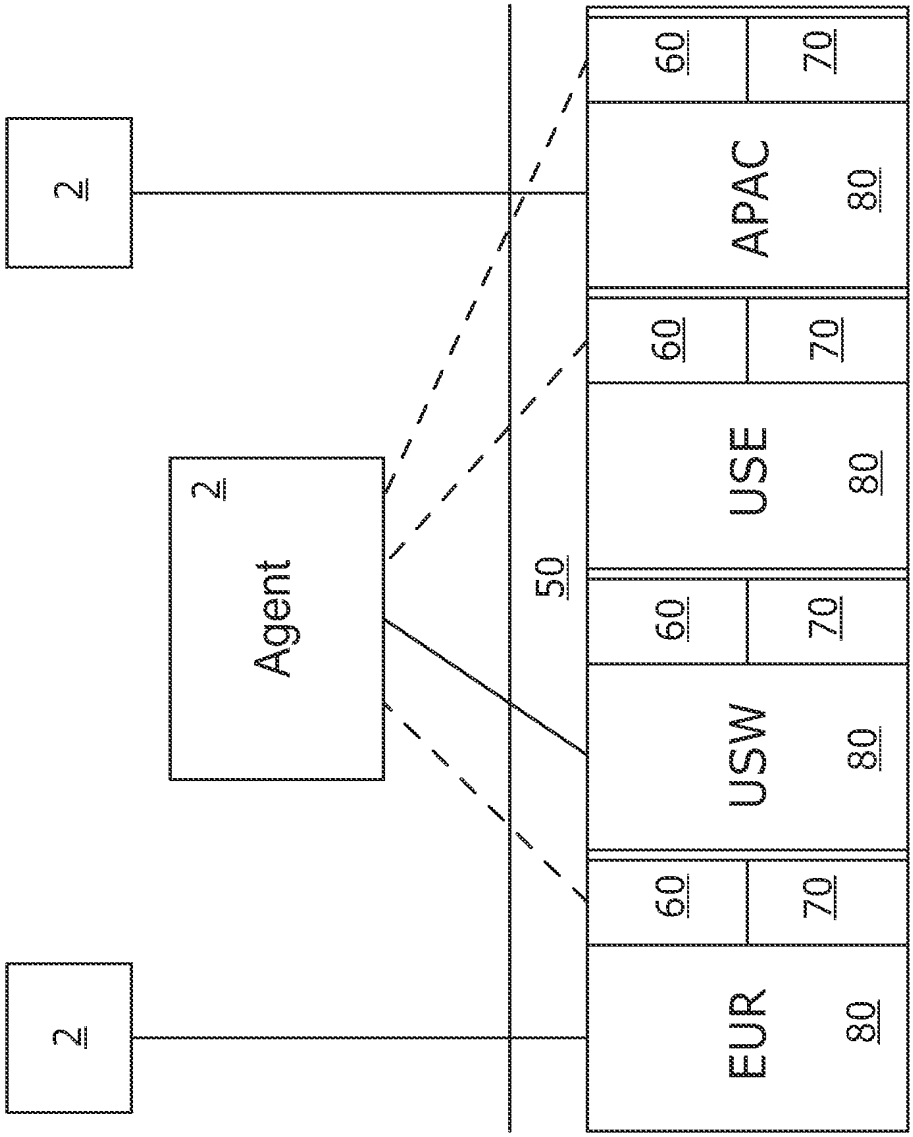


Fig. 4

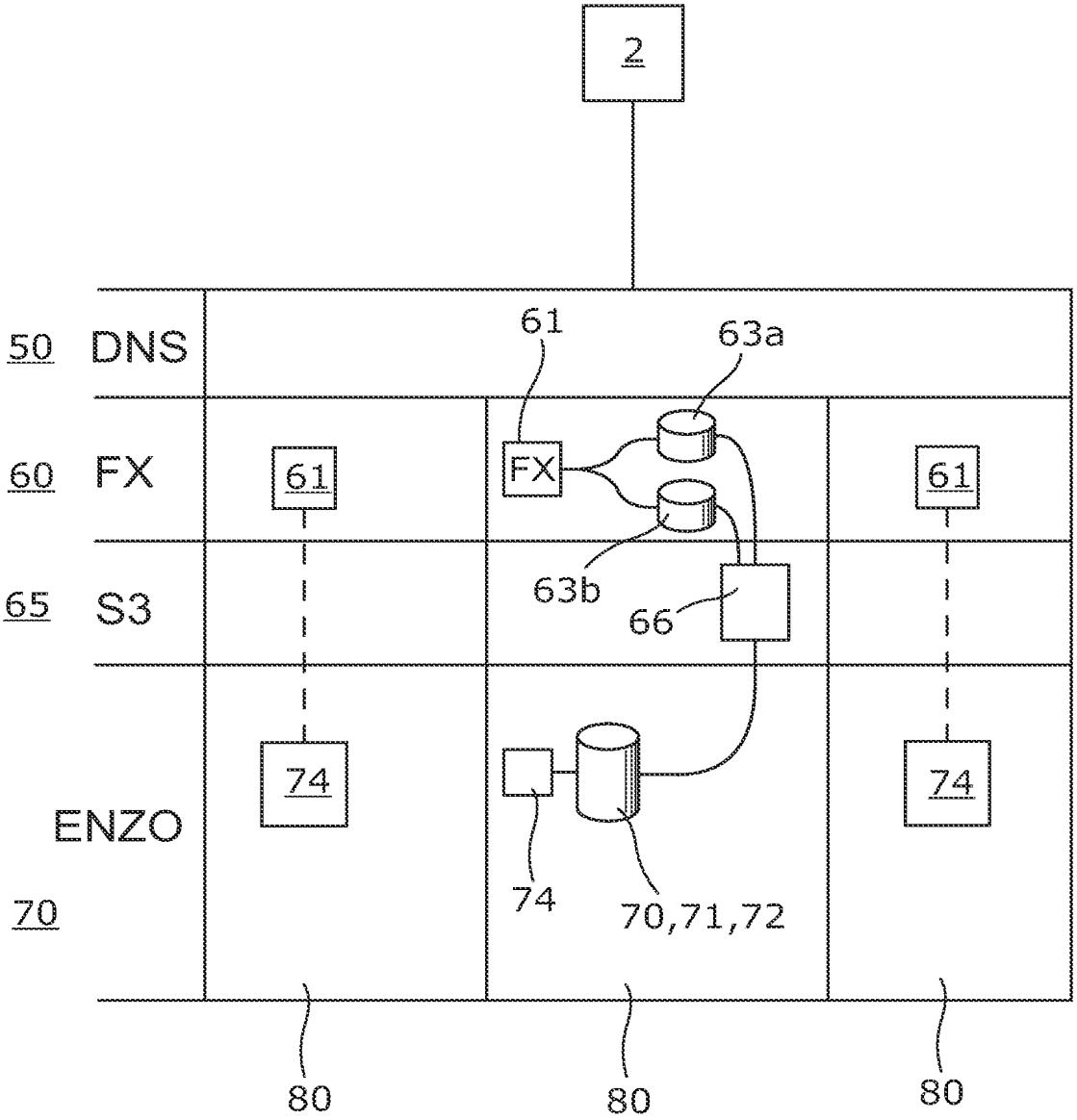

2
50 DNS
61
63a
60 FX
61
FX
61
63b
65 S3
66
74
74
ENZO
70
74
70,71,72
80
80
80

Fig. 5

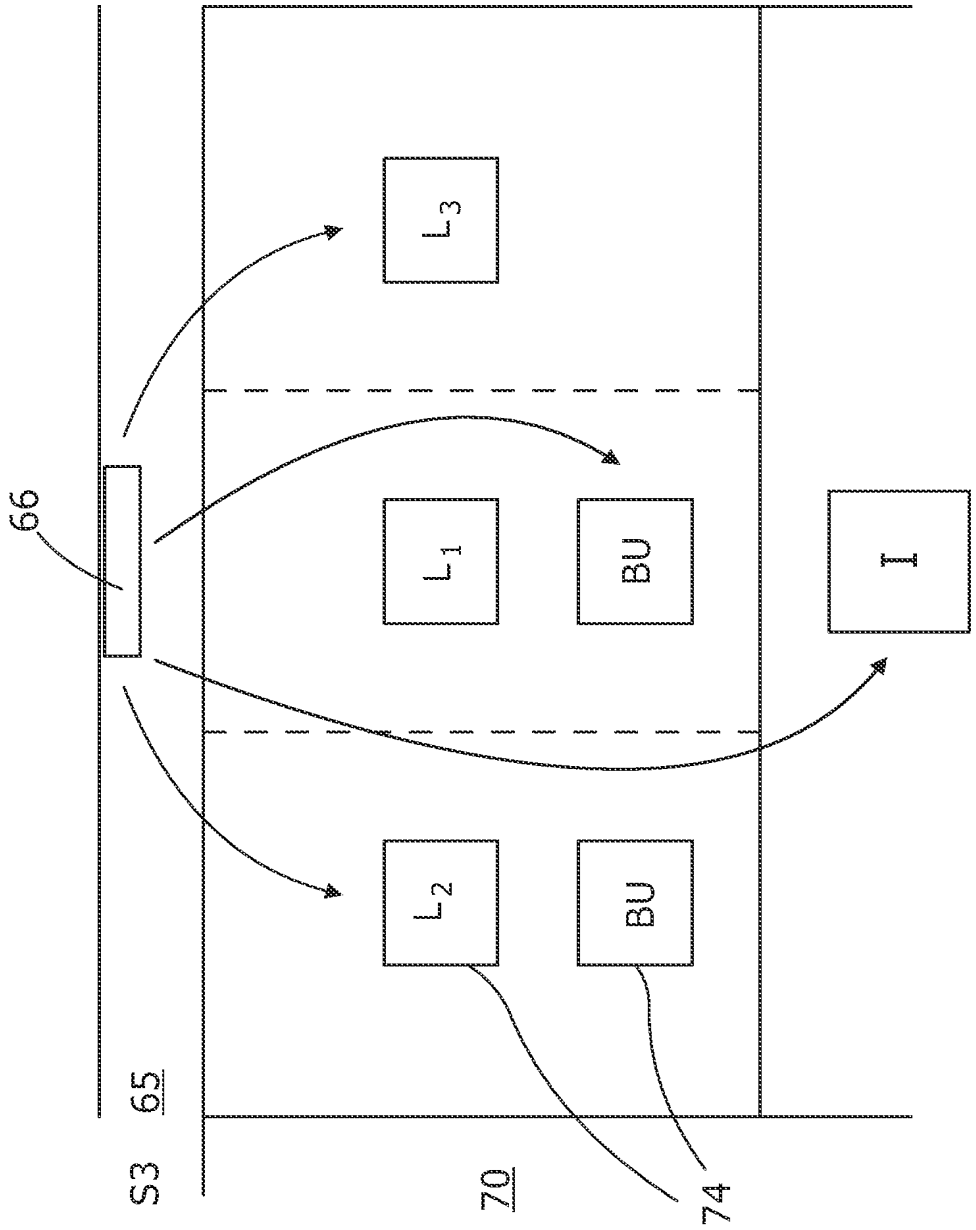


Fig. 6

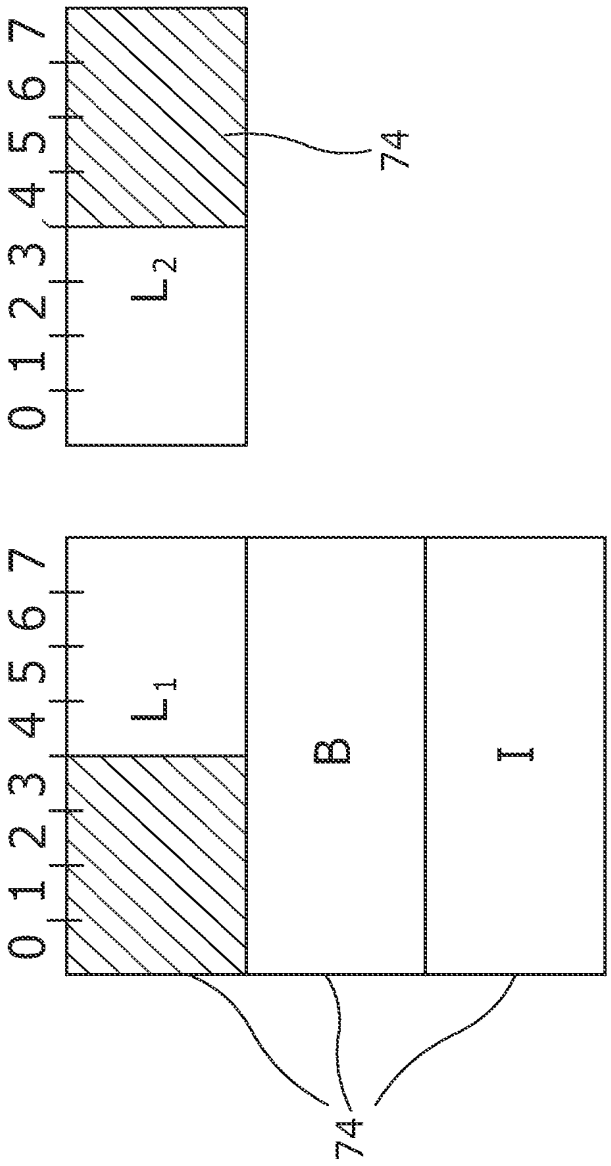


Fig. 7

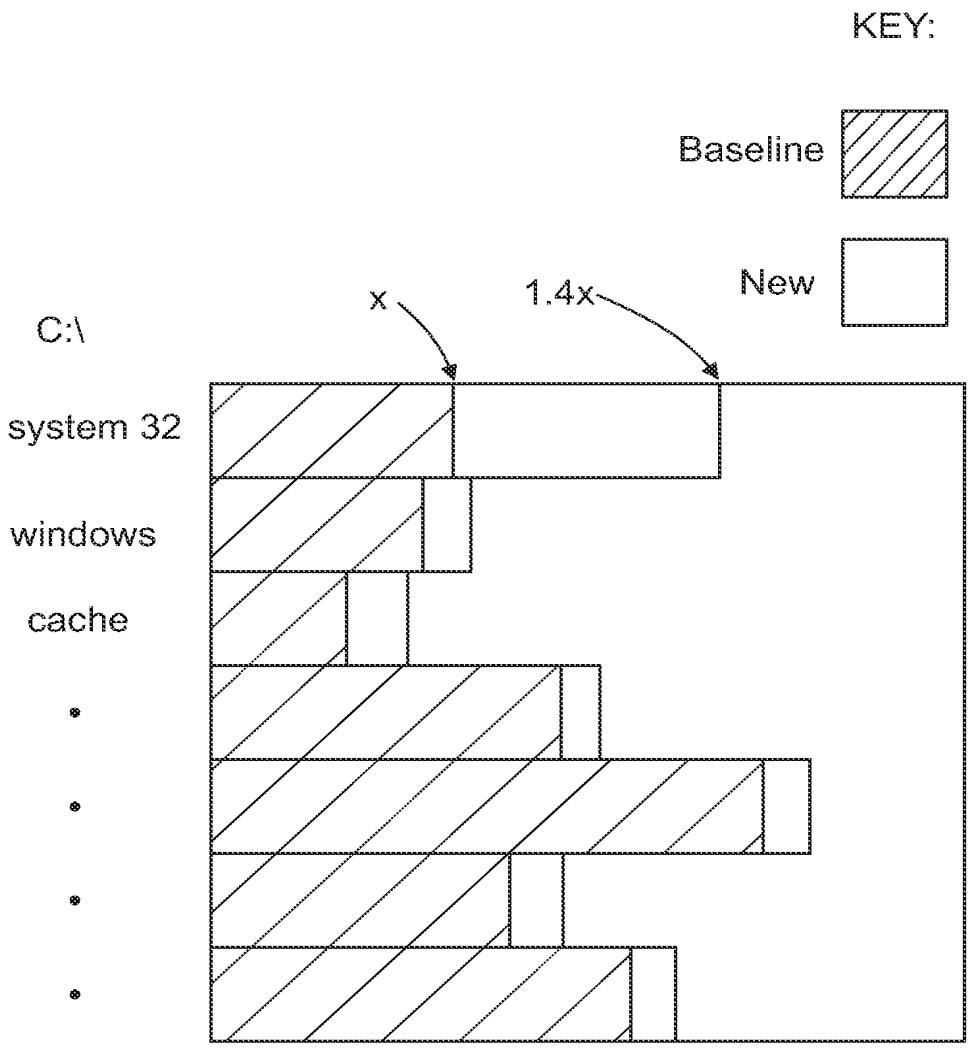


Fig. 8

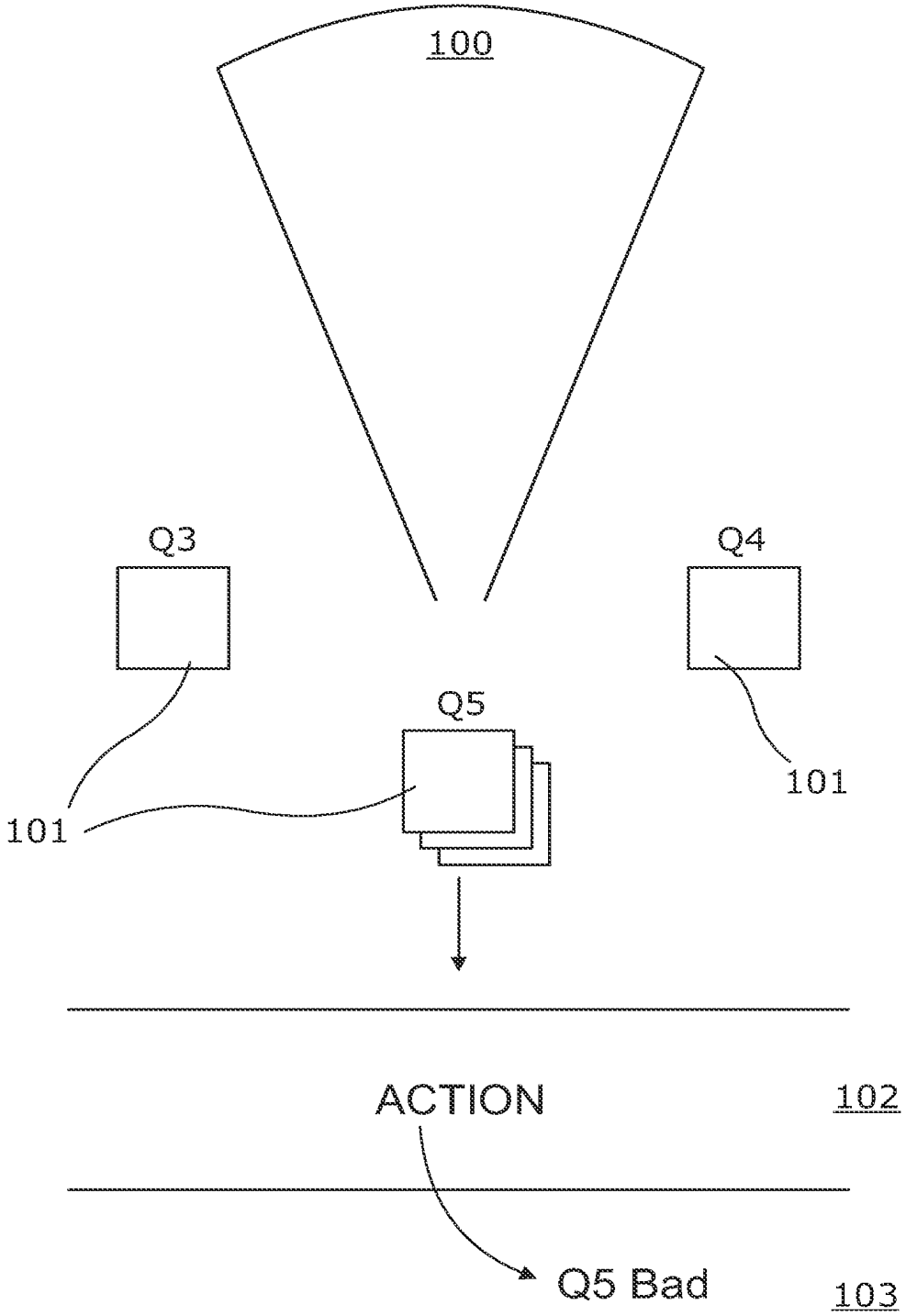


Fig. 9

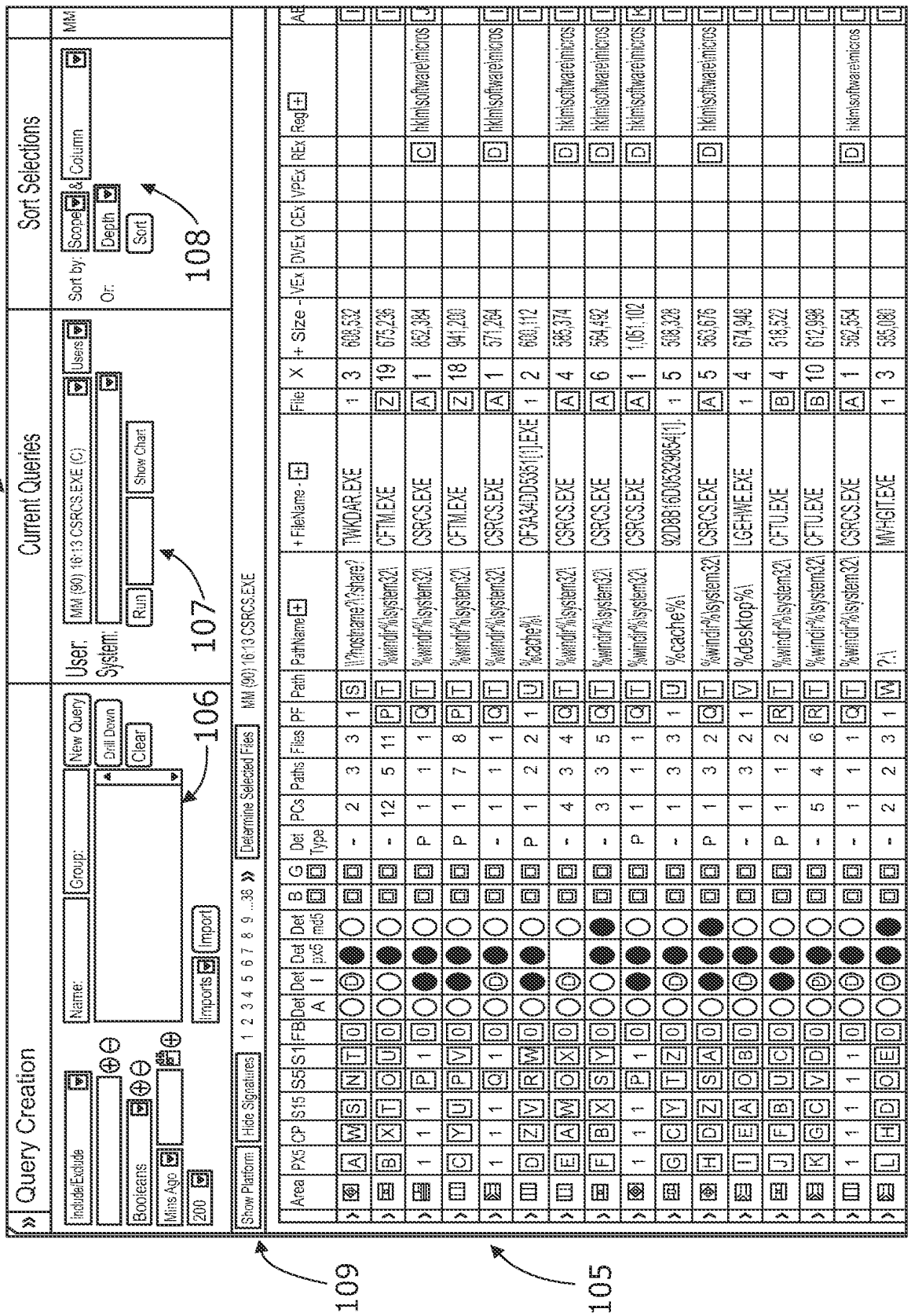

105
Query Creation
Current Queries
Sort Selections
IncludeExclude
Name:
Group:
New Query
Drill Down
Clear
Booleans
Mins Ago
1200
Imports
Import
106
User:
System:
MM (90) 16:13 CSRCS.EXE (C)
Users
Run
Show Chart
107
Sort by:
Scope
&
Column
On:
Depth
Sort
108
Show Platform
Hide Signatures
1 2 3 4 5 6 7 8 9 ...38
Determine Selected Files
MM (90) 16:13 CSRCS.EXE
109
105
Area
PX5
CP
S15
S5
S1
FB
Det A
Det I
Det px5
Det md5
B
G
Det Type
PCs
Paths
Files
PF
Path
PathName
+FileName -
File
X
+ Size -
VEx
DVEx
CEx
VPEx
REx
Reg
AE
TWKDAR.EXE
CFTM.EXE
CSRCS.EXE
OF3A34DD53B1[1].EXE
92D8B16D0632905410...
CFTU.EXE
LGEHWE.EXE
MVHGIT.EXE
hklm\software\micros

Fig. 10

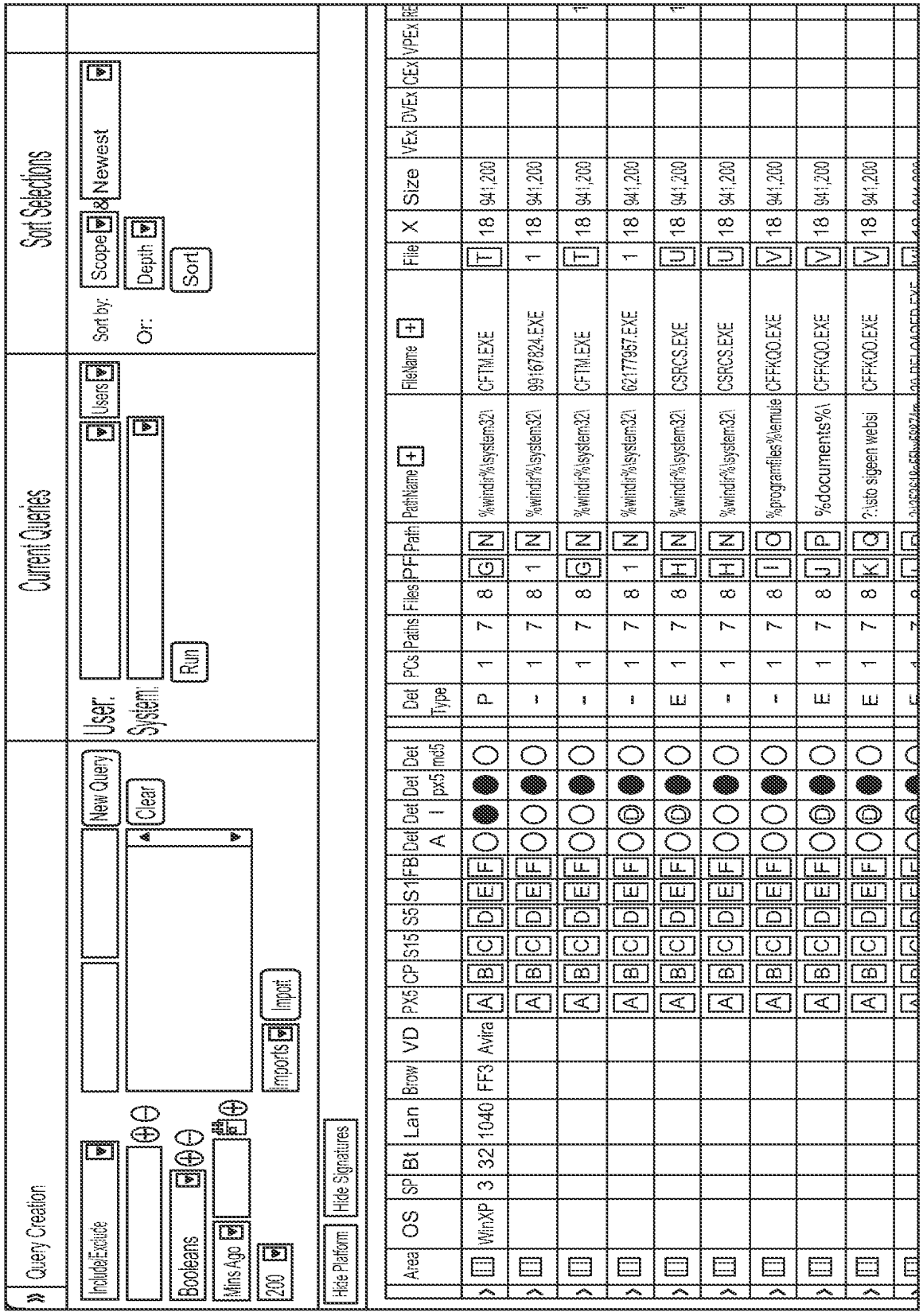

Query Creation
Current Queries
Sort Selections
Include/Exclude
New Query
Clear
Booleans
Mins Ago
200
Imports
Import
User:
System:
Run
Users
Sort by:
Scope
Newest
Or:
Depth
Sort
Hide Platform
Hide Signatures
Area
OS
SP
Bt
Lan
Brow
VD
PX5
CP
S15
S5
S1
FB
Det A
Det I
Det px5
Det md5
Det Type
PCs
Paths
Files
PF
Path
PathName
FileName
File
X
Size
VEx
DVEx
CEx
VPEx
WinXP
3
32
1040
FF3
Avira
%windir%\system32\
CFTM.EXE
%programfiles%\emule
CFFKQO.EXE
%documents%\
?:\sto sigeen websi
941,200

Fig. 11

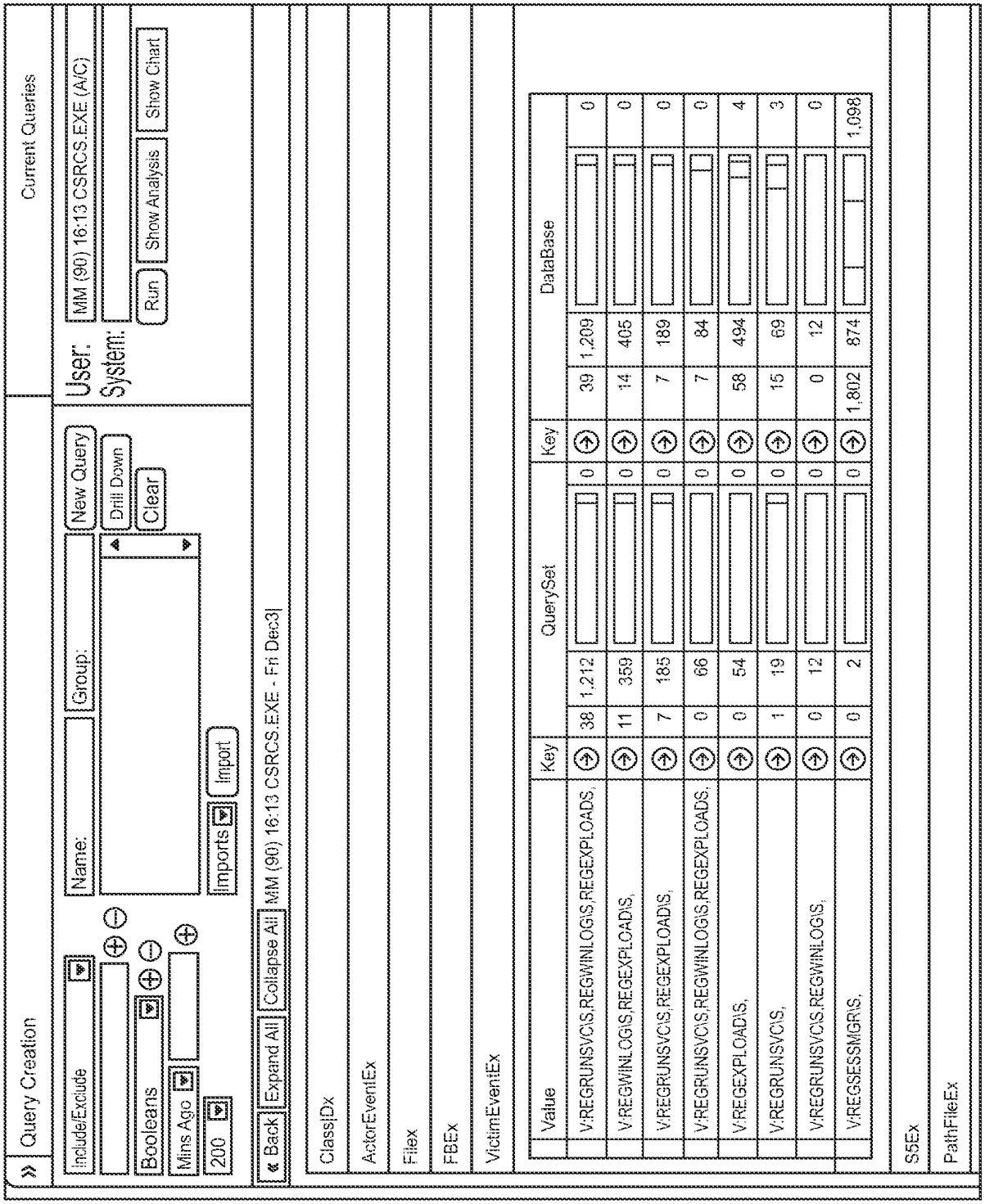

Query Creation
Current Queries
Include/Exclude
Name:
Group:
New Query
Drill Down
Clear
User:
System:
MM (90) 16:13 CSRCS.EXE (A/C)
Booleans
Mins Ago
200
Imports
Import
Run
Show Analysis
Show Chart
« Back
Expand All
Collapse All
MM (90) 16:13 CSRCS.EXE - Fri Dec3
ClassIDx
ActorEventEx
FileEx
FBEx
VictimEventEx
Value
Key
QuerySet
Key
DataBase
V:REGRUNSVCS,REGWINLOGIS,REGEXPLOADS,
V:REGWINLOGIS,REGEXPLOADIS,
V:REGRUNSVCIS,REGEXPLOADIS,
V:REGRUNSVCIS,REGWINLOGIS,REGEXPLOADS,
V:REGEXPLOADIS,
V:REGRUNSVCIS,
V:REGRUNSVCS,REGWINLOGIS,
V:REGSESSMGRIS,
S5Ex
PathFileEx

Fig. 12

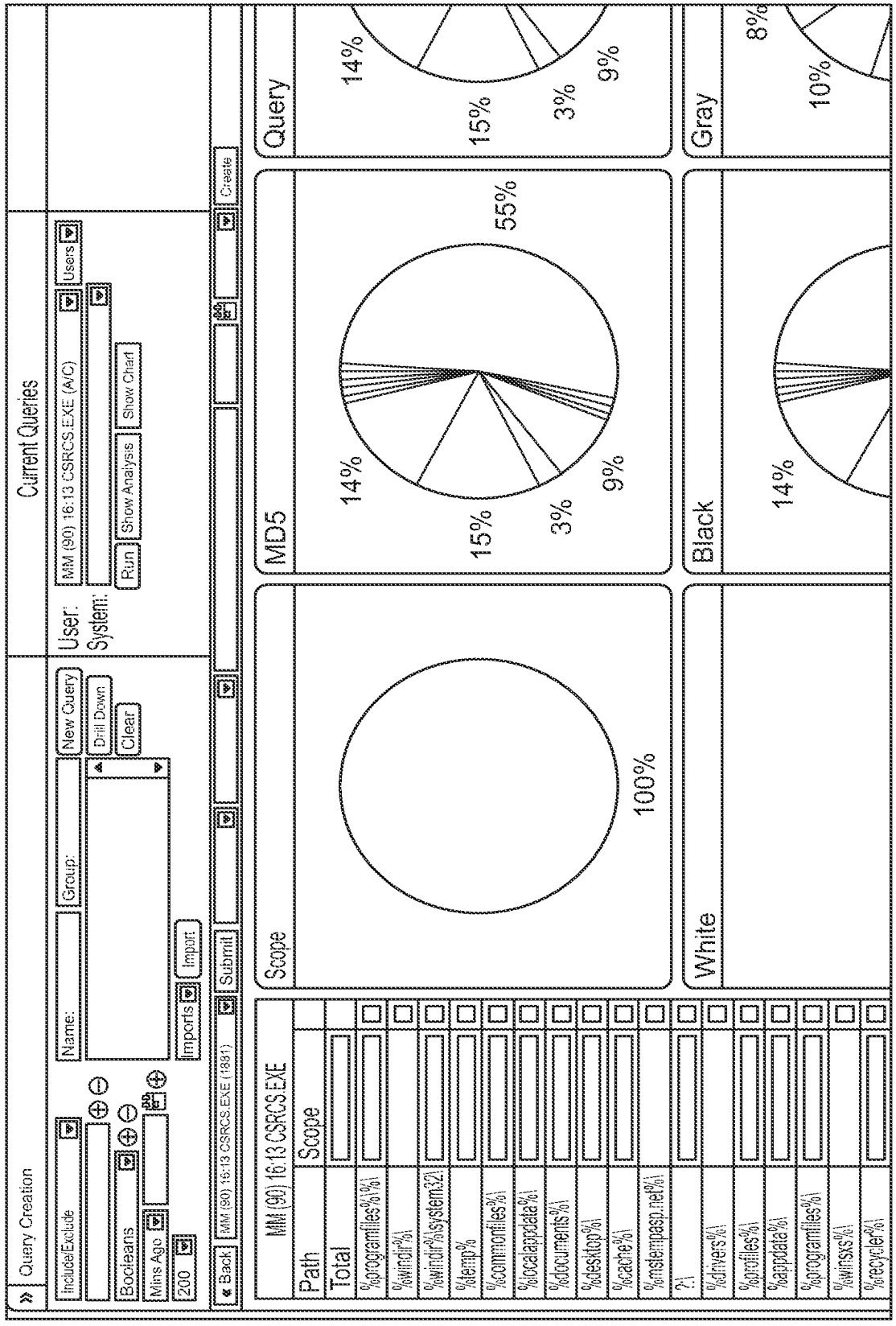

Query Creation
Current Queries
Include/Exclude
Name:
Group:
New Query
Drill Down
Clear
Booleans
Mins Ago
200
Imports
Import
User:
System:
MM (90) 16:13 CSRCS.EXE (A/C)
Users
Run
Show Analysis
Show Chart
Back
MM (90) 16:13 CSRCS.EXE (1881)
Submit
Create
MM (90) 16:13 CSRCS.EXE
Path
Scope
Total
%programfiles%\%1
%windir%\
%windir%\system32\
%temp%
%commonfiles%\
%localappdata%\
%documents%\
%desktop%\
%cache%\
%systemroot%\
?:\
%drivers%\
%profiles%\
%appdata%\
%programfiles%\
%winsxs%\
%recycler%\
Scope
100%
MD5
14%
15%
55%
3%
9%
Query
14%
15%
3%
9%
White
Black
14%
Gray
8%
10%

Fig. 13

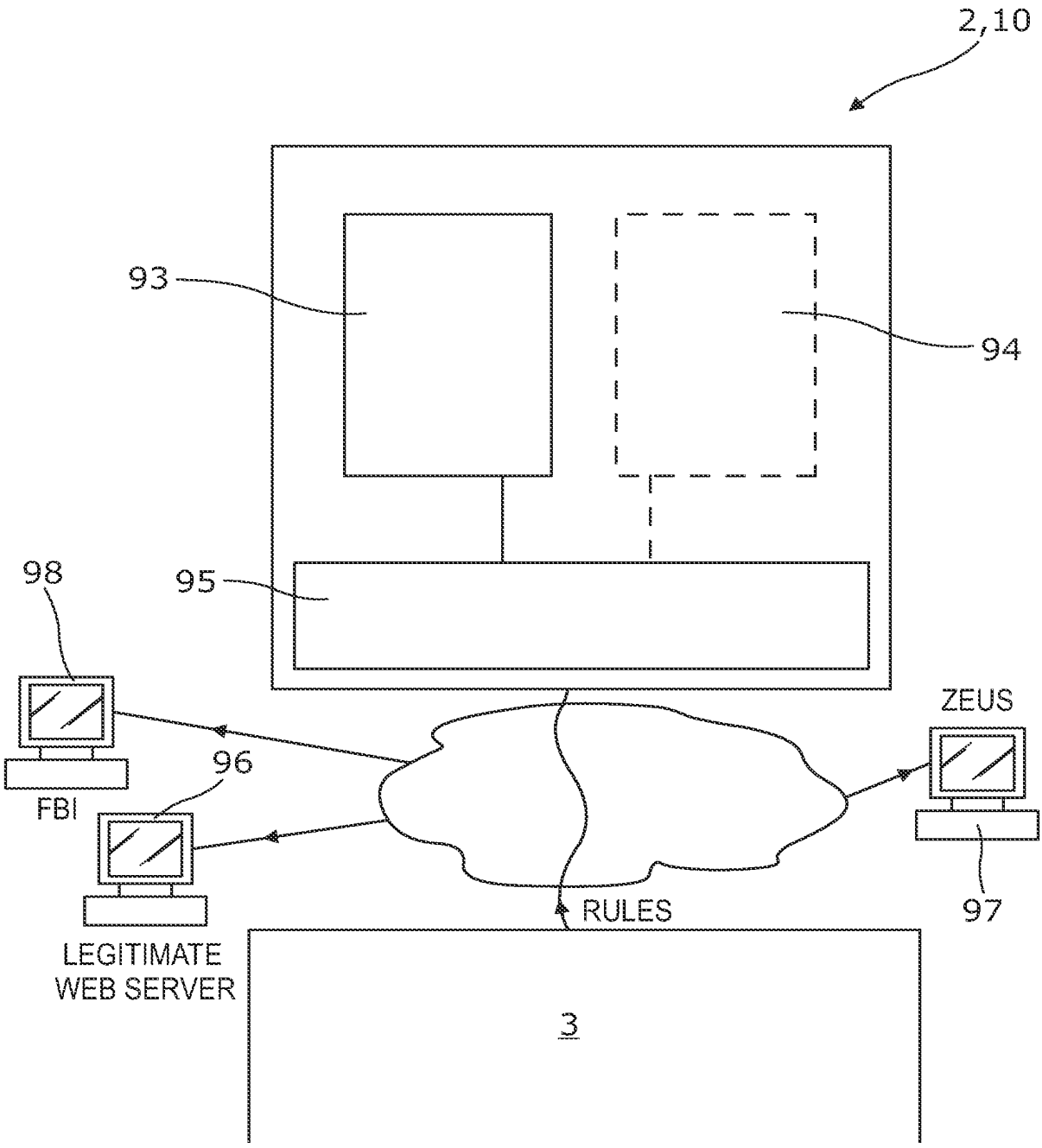


Fig. 14

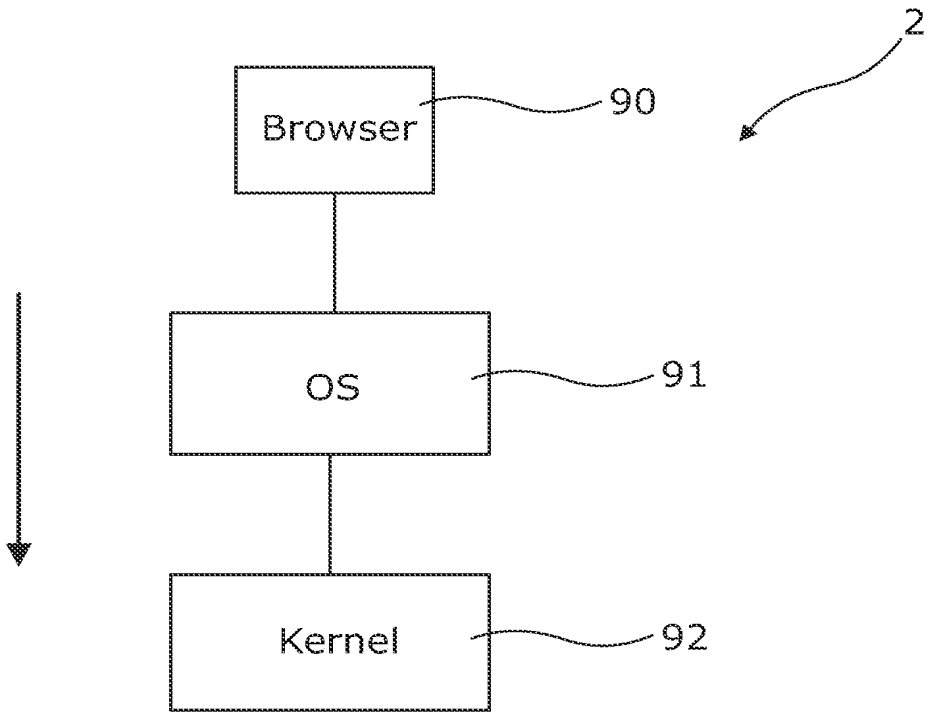


Fig. 15

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Filer:	Sean Ryan Odowd/Rene Roskam
Attorney Docket Number:	9400.004.02

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility application filing	1011	1	380	380
Utility Search Fee	1111	1	620	620
Utility Examination Fee	1311	1	250	250
Pages:				
Claims:				
Claims in excess of 20	1202	4	60	240
Independent claims in excess of 3	1201	1	250	250
Miscellaneous-Filing:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1740**

Electronic Acknowledgement Receipt

EFS ID:	12066208
Application Number:	13372375
International Application Number:	
Confirmation Number:	2918
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Customer Number:	61529
Filer:	Sean Ryan Odowd/Rene Roskam
Filer Authorized By:	Sean Ryan Odowd
Attorney Docket Number:	9400.004.02
Receipt Date:	13-FEB-2012
Filing Date:	
Time Stamp:	19:46:53
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$1740
RAM confirmation Number	6706
Deposit Account	504828
Authorized User	BARRETT,BERNADETTE

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	9400_004_02_ADS_02132012.pdf	1031271 f2a5a74d74fafda6c317c8cdcb60f9cddbed88e5	no	4
Warnings:					
Information:					
2		9400_004_02_Spec.pdf	259013 029f2e6558c30e7ef225d6a6b56bc4a2a58b0ef7	yes	41

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Specification	1	35
	Claims	36	40
	Abstract	41	41

Warnings:					
Information:					
3	Drawings-only black and white line drawings	9400_004_02FIGS.pdf	104175 ccf52d1b8f79e4fbd1a93800b05793d4d0743e52	no	15
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	38036 2bed3813e3dde12f2420609e8cf5c2debf77d512	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1432495		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/372,375

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	380
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	620
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	250
TOTAL CLAIMS (37 CFR 1.16(i))	24 minus 20 =	* 4			OR	x 60 =	240
INDEPENDENT CLAIMS (37 CFR 1.16(h))	4 minus 3 =	* 1				x 250 =	250
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	1740

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/372,375	02/13/2012	2431	1740	9400.004.02	24	4

CONFIRMATION NO. 2918

61529
Neugeboren O'Dowd PC
1227 Spruce Street
SUITE 200
BOULDER, CO 80302

FILING RECEIPT



Date Mailed: 03/01/2012

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Melvyn Morris, Belper, UNITED KINGDOM;
Joseph Jaroch, Elk Grove Village, IL;

Assignment For Published Patent Application

WEBROOT INC., Broomfield, CO

Power of Attorney: None

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/443,095 02/15/2011

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)

If Required, Foreign Filing License Granted: 02/24/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/372,375**

Projected Publication Date: To Be Determined - pending completion of Missing Parts

Non-Publication Request: No

Early Publication Request: No

Title

METHODS AND APPARATUS FOR DEALING WITH MALWARE

Preliminary Class

726

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/372,375	02/13/2012	Melvyn Morris	9400.004.02

CONFIRMATION NO. 2918

61529
Neugeboren O'Dowd PC
1227 Spruce Street
SUITE 200
BOULDER, CO 80302

FORMALITIES LETTER

OC000000052784494

Date Mailed: 03/01/2012

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The oath or declaration is missing.
  A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.
  Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- A surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of $**130** for a non-small entity, must be submitted.

SUMMARY OF FEES DUE:

Total fee(s) required within **TWO MONTHS** from the date of this Notice is $**130** for a non-small entity
- $**130** Surcharge.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/ldvan/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13372375
Filing Date	2012-02-13
First Named Inventor	Morris
Art Unit	2431
Examiner Name	
Attorney Docket Number	9400.004.02

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20070016953	A1	2007-01-18	Morris, et al.	
	2	20110197177	A1	2011-08-11	Mony	
	3	20110197272	A1	2011-08-11	Mony	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1315066	EP	A1	2003-05-28	British Telecommunications		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13372375
	Filing Date	2012-02-13
	First Named Inventor	Morris
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	9400.004.02

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	MORRIS, ET AL., "Specification for related U.S. Patent Application No. 13/372,433 (Attorney Docket No. 9400.004.03)," filed 02/13/2012, Page(s) 58, to be published in: US	☐
	2	MORRIS, ET AL., "Specification for related U.S. Patent Application No. 13/372,439 (Attorney Docket No. 9400.004.04)," filed 02/13/2012, Page(s) 54, to be published in: US	☐
	3	SOGNO-PABIS, ELZBIETA, "Partial International Search Report re application PCT/EP2012/052497", 05/04/2012, Page(s) 7, Published in: NL	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13372375
	Filing Date	2012-02-13
	First Named Inventor	Morris
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	9400.004.02

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Sean R. O'Dowd/	Date (YYYY-MM-DD)	2012-05-30
Name/Print	O'Dowd, Sean R.	Registration Number	53403

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	12887395
Application Number:	13372375
International Application Number:	
Confirmation Number:	2918
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Customer Number:	61529
Filer:	Sean Ryan Odowd/Rene Roskam
Filer Authorized By:	Sean Ryan Odowd
Attorney Docket Number:	9400.004.02
Receipt Date:	31-MAY-2012
Filing Date:	13-FEB-2012
Time Stamp:	19:15:39
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Foreign Reference	EP1315066A1.pdf	1589676 9767b00f190799e21e658b635c77a0937d30a62d	no	28

Warnings:	
Information:	

2	Non Patent Literature	9400_004_03_Spec.pdf	302872 a2b944263cf79a1c20101664c7293feab6b8eb1c	no	58
Warnings:					
Information:					
3	Non Patent Literature	9400_004_04_Spec.pdf	328112 d5d64162efdd71abb67ea45ae23c59c9c5d44b7e	no	54
Warnings:					
Information:					
4	Non Patent Literature	PCTEP2012052497_Search_Report.pdf	327368 eac45232f82f0d4d9316b7c6926fe3f126795693	no	7
Warnings:					
Information:					
5	Information Disclosure Statement (IDS) Form (SB08)	9400_004_02US_IDS_05302012.pdf	612426 1f24182f3ec110179919629f4ec245b8fd6b3722	no	4
Warnings:					
Information:					
		Total Files Size (in bytes):	3160454		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 315 066 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
28.05.2003 Bulletin 2003/22

(51) Int Cl.[7]: **G06F 1/00**, H04L 29/06

(21) Application number: **01309795.1**

(22) Date of filing: **21.11.2001**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant: **BRITISH TELECOMMUNICATIONS public limited company**
London EC1A 7AJ (GB)

(72) Inventor: **The designation of the inventor has not yet been filed**

(74) Representative: **Nash, Roger William et al**
BT Group Legal Services,
Intellectual Property Department,
Holborn Centre, 8th Floor,
120 Holborn
London EC1N 2TE (GB)

(54) Computer security system

(57) A computer security system for use in a network environment comprising at least a plurality of user computers arranged to communicate over a network, the system comprising a warning message exchange system operable to allow the communication from the user computers of warning messages relating to suspect data identified as a possible security threat; a message counting system operable to maintain a count for every particular piece or set of suspect data based on the number of warning messages communicated relating thereto; and network security means operable to act against any particular piece or set of suspect data for which the count maintained therefor exceeds at least one threshold value

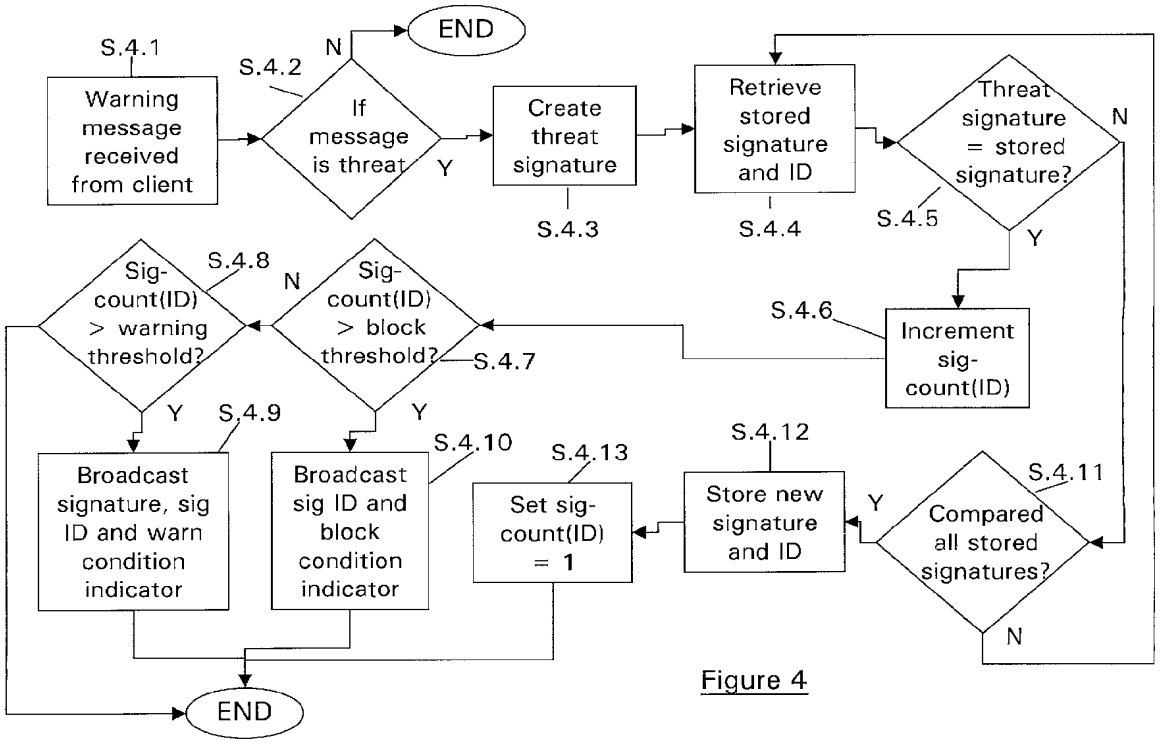


Figure 4

EP 1 315 066 A1

Sophos Ex. 1002
Page 78 of 683

Description

Technical field

[0001] The present invention relates to a computer security system for use in a networked environment, the system providing a measure of security against suspect data such as computer viruses and the like.

Background to the Invention

[0002] Malicious attacks on computer systems have plagued individuals and organisations for many years. Initially these attacks mostly took the form of viruses in which a rogue program infected a machine via an infected floppy disk or network location for example. More recently so called worms and Trojan horses have caused much disruption in which the user is deceived into running a program via an attachment to an e-mail or a rogue program masquerading as something more innocuous. A large industry has grown up around protection from such attacks. These companies provide anti-virus software that typically resides on individual machines and monitors the system to check for the presence of known viruses. These viruses can take many forms - some more advanced forms are fully polymorphic in that the byte code "signature" is entirely different from one instance of the virus to the next. This is achieved through the use of encryption technology and/or the addition of spurious and random code to the virus. However, the majority of viruses that are in the "wild" and the cause of costly disruption to computer systems are relatively simple and can be detected by simple byte-code signature matching. Many of the current anti-virus programs use just such techniques and are successful if the signature of a discovered virus can be delivered to machines before the virus strikes.

[0003] The operation of such anti-virus programs and systems is well known in the art, and is usually as follows. A computer user will have installed on their computer an anti-virus program which is provided with a database of known computer virus byte-code signatures. The program will tend to run in the background continuously monitoring operations performed on the computer, and data received at and transmitted from the computer. If the byte-code signature of a known virus stored in the anti-virus program's database is detected by the program, the anti-virus program informs the user and takes appropriate action against the data, such as deleting it or storing it in a protected drive.

[0004] Such prior approaches tend to suffer from a big problem, however - delay. Even the simplest of viruses and worms may still cause great disruption at enormous cost to organisations. This is because the process from discovery of a new virus to delivering its signature to all protected machines takes too long, and requires an administrative authority such as the anti-virus program manufacturer (or in some cases an organisation's IT department) to recognise the problem, take action to identify the virus's signature, update the anti-virus database, and distribute the updated database to each user. By the time such a sequence of actions is complete the damage has already been done in many cases. What is required is a much more rapid approach - one that can operate on the same time scales as the spread of the virus and thus provide much more rapid and cost-saving protection.

Prior Art

[0005] There is much work exploring the use of agent technology to provide rapid reaction to malicious attack. In this work computer systems are inhabited by a number of agents whose job it is to detect intrusions. One interesting approach aims to draw metaphor from immune systems, which allow an organism to rapidly respond to previously unseen foreign objects through a "real-time" evolutionary system, as disclosed in Artificial Life IV, Proceedings of the Fourth International Workshop on Synthesis and Simulation of Living Systems, Rodney A. Brooks and Pattie Maes, eds., MIT Press, Cambridge, Massachusetts, 1994, pp. 130-139 These kinds of agent systems may prove useful in future security systems, but rely on the successful development and deployment of software agents which can detect intrusions. Many other potential future anti-virus systems are also discussed at http://www.research.ibm.com/antivirus/SciPapers.htm. In the meantime until the potential of these ideas is exploited, there is still a need for a system which allows for more rapid prevention of the spread of computer viruses.

[0006] One such prior art system which claims to increase response times is that of the Symantec® Digital Immune System (DIS) , which is described at http://securityresponse.symantec.com/avcenter/reference/dis.tech.brief.pdf. The DIS operates by providing an heuristic search engine which automatically identifies possible viruses at either the user's desktop, the server, or the network gateway. A secure channel is then provided direct to Symantec's security response centre over which the suspect data can be transmitted. At the security response centre the received data is subject to a number of automatic filters to detect, for example, known clean files, files which are known to return false positives from the heuristic search engine, and known virus files. If the suspect data is not filtered out by any of these filters then it is directed to an analysis program for further analysis and action.

[0007] The DIS system therefore allows for the automatic identification, secure submission, automatic prioritisation, and subsequent analysis of suspect data, but ultimately still involves a central authority in the loop to analyse suspect files which make it through the filters. Thus, whilst DIS may improve response times to virus infection through it's automatic filtering processes, it still relies on a central authority to analyse the suspect data

Sophos Ex. 1002
Page 79 of 683

and decide on appropriate action, which must then be communicated outwards to each user. There is therefore still a need for a system which removes this centralised analysis step to speed the response.

Summary of the Invention

[0008] In order to address the above problems, the present invention provides a collaborative computer security system wherein the responsibility for detection of malicious data such as a computer virus is removed from that of any central authority, and is instead placed in the hands of each and every user of the network. More particularly, the present invention provides a distributed virus identification system which allows individual users or software agents running on a user's computer to identify malicious data when they receive it, and to pass a warning message concerning the received data to either their peers, or to a central server. A record is kept either at the server or at each peer computer as to the number of warning messages communicated concerning any particular piece or set of suspect data, and then appropriate security actions such as issuing warnings to users or blocking the transmission of the suspect data can be taken once the number of warning messages communicated from users has passed a certain threshold level. The advantages of the invention are that an organisation's response to a computer virus intrusion can be much more rapid than was previously the case where a central authority had to identify the problem and take action.

[0009] In view of the above, the present invention provides a computer security system for use in a network environment comprising at least a first group of user computers arranged to communicate over a network, the system comprising a warning message exchange system operable to allow the communication from the user computers of warning messages relating to suspect data identified as a possible security threat; a message counting system operable to maintain a count for every particular piece or set of suspect data based on the number of warning messages communicated relating thereto; and network security means operable to act against any particular piece or set of suspect data for which the count maintained therefor exceeds at least one threshold value

[0010] The primary advantage of the invention is that it allows the security system to work on the same time scales as the spread of the attack. The more the computer virus or worm spreads the more likely it is that enough positive identifications are made to allow its signature to be ascertained and protection to be installed. This overcomes the problem of traditional security systems where an authority has to learn of the virus, take action, and then distribute associated protective measures to the users.

[0011] A further advantage of the system is that it allows a lot of information to be rapidly collected about a computer virus. For example, current "worms" that are "in the wild" are mostly identical at the byte code level, however it is likely that in the future this will no longer be the case, and that there will be variations in different instances of the same worm. In such a case, the more instances of the worm that can be collected the more likely that it will be that suitable protection can be devised. By allowing for individual identification of a worm at each computer by the user, the present invention allows for multiple instances of the same virus to be identified and collected.

[0012] The one or more "threshold values" against which the respective counts for pieces or sets of suspect data are compared may be any value, and may be fixed or dynamically adaptive. Furthermore the actual values may be generated by any appropriate function, such as for example by a random number generator, or as a function of some metric of accuracy of users in identifying viruses. Furthermore, in other embodiments it is foreseen that the threshold values may not simply be actual numbers which the respective counts must be greater than, but could instead be probabilistic in nature. Furthermore, various logical functions or rules can be used for their creation, including for example, fuzzy logic.

[0013] Preferably, the judgement as to whether any piece or set of data present at any one or more of the user computers is a possible threat is performed by the respective human user or users of the or each user computer. Such an arrangement exploits the massive untapped resources and expertise of many computer users, and again allows for a rapid response to the spread of a computer virus.

[0014] Preferably, the network security means is further operable to compare the maintained count for a particular piece or set of suspect data against a plurality of different thresholds, and to take different action against the data dependent upon which threshold or thresholds are exceeded.

[0015] Such an approach allows the computer security systems to have a graded response to a computer virus intrusion, and to take different actions depending on the number of warnings received from users. Furthermore, it is also possible to weight warnings from different users, such that a warning from a user who is particularly expert in the field is weighted more heavily than a casual user of the system.

[0016] Preferably, the action taken by the network security means comprises warning each of the users as to the suspect nature of a particular piece or set of data. Furthermore, the action may also comprise preventing the transmission of the particular piece or set of suspect data across the network. Usually, the warning action will be taken when the number of messages communicated exceeds a lower threshold than a second threshold which must be crossed in order for the transmission blocking action to take place.

[0017] Preferably, the or each warning message com-

Sophos Ex. 1002
Page 80 of 683

prises at least an identifier of the piece or set of suspect data to which it relates. The identifier may be the actual piece or set of suspect data itself, or a repeatably generatable signature substantially unique to the piece or set of data. By allowing for the collection of such identifiers, the security system also provides a means of collecting information on multiple computer viruses, and also on adaptive computer viruses whose byte code signature may change in each instantiation on a users machine.

[0018] In a preferred embodiment, the computer security system further comprises a network server arranged to receive the or each warning message communicated from the user computers, and further arranged to host the message counting system and at least part of the network security system, wherein that part of the network security system hosted by the server is operable to determine the action which should be taken against a particular piece or set of suspect data, and to communicate an action condition indicator indicative of the determined action to each of the plurality of users.

[0019] By using a central server to maintain the warning message counts and to receive the warning messages themselves, the network traffic generated by the computer security system is minimised, as users need only send a warning message direct to the server, which can then broadcast warnings about suspect data as appropriate to all the users.

[0020] In another embodiment, the warning messages generated by a user computer are broadcast to every other user computer, and each user computer is further arranged to host its own message counting system and network security system operable in accordance with any of the above. Such an approach represents a "peer-to-peer" system, and provides advantages that it is not dependent upon a central server for its operation, thereby presenting a more robust distributed system. Such a peer-to-peer system has a potential disadvantage, however, in that depending on the exact implementation it may be that the network traffic required to broadcast the warning messages from each user to every other user is unacceptably high.

[0021] To at least partially overcome this problem, in another embodiment there is provided an inter-group communications system operable to allow the communication of warning messages relating to suspect data identified as a possible security threat from the first group of user computers to one or more other groups of other user computers. By splitting the user computers intro groups, the number of warning messages which are required to be transmit is substantially reduced, thereby conserving network signalling bandwidth.

[0022] Preferably, the inter sub-set warning messages are transmitted by the inter-sub-set communications system if the number of warning messages communicated by the user computers in the sub-set concerning a particular piece or set of data exceeds at least one threshold value. Preferably the threshold value or values is/are the same as those at which the network security system takes action.

[0023] In further embodiments, the message counting system is further arranged to store one or more weighting coefficients relating to one or more particular user computers, and to increment the count maintained for a particular piece or set of suspect data by an amount based upon the weighting coefficient when a warning is received from the one or more particular user computers relating to the particular piece or set of suspect data

[0024] From a second aspect, the present invention also provides a computer readable storage medium storing one or more computer programs which when run on a computer cause the computer to operate in the manner of the computer security system as described above. Such a computer security system may provide all the additional features and advantages mentioned previously.

Brief Description of the Drawings

[0025] An overview of the operation of the invention, together with a description of a number of embodiments thereof, presented by way of example only, will now be made with reference to the accompanying drawings, wherein like reference numerals refer to like parts, and wherein:-

Figure 1 illustrates a typical network environment in which the computer security system of the present invention is intended to operate;

Figure 2 illustrates a computer storage medium located within each users computer, and depicts the programs and data stored thereon in a first embodiment of the invention;

Figure 3 depicts a computer storage medium located at a server used within the first embodiment of the inventions, and further depicts the programs and data stored thereon;

Figure 4 is a flow diagram showing the operation steps performed by the warning creation program stored at the server in the first embodiment of the present invention;

Figure 5 is a flow diagram showing the method steps performed by the warning receipt program stored at a users computer in the first embodiment;

Figure 6 is a flow diagram showing the steps performed by a filter program in either of the embodiments of the invention;

Figure 7 depicts a computer readable storage medium located at a users computer in a second embodiment of the present invention, and further depicts the programs and data stored thereon;

Figure 8 is a flow diagram of the steps performed by a warning creation program in the second embodiment of the present invention;

Figure 9 is a flow diagram of the steps performed by a warning receipt program in the second embod-

Sophos Ex. 1002
Page 81 of 683

iment of the present invention;

Figure 10 is a flow diagram illustrating the steps performed by one of the functions in both Figures 8 and 9; and

Figure 11 illustrates an organisational architecture of user computers which may be used in another embodiment of the invention.

Overview of the operation of the invention

[0026] The present invention recognises and makes use of the fact that a computer system is already inhabited by a number of intelligent agents - the users themselves. In order to summarise the operation of the invention consider an attack by an e-mail "worm" (a type of computer virus such as the "Melissa" virus which was encountered in 2001). A worm is sent to an employee of a given organisation. With some probability the employee opens the e-mail attachment and unwittingly unleashes the worm that causes some damage to the individuals machine and propagates itself to a number of other machines through use of the individuals e-mail system and address book. In each of these cases there is some probability that the user will open the attachment and further propagate the virus. Thus, the statistics are in the worm's favour - not everyone will open the attachment but it only takes a small fraction to do so for the worm to propagate throughout an organisation's computer system. However, for every user who opens the attachment there are likely to be many more who correctly recognise the e-mail as a potential threat and discard it. Vital information is thus gained in this process - an intelligent agent has successfully detected an intrusion - and it is this information that the present invention exploits to its full effect. Doing so opens up the potential for the statistics to be turned against the worm and in favour of the protection system.

[0027] Within the invention the user informs the system of the recognition by forwarding the mail or passing the mail or other program to an anti-virus program that is running on that machine, which then passes it to the server (or in an alternative embodiment direct to the user's peers). The signature of the worm is then quickly ascertained and a count kept of the number of warnings received from users about the worm. Once the count reaches a certain threshold the signature of the worm is distributed to all the other individual machines, who then use the signature to filter any received data or mail. As an alternative the server itself could simply filter out all e-mails with such a signature. In either case the technique of allowing users (or user machines provided with appropriate software agents) to detect and provide warning of the worm aligns well with the trends in the industry towards peer to peer systems where the vast untapped resources at the edges of the network are beginning to be used to greatly enhance storage and computational power for example. The invention is therefore essentially a peer to peer security system that may tap the vast unused resource of the user's knowledge and experience, or the user computer's processing power.

Description of the embodiments

[0028] Two specific embodiments of the invention will now be described in detail, followed by description of various alterations that may be made to each to provide additional embodiments. Both main embodiments of the invention implement a computer security system for use in a network environment. A typical network environment in which the invention may be used is depicted in Figure 1.

[0029] Figure 1 illustrates a typical local area network (LAN) configuration. Here, a plurality of user computers 15 are connected to a network 10 which is another control of a network server 12. The network 10 provides typical network functionality, such as the ability to allow users 15 to communicate with each other and with the server over the network. The network 10 in the invention may be any particular network technology, may be wired or wireless, and may be scaled to any network size or architecture known in the art. Therefore, whilst the present invention is particularly useful for use within individual organisations provided with a LAN, it may also be used on a wider scale in a metropolitan area network (MAN) or a wide area network (WAN). Within the embodiments, each of the user computers 15, the network itself 10, and the server 12 are provided with appropriate equipment and software to permit the usual network communication functions as are known in the art.

[0030] Although the above makes reference to the user computers 15 being part of the same network, it should be noted that it is not essential that each user-computer be located in the same actual network (although this may be preferable). This is because all that the invention requires is the ability for any particular user computer to be able to send messages either to its peers or to a server, and hence all that is required is some message transport mechanism between such parties. Such a message transport mechanism may be a single network to which all the user computers and servers (where required) are connected, or may be a sequence of interconnected networks such as the Internet, with different user-computers actually being part of different networks.

[0031] Having described the context in which the invention is intended to operate, a first, preferred, embodiment which represents the best mode of the invention will now be described with reference to Figures 2 to 6.

[0032] The first embodiment of the invention provides a computer security system wherein identification of suspect data is performed by the users or suitable software agents installed and running on the user's computers at the user's computers themselves, and upon identification of a suspect piece or set of data a warning message is transmitted from the user's computer to the network server 12. At the server the number of warning

Sophos Ex. 1002
Page 82 of 683

messages received about a particular piece or set of data is counted, and once the count passes a first warning threshold, a warning message is broadcast to all users, the message containing a signature of the suspect data, such that an anti-virus program located at each user's computer can filter incoming data for the suspect data. If further warnings are received from users by the server, and the count of warning messages exceeds a second threshold, then the server broadcasts a second message to all of the users on the network instructing the anti-virus programs located at each user computer to block the suspect data to prevent any onward transmission or infection.

[0033] Given the above overview, within the first embodiment each user computer 15 contains a computer readable storage medium 22, as shown in Figure 2. The computer readable storage medium will typically be a magnetic hard drive, or may equally be a DVD RAM, DVD-RW, DVD+RW, solid state memory, optical disc, magneto optical disc, or the like. The computer readable storage medium 22 at each user computer 15 is arranged to store a data filter program 24, and a warning receipt program 26. In addition, storage space is also provided for suspect data signatures and ID's, stored in the form of a data base 28.

[0034] The server 12 within the first embodiment also contains a computer readable storage medium 32 which will typically be a magnetic hard disc, but may also be any of the storage devices mentioned previously in respect of the or each user computer 15. Within the first embodiment the computer readable storage medium 32 stores a warning creation program 34, and a suspect data signature and ID database 36. Optionally, the computer readable storage medium 32 may also store a data filter program 38, to provide an alternative method of operation as will be described later.

[0035] Having described the main system hardware elements required by the first embodiment, the operation thereof will now be discussed with reference to the flow diagrams of Figures 4, 5, and 6.

[0036] Assume that a user computer 15 connected to the network 10 receives a message over the network which contains a computer virus or the like (referred to hereafter as suspect data). Within the first embodiment of the invention a user of the user computer 15 upon reading the message recognises that the message contains such suspect data, and hence within the first embodiment then forwards the suspect data as the payload in a warning message of predetermined format to the server 12. By forwarding the data as the payload encapsulated in a warning message of known format, the server knows that the payload is potentially suspect data, and hence will not become victim to the computer virus itself. At the server, upon receipt of such a warning message from one of the user computers 15, the warning creation program 34 is run, and the steps performed by this program are shown in Figure 4.

[0037] Firstly, at step 4.1 the server receives a warning message from one of its clients, being one of the user computers 15 (as described above). Then, at step 4.2 the server parses the warning message to retrieve the suspect data, and checks the message to see if it could be a computer virus. Such checking preferably takes the form of determining the data type to see if it could feasibly be a virus. Viruses are frequently executable files, such as .exe or .bat on a PC, or macros such as are found in Microsoft® Word® or Excel®. Such a check can conveniently be performed by looking at any file extension on the data. If such checking does not indicate that the data could be a virus then processing ends, as it is assumed that the user has simply made a mistake. Instead, if the warning message is in fact a true warning and the suspect data could possibly be a virus, then processing proceeds to step 4.3.

[0038] Note here that the checking step of step 4.2 is performed in the preferred embodiment, but in other embodiments may not be performed, and as such is optional. Where step 4.2 is not performed processing proceeds directly from step 4.1 to 4.3.

[0039] At step 4.3 the server reads the suspect data from the payload, and creates a "signature" for the suspect data, to permit the particular piece or set of suspect data to be identified in the future. Such a signature may be conveniently created by running the suspect data through a hash function. Hash functions are well known in the art, and commonly provide a 16 or 20 bit output word unique to any particular piece or set of data input thereto. The key feature of hash functions which may be of use in the present invention, however, is that the same output word is always output from the hash function for the same piece or set of input data. Thus the hash value for a certain piece or set of suspect data will always be the same, no matter where the suspect data has been received from.

[0040] It should be noted that other forms of signature creation other than the use of hash functions may also be of use, the only requirement being that an identifiable unique signature is generated for any particular piece or set of suspect data input into the signature creation function at any time.

[0041] Following the creation of the data signature, at step 4.4 the signature and ID database 36 is accessed to retrieve the first previously stored signature and accompanying signature ID therefrom. The signature and ID database 36 in the server 12 is used to store the generated signature ID's from pieces of suspect data received in previous warning messages. At step 4.4 the first signature and ID in the data base is retrieved the first time the controlling function for step 4.4 is called, and thereafter at succeeding calls the next signature and ID in the database list are successfully retrieved.

[0042] At step 4.5, the threat signature of the received suspect data generated at step 4.3 is compared with the stored signature retrieved from the database at step 4.4. If the threat signature is not the same as the retrieved stored signature then processing proceeds to step 4.11,

Sophos Ex. 1002
Page 83 of 683

wherein a check of the signature and ID database 36 is made to see if all stored signatures have been compared with the new signature. If not then processing proceeds to step 4.4, which retrieves the next signature and ID from the database 36 for evaluation at step 4.5 with the generated data signature for the presently received.

[0043] If at step 4.11 it is determined that all of the stored signatures have been compared with the newly created threat signature then it must be the case that the warning message received from the user computer at step 4.1 is the first warning message from any of the user computers to bring to the server's attention the particular piece or set of suspect data contained in the warning message payload. In this case it is necessary for the server to store information on the suspect data, and this is achieved by storing the suspect data signature created at step 4.3 together with a new unique signature ID within the signature and ID database 76. This storing function is accomplished at step 4.12, and thereafter processing proceeds to step 4.13, wherein a count of warning messages received for the particular piece of suspect data is established, and initiated to a value of one. It will be appreciated that a separate count is maintained for every different piece or set of suspect data received in a warning message, and hence at any one time the server will be maintained in several different counts. Therefore, conveniently the various counts may be maintained in a one dimensional array structure, indexed by the particular suspect data's signature ID. Such storage of the count is shown in step 4.13.

[0044] Following the storage of the data signature, signature ID, and establishment of the message count for the suspect data, then in the case that the suspect data had never been received before processing then ends.

[0045] Returning to a consideration of step 4.5, if it turns out that the particular piece or set of suspect data included in the warning message has been received before in a previous warning message then at some point in the loop formed by steps 4.4, 4.5, and 4.11, the evaluation performed at step 4.5 will return a positive value, in that the threat signature generated at step 4.3 will match a previously stored signature. In this case processing then proceeds to step 4.6, wherein the ID of the stored signature is used at an index into the signature count array, and the particular count for the stored signature is incremented by one to reflect the receipt of an additional warning message relating to the particular piece or set of suspect data to which the signature relates. Following the incrementing of the signature count, processing proceeds to step 4.7.

[0046] Step 4.7 represents the first thresholding evaluation performed to determine whether or not a sufficient number of warnings have been received from the user computers concerning a particular piece or set of data such that action should then be taken against that data. Therefore, at step 4.7 an evaluation is performed to determine whether the signature count for the particular piece or set of suspect data is greater than a "block" threshold value. If so processing proceeds to step 4.10, wherein the server then broadcasts a message to all of the user computers 15 on the network, the message containing the particular data signature ID, and a message condition indicator field which in this case contains data instructing the user computers to block the suspect data if it is received thereat. Blocking of the suspect data is performed by the data filter program 24 provided at each user computer 15, the operation of which is described later.

[0047] It should be noted that at step 4.10 the message from the server to the clients contained only the signature ID and the condition indicator and does not contain the actual signature itself. The reason for this is that it is assumed that prior to any particular piece or set of suspect data becoming blocked a warning message will have been transmitted from the server to the user computers containing the suspect data signature, and hence there is no need to retransmit the signature at step 4.10.

[0048] If the evaluation at step 4.7 returns a negative, processing proceeds to the evaluation at step 4.8 wherein the signature count for the particular piece or set of suspect data is compared against a warning threshold level. It should be noted here that the warning threshold level is set less than the block threshold level such that the evaluation of step 4.8 is always found positive before the evaluation of step 4.7. If the evaluation of step 4.8 returns a negative such that the count is less than the warning threshold then this means that not enough warning messages have been received from user computers concerning the particular piece or set of suspect data such that no action should be taken as yet. In this case processing of the warning creation program 34 then ends.

[0049] In contrast, if the evaluation at step 4.8 is positive, the processing proceeds to step 4.9 wherein the server broadcasts a message over the network to all the user computers 15, the message containing the suspect data's signature as generated at step 4.3, a new data signature ID, being simply an identifier of the signature which can be used as a short hand means of identifying the particular piece or set of suspect data, as well as a "warn" flag in a data condition field of the message. The presence of the warn flag in the data condition field of the message causes the data filter program 24 at the user computer to warn the user whenever the suspect piece of data is received, as will be described later. Following the broadcast of the warning message at step 4.9, processing by the warning creation program 34 ends.

[0050] The output of the warning creation program 34 is therefore a warning message broadcast to all the user computers 15 instructing the user computers to upgrade their threat levels for a particular piece or set of suspect data provided that enough warning messages have been received at the server concerning the particular

Sophos Ex. 1002
Page 84 of 683

suspect data. At each user computer upon receipt of a warning message from the server the warning receipt program 26 is run, and the steps performed thereby are shown in Figure 5.

[0051] With reference to Figure 5, at step 5.1 a warning message containing the information described earlier is received from the server. Following this, at step 5.2 the user computer 15 passes the warning message to determine whether or not the message contains a data signature.

[0052] If the message does not contain a data signature, then this means that a warning message must have been received at some point in the past from the server containing the data signature, and therefore the data signature will be already stored in the ID database 28 at the user computer 15. In this case processing proceeds to step 5.4, wherein the signature ID contained within the received warning message is used to index and retrieve the appropriate signature from the database 28, whereupon processing then proceeds to step 5.6.

[0053] At step 5.6 the data condition indicator which is contained in the warning message received from the receiver is read, and a condition field in the database 28 related to the particular suspect data signature is updated to match the condition indicated in the warning message from the server. In this case, as a warning message will have already been received concerning the particular suspect data and hence a "warn" condition already set, it is likely that the condition is being updated to a "block" condition. Following step 5.6 the processing by the warning receipt program ends.

[0054] If at step 5.2 it is determined that the warning message from the server does contain a data signature, then this will be the first warning message received from the server concerning the particular suspect data. In this case, processing proceeds to step 5.3 wherein the received signature is stored in the database 28 indexed by the ID which is also contained in the received message. Furthermore, a condition field in the database related to the signature is also set, at step 5.4. In this case, as this will be the first warning message received from the server about the particular suspect data the condition will be set to a "warn" condition. Following step 5.4 the processing by the warning receipt program 26 ends.

[0055] It has thus been described how users can generate warnings about suspect data which are then transmitted to the server, which then broadcasts warnings to all users if enough user's specific warnings have been received. Users can then record the particular security advice broadcast from the server concerning a piece or set of suspect data, and we now describe how user computers 15 may use the broadcast warnings within the data filter program 24.

[0056] More particular, as mentioned previously each user computer 15 is provided with a data filter program 24 which is arranged to run in the background of the computer all the time the computer is operating in a similar manner to anti-virus and other security programs of the prior art. The data filter program 24 acts to monitor all data received at the user computer 15 upon which it is stored to determine if any of the received data matches the signatures of any suspect data stored in the signature and ID database 28. The steps performed by the data filter program 24 in performing this function are shown in Figure 6.

[0057] At step 6.1 assume that the user computer 15 has received some data in the form of an email message or the like over the network 10. At step 6.2 the data filter program 24 acts to create a signature of the received data using the same signature generation function as is used in the server 12. That is, the signature of the received data may be created using a hash function or indeed any other signature generating function which provides a repeatably generatable unique signature for a given set of input data.

[0058] Following the creation of the data signature, at step 6.3 the signature and ID database 28 at the user computer 15 is accessed and the first signature and signature ID within the database is retrieved therefrom. Upon subsequent calls to the controlling function of step 6.3 the next signature and signature ID in the database list is retrieved successively.

[0059] Following step 6.3 processing proceeds to the evaluation of step 6.4, wherein the data signature created at step 6.2 is compared with the retrieved signature from the database 28. If these signatures do not match then processing proceeds to the evaluation of step 6.10, wherein the database is again accessed to see if all signatures have been accessed and compared. If at step 6.10 it turns out that all of the signatures stored in the database have been compared against the signature of the received data and no match has been found, then it can be concluded that the received data is not suspect data, and hence the data filter program ends. In such a case the user is then free to use the received data in whatever manner she chooses.

[0060] In contrast, if at step 6.10 it is determined that not all of the stored signatures have been compared against the received data signature, processing returns to step 6.3 wherein the next stored signature and ID in the database are retrieved, and the evaluation of 6.4 is performed once again.

[0061] If at step 6.4 it is determined that the received data signature is the equivalent of a previously stored signature then processing proceeds to step 6.5. Here, the database is again accessed to retrieve the signature condition associated with the stored signature to determine what security condition was attached to the signature by the server in the last warning message received from the server concerning the particular signature. Following step 6.5 the retrieved condition is checked at step 6.6 to see if it is a "warn" condition, and if so processing proceeds to step 6.7, wherein a warning is displayed on the user computer's screen to warn the user about the received data. Following the display of the warning the particular process performed by the data filter program

Sophos Ex. 1002
Page 85 of 683

24 ends, although it should be noted that the data filter program will continue to run continuously in the background to check whenever data is received.

[0062] If the retrieved signatory condition is not a "warn" condition then processing proceeds to the evaluation of step 6.8 wherein the condition is checked to see if it is a "block" condition. If so then at step 6.9 the data filtering program 24 acts to block the receipt of the suspect data either by preventing the computer from downloading it from the server or from merely deleting it from the user computer's local storage, and again the user is preferably informed of this action. Following this action the processing performed by the data filter program 24 ends, although again the program will continue to run in the background to detect the receipt of new data.

[0063] If the evaluation of step 6.8 does not indicate that the retrieved signature is a "block condition", then the data filter program 24 processing ends, and the program returns to running in the background, as described previously.

[0064] The first embodiment of the invention therefore presents a computer security system whereby computer viruses and the like can be detected by individual users, who transmit warnings to a server which then broadcasts warnings as appropriate to all users if the number of individual warnings received from individual users exceeds certain thresholds. The use of thresholding in the server instils in the invention a degree of order, in that it is only once a particular threshold level of warnings have been received that action is taken by the server and user computers against the suspect data. This prevents, for example, inexperienced users who may mistake acceptable data for suspect data from initiating a security alert on the acceptable data which may prevent other users from receiving that data, for example.

[0065] Furthermore, the threshold levels for both the "warn" and "block" conditions may of course be set at any level required, and may even be simply one. The assumption is made, however, that in order for the embodiment to operate in a meaningful manner the warn threshold is less than or equal to the block threshold.

[0066] Within the preferred embodiment we have described the data filter program 24 as being located at each of the user computers 15 and running thereat. However, in a slight variation of the first embodiment it would of course be possible for the data filter program 24 to also run at the server to screen messages and data routed therethrough. In this case the operation of the data filter program would be exactly the same as previously described with respect to Figure 6, however it would mean that the user computers 15 would neither need the data filter program 24, the warning receipt program 26, or the signature and ID database 28, as all blocking operations could be performed centrally. However, in the case that it is desirable for users to be warned about data to be received, then it will still be necessary to have the data filter program 24, warning receipt program 26, and signature and ID database 28 at the user computer 15 as described previously in order to allow such warnings.

[0067] In another variation of the first embodiment, in another embodiment a step equivalent to step 4.2 can be performed at the user computers before a warning message is generated. Here, after a user has identified a piece of data as suspect and instructed her computer to send a warning message to the server, prior to compiling and sending the message the warning creation program 34 controls the computer to check if the data identified as suspect by the user could possibly be a virus. Such checking is substantially identical to the check performed at step 4.2, i.e. takes the form of determining the data type to see if it could feasibly be a virus. Viruses are frequently executable files, such as .exe or .bat on a PC, or macros such as are found in Microsoft® Word® or Excel®. Such a check can conveniently be performed by looking at any file extension on the data. If such checking does not indicate that the data could be a virus then no warning message is sent, as it is assumed that the user has simply made a mistake. Instead, if the data is of a data type which could be a virus (e.g. an executable or the like) then the warning message is transmitted.

[0068] The primary advantage of the first embodiment which makes use of the server to keep track of the number of warning messages received about a particular piece of suspect data is that the network traffic overhead introduced by the security system is minimised, as users need only send warning messages to the server, which can then broadcast warning condition messages as appropriate.

[0069] A second embodiment of the invention will now be described with reference to Figures 7 to 10.

[0070] The second embodiment of the invention presents a pure "peer to peer" system which does without the server 12 of the first embodiment. Instead, within the second embodiment each user computer 15 itself individually keeps count of the number of warning messages received from its peers concerning suspect data, and in turn when a user computer detects suspect data it generates and broadcasts a warning message to all of its peers. This arrangement has the advantage that it is not dependent upon a central server for operation, and is therefore much more robust and immune to the loss of one or more of its elements than the client-server architecture of the first embodiment.

[0071] Figure 7 illustrates the software elements present at a user computer 15 in the second embodiment of the invention. More particularly, as in the first embodiment the user computer 15 is provided with a computer readable storage medium 22 on which is stored a data filter program 24, a warning creation program 72, a warning receipt program 74, and a signature and ID database 76.

[0072] Within the second embodiment the data filter program 24 and the warning creation program 72 both

Sophos Ex. 1002
Page 86 of 683

continuously run in the background on the users computer at all times. The data filter program 24 operates in exactly the same manner as previously described in the first embodiment with respect to Figure 6, that is it acts to check the signature of received data against signatures of suspect data stored in the signature database 76, and takes action against any received suspect data as necessary. In this respect, the operation of the second embodiment is exactly the same as that of the first embodiment. The difference between the second embodiment and the first embodiment lies, however, in the fact that each user computer 15 directly broadcasts warnings to each of its peer computers (i.e. the other user computers 15), and in addition each user computer 15 also keeps its own track of the count of warning messages received against each piece of suspect data. These functions are performed by the warning creation program 72 and the warning receipt program 74, as described next.

[0073] The operation of the warning creation program 72 is shown in Figure 8. Here, at step 8.1 data is received at the user computer 15 over the network 10. At step 8.2 an evaluation is performed to determine whether the received data is a security threat or not. As with the first embodiment, this evaluation is preferably performed by the actual human user of the computer 15 who employs her expertise to determine whether or not the received data is a computer virus or the like. In alternative embodiments, however, it may be that this evaluation could be performed by a software agent installed on the users computer, the software agent acting to monitor the functions of the computer to determine if it is under attack from a computer virus. Within the first and second embodiments, however, we prefer the use of a human operator to perform the evaluation.

[0074] If the evaluation at step 8.2 concludes that the received data is not a threat then the processing performed by the warning creation program on the received data ends and the program returns to running in the background until further data is received in the future.

[0075] If it is determined at step 8.2 that the received data is a threat, then at step 8.3 a data signature for the received data is created. As in the first embodiment, the signature generation function may be a hash function or the like or any other suitable signature generation function which is capable of repeatably generating the same signature for a given set of input data. Furthermore, it should be noted here that each user computer 15 must use the same signature generation function, such that when the same set or piece of suspect data arrives at any of the user computers, each of them creates the same signature therefor.

[0076] At step 8.4 a check is made to see whether the generated data signature has already been stored in the signature and ID database 76, and if not then at step 8.8 the signature is stored in the database, and is allocated a globally unique ID. The ID for the signature is generated by the user computer, preferably from a list of ID's which have been specifically allocated to that user computer for allocation to signatures thereby.

[0077] Following step 8.8, at step 8.9 a message count is instantiated for the particular signature generated by the received data, and is set to the value one. As in the first embodiment, the various count values for each piece of suspect data may be stored in a one dimensional array indexed by signature ID.

[0078] Following step 8.9 at step 8.10 the warning creation program causes the user computer to broadcast the data signature and the signature ID to all of its peers as a warning message. As in the first embodiment, the warning message preferably takes a known format, with the signature and signature ID as particular fields within the warning message. Following the broadcast of the warning message, at step 8.10 processing of the warning creation program ends, and it returns to run in the background.

[0079] Returning to the evaluation at step 8.4, if it is determined that the data signature for the received data has already been stored (i.e. the data has already been identified as suspect by either the present user, or one of the other users who have then broadcast a warning message which has been received at each user computer) then processing proceeds to step 8.5, wherein the message count maintained for the particular signature is incremented to reflect the fact that the data has in fact been identified once again as a threat.

[0080] Next, at step 8.6 the signature ID is broadcast to every other user in the system as part of a warning message, and then following that at step 8.7 the appropriate warning or block conditions are set for the signature based on the warning and block threshold values. The specific operations required by step 8.7 are shown in more detail in Figure 10.

[0081] With reference to Figure 10, the steps required for setting the warning or block conditions for a particular data signature are as follows. At step 10.1 the message count for the particular data signature is retrieved, by indexing into the counter array using the signature ID. Then, at step 10.2 the retrieved message count is compared against the block threshold, and if larger than the threshold at step 10.3 the security condition for the data signature is set to "block". As in the first embodiment, this security condition is stored in the signature and ID database 76, and is used by the data filter program 24 to filter received data.

[0082] If the warning message count for the particular data signature is not greater than the block threshold then the message count is compared against the warning threshold. If it is not greater than the warning threshold then no warning or block condition is set for the particular data signature. In contrast, if it is greater than the warning threshold then the security condition for the particular data signature is set to "warn", which is again used by the filter data program 24 as described before in respect of the first embodiment.

[0083] Returning to Figure 8, once the warning or

Sophos Ex. 1002
Page 87 of 683

block conditions have been set for the data signature, the specific processing performed by the warning creation program 72 ends, and it returns to running in the background until further data is received.

[0084] Turning now to the operation of the warning receipt program 74, this program operates whenever a warning message generated by a warning creation program stored on another user's computer is received. The operation of the warning receipt program 74 is shown in Figure 9.

[0085] At step 9.1, a warning message is received from one of the other user computers. The warning message is of course in a predetermined format which identifies it as such. Then, at step 9.2 the warning receipt program 74 acts to parse the message to see if it contains a data signature relating to suspect data. Recall here that the data will have been determined as suspect by the user of the user computer from which the message was received. If it is determined that the message does not contain a signature, then this means that the data will have already been determined as suspect previously, and hence should already be stored in the user computer's signature and ID database 76. Therefore, at step 9.3 the warning receipt program acts to retrieve the message count for the particular suspect data to which the warning message relates, using the signature ID which will have been included in the warning message (recall here that at step 8.6 in the warning creation program where the suspect data has already been identified as such a warning message is still sent out including the suspect data signature ID). Then, at step 9.4 the retrieved message count for the suspect data is incremented to reflect the additional warning, and at step 9.5 the warning or block conditions for the data signature are also set, following the procedure of Figure 10, as described previously.

[0086] If it is determined at step 9.2 that the message does contain a signature, then processing proceeds to the evaluation of step 9.6 wherein it is determined whether or not the received signature has already been stored. If not processing proceeds to step 9.7 wherein the signature is stored in the signature and ID database 76 indexed by the signature ID included in the received warning message. At step 9.8 a message count is instantiated for the newly stored data signature, and is set to one. As described previously, the count values for each particular signature can be stored in a one dimensional array, indexed by each signature ID.

[0087] Following step 9.8 processing proceeds to step 9.5, wherein the warning or block conditions are set for the particular signature, using the procedure of Figure 10.

[0088] Returning to step 9.6, if it is determined that the signature received in the warning message has already been stored then processing proceeds to step 9.9, wherein the received signature ID is stored for use as another key to the signature. In such a case a count value should be instantiated related to the received signature ID, with its value set to the same value as the count indexed by the ID of the already stored signature which matches the received signature. Then, at step 9.10 both of the count values stored for each ID (the received ID, and the ID of the previously stored ID which matches the received signature) are incremented to reflect the receipt of the additional warning. Finally, following the increment of the message counts for the signature the warning and block conditions are set for the signature once more, using the procedure of Figure 10.

[0089] Therefore, as described the second embodiment provides a pure peer to peer system which incorporates the distributed warning capabilities of the security system of the present invention with the ability to threshold the warnings so as to be able to provide a graded reaction locally at each user computer. The provision of such a peer-to-peer operation provides for a more robust system, but as mentioned earlier might have detrimental network overheads due to the need to broadcast every warning message to every user.

[0090] As a modification to the operation of the second embodiment, an additional checking step analogous to step 4.2 of the first embodiment may be performed between steps 8.2 and 8.3 of Figure 8 depicting the operation of the warning creation program 72. Here, after the human user has identified data as suspect at step 8.2, an additional check is made to see if the data could possibly be a computer virus. Such checking preferably takes the form of determining the data type to see if it could feasibly be a virus. Viruses are frequently executable files, such as .exe or .bat on a PC, or macros such as are found in Microsoft® Word® or Excel®. Such a check can conveniently be performed by looking at any file extension on the data. If such checking does not indicate that the data could be a virus then processing ends, as it is assumed that the user has simply made a mistake. Instead, if the warning message is in fact a true warning and the suspect data could possibly be a virus, then processing proceeds to step 8.3, and onwards as previously described. The operation of the other programs in the second embodiment remains unchanged.

[0091] It should be noted here that as the second embodiment does not require a server to act centrally, but rather is a true peer-to-peer system, it is particularly suitable for implementation on networks such as ETHERNET and the like.

[0092] Various further modifications may be made to either of the first or second embodiments to produce further embodiments, as described next.

[0093] In further embodiments it is possible to add more sophistication to increase the power of the system. For example, users could be given the ability to respond to a warning to inform the server of whether they agree with the assessment or not - this would give the potential of reducing the count number if appropriate. The decision as to whether a particular program was a threat or not would then be a collective decision from the whole community.

Sophos Ex. 1002
Page 88 of 683

[0094] Furthermore it is also possible to build in trust models for each user such that some users have greater influence than others. Such trust models could be predefined according to the users position within the community/organisation, such that a warning received from a user with a high trust rating increments the signature count for a particular piece or set of suspect data more than another user with a lower trust rating. Each trust model may then also be adaptively varied by judging the accuracy of a prediction that a user has made against a final collective decision, and any further warnings registered by that user could be weighted according to the trust in that users demonstrated decision-making ability.

[0095] In other embodiments a community of organisations could be formed that would extend the collaboration beyond the limits of a single organisation through sharing of knowledge. Any discoveries in one organisation could be passed on to all other organisations in the community and vice versa. This would greatly extend the power of the system and in many cases allow rapid response to intrusions experienced in other organisations without any internal hits being experienced to the remaining organisations using the system.

[0096] Moreover, in another embodiment the actual number of warnings received concerning a particular piece or set of suspect data could be displayed to the user if the suspect data is received at the user's computer, and the user could then decide what action to take himself. Such a scheme is akin to the "warn" action of the primary embodiments, but provides the user with the additional information of how many other users have determined the data to be threat, thus providing the user with an assessment analogous to a community "confidence-level" in the data, such a level being of greater resolution than the simple "warn" or "block" conditions. Furthermore, such a scheme would not require the system to actually perform automatic blocking of suspect data, as this could be left to the user to do himself. This mode of operation provides the additional potential advantage that a highly skilled or confident user may not wish to act on the community warning if he is sure that it may be wrong, thus increasing the flexibility of the system.

[0097] Furthermore, in another embodiment based on the peer-to-peer architecture of the second embodiment, rather than broadcast to all peers e.g. all users in BT - sub-communities of peers are formed so that the initial broadcasting of warning messages concerning a particular is limited to a smaller number of peers. An example of such an architecture is shown in Figure 11, whence it will be seen that a plurality of sub-communities 111, 112, 113, and 114 may be provided, each connected to each other. Only when the count passes the warning threshold in one of the sub-communities is the suspect data signature distributed further. This limits the overheads incurred by false positives in that any particular sub-community would need to agree that a particular piece or set of data was a threat before it was broadcast to the wider community. "Crossover points" are provided between the sub-communities so that inter-group (or alternatively "inter-community") warnings may be passed on to other sub-communities by the provision of one of the peers 115 in a particular sub-community acting as the bridge via a communications link to another peer in a neighbouring sub-community, and only communicating with that other peer when the warning (or block) threshold has been passed in its own parent sub-community i.e. the sub-community has decided that the particular piece or set of suspect data really could be a threat.

[0098] The processing steps involved in such an embodiment are almost identical to those required in the second embodiment, with the addition that the processing steps depicted in Figure 10 are altered to include an additional step after step 10.3 or 10.5 wherein once the filter condition has changed (as a consequence of either step 10.3 or 10.5) if the computer is a bridging peer to another sub-community then an inter-group warning message is sent to the connected sub-community informing the other peer that a change in the filter condition has occurred for a particular piece or set of suspect data. Such an inter-group warning message should preferably include at least the data signature, as well as a warning condition indicator to communicate the threat level (e.g. warn or block) decided by the sending sub-community. By sending such a warning message to other sub-communities, the bridging peer is effectively declaring to the other sub-communities to which it is connected that its peers in its own sub-community have found the suspect data identified in the warning message to be a security threat.

[0099] Conversely, when an inter-group warning message is received at a bridging peer from another sub-community, the bridging peer should broadcast the inter-group warning message onwards to all its own peers as an intra-group message, to inform them of the threat assessment made by the neighbouring community. Each peer can then store the suspect data signature in its signature and ID database 76, for future reference by the data filter program 24 as needed (and in the same manner as already described in relation to the second embodiment).

[0100] Whether or not a user computer in a sub-community uses a forwarded inter-group warning message directly to initiate action (such as "warn" or "block" for the indicated suspect data) is optional, as it could be that it may wish to wait until it's own community has also agreed on action in respect of the same suspect data before actually initiating a "warn" or "block" condition for the data. Conversely, where a particular user-computer's own sub-community has already come to agreement on a particular piece or set of suspect data (i.e. either the "warn" or "block" threshold has been passed), then it may be that the user-computer may wish to wait until one or more connected sub-communities have also made the same finding before setting the appropriate

Sophos Ex. 1002
Page 89 of 683

condition in its database for the data. It will be apparent that there are a multitude of possibilities as to when any particular user computer may wish to actually set an action condition for a particular piece or set of suspect data. For example, an action condition may be set for a particular piece or set of suspect data only if a user computer's own sub-community has agreed on the action in addition to a threshold number of other sub-communities, or alternatively if merely a threshold number out of the total number of sub-communities has agreed on the action regardless of the particular user computer's own sub-community's finding. Other such alternatives representing possible combinations of the logical conditions required in order to set an action condition will be apparent to the intended reader.

[0101] It is clear that such an architecture of sub-communities is analogous to a plurality of inter-connected local area networks, although it is not essential that each peer in a particular sub-community need actually be located in the same actual LAN (although this may be preferable). This is because all that defines any particular sub-community is the common cause that upon detecting suspect data a user broadcasts a message to all of its peers in the same sub-community, and hence all that is required is some message transport mechanism between peers. Such a message transport mechanism may be a single LAN to which all the peers are connected, or may be a sequence of interconnected networks such as the Internet, with different peers in a sub-community actually being part of different networks.

[0102] The modification to the second embodiment to split the user computers into sub-communities provides the additional advantage over the basic second embodiment that it, at least partially, overcomes the primary disadvantage of the high signalling bandwidth which would be required for the transmission of the warning messages to every other peer, and hence allows for scalability to add more users. As an example, consider the case where a community consists of n peers, such that when a warning message is broadcast from one of them to each of the others $(n-1)$ individual intra-group warning messages are sent. Now, assume that in order to agree on action about a particular piece or set of data a proportion of $1/a$ peers have to agree i.e. the action threshold is n/a. In such a case a total of $n(n-1)/a$ intra-group warning messages have to be transmitted in total for any one particular piece or set of data. Thus, where there are 40 peers, and half of them have to agree before action can be taken, a total of 780 warning messages would have to be transmitted (without error) before the action is agreed upon.

[0103] Now consider that the community of n peers is split equally into x sub-communities, as shown in Figure 11. In this case, within a sub-community for any single warning from one peer a total of $(n/x - 1)$ intra-group warning messages are broadcast. Assuming that in order to agree on action about a particular piece or set of data a proportion of $1/a$ peers have to agree i.e. the action threshold is n/ax, then a total of $n(n-x)/ax^2$ intra-group warning messages have to be broadcast within a single sub-community for action to be agreed on a single piece of suspect data. Assuming that each sub-community has to reach agreement within itself and communicate to each other group that it has so agreed before action can be taken by any peer in any sub-community, there will still only be a total of $n(n-x)/ax$ intra-group warning messages broadcast in total (the sum of the number of warning messages in total broadcast in each sub-community), plus $x(x-1)$ inter-group messages between sub-communities, plus $(n/x - 1)$ further intra-group messages from the bridging peer in each sub-community to each other peer in its respective community informing them of the findings of other sub-communities (i.e. forwarding received inter-group messages onwards). Note that with respect to this latter number of intra-group messages, $(n/x - 1)$ messages are sent from a bridging peer in a sub-community for each inter-group warning message received from another sub-community, such that where full knowledge of every other sub-community's findings about a particular piece or set of suspect data is required to be disseminated throughout a particular sub-community, the total number of intra-group messages transmitted by a single bridging node forwarding on the findings of other sub-communities would be $(x-1)(n/x - 1)$. This leads to the total number of intra-group messages forwarding inter-group messages across the entire community of users of $x(x-1)(n/x-1)$.

[0104] For example, if there are 40 peers split into 2 sub-communities of 20, then in each sub-community 190 messages are sent before action is agreed (i.e. the action threshold is reached) in each sub-community, 2 messages are exchanged between the respective bridging peers of each sub-community, one in each direction, and then the respective bridging peers each send 19 messages to inform their own peers of the finding of the other sub-community, to give a total of 420 messages. This is substantially less than the 780 messages which were required when the peers were not split into sub-communities.

[0105] It should be apparent that the above numeric examples are dependent solely on the logical conditions which were ascribed to the group operation, and in particular in the example above the need for every sub-community to agree on action about a particular piece or set of data and each issue its own inter-group warning message before any action is taken. Where slightly lower thresholds are set for action (e.g. if only half the number of sub-communities are required to agree), then the number of both inter- and intra-group warning messages which would be required to be broadcast before action is agreed would be further reduced.

[0106] In any of the embodiments of the invention described above and in other embodiments not described it should be noted that the one or more "threshold values" against which the respective counts for pieces or sets of suspect data are compared may be any value,

Sophos Ex. 1002
Page 90 of 683

and may be fixed or dynamically adaptive. Furthermore the actual values may be generated by any appropriate function, such as for example by a random number generator, or as a function of some metric of accuracy of users in identifying viruses. Furthermore, it is foreseen that the threshold values may not simply be actual numbers which the respective counts must be greater than, but could instead be probabilistic in nature. Furthermore, various logical functions or rules can be used for their creation, including for example, fuzzy logic. The threshold values may therefore be any values, derived by any function or method, and are not limited to the particular examples of threshold values given in the specific embodiments described herein.

[0107] As described, the present invention therefore provides a collaborative computer security system wherein a distributed decision is taken involving all or substantially all of the users of the system, to effectively allow the users to "vote" on whether or not a particular piece or set of suspect data is a threat. By providing such a distributed system the response time to a computer virus attack can be improved over the prior art case where a central authority is required to perform analysis and take action, thereby reducing the potential damage which may be caused by such an attack.

Claims

1. A computer security system for use in a network environment comprising at least a first group of user computers arranged to communicate over a network, the system comprising a warning message exchange system operable to allow the communication from the user computers of warning messages relating to suspect data identified as a possible security threat; a message counting system operable to maintain a count for every particular piece or set of suspect data based on the number of warning messages communicated relating thereto; and network security means operable to act in respect of any particular piece or set of suspect data for which the count maintained therefor is substantially equal to or greater than at least one threshold value.

2. A computer security system according to claim 1, wherein the judgement as to whether any piece or set of data present at any one or more of the user computers is a possible threat is performed by the respective human user or users of the or each user computer.

3. A computer security system according to any of the preceding claims, wherein the network security means is further operable to compare the maintained count for a particular piece or set of suspect data against a plurality of different thresholds, and to take different action in respect of the data dependent upon which threshold or thresholds are met.

4. A computer security system according to any of the preceding claims, wherein the action taken by the network security means comprises warning each of the users as to the suspect nature of a particular piece or set of data.

5. A computer security system according to any of the preceding claims, wherein the action taken by the network security means comprises preventing the transmission of the particular piece or set of suspect data across the network.

6. A computer security system according to any of the preceding claims, wherein the or each warning message comprises at least an identifier of the piece of or set of suspect data to which it relates.

7. A computer security system according to claim 6, wherein the identifier is the piece or set of suspect data itself.

8. A computer security system according to claim 6, wherein the identifier is a repeatably generatable signature substantially unique to the piece or set of data.

9. A computer security system according to any of the preceding claims, and further comprising a network server arranged to receive the or each warning message communicated from the user computers, and further arranged to host the message counting system and at least part of the network security system, wherein that part of the network security system hosted by the server is operable to determine the action which should be taken against a particular piece or set of suspect data, and to communicate an action condition indicator indicative of the determined action to each of the plurality of users.

10. A computer security system according to any of the preceding claims, wherein a warning message generated by a user computer is broadcast to every other user computer, and each user computer is further arranged to host its own message counting system and network security system operable in accordance with any of the preceding claims.

11. A computer security system according to any of the preceding claims, and further comprising an inter-group communications system operable to allow the communication of warning messages relating to suspect data identified as a possible security threat from the first group of user computers to one or more other groups of other user computers.

Sophos Ex. 1002
Page 91 of 683

12. A computer security system according to claim 11, wherein the inter group warning messages are transmitted by the inter-group communications system if the number of warning messages communicated by the user computers in the first group concerning a particular piece or set of data is substantially equal to or greater than at least one threshold value.

13. A computer security system according to claim 12, wherein the threshold value or values is/are the same as those at which the network security system takes action.

14. A computer security system according to any one of claims 11, 12, or 13, wherein the inter-group communications system is further arranged to receive inter-group warning messages from the one or more other groups of user computers.

15. A computer security system according to claim 14, and further comprising a second message counting system operable to maintain a count for every particular piece or set of suspect data based on the number of inter-group warning messages communicated relating thereto; and wherein the network security means is further operable to act against any particular piece or set of suspect data for which the count maintained therefor by the second message counting system is substantially equal to or greater than at least one inter-group threshold value.

16. A computer security system according to claim 15, wherein the network security means is further arranged to act against a particular piece or set of suspect data only if both the respective counts maintained by the message counting system and the second message counting system are substantially equal to or greater than at least the threshold value and the inter-group threshold value respectively.

17. A computer security system according to any of the preceding claims, wherein the message counting system is further arranged to store one or more weighting coefficients relating to one or more particular user computers, and to increment the count maintained for a particular piece or set of suspect data by an amount based upon the weighting coefficient when a warning is received from the one or more particular user computers relating to the particular piece or set of suspect data.

18. A computer readable storage medium storing one or more computer programs which when run on a computer causes the computer to operate in the manner of a system according to any of the preceding claims.

Sophos Ex. 1002
Page 92 of 683

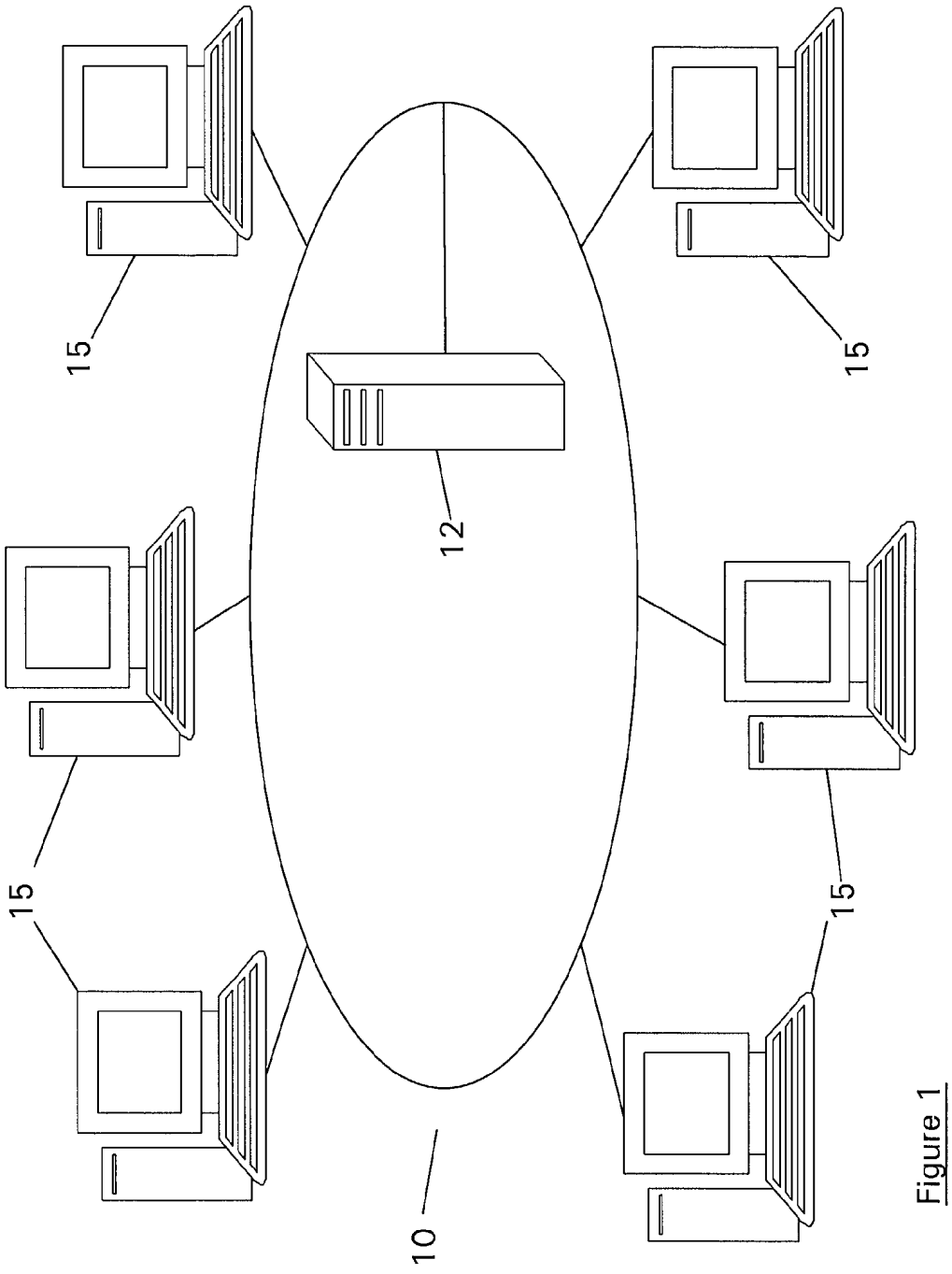


Figure 1

Sophos Ex. 1002
Page 93 of 683

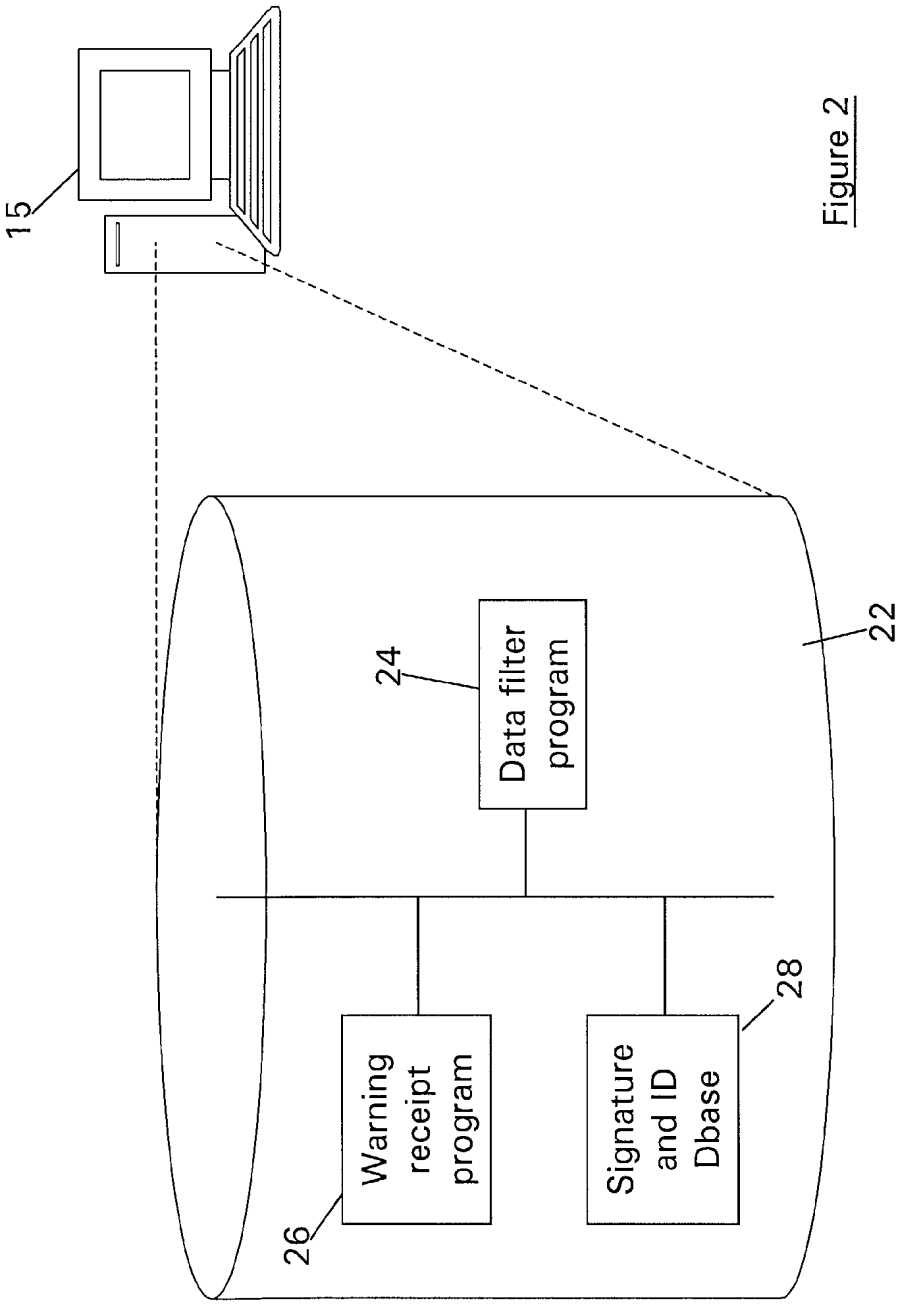


Figure 2

Sophos Ex. 1002
Page 94 of 683

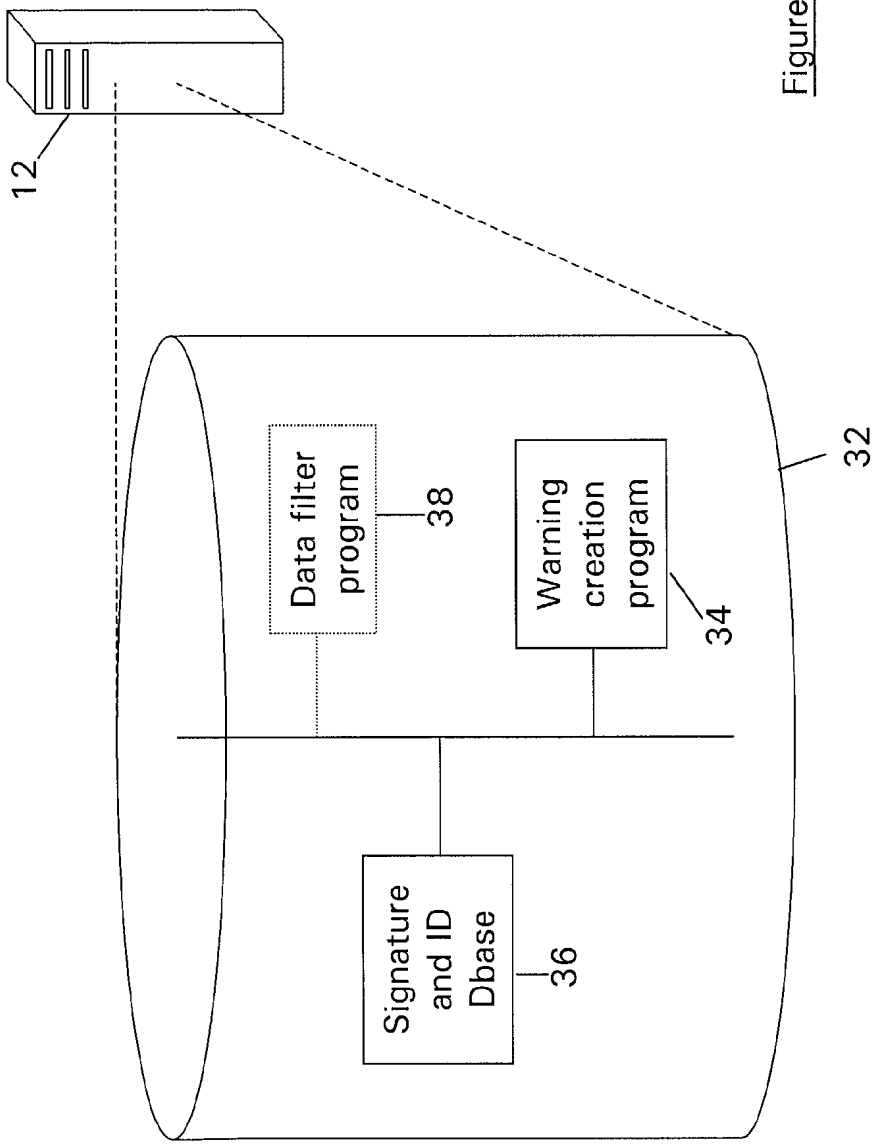


Figure 3

Sophos Ex. 1002
Page 95 of 683

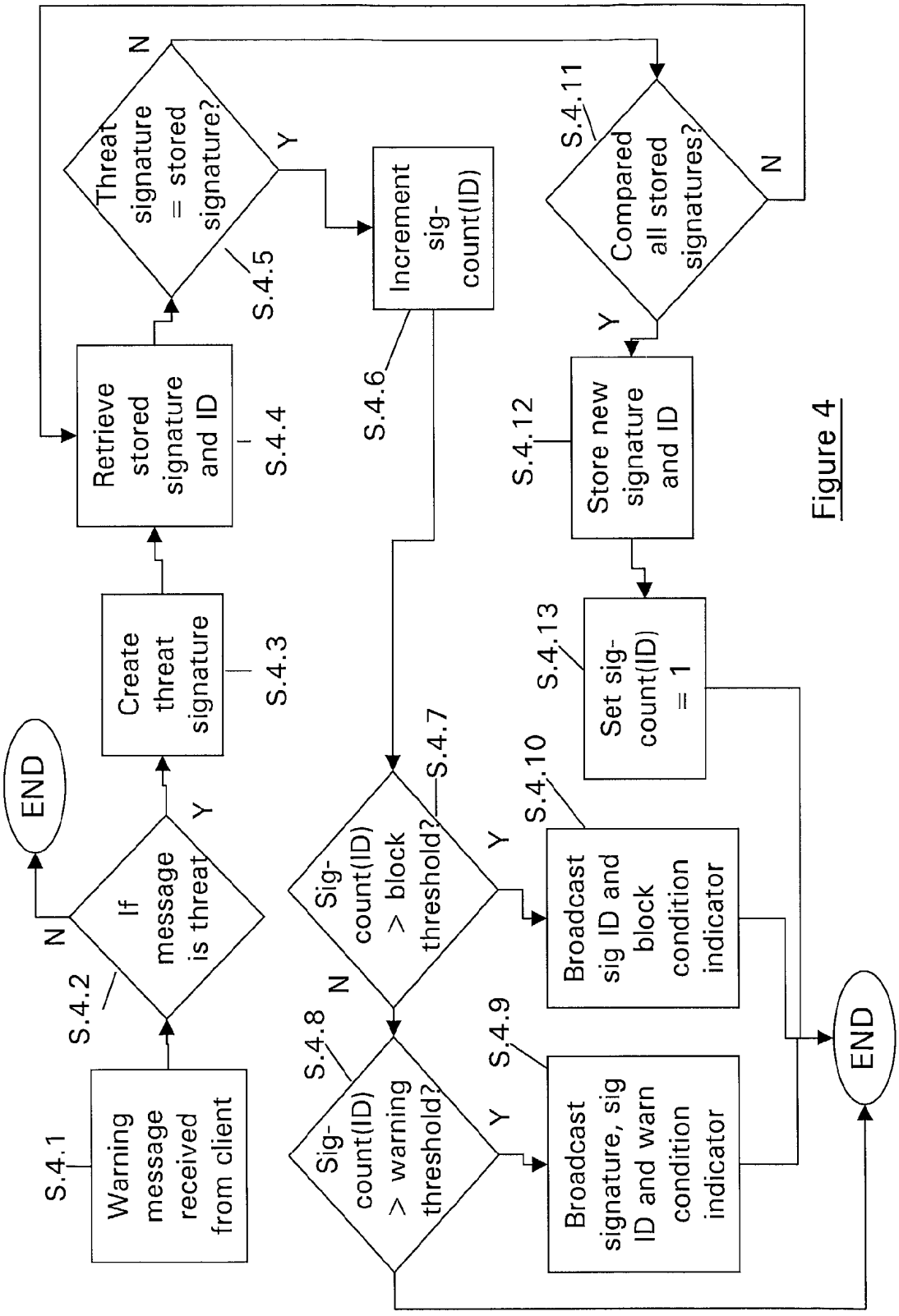


Figure 4

Sophos Ex. 1002
Page 96 of 683

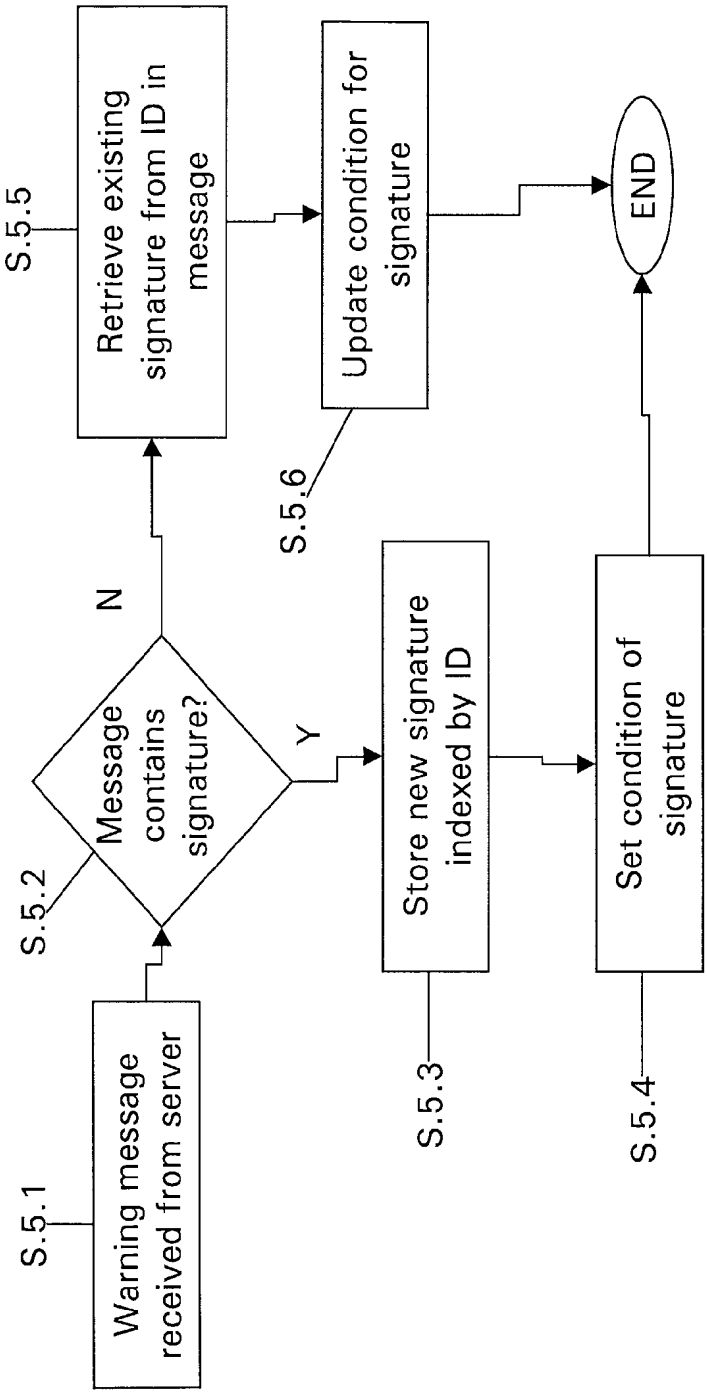


Figure 5

Sophos Ex. 1002
Page 97 of 683

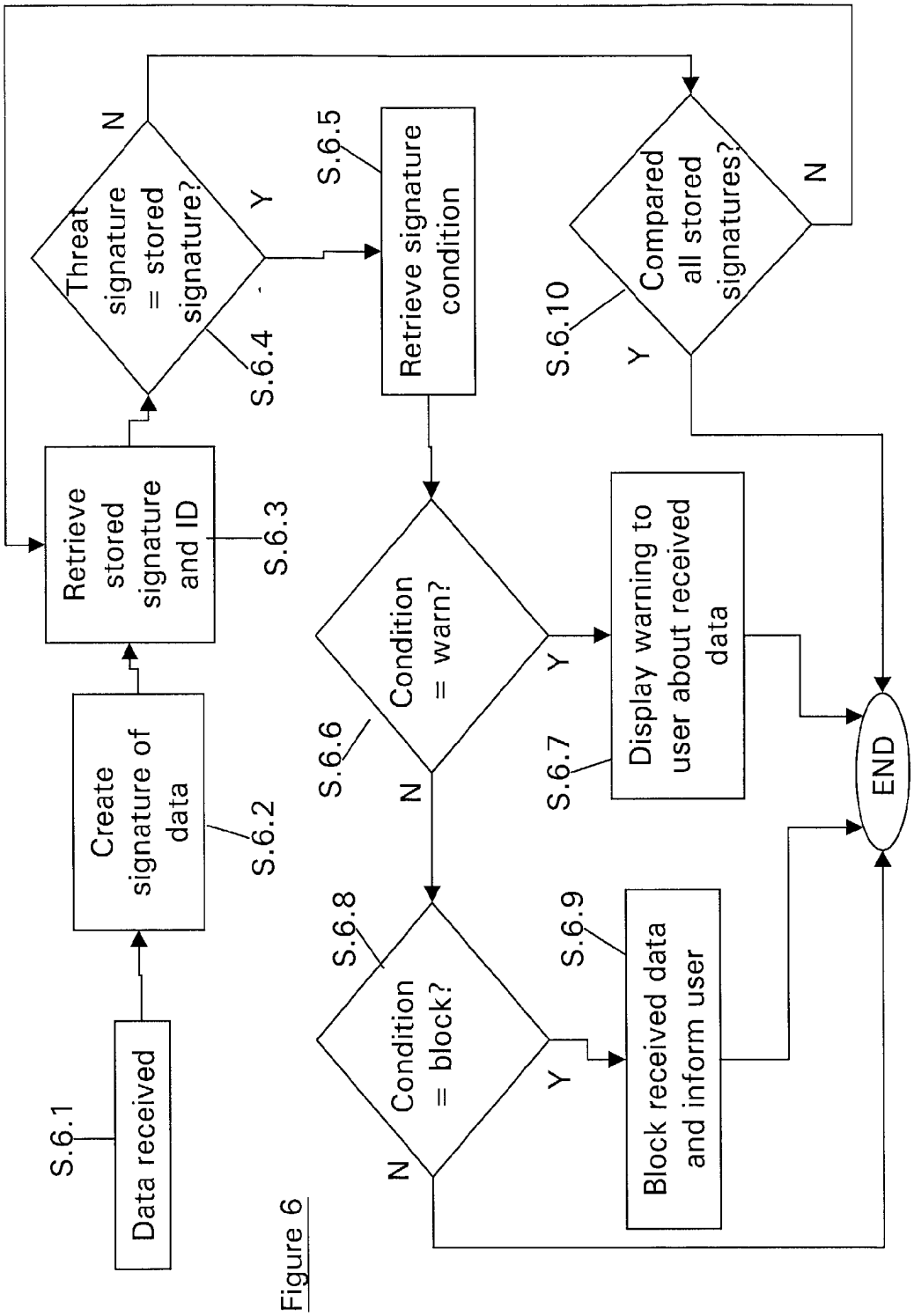


Figure 6

Sophos Ex. 1002
Page 98 of 683

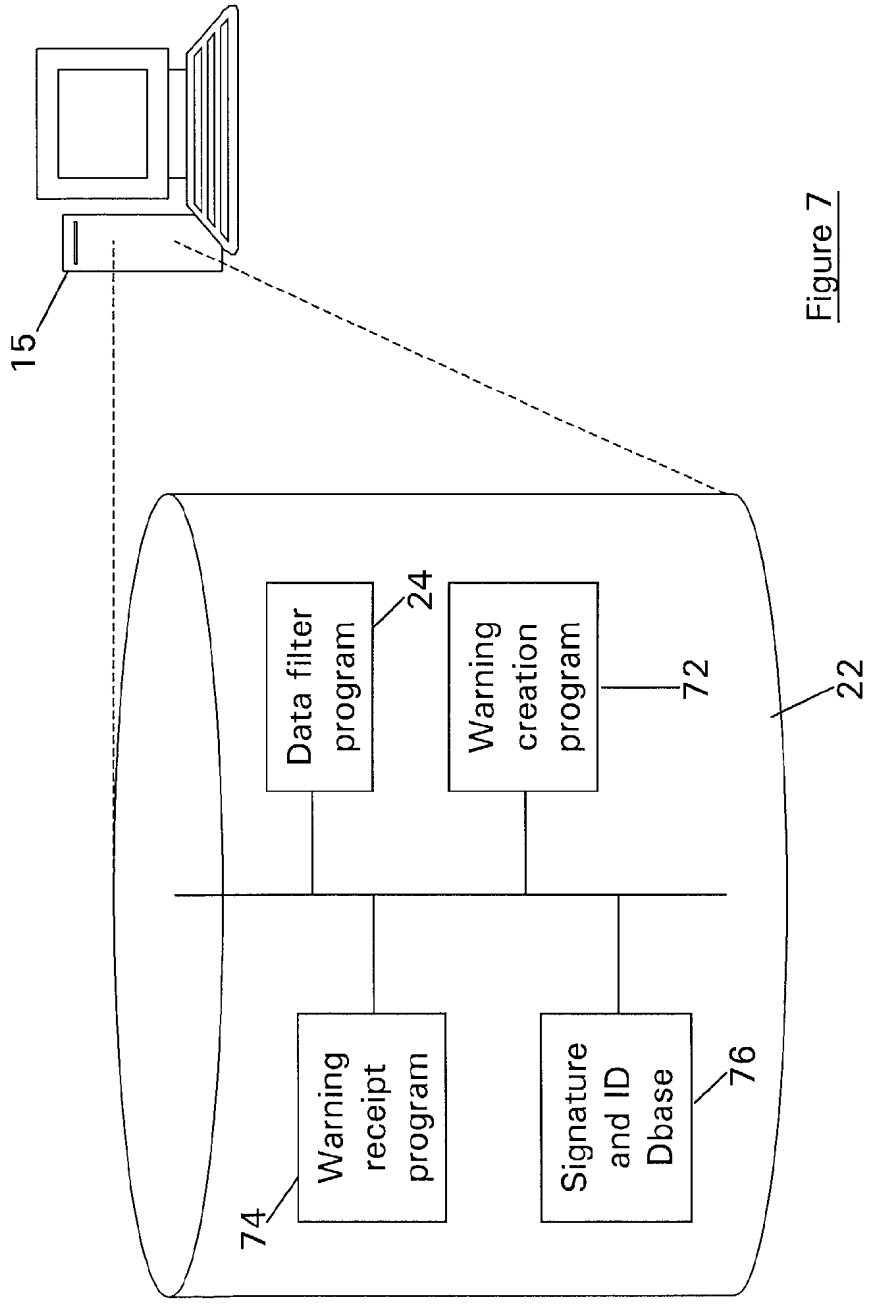


Figure 7

Sophos Ex. 1002
Page 99 of 683

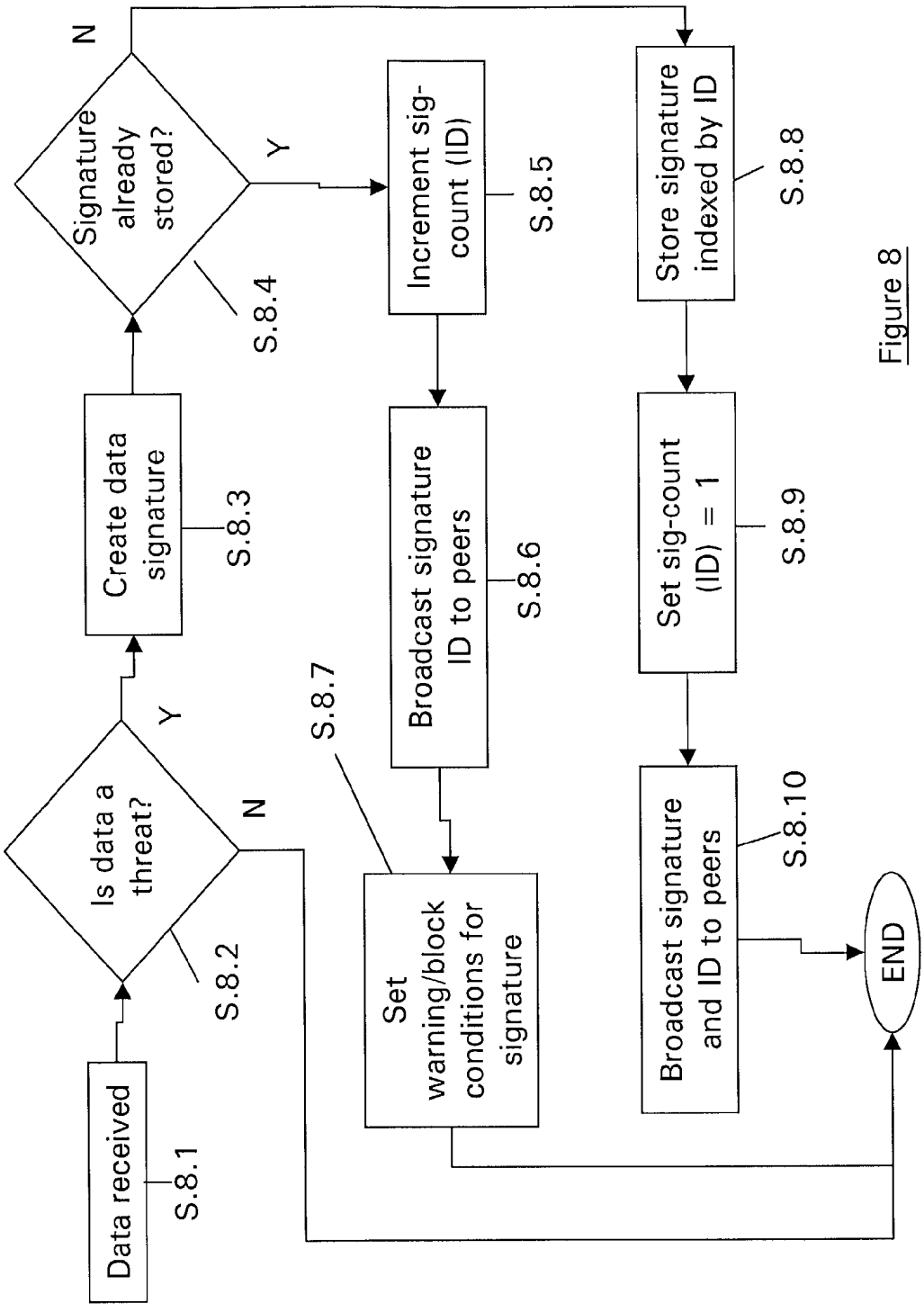


Figure 8

Sophos Ex. 1002
Page 100 of 683

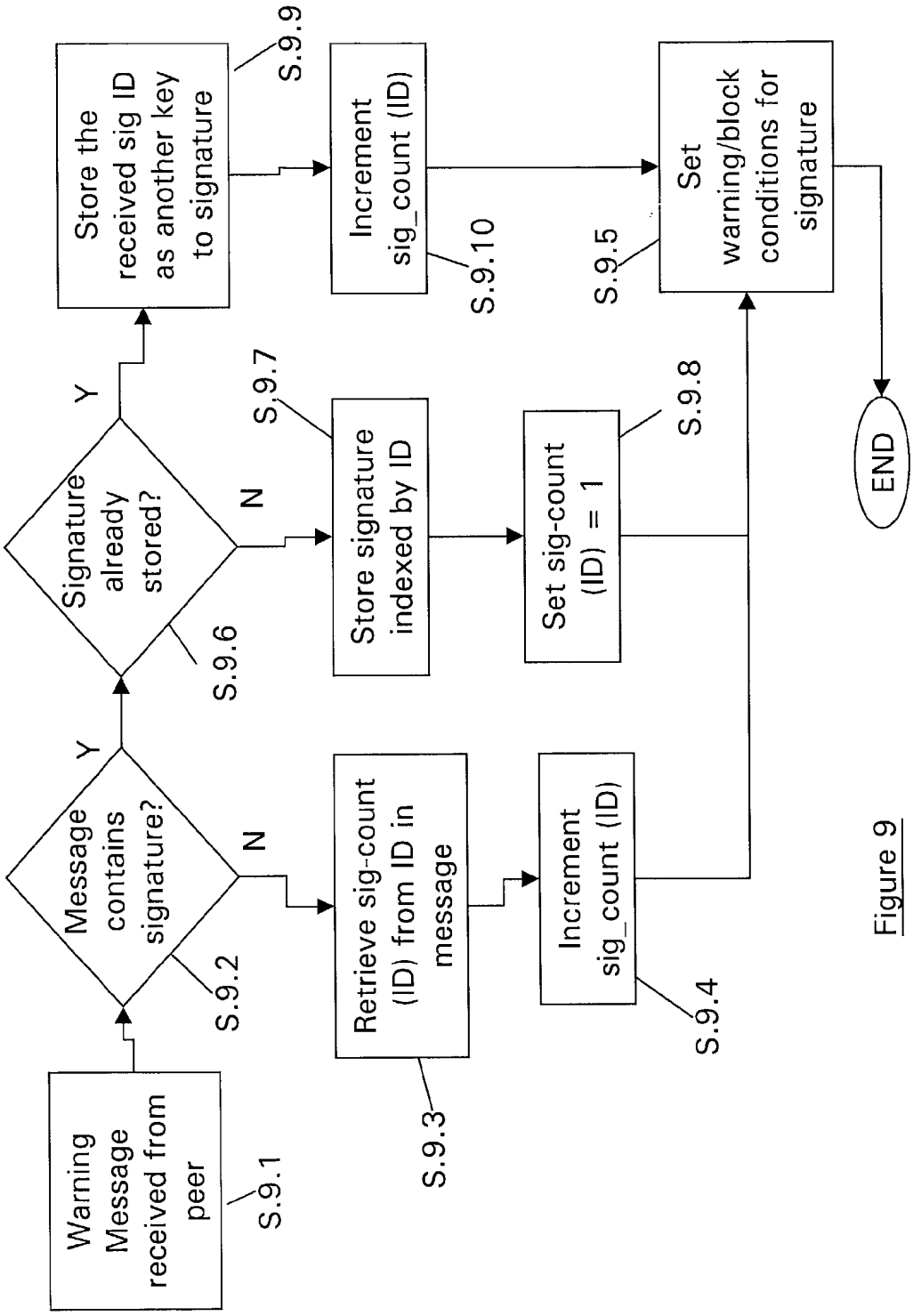


Figure 9

Sophos Ex. 1002
Page 101 of 683

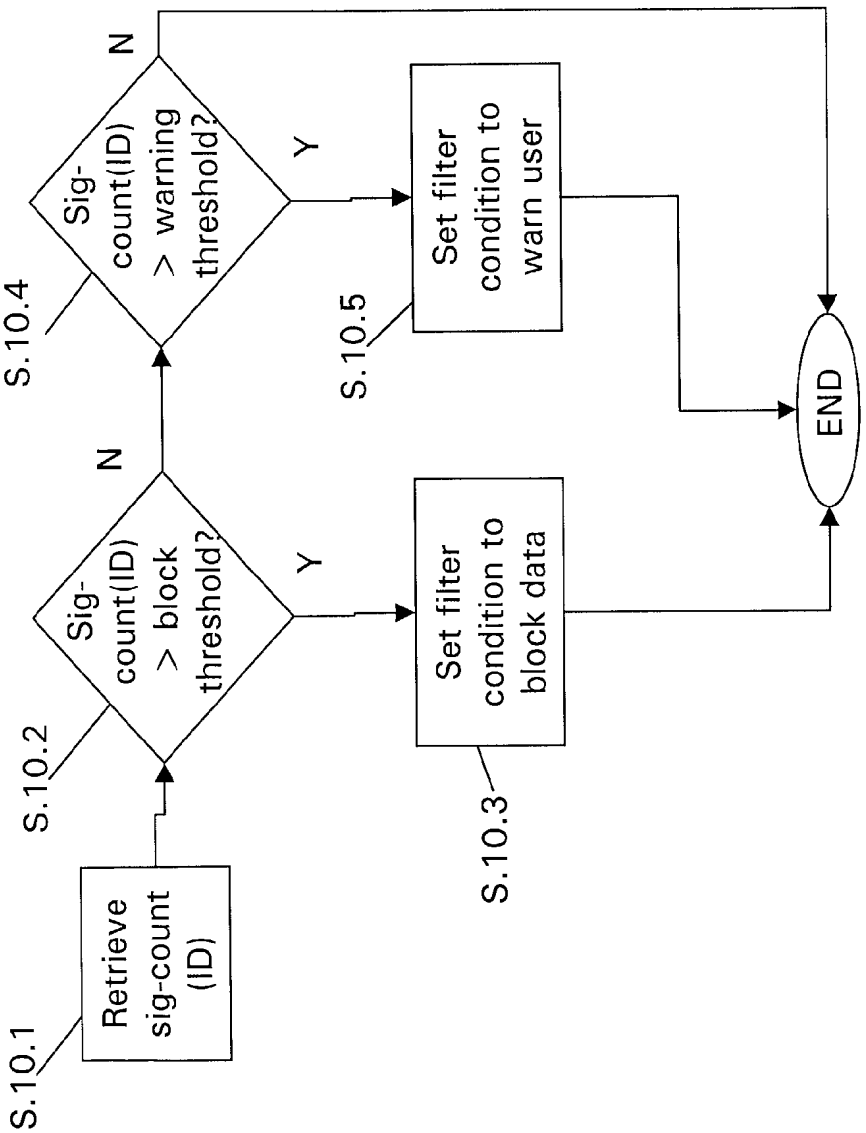


Figure 10

Sophos Ex. 1002
Page 102 of 683

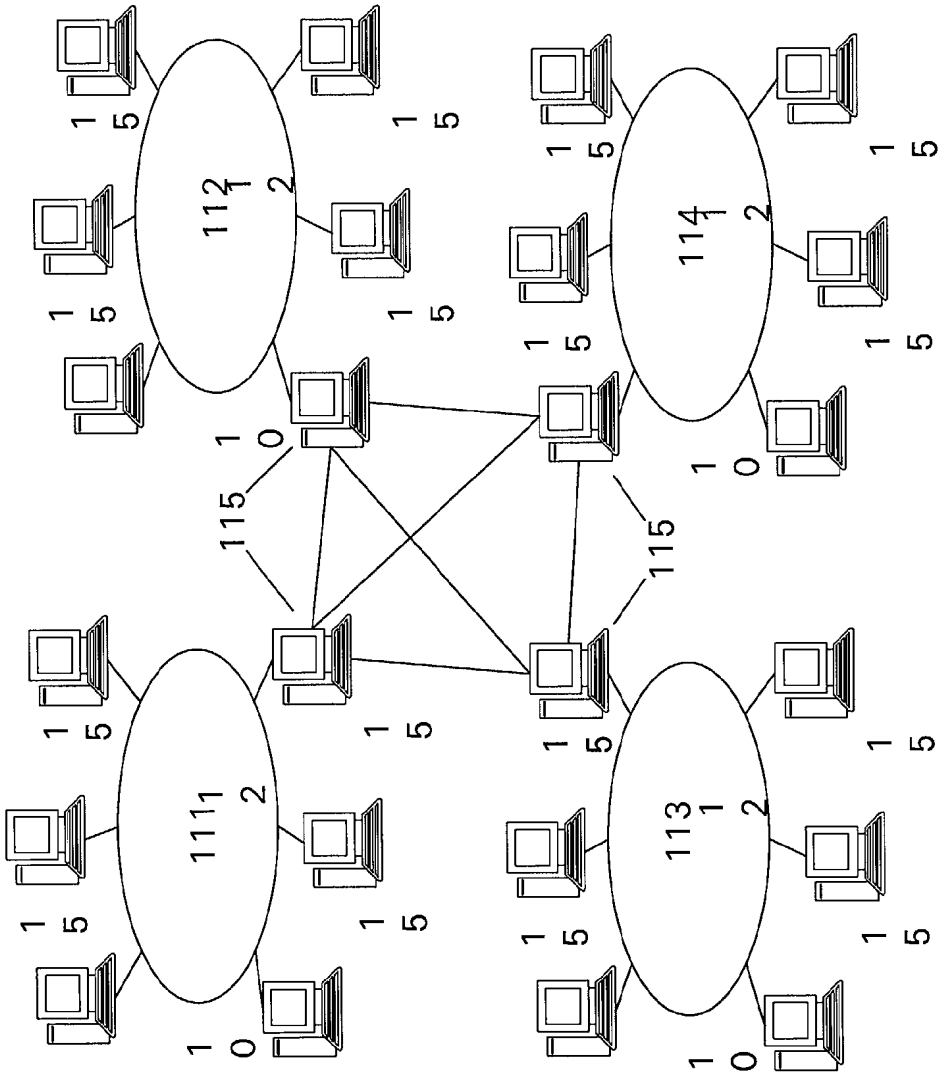


Figure 11

Sophos Ex. 1002
Page 103 of 683

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 30 9795

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	US 5 440 723 A (KEPHART JEFFREY O ET AL) 8 August 1995 (1995-08-08) * abstract; figures 2,3,7,8 * * column 4, line 29 - column 5, last line * * column 19, line 45 - column 20, last line *	1	G06F1/00 H04L29/06
A		2,3,5-8, 10-14	
A	US 5 621 889 A (EMERY THIERRY ET AL) 15 April 1997 (1997-04-15) * abstract; figure 2 * * column 2, line 9 - line 55 * * column 3, line 30 - column 4, line 43 *	1-3,17	
A	WO 01 71499 A (COUNTERPANE INTERNET SECURITY) 27 September 2001 (2001-09-27)		
A	ZENKIN D: "Fighting Against the Invisible Enemy - Methods for detecting an unknown virus" COMPUTERS & SECURITY. INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, NL, vol. 20, no. 4, 31 July 2001 (2001-07-31), pages 316-321, XP004254268 ISSN: 0167-4048		TECHNICAL FIELDS SEARCHED (Int.Cl.7) G06F H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	31 July 2002	Powell, D

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

Sophos Ex. 1002
Page 104 of 683

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 01 30 9795

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

31-07-2002

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5440723 A	08-08-1995	NONE	
US 5621889 A	15-04-1997	FR 2706652 A1	23-12-1994
		CA 2125445 A1	10-12-1994
		DE 69428631 D1	22-11-2001
		EP 0629940 A1	21-12-1994
		ES 2164091 T3	16-02-2002
		NO 942108 A	12-12-1994
WO 0171499 A	27-09-2001	US 2002087882 A1	04-07-2002
		AU 4735101 A	03-10-2001
		WO 0171499 A1	27-09-2001

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

Sophos Ex. 1002
Page 105 of 683

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

RECEIVED
10 MAY 2012

PCT

To:
Bebbington, Nicholas
BECK GREENER
Fulwood House
12 Fulwood Place
London
WC1V 6HR
ROYAUME UNI

INVITATION TO PAY ADDITIONAL FEES AND, WHERE APPLICABLE, PROTEST FEE

(PCT Article 17(3)(a) and Rule 40.1 and 40.2(e))

Date of mailing *(day/month/year)*	4 May 2012 (04-05-2012)
Applicant's or agent's file reference NB2/P17048WO	**PAYMENT DUE** within **ONE MONTH** from the above date of mailing
International application No. PCT/EP2012/052497	International filing date *(day/month/year)* 14 February 2012 (14-02-2012)
Applicant PREVX LIMITED	

1. This International Searching Authority

(i) considers that there are 6 *(number of)* inventions claimed in the international application covered by the claims indicated on an extra sheet:

(ii) therefore considers that **the international application does not comply with the requirements of unity of invention** (Rules 13.1, 13.2 and 13.3) for the reasons indicated on an extra sheet:

(iii) [X] has carried out a partial international search (see Annex) [ ] will establish the international search report on those parts of the international application which relate to the invention first mentioned in claims Nos.:

see extra sheet

(iv) will establish the international search report on the other parts of the international application only if, and to the extent to which, additional fees are paid.

2. Consequently, the applicant is hereby **invited to pay**, within the time limit indicated above, the amount indicated below:

EUR 1.785,00	x	5	=	EUR 8.925,00
Fee per additional invention		number of additional inventions		currency/total amount of additional fees

3. The applicant is informed that, according to Rule 40.2(c), **the payment of any additional fee may be made under protest,** i.e., a reasoned statement to the effect that the international application complies with the requirement of unity of invention or that the amount of the required additional fee is excessive, where applicable, subject to the payment of a protest fee.

Where the applicant pays additional fees under protest, the applicant is hereby invited, within the time limit indicated above, to pay a protest fee (Rule 40.2(e)) in the amount of EUR 830,00 *(currency/amount)*

Where the applicant has not, within the time limit indicated above, paid the required protest fee, the protest will be considered not to have been made and the International Searching Authority will so declare.

4. [ ] Claim(s) Nos. _____ have been found to be unsearchable under Article 17(2)(b) because of defects under Article 17(2)(a) and therefore have not been included with any invention.

Name and mailing address of the International Searching Authority	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040 Fax: (+31-70) 340-3016	SOGNO-PABIS, Elzbieta Tel: +31 (0)70 340-2414

Form PCT/ISA/206 (April 2005)
Registered Mail

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-25, 31-35

   Classifying a computer object as malware
   ---

2. claims: 21, 26-31, 36-40

   Identifying malware based on rules
   ---

3. claims: 41, 42

   Monitoring objects running on a computer
   ---

4. claims: 43-47

   Operating security program on computer
   ---

5. claims: 48-56

   Connecting remote computer to a server
   ---

6. claims: 57-62

   Protecting network against malware

They are not so linked as to form a single general inventive concept (Rule 13.1 PCT) for the following reasons.
The prior art as been identified as US 2007/0016953 A1: "Methods and Apparatus for Dealing with Malware" (D1). Document D1 discloses (references in parentheses applying to this document):
A method of classifying a computer object as malware, the method comprising:
at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored and or processed (paragraph 81);
wherein the base computer [...] receives said data from the plural remote computers and apply rules and or heuristics against that data in real time to determine whether or not said object is malware and to communicate said determination to the remote computers (paragraphs 81-83);
-said base computer [...] is arranged to receive said data about objects from [...] [the remote computers] to maintain a master database of data received about objects from all of the [...] [the remote computers] (paragraphs 81-83).

Claim 1 therefore differs from D1 in that the base computer comprises:

Sophos Ex. 1002
Page 107 of 683

-plural threat servers that receive data about objects from the remote computers, and
-one central server in communication with the threat servers where the master database is maintained

The above differences solve the problem of server availability when faced with high number of requests. D1 hints this problem when in paragraphs 20 and 81 it is stated that there may be millions of remote computers connected to the base computer.
When faced with this problem the person skilled in the art (of server load/availability in a networked environment) would choose from one of the straightforward well known solutions of providing a plurality of servers and include it with the teachings of D1 without the exertion of an inventive step. The functionality at the base computer (in D1)that deals with the reception of the data objects is replaced in a straightforward way with the plurality of threat servers.
Therefore the subject-matter of claim 1 is not inventive (Article 33(3) PCT).

The subject-matter of the first invention is set out in claims 1-8, 9-16 and 17-18, 19-20 and 21-25, 31-35.

An equivalent reasoning (as for claim 1 above) may be used in the analysis of independent claim 9 which is therefore also considered not inventive (Article 33(3) PCT).

Independent claim 17 is not new (Article 33(2) PCT) for the following reasons. Document D1 discloses (references in parenthesis applying to this document):
A method of classifying a computer object as malware, the method comprising:
at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored and or processed;
(paragraph 81)
counting the number of times in a given time period objects having one or more common attributes or behaviours that have been seen by the remote computers;
comparing the counted number with the expected number based on past observations; and,
if the comparison exceeds some predetermined threshold, flagging the objects as unsafe or as suspicious
(paragraph 101).

An equivalent reasoning (as for claim 17 above) may be used in the analysis of independent claim 19 which is therefore also considered not new (Article 33(2) PCT).

Independent claim 21 is not inventive (Article 33(3) PCT) for the following reasons. Document D1 discloses (references in parenthesis applying to this document):
A method of classifying a computer object as malware, the method comprising:
at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored

Sophos Ex. 1002
Page 108 of 683

and or processed (paragraph 81);
storing said data in a database (paragraph 81).

Claim 21 therefore differs from D1 in that:
-the user is presented with a display of information relating to a group of plural objects and various attributes of those objects, the display being arranged such that commonality is shown between objects, wherein the group of objects displayed correspond to a user query of the database.
This feature is a mere presentation of information (e.g. displaying the result of a database with a grouping clause) that the person skilled in the art would implement when instructed to do so in a straightforward manner. This feature does not therefore contribute to an inventive step.

An equivalent reasoning (as for claim 21 above) may be used in the analysis of independent claim 31 which is therefore also considered not inventive (Article 33(3) PCT).

Dependent claims 2-8, 10-16, 18, 20, 22-25 and 32-35 are either also disclosed in D1 or are considered trivial and well known in the prior art (see D1-D2 and the relevant passages cited in the Search Report). Particularly in what refers to dependent claims 2-5, they define well known features of maintaining backup and/or replication servers. Therefore no Special Technical Features (STFs) can be seen to make a contribution over D1 (Rule 13.1 PCT).

The subject-matter of the second invention is set out in claims 21, 26-30 and 31, 36-40.
This differs from D1 by the creation of a rule from a user query if the query identifies malware. These may be considered the Special Technical Features (STFs) of the second invention (Rule 13.1 PCT). These STFs solve the problem of "How to use user knowledge to identify malware".

The subject-matter of the third invention is set out in claims 41, 42.
This differs from D1 in that a security program is operated to impersonate the operating system. These may be considered the Special Technical Features (STFs) of the third invention (Rule 13.1 PCT). These STFs solve the problem of "How to determine whether objects are malware".

The subject-matter of the fourth invention is set out in claims 43-44, 45-47.
This differs from D1 in that a program is loaded per component. These may be considered the Special Technical Features (STFs) of the fourth invention (Rule 13.1 PCT). These STFs solve the problem of "How to execute a program if malware prevents loading".

The subject-matter of the fifth invention is set out in claims 48-51, 52-56.
This differs from D1 in that an agent runs at a remote computer to allocate it to a server. These may be considered the Special Technical Features (STFs) of the fifth invention (Rule 13.1 PCT). These STFs solve the problem of "How to allocate a remote computer to a server".

The subject-matter of the sixth invention is set out in claims 57-59, 60-62.

Sophos Ex. 1002
Page 109 of 683

This differs from D1 in that an agent running at a remote computer configures a firewall according to a base computer. These may be considered the Special Technical Features (STFs) of the sixth invention (Rule 13.1 PCT). These STFs solve the problem of "Protect network communications against malware".

The STFs of the six inventions are clearly not the same. Also because they solve different (and unrelated) problems they are not corresponding as required by Rule 13.2 PCT. The application therefore lacks unity.

Sophos Ex. 1002
Page 110 of 683

Annex to Form PCT/ISA/206
COMMUNICATION RELATING TO THE RESULTS OF THE PARTIAL INTERNATIONAL SEARCH

International Application No
PCT/EP2012/052497

1. The present communication is an Annex to the invitation to pay additional fees (Form PCT/ISA/206). It shows the results of the international search established on the parts of the international application which relate to the invention first mentioned in claims Nos.:
see 'Invitation to pay additional fees'
2. This communication is not the international search report which will be established according to Article 18 and Rule 43.

3. If the applicant does not pay any additional search fees, the information appearing in this communication will be considered as the result of the international search and will be included as such in the international search report.

4. If the applicant pays additional fees, the international search report will contain both the information appearing in this communication and the results of the international search on other parts of the international application for which such fees will have been paid.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007/016953 A1 (MORRIS MELVYN [GB] ET AL) 18 January 2007 (2007-01-18) cited in the application paragraph [0001] - paragraph [0144]	1-25, 31-35
A	EP 1 315 066 A1 (BRITISH TELECOMM [GB]) 28 May 2003 (2003-05-28) the whole document	1-25, 31-35

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Sophos Ex. 1002
Page 111 of 683

Patent Family Annex

Information on patent family members

International Application No
PCT/EP2012/052497

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007016953 A1	18-01-2007	CN 101213555 A	02-07-2008
		CN 102096784 A	15-06-2011
		CN 102176224 A	07-09-2011
		EP 1899884 A2	19-03-2008
		JP 2009500706 A	08-01-2009
		US 2007016953 A1	18-01-2007
		WO 2007003916 A2	11-01-2007
EP 1315066 A1	28-05-2003	CA 2467186 A1	05-06-2003
		EP 1315066 A1	28-05-2003
		EP 1446709 A1	18-08-2004
		US 2005022014 A1	27-01-2005
		WO 03046699 A1	05-06-2003

PTO/SB/01A (01-09)
Approved for use through 09/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	METHODS AND APPARATUS FOR DEALING WITH MALWARE

As the below named inventor(s), I/we declare that:

This declaration is directed to:

☐ The attached application, or

☒ Application No. 13372375, filed on February 13, 2012,

☐ as amended on _____ (if applicable);

I/we believe that I/we am/are the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought;

I/we have reviewed and understand the contents of the above-identified application, including the claims, as amended by any amendment specifically referred to above;

I/we acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me/us to be material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT International filing date of the continuation-in-part application.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

All statements made herein of my/own knowledge are true, all statements made herein on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001, and may jeopardize the validity of the application or any patent issuing thereon.

FULL NAME OF INVENTOR(S)

Inventor one: Melvyn Morris Date: 25th June 2012

Signature: _____ Citizen of: GB

Inventor two: Joseph Jaroch Date: _____

Signature: _____ Citizen of: US

☒ Additional inventors or a legal representative are being named on 1 additional form(s) attached hereto.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/01A (01-09)
Approved for use through 09/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	METHODS AND APPARATUS FOR DEALING WITH MALWARE

As the below named inventor(s), I/we declare that:

This declaration is directed to:

☐ The attached application, or

☒ Application No. 13372375, filed on February 13, 2012,

☐ as amended on _____ (if applicable):

I/we believe that I/we am/are the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought;

I/we have reviewed and understand the contents of the above-identified application, including the claims, as amended by any amendment specifically referred to above;

I/we acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me/us to be material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT International filing date of the continuation-in-part application.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

All statements made herein of my/own knowledge are true, all statements made herein on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001, and may jeopardize the validity of the application or any patent issuing thereon.

FULL NAME OF INVENTOR(S)

Inventor one: Melvyn Morris Date: _____

Signature: _____ Citizen of: GB

Inventor two: Joseph Jaroch Date: 3/2/2012

Signature: [signature] Citizen of: US

☐ Additional inventors or a legal representative are being named on _____ additional form(s) attached hereto.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Patent Application Fee Transmittal

Application Number:	13372375
Filing Date:	13-Feb-2012
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Filer:	Sean Ryan Odowd/Rene Roskam
Attorney Docket Number:	9400.004.02

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Late filing fee for oath or declaration	1051	1	130	130
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 2 months with $0 paid	1252	1	560	560
Miscellaneous:				
			Total in USD ($)	**690**

Electronic Acknowledgement Receipt

EFS ID:	13101298
Application Number:	13372375
International Application Number:	
Confirmation Number:	2918
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Customer Number:	61529
Filer:	Sean Ryan Odowd/Rene Roskam
Filer Authorized By:	Sean Ryan Odowd
Attorney Docket Number:	9400.004.02
Receipt Date:	26-JUN-2012
Filing Date:	13-FEB-2012
Time Stamp:	13:59:27
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$690
RAM confirmation Number	205
Deposit Account	504828
Authorized User	BARRETT,BERNADETTE

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Oath or Declaration filed	9400_004_02US_Declaration_Signed_06252012_.pdf	3830319 096bb794066d8c94aee0e3d0bd889322009062b1	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	32374 63bddff6060a3ca6cbd7fabfb0a8b1e71aa143e2	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	3862693		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronic Acknowledgement Receipt

EFS ID:	13101298
Application Number:	13372375
International Application Number:	
Confirmation Number:	2918
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Customer Number:	61529
Filer:	Sean Ryan Odowd/Rene Roskam
Filer Authorized By:	Sean Ryan Odowd
Attorney Docket Number:	9400.004.02
Receipt Date:	26-JUN-2012
Filing Date:	13-FEB-2012
Time Stamp:	13:59:27
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$690
RAM confirmation Number	205
Deposit Account	504828
Authorized User	BARRETT,BERNADETTE

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Oath or Declaration filed	9400_004_02US_Declaration_Signed_06252012_.pdf	3830319 096bb794066d8c94aee0e3d0bd889322009062b1	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	32374 63bddff6060a3ca6cbd7fabfb0a8b1e71aa143e2	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	3862693		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/372,375	02/13/2012	2431	1870	9400.004.02	24	4

CONFIRMATION NO. 2918

UPDATED FILING RECEIPT

61529
Neugeboren O'Dowd PC
1227 Spruce Street
SUITE 200
BOULDER, CO 80302

OC00000055139187

Date Mailed: 07/03/2012

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Melvyn Morris, Belper, UNITED KINGDOM;
Joseph Jaroch, Elk Grove Village, IL;

Assignment For Published Patent Application

WEBROOT INC., Broomfield, CO

Power of Attorney: None

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/443,095 02/15/2011

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)

If Required, Foreign Filing License Granted: 02/24/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/372,375**

Projected Publication Date: 10/11/2012

Non-Publication Request: No

Early Publication Request: No

Sophos Ex. 1002
Page 121 of 683

Title

METHODS AND APPARATUS FOR DEALING WITH MALWARE

Preliminary Class

726

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/372,375

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	380
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	620
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	250
TOTAL CLAIMS (37 CFR 1.16(i))	24 minus 20 =	* 4			OR	x 60 =	240
INDEPENDENT CLAIMS (37 CFR 1.16(h))	4 minus 3 =	* 1				x 250 =	250
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	1740

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

PTO/AIA/80 (07-12)
Approved for use through 11/30/2014. OMB 0651-0035
U.S. Patent and Trademark Office; U.S DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

I hereby appoint:

■ Practitioners associated with Customer Number: 22442

OR

☐ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number

Name	Registration Number

As attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignments documents attached to this form in accordance with 37 CFR 3.73(c).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(c) to:

■ The address associated with Customer Number: 22442

OR

☐

Firm or Individual Name			
Address			
City		State	Zip
Country			
Telephone		Email	

Assignee Name and Address: WEBROOT INC.
385 Interlocken Crescent, Ste. 800
Broomfield, Colorado 80021

A copy of this form, together with a statement under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent) is required to be Filed in each application in which this form is used. The statement under 37 CFR 3.73(c) may be completed by one of The practitioners appointed in this form, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature	David Huberman	Date	1 OCT 2012
Name	David Huberman, Esq.	Telephone	720-842-3627
Title	General Counsel		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt

EFS ID:	13881366
Application Number:	13372375
International Application Number:	
Confirmation Number:	2918
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Customer Number:	61529
Filer:	Jason Vick/Joanne Vos
Filer Authorized By:	Jason Vick
Attorney Docket Number:	9400.004.02
Receipt Date:	01-OCT-2012
Filing Date:	13-FEB-2012
Time Stamp:	15:44:59
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		Statement_under_373c_w_POA.pdf	97727 978b60ecf19c82887cf6b8a0aa9049db401b8d12	yes	3

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Assignee showing of ownership per 37 CFR 3.73.	1	2
	Power of Attorney	3	3
Warnings:			
Information:			
	Total Files Size (in bytes):	97727	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: WEBROOT, INC.

Application No./Patent No.: 13/372,375 Filed/Issue Date: February 13, 2012

Titled: METHODS AND APPARATUS FOR DEALING WITH MALWARE

WEBROOT, INC., a Corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☑ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 028443, Frame 0609, or for which a copy thereof is attached.

B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: _____ To: _____

   The document was recorded in the United States Patent and Trademark Office at

   Reel _____, Frame _____, or for which a copy thereof is attached.

2. From: _____ To: _____

   The document was recorded in the United States Patent and Trademark Office at

   Reel _____, Frame _____, or for which a copy thereof is attached.

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450**.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☑ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Jason H. Vick/	October 1, 2012
Signature	Date
Jason H. Vick	45,285
Printed or Typed Name	Title or Registration Number

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/372,375	02/13/2012	Melvyn Morris	9400.004.02

CONFIRMATION NO. 2918

POA ACCEPTANCE LETTER

22442
Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

OC000000056939425

Date Mailed: 10/10/2012

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 10/01/2012.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/ttkim/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/372,375	02/13/2012	Melvyn Morris	6890-89-1

CONFIRMATION NO. 2918

22442
Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

PUBLICATION NOTICE

OC000000057014163

Title:METHODS AND APPARATUS FOR DEALING WITH MALWARE

Publication No.US-2012-0260340-A1
Publication Date:10/11/2012

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/372,375	02/13/2012	Melvyn Morris	6890-89-1	2918

22442 7590 04/05/2013

Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

EXAMINER
CHIANG, JASON

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
04/05/2013	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

e-docket@sheridanross.com
srlaw@sheridanross.com

Office Action Summary	Application No. 13/372,375	Applicant(s) MORRIS ET AL.	
	Examiner JASON C. CHIANG	Art Unit 2431	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 1 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 February 2012*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-24* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☐ Claim(s) _____ is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☒ Claim(s) *1-24* are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some * c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Interim copies:

a)☐ All b)☐ Some c)☐ None of the: Interim copies of the priority documents have been received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

1. Restriction to one of the following inventions is required under 35 U.S.C 121:

   I. Claims 1-16, drawn to a method/apparatus of classifying a computer object as malware, classified in class 726, subclass 023.

   II. Claims 17-24, drawn to a method of connecting a remote computer to one of a plurality of servers, classified in class 370, subclass 254.

2. The inventions are independent or distinct, each from the other because:

Inventions I and II are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct if they do not overlap in scope and not obvious variants, and if it is shown that at least one subcombination is separately usable.

In the instance case, subcombination I has separate utility such as subject matter comprising systems, methods, and apparatus for ensuring data integrity by scanning of software or data or otherwise monitoring data to prevent or detect attacks. Subcombination II has separate utility such as subject matter including apparatus or techniques for determining what or how network elements are interconnected. See MPEP § 806.05(d).

The examiner has required restriction between subcombinations usable together. Where Applicants elect a subcombination and claims thereto are subsequently found allowable, any claim(s) depending from or otherwise requiring all the limitations of the

allowable subcombination will be examined for patentability in accordance with 37 CFR 1.104. See MPEP § 821.04(a). Applicants are advised that if any claim presented in a continuation or divisional application is anticipated by, or includes all the limitations of, a claim that is allowable in the present application, such claim may subject to provisional statutory and/or nonstatutory double patenting rejections over the claims of the instant applicant.

3. Restriction for examination purpose as indicated is proper because all these inventions listed in this action are independent or distinct for the reasons given above and there would be a serious search and/or examination burden if restriction were not required because at least the following reason(s) apply:

- the inventions have a acquired a separate status in the art in view of their different classification; and
- the inventions require a different field of search (e.g., searching different classes/subclasses or electronic resources, or employing different search strategies or search queries).

4. **Applicants are advised that the reply to this requirement to be complete must include (i) an election of a invention to be examined** even though the requirement may be traversed (37 CFR 1.143) **and (ii) identification of the claims encompassing the elected invention**.

The election of an invention may be made with or without traverse. To reserve a right to petition, the election must be made with traverse. If the reply does not distinctly and specifically point out supposed errors in the restriction requirement, the election

shall be treated as an election without traverse. Traversal must be presented at the time of election in order to be considered timely. Failure to timely traverse the requirement will result in the loss of right to petition under 37 CFR 1.144. If claims are added after the election, application must indicate which of these claims are readable upon the elected invention.

Should Applicants traverse on the ground that the inventions are not patentably distinct, Applicant should submit evidence or identify such evidence now of record showing the inventions to be obvious variants or clearly admit on the record that this is the case. In either instance, if the examiner finds one of the inventions unpatentable over the prior art, the evidence or admission may be used in a rejection under 35 U.S.C. 103(a) of the other invention.

5. Applicants are reminded that upon the cancellation of claims to a non-elected invention, the inventorship must be amended in compliance with 37 CFR 1.48(b) if one or more of the currently named inventors is no longer an inventor of at least one claim remaining in the applicant. Any amendment of inventorship must be accompanied by a request under 37 CFR 1.48(b) and by the fee required under 37 CFR 1.17(i).

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JASON C. CHIANG whose telephone number is (571)270-3393. The examiner can normally be reached on 9AM to 6PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, NATHAN J. FLYNN can be reached on (571)272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/J.C./
Examiner, Art Unit 2431
/NATHAN FLYNN/

Supervisory Patent Examiner, Art Unit 2431

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.:	13/372,375	Confirmation No.:	**2918**
Applicant:	Melvyn MORRIS	TC/A.U.	2431
Filed:	02/13/2012	Examiner:	CHIANG, JASON
Docket No.:	6890-89-1		
For:	METHODS AND APPARATUS FOR DEALING WITH MALWARE		

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE TO RESTRICTION REQUIREMENT

Commissioner:

In an Office Action dated April 5, 2013, the Examiner issued a Restriction Requirement with regard to the above-identified patent application. Generally, the Examiner indicated that **Group I** is directed to Claims 1-16; and **Group 2** is directed to Claims 17-24, are separate inventions. Applicants hereby elect to prosecute Group I - Claims 1-16 in this patent application. However, Applicants respectfully reserve the right to pursue Group 2 – Claims 17-24 in a subsequent divisional/continuation application.

Although Applicant believes that no fees are due in connection with filing this Amendment and Response, please charge any fees deemed necessary to Deposit Account No. 19-1970.

Respectfully submitted,

SHERIDAN ROSS P.C.

Date: May 6, 2013

By: /Brent R. Lindon/

Brent R. Lindon
Reg. No.67,424
1560 Broadway, Suite 1200
Denver, Colorado 80202
Telephone: 303-863-9700

Electronic Acknowledgement Receipt

EFS ID:	15696173
Application Number:	13372375
International Application Number:	
Confirmation Number:	2918
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Customer Number:	22442
Filer:	Brent Robert Lindon/Kathy Johnston
Filer Authorized By:	Brent Robert Lindon
Attorney Docket Number:	6890-89-1
Receipt Date:	06-MAY-2013
Filing Date:	13-FEB-2012
Time Stamp:	18:38:42
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Response to Election / Restriction Filed	RESP_TO_RR.pdf	68609 5bdfa51caa68cb97fdf2bd00534a4585c061661a	no	1

Warnings:	
Information:	

Total Files Size (in bytes):	68609

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	1	of	2

Complete if Known	
Application Number	13/372,375
Filing Date	February 13, 2012
First Named Inventor	Melvyn Morris
Art Unit	2431
Examiner Name	Jason Chiang
Attorney Docket Number	6890-89-1

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	7343626	03/11/2008	Gallagher	
	2	7707634	04/27/2010	Sandu et al.	
	3	8042184	10/18/2011	Batenin	
	4	8146135	03/27/2012	Waissbein et al.	
	5	8307435	11/06/2012	Mann et al.	
	6	2006/0069912	03/30/2006	Zheng et al.	
	7	2006/0101334	05/11/2006	Liao et al.	
	8	2006/0117055	06/01/2006	Doyle	
	9	2009/0292791	11/26/2009	Livshits et al.	
	10	2009/0300764	12/03/2009	Freeman	
	11	2010/0043072	02/18/2010	Rothwell	
	12	2010/0064368	03/11/2010	Stolfo et al.	
	13	2010/0306851	12/02/2010	Zhou	
	14	2010/0313183	12/09/2010	Ellen et al.	
	15	2011/0083183	04/07/2011	Freeman	
	16	2011/0138361	06/09/2011	McEntee et al.	
	17	2012/0017200	01/19/2012	Ghosh et al.	
	18	2012/0260304	10/11/2012	Morris et al.	
	19	2012/0266208	10/18/2012	Morris et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]; Number[4]; Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*				Application Number	13/372,375
				Filing Date	February 13, 2012
				First Named Inventor	Melvyn Morris
				Art Unit	2431
				Examiner Name	Jason Chiang
Sheet	2	of	2	Attorney Docket Number	6890-89-1

NON-PATENT LITERATURE DOCUMENTS		
Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	20	CLARKE, "Fuzzing for Software Vulnerability Discovery - Technical Report RHUL-MA-2009-04," Department of Mathematics, Royal Holloway, University of London, Feb 17, 2009, 178 pages. Retrieved from: www.ma.rhul.ac.uk/static/techrep/2009/RHUL-MA-2009-04.pdf
	21	SU et al., "The Essence of Command Injection Attacks in Web Applications," Conference record of the 33rd ACM SIGPLAN-SIGACT symposium on Principles of programming languages (POPL '06), 2006, pages 372-382.
	22	Official Action for U.S. Patent Application No. 12/703,074 mailed Sep. 12, 2012 (Attorney Ref. No. 6890-87), 16 pages.
	23	Notice of Allowance for U.S. Patent Application No. 12/703,074 mailed Nov. 21, 2012 (Attorney Ref. No. 6890-87), 5 pages.
	24	Notice of Allowance for U.S. Patent Application No. 13/010,639 mailed Mar. 20, 2013 (Attorney Ref. No. 6890-87-CIP), 15 pages.
	25	Official Action for U.S. Patent Application No. 13/372,433 mailed Apr. 24, 2013 (Attorney Ref. No. 6890-89-2), 6 pages.
	26	Official Action for U.S. Patent Application No. 13/372,439 mailed Apr. 22, 2013 (Attorney Ref. No. 6890-89-3), 6 pages.

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Electronic Acknowledgement Receipt

EFS ID:	15756810
Application Number:	13372375
International Application Number:	
Confirmation Number:	2918
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Customer Number:	22442
Filer:	Brent Robert Lindon/David Voegtle
Filer Authorized By:	Brent Robert Lindon
Attorney Docket Number:	6890-89-1
Receipt Date:	13-MAY-2013
Filing Date:	13-FEB-2012
Time Stamp:	14:03:30
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	CLARK_Fuzzing_for_software_vulnerability.pdf	10539470 7f4e1b96933aed8f878d0301b094ce0c4dff57b7	no	178

Warnings:	
Information:	

2	Non Patent Literature	SU_Essence_of_Command_Injection_Attacks.pdf	1059650 b0e02b54c3f39bc033e241252607b4b76627a467	no	11
Warnings:					
Information:					
3	Non Patent Literature	6890-87_OA_09-12-2012.pdf	545067 f1807541da71a5166b4c2c24cbdcc022a84e5ca6	no	16
Warnings:					
Information:					
4	Non Patent Literature	6890-87_NOA_11-21-2012.pdf	329695 785599514584 20fbd00e16c603b70e54b1362fb9	no	5
Warnings:					
Information:					
5	Non Patent Literature	6890-87-CIP_NOA_03-20-2013.pdf	576540 4ee48489fd88c1cf02fddad48a2130a6eddb91a4	no	15
Warnings:					
Information:					
6	Non Patent Literature	6890-89-2_RR_04-24-2013.pdf	213122 d856c4067e03ca85e31a5e2c4b08d54f69ffc427	no	6
Warnings:					
Information:					
7	Non Patent Literature	6890-89-3_RR_04-22-2013.pdf	219453 0f6d3b7527071cb19c332cb4d9c631bb353c04fb	no	6
Warnings:					
Information:					
8		IDS_02.pdf	500279 2bf379527d57dcd024e65c7d5ad8eb1013f2bc63	yes	5

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	3
	Information Disclosure Statement (IDS) Form (SB08)	4	5

Warnings:	
Information:	
Total Files Size (in bytes):	13983276

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:	)	Group Art Unit: 2431
Melvyn Morris	)	Confirmation No.: 2918
Serial No.: 13/372,375	)	Examiner: Jason Chiang
Filed: February 13, 2012	)	SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT
Atty. File No.: 6890-89-1	)	
Entitled: "Methods and Apparatus for Dealing with Malware"	)	*Electronically Submitted*

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

The references cited on attached Form PTO/SB08 are being called to the attention of the Examiner.

☒ Copies of the cited non-patent and/or foreign references are enclosed herewith.

☐ Copies of the cited U.S. patents and/or patent applications are enclosed herewith.

☒ Copies of the cited U.S. patents/patent application publications are not enclosed in accordance with 37 C.F.R. § 1.98(a).

☐ Copies of the cited references are not enclosed, in accordance with 37 C.F.R. § 1.98(d), because the references were cited by or submitted to the U.S. Patent and Trademark Office in prior application Serial No. _____ filed _____, which is relied upon for an earlier filing date under 35 U.S.C. § 120.

☐ To the best of applicants' belief, the pertinence of the foreign-language references is believed to be summarized in the attached English abstracts and/or in the figures, although applicants do not necessarily vouch for the accuracy of the translation.

☒ Examiner's attention is drawn to the following related applications:

- Serial No. 12/703,074 filed 02/09/2010 now U.S. Patent No. 8,407,790 (Attorney's Ref. No. 6890-87)
- Serial No. 13/010,639 filed 01/20/2011 (Attorney's Ref. No. 6890-87-CIP)
- Serial No. 13/372,433 filed 02/13/2012 (Attorney's Ref. No. 6890-89-2)
- Serial No. 13/372,439 filed 02/13/2012 (Attorney's Ref. No. 6890-89-3)

Sophos Ex. 1002
Page 146 of 683

☐ Other:_____

Submission of the above information is not intended as an admission that any item is citable under the statutes or rules to support a rejection, that any item disclosed represents analogous art, or that those skilled in the art would refer to or recognize the pertinence of any reference without the benefit of hindsight, nor should an inference be drawn as to the pertinence of the references based on the order in which they are presented. Submission of this statement should not be taken as an indication that a search has been conducted, or that no better art exists.

It is respectfully requested that the cited information be expressly considered during the prosecution of this application and the references made of record therein.

FEES

☒	**37 CFR 1.97(b)**: No fee is believed due in connection with this submission, because the information disclosure statement submitted herewith is satisfied by one of the following conditions ("X" indicates satisfaction): ☐ Within three months of the filing date of a national application other than a continued prosecution application under 37 CFR 1.53(d), or ☐ Within three months of the date of entry of the national stage as set forth in § 1.491 in an international application, or ☒ Before the mailing date of a first Office Action on the merits, or ☐ Before the mailing of a first Office action after the filing of a request for continued examination under 37 CFR 1.114. Although no fee is believed due, if any fee is deemed due in connection with this submission, please charge such fee to Deposit Account 19-1970.
☐	**37 CFR 1.97(c)**: The information disclosure statement transmitted herewith is being filed after all the above conditions (37 CFR 1.97(b)), but before the mailing date of any one of the following conditions: (1) a final action under 37 C.F.R. 1.113, or (2) a notice of allowance under 37 C.F.R. 1.311, or (3) an action that otherwise closes prosecution in the application. This Information Disclosure Statement is accompanied by: ☐ A Certification (below) as specified by 37 C.F.R. 1.97(e). Although no fee is believed due, if any fee is deemed due in connection with this submission, please charge such fee to Deposit Account 19-1970. OR ☐ Please charge Deposit Account 19-1970 in the amount of $180.00 for the fee set forth in 37 C.F.R. 1.17(p) for submission of an information disclosure statement. Please credit any overpayment or charge any underpayment to Deposit Account 19-1970.
☐	**37 CFR 1.97(d)**: This Information Disclosure Statement is being submitted after the period specified in 37 CFR 1.97(c). ☐ This information Disclosure Statement includes a Certification (below) as specified by 37 C.F.R. 1.97(e) AND ☐ Applicants hereby requests consideration of the reference(s) disclosed herein. Please charge Deposit Account 19-1970 in the amount of $180.00 under 37 C.F.R. 1.17(p). Please credit any overpayment or charge any underpayment to Deposit Account 19-1970. Election to pay the fee should not be taken as an indication that applicant(s) cannot execute a certification.

Sophos Ex. 1002
Page 147 of 683

Certification (37 C.F.R. 1.97(e))
(Applicable only if checked)

☐ The undersigned certifies that:

☐ Each item of information contained in this information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this statement. 37 C.F.R. 1.97(e)(1).

☐ A copy of the communication from the foreign patent office is enclosed.

OR

☐ No item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned after making reasonable inquiry, no item of information contained in this Information Disclosure Statement was known to any individual designated in 37 C.F.R. 1.56(c) more than three months prior to the filing of this statement. 37 C.F.R. 1.97(e)(2).

Respectfully submitted,

SHERIDAN ROSS P.C.

By: 

Brent R. Lindon
Registration No. 67424
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: MAY 07, 2013

Sophos Ex. 1002
Page 148 of 683

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/372,375	02/13/2012	Melvyn Morris	6890-89-1	2918

22442 7590 06/17/2013

Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

EXAMINER	
CHIANG, JASON	
ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
06/17/2013	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

e-docket@sheridanross.com
srlaw@sheridanross.com

Office Action Summary	Application No. 13/372,375	Applicant(s) MORRIS ET AL.	
	Examiner JASON C. CHIANG	Art Unit 2431	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *6 May 2013*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-16* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-16* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *13 February 2012* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some * c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Interim copies:

a)☐ All b)☐ Some c)☐ None of the: Interim copies of the priority documents have been received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *05/31/2012, 05/13/2013*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on 05/06/2013.

2. Claims 1-16 are under examination. Claims 17-24 are non-elected.

3. The Information Disclosure Statements filed on 05/31/2012 and 05/13/2013 has been entered and considered.

Priority

4. Applicant's claim for the benefit of a prior-filed application under 35 U.S.C. 119(e) or under 35 U.S.C. 120, 121, or 365(c) is acknowledged.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 9, 14-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boisjolie et al. (US 8,332,946 B1) and Meyer et al. (US 2011/0191341 A1).

Regarding claim 1, Boisjolie et al. discloses:

A method of classifying a computer object as malware **[Abstract, "The malware-protection method employs a number of techniques and relies on multiple layers of protection to identify trusted files, prevent execution of untrustworthy files, accurately detect corrupted files, analyze questionable files, and quarantine files"]**, the method comprising:

at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored or processed **[Col. 4, lines 53-64, "At STEP 2, a new file from an external source enters the endpoint 102. One of ordinary skill in the art will recognize that the new file may be of a variety of types, including, for example, audio, video, multi-media, text, executable, archives, HTML, and the like. Other types for the new file, other than those listed herein, will be apparent to one of ordinary skill in the art. From STEP 2, the method 100 proceeds to STEP 3. At STEP 3, a fingerprint for the new file (i.e., a new-file fingerprint) is created by the endpoint 102 and the new-file fingerprint is sent to application-verification servers 104 for verification"]**;

wherein the base computer comprises plural threat servers arranged to receive the data from the plural remote computers and apply rules or heuristics against the data in real time to determine whether or not the object is malware and to communicate the determination to the remote computers **[Col. 5, lines 4-7, "At STEP 4, the application verification servers 104 attempt to verify the new-file fingerprint against an application-data-signature whitelist in data communication with the application-verification servers 104", lines 30-37, "At STEP 5, if the verification of the new-file**

fingerprint in STEP 4 returns that the new file cannot be identified as either good or bad (i.e., is unknown), the new file is sent from the endpoint 102 to malware-scan servers 106 for scanning Various scanning techniques are typically used to detect malware such as, for example, traditional virus-signature-based definition comparison, heuristics, sandbox emulation, analysis, and prediction, and the like.", Fig. 1, Backend identifies threat and notifies client];

Boisjolie et al. does not explicitly disclose the base computer further comprising at least one central server in communication with the threat servers and arranged to receive the data about objects from the threat servers to maintain a master database of data received about objects from all threat servers.

However, Meyer et al. in the field relates to systems and methods for sharing the results of computing operations (such as malware or data-loss-prevention scans) performed on shared or common files among related computing systems teaches the base computer further comprising at least one central server in communication with the threat servers and arranged to receive the data about objects from the threat servers to maintain a master database of data received about objects from all threat servers **[Paragraph 0029, "Shared store 216 generally represents any type or form of physical or virtualized storage that may be shared or accessed by a group of related computing systems, such as virtual machines 202(1)-(N) in FIG. 2. In some examples, shared store 216 may contain or comprise a file-attribute database (such as file-attribute database 120 in FIGS. 1 and 5) that may contain, for each of a plurality of files encountered by a group of computing systems (such as virtual**

machines 202(1)-(N)): 1) a hash of the file, 2) the results of at least one computing operation performed in connection with the file (such as a classification assigned to the file during a malware analysis, at least one rationale for the classification assigned to the file during the malware analysis, at least one virus definition set or heuristic used when performing the malware analysis, or the like), 3) the date of at least one computing operation performed in connection with the file (such as the date of the most-recent malware scan performed on the file), and/or 4) any other potentially useful information that may be shared among related computing systems"].

At the time of the invention, it would have been obvious to a person having ordinary skill in the art to incorporate the teaching of Meyer et al. into the teaching of Boisjolie et al. with the motivation of sharing the results of computing operations among related computing systems as taught by Meyer et al. **[Meyer et al.: abstract]**.

Regarding claim 9, it recites similar limitations as of claim 1. The reasons for the rejection of claim 1 are incorporated herein.

Regarding claim 14, the rejection of claim 9 is incorporated.

Boisjolie et al. discloses a method of classifying a computer object as malware.

Meyer et al. further discloses the central server has databases including at least one of a) object signatures and metadata about that object; b) object behavior; and c) information about what objects are present on what remote computers **[Paragraph 0029, "Shared store 216 generally represents any type or form of physical or virtualized storage that may be shared or accessed by a group of related**

computing systems, such as virtual machines 202(1)-(N) in FIG. 2. In some examples, shared store 216 may contain or comprise a file-attribute database (such as file-attribute database 120 in FIGS. 1 and 5) that may contain, for each of a plurality of files encountered by a group of computing systems (such as virtual machines 202(1)-(N)): 1) a hash of the file, 2) the results of at least one computing operation performed in connection with the file (such as a classification assigned to the file during a malware analysis, at least one rationale for the classification assigned to the file during the malware analysis, at least one virus definition set or heuristic used when performing the malware analysis, or the like), 3) the date of at least one computing operation performed in connection with the file (such as the date of the most-recent malware scan performed on the file), and/or 4) any other potentially useful information that may be shared among related computing systems"].

At the time of the invention, it would have been obvious to a person having ordinary skill in the art to incorporate the teaching of Meyer et al. into the teaching of Boisjolie et al. with the motivation of sharing the results of computing operations among related computing systems as taught by Meyer et al. **[Meyer et al.: abstract]**.

Regarding claim 15, the rejection of claim 14 is incorporated.

Boisjolie et al. further discloses the threat and central servers are implemented using cloud computing **[Col. 2, lines 28-30, "Responsive to a determined status of unknown in response to a malware scan, the new file is sent to a cloud-based malware-scanning engine"]**.

7. Claims 2-3, 6-7 and 10-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boisjolie et al. (US 8,332,946 B1) and Meyer et al. (US 2011/0191341 A1) as applied to claims 1, 9, 14-15, and in view of Nishikawa et al. (US 2003/0093429 A1).

Regarding claim 2, the rejection of claim 1 is incorporated.

Boisjolie et al. further discloses at least one threat server comprises at least one database for holding information received from remote computers to which it is attached, the method comprising storing the data in at least one database at the threat server **[Col. 4, lines 61-64, "At STEP 3, a fingerprint for the new file (i.e., a new-file fingerprint) is created by the endpoint 102 and the new-file fingerprint is sent to application-verification servers 104 for verification", Fig. 1, Application database]**;

Meyer et al. discloses the server in communication with the threat servers and arranged to receive the data about objects from the threat servers to maintain a master database of data received about objects from all threat servers with timestamp **[Fig. 5]**.

Both Boisjolie et al. and Meyer et al. do not teach at intervals, storing the contents of the database in storage and clearing the database.

Nishikawa et al. in the field relates to a data storage system teaches at intervals, storing the contents of the database in storage and clearing the database **[Paragraph 0030, "The server 102 is referred to as a "dynamic database server," in part, because it is updated with new data or records that have been inputted into the**

saving job DB 118 since the last batch process. Accordingly, the server 102 has more current data than the DWH server 105 that receives data periodically from the batch extraction step 119. As used herein, the term "dynamic database" is a database that is stored with data more recent than the DWH. In the present embodiment, the dynamic database is a temporarily database that is periodically purged of redundant or old data that have been copied into the DWH"].

At the time of the invention, it would have been obvious to a person having ordinary skill in the art to incorporate the teaching of Nishikawa et al. into the teaching of Boisjolie et al. and Meyer et al. with motivation to allow the system to delete old data and save new records **[Nishikawa et al.: Paragraph 0033]**.

Regarding claim 3, the rejection of claim 2 is incorporated.

Boisjolie et al. discloses a method of classifying a computer object as malware.

Meyer et al. further discloses the method according to claim 2 comprising creating a backup central server by receiving at a central server all of the time-stamped blocks of data and incorporating them into its database **[Paragraph 0029, "Shared store 216 generally represents any type or form of physical or virtualized storage that may be shared or accessed by a group of related computing systems, such as virtual machines 202(1)-(N) in FIG. 2. In some examples, shared store 216 may contain or comprise a file-attribute database (such as file-attribute database 120 in FIGS. 1 and 5) that may contain, for each of a plurality of files encountered by a group of computing systems (such as virtual machines 202(1)-(N)): 1) a hash of the file, 2) the results of at least one computing operation performed in**

connection with the file (such as a classification assigned to the file during a malware analysis, at least one rationale for the classification assigned to the file during the malware analysis, at least one virus definition set or heuristic used when performing the malware analysis, or the like), 3) the date of at least one computing operation performed in connection with the file (such as the date of the most-recent malware scan performed on the file), and/or 4) any other potentially useful information that may be shared among related computing systems", Fig. 5].

At the time of the invention, it would have been obvious to a person having ordinary skill in the art to incorporate the teaching of Meyer et al. into the teaching of Boisjolie et al. with the motivation of sharing the results of computing operations among related computing systems as taught by Meyer et al. **[Meyer et al.: abstract]**.

Regarding claim 6, the rejection of claim 2 is incorporated.

Boisjolie et al. discloses a method of classifying a computer object as malware.

Meyer et al. further discloses the central server has databases including at least one of a) object signatures and metadata about that object; b) object behavior; and c) information about what objects are present on what remote computers **[Paragraph 0029, "Shared store 216 generally represents any type or form of physical or virtualized storage that may be shared or accessed by a group of related computing systems, such as virtual machines 202(1)-(N) in FIG. 2. In some examples, shared store 216 may contain or comprise a file-attribute database (such as file-attribute database 120 in FIGS. 1 and 5) that may contain, for each of**

a plurality of files encountered by a group of computing systems (such as virtual machines 202(1)-(N)): 1) a hash of the file, 2) the results of at least one computing operation performed in connection with the file (such as a classification assigned to the file during a malware analysis, at least one rationale for the classification assigned to the file during the malware analysis, at least one virus definition set or heuristic used when performing the malware analysis, or the like), 3) the date of at least one computing operation performed in connection with the file (such as the date of the most-recent malware scan performed on the file), and/or 4) any other potentially useful information that may be shared among related computing systems"].

At the time of the invention, it would have been obvious to a person having ordinary skill in the art to incorporate the teaching of Meyer et al. into the teaching of Boisjolie et al. with the motivation of sharing the results of computing operations among related computing systems as taught by Meyer et al. **[Meyer et al.: abstract]**.

Regarding claim 7, the rejection of claim 2 is incorporated.

Boisjolie et al. further discloses the threat and central servers are implemented using cloud computing **[Col. 2, lines 28-30, "Responsive to a determined status of unknown in response to a malware scan, the new file is sent to a cloud-based malware-scanning engine"]**.

Regarding claim 10, it recites similar limitations as of claim 2. The reasons for the rejection of claim 2 are incorporated herein.

Regarding claim 11, it recites similar limitations as of claim 3. The reasons for the rejection of claim 3 are incorporated herein.

8. Claims 4 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boisjolie et al. (US 8,332,946 B1), Meyer et al. (US 2011/0191341 A1) and Nishikawa et al. (US 2003/0093429 A1) as applied to claims 2-3, 6-7 and 10-11, and in view of Chen et al. (US 2009/0070304).

Regarding claim 4, the rejection of claim 2 is incorporated.

Boisjolie et al. discloses a method of classifying a computer object as malware.

Meyer et al. further discloses creating a backup central server by receiving at a central server all of the time-stamped blocks of data and incorporating them into its database.

Nishikawa et al. teaches at intervals, storing the contents of the database in storage and clearing the database.

They do not teach taking a central server off-line for a period of time such that it does not receive updates of data from the threat servers during that period of time; after the period of time has elapsed, updating the database of the central server with time-stamped blocks of data from the storage that have a timestamp later than the time when the central server went off-line; and bringing the central server back on line.

However, Chen in the field relates to database systems teaches taking a central server off-line for a period of time such that it does not receive updates of data from the

threat servers during that period of time; after the period of time has elapsed, updating the database of the central server with time-stamped blocks of data from the storage that have a timestamp later than the time when the central server went off-line; and bringing the central server back on line **[Paragraph 0004, "Applications commonly use this timestamp column for controlling optimistic locking schemes as follows: the application retrieves one or more rows from the table, including the timestamp column; the application logically or physically disconnects from the database system; the application makes updates to the rows that were retrieved from the database; and sometime later, the application reconnects to the database so that it can record the updates in the database"]**.

At the time of the invention, it would have been obvious to a person having ordinary skill in the art to incorporate the teaching of Chen et al. into the teaching of Boisjolie et al., Meyer et al. and Nishikawa et al. with the motivation of ensuring data consistency **[Chen et al.: paragraph 0003]**.

Regarding claim 12, it recites similar limitations as of claim 4. The reasons for the rejection of claim 4 are incorporated herein.

9. Claims 5 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boisjolie et al. (US 8,332,946 B1), Meyer et al. (US 2011/0191341 A1) and Nishikawa et al. (US 2003/0093429 A1) as applied to claims 2-3, 6-7 and 10-11, and in view of McGrattan et al. (US 7814056 B2).

Regarding claim 5, the rejection of claim 2 is incorporated.

Boisjolie et al. discloses a method of classifying a computer object as malware.

Meyer et al. further discloses creating a backup central server by receiving at a central server all of the time-stamped blocks of data and incorporating them into its database.

Nishikawa et al. teaches at intervals, storing the contents of the database in storage and clearing the database.

They do not teach rolling back the database of a central server to a point of time in the past; updating the database of the central server with time-stamped blocks of data from storage that have a timestamp later than the past point of time; and bringing the central server back on line.

However McGrattan et al. in the field relates to storage backup teaches rolling back the database of a central server to a point of time in the past **[Col. 5, lines 1-13, "A method for restoring backup data from a database, according to one embodiment, will be described with reference to FIG. 2. The backup data is stored in the database as a plurality of data blocks. Each data block is typically stored with associated timestamp information in the database. A specification of a time to which data restoration is desired is received (step S21). The specified time is compared to timestamp information stored (step S23) for each of the data blocks of the backup data in the database. A selected data block of the backup data is retrieved if the selected data block has a timestamp at or earlier than the specified time and no other data blocks of the backup data which correspond to**

the selected data block have more contemporaneous timestamps between the specified time and the associated timestamp of the selected data block (step S25)"]; updating the database of the central server with time-stamped blocks of data from storage that have a timestamp later than the past point of time; and bringing the central server back on line **[Col. 9, lines 4-34, "When a request for the operation "refresh object" is received, process software 602 collects the latest timestamps associated with the objects in the specified object set and correlates them to the data block digests for each data block in each of the objects of the object set (step S1). A list of the data block digests for the entire specified object set 901 is compiled and sorted in order of an object system directories walk-through (for example, data block digests are collected block-by-block for each object in the object set, and the collected data block digests are sorted) and is then sent to object system agent 601 (step S91). Object attributes are then read from Object system 600 for the object to be "refreshed" (step S92). The modification date of the object to be "refreshed" is compared to the timestamp information for the stored objects. If the modification date is higher than the latest timestamp for the object, then the object is read (step S92). For every block of size n in the object, a new data block digest is generated and compared against the ones in the list received by object system agent 601 at step 91 (step S93). If the data block digests are not equivalent, then the data block and the generated data block digest are both sent to process software 602 (step S94). If the data block digests are equivalent, then the data block is dropped and the system proceeds to the**

next block (step S94). Once process software 602 receives the new data blocks, it sends the metadata for the data blocks to database server 603 to be cataloged in database catalog 604 (step S95b) and the data block and data block digest are forwarded to media server 605 to be stored in database 609 (step S95b)", Col. 1, lines 21-43, "Enterprises and individuals who use computers that contain critical data, need disaster recovery plans in place in the event of a disaster, in order to safeguard vital information stored on the computers. Even in non-disaster situations, in which users may just want to archive their information, it is beneficial to implement "backup" and recovery plans", "A partial backup can be either differential, in which all of the files that were changed since the last complete backup are considered, or incremental, in which all of the files that were changed since the last backup are considered, or user-defined, in which only sets of files specified by a user are considered"].

At the time of the invention, it would have been obvious to a person having ordinary skill in the art to incorporate the teaching of McGrattan et al. into the teaching of Boisjolie et al., Meyer et al. and Nishikawa et al. with the motivation of able to restoring backup data from a database by using the timestamp as taught by McGrattan et al. **[McGrattan et al.: abstract]**.

Regarding claim 13, it recites similar limitations as of claim 5. The reasons for the rejection of claim 5 are incorporated herein.

10. Claims 8 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boisjolie et al. (US 8,332,946 B1) and Meyer et al. (US 2011/0191341 A1) as applied to claims 1, 9, 14-15, and in view of Quinlan (US 7921063 B1).

Regarding claim 8, the rejection of claim 1 is incorporated.

Boisjolie et al. discloses maintaining at a threat server, a list of objects previously seen at the threat server **[Col. 4, lines 53-64, "At STEP 2, a new file from an external source enters the endpoint 102. One of ordinary skill in the art will recognize that the new file may be of a variety of types, including, for example, audio, video, multi-media, text, executable, archives, HTML, and the like. Other types for the new file, other than those listed herein, will be apparent to one of ordinary skill in the art. From STEP 2, the method 100 proceeds to STEP 3. At STEP 3, a fingerprint for the new file (i.e., a new-file fingerprint) is created by the endpoint 102 and the new-file fingerprint is sent to application-verification servers 104 for verification"]**.

Meyer et al. further discloses forwarded it to the central server; and if an object has not been seen before, sending the data about that object to the central server **[Paragraph 0029, "Shared store 216 generally represents any type or form of physical or virtualized storage that may be shared or accessed by a group of related computing systems, such as virtual machines 202(1)-(N) in FIG. 2. In some examples, shared store 216 may contain or comprise a file-attribute database (such as file-attribute database 120 in FIGS. 1 and 5) that may contain, for each of a plurality of files encountered by a group of computing systems (such as virtual**

machines 202(1)-(N)): 1) a hash of the file, 2) the results of at least one computing operation performed in connection with the file (such as a classification assigned to the file during a malware analysis, at least one rationale for the classification assigned to the file during the malware analysis, at least one virus definition set or heuristic used when performing the malware analysis, or the like), 3) the date of at least one computing operation performed in connection with the file (such as the date of the most-recent malware scan performed on the file), and/or 4) any other potentially useful information that may be shared among related computing systems"].

They do not teach if an object has been seen before, increasing the count for that object instead of sending the data.

However, Quinlan in the field relates to network data communications teaches if an object has been seen before, increasing the count for that object instead of sending the data **[Col. 6, lines 10-15, "threat information source 104 generates counts of received messages that have suspicious attachments, and provides the counts to threat information processor 108, or allows an external process to retrieve the counts and store them in a specialized database"]**.

At the time of the invention, it would have been obvious to a person having ordinary skill in the art to incorporate the teaching of Quinlan into the teaching of Boisjolie et al., Meyer et al. and Nishikawa et al. with the motivation for use in managing computer virus outbreaks as taught by Quinlan **[Quinlan: col. 6, lines 6-15]**.

Regarding claim 16, it recites similar limitations as of claim 8. The reasons for the rejection of claim 8 are incorporated herein.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to Applicant's disclosure:

US 8195938 B2 Cloud-based application whitelisting

US 8296178 B2 Services using globally distributed infrastructure for secure content management

US 7231440 B1 System and method for distributing portable computer virus definition records with binary file conversion

US 8347386 B2 System and method for server-coupled malware prevention

US 8448243 B1 Systems and methods for detecting unknown malware in an executable file

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JASON C. CHIANG whose telephone number is (571)270-3393. The examiner can normally be reached on 9AM to 6PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, NATHAN J. FLYNN can be reached on (571)272-1915. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/J.C./
Examiner, Art Unit 2431

/CAROLYN B KOSOWSKI/
Primary Examiner, Art Unit 2431

Notice of References Cited	Application/Control No. 13/372,375	Applicant(s)/Patent Under Reexamination MORRIS ET AL.	
	Examiner JASON C. CHIANG	Art Unit 2431	Page 1 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2003/0093429 A1	05-2003	Nishikawa et al.	707/10
*	B	US-7,188,173 B2	03-2007	Anderson et al.	709/225
*	C	US-7,231,440 B1	06-2007	Kouznetsov et al.	709/224
*	D	US-2009/0070304 A1	03-2009	CHEN et al.	707/3
*	E	US-7,814,056 B2	10-2010	McGrattan et al.	707/640
*	F	US-2010/0332593 A1	12-2010	Barash et al.	709/203
*	G	US-7,921,063 B1	04-2011	Quinlan, Daniel	706/12
*	H	US-2011/0191341 A1	08-2011	Meyer et al.	707/736
*	I	US-2011/0191299 A1	08-2011	Huynh Huu et al.	707/646
*	J	US-8,116,732 B2	02-2012	Issa et al.	455/410
*	K	US-8,195,938 B2	06-2012	Fanton et al.	713/165
*	L	US-8,234,709 B2	07-2012	Viljoen et al.	726/24
*	M	US-8,276,202 B1	09-2012	Dubrovsky et al.	726/22

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 13/372,375	Applicant(s)/Patent Under Reexamination MORRIS ET AL.	
	Examiner JASON C. CHIANG	Art Unit 2431	Page 2 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-8,296,178 B2	10-2012	Hudis et al.	370/401
*	B	US-8,301,904 B1	10-2012	Gryaznov, Dmitry O.	713/188
*	C	US-8,321,540 B2	11-2012	Webb-Johnson, Mark Crispin	709/221
*	D	US-8,321,944 B1	11-2012	Mayer et al.	726/25
*	E	US-8,336,100 B1	12-2012	Glick et al.	726/23
*	F	US-8,332,946 B1	12-2012	Boisjolie et al.	726/24
*	G	US-8,347,386 B2	01-2013	Mahaffey et al.	726/23
*	H	US-8,347,375 B2	01-2013	Graham et al.	726/13
*	I	US-8,352,484 B1	01-2013	Schneider, Scott	707/758
*	J	US-8,448,243 B1	05-2013	Sankruthi, Anand	726/22
*	K	US-8,453,244 B2	05-2013	Dai et al.	726/24
*	L	US-8,443,447 B1	05-2013	Chen et al.	726/24
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13372375	MORRIS ET AL.
	Examiner	**Art Unit**
	JASON C CHIANG	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/09/2013								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	N								
	18	N								
	19	N								
	20	N								
	21	N								
	22	N								
	23	N								
	24	N								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13372375	MORRIS ET AL.
	Examiner	Art Unit
	JASON C CHIANG	2431

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	23	06/04/2013	JC

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor search in East	06/04/2013	JC
Text search in East of USPGPUB, USPAT, USOCR, FPRS, EPO, JPO, DERWENT, IBM_TDB	06/05/2013	JC

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/JASON C CHIANG/ Examiner.Art Unit 2431	

Sophos Ex. 1002
Page 172 of 683

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13372375
Filing Date	2012-02-13
First Named Inventor	Morris
Art Unit	2431
Examiner Name	
Attorney Docket Number	9400.004.02

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/J.C./	1	20070016953	A1	2007-01-18	Morris, et al.	
/J.C./	2	20110197177	A1	2011-08-11	Mony	
/J.C./	3	20110197272	A1	2011-08-11	Mony	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
/J.C./	1	1315066	EP	A1	2003-05-28	British Telecommunications		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13372375
	Filing Date	2012-02-13
	First Named Inventor	Morris
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	9400.004.02

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
/J.C./	1	MORRIS, ET AL., "Specification for related U.S. Patent Application No. 13/372,433 (Attorney Docket No. 9400.004.03)," filed 02/13/2012, Page(s) 58, to be published in: US	☐
/J.C./	2	MORRIS, ET AL., "Specification for related U.S. Patent Application No. 13/372,439 (Attorney Docket No. 9400.004.04)," filed 02/13/2012, Page(s) 54, to be published in: US	☐
/J.C./	3	SOGNO-PABIS, ELZBIETA, "Partial International Search Report re application PCT/EP2012/052497", 05/04/2012, Page(s) 7, Published in: NL	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Jason Chiang/	Date Considered	06/04/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13372375
	Filing Date	2012-02-13
	First Named Inventor	Morris
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	9400.004.02

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Sean R. O'Dowd/	Date (YYYY-MM-DD)	2012-05-30
Name/Print	O'Dowd, Sean R.	Registration Number	53403

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 2918

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/372,375	02/13/2012	726	2431	6890-89-1

APPLICANTS

Melvyn Morris, Belper, UNITED KINGDOM;
Joseph Jaroch, Elk Grove Village, IL;

**** CONTINUING DATA ***************************

This appln claims benefit of 61/443,095 02/15/2011

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

02/24/2012

Foreign Priority claimed	35 USC 119(a-d) conditions met	Verified and Acknowledged	Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
☐ Yes ☑ No	☐ Yes ☑ No	/JASON CHIANG/ Examiner's Signature	☐ Initials	UNITED KINGDOM	15	24	4

ADDRESS

Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202
UNITED STATES

TITLE

METHODS AND APPARATUS FOR DEALING WITH MALWARE

FILING FEE RECEIVED		
1870	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	1	of	2

Complete if Known	
Application Number	13/372,375
Filing Date	February 13, 2012
First Named Inventor	Melvyn Morris
Art Unit	2431
Examiner Name	Jason Chiang
Attorney Docket Number	6890-89-1

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	7343626	03/11/2008	Gallagher	
	2	7707634	04/27/2010	Sandu et al.	
	3	8042184	10/18/2011	Batenin	
	4	8146135	03/27/2012	Waissbein et al.	
	5	8307435	11/06/2012	Mann et al.	
	6	2006/0069912	03/30/2006	Zheng et al.	
	7	2006/0101334	05/11/2006	Liao et al.	
	8	2006/0117055	06/01/2006	Doyle	
	9	2009/0292791	11/26/2009	Livshits et al.	
	10	2009/0300764	12/03/2009	Freeman	
	11	2010/0043072	02/18/2010	Rothwell	
	12	2010/0064368	03/11/2010	Stolfo et al.	
	13	2010/0306851	12/02/2010	Zhou	
	14	2010/0313183	12/09/2010	Ellen et al.	
	15	2011/0083183	04/07/2011	Freeman	
	16	2011/0138361	06/09/2011	McEntee et al.	
	17	2012/0017200	01/19/2012	Ghosh et al.	
	18	2012/0260304	10/11/2012	Morris et al.	
	19	2012/0266208	10/18/2012	Morris et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]; Number[4]; Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.C./

Examiner Signature	/Jason Chiang/	Date Considered	06/04/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*				Application Number	13/372,375
				Filing Date	February 13, 2012
				First Named Inventor	Melvyn Morris
				Art Unit	2431
				Examiner Name	Jason Chiang
Sheet	2	of	2	Attorney Docket Number	6890-89-1

NON-PATENT LITERATURE DOCUMENTS		
Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	20	CLARKE, "Fuzzing for Software Vulnerability Discovery - Technical Report RHUL-MA-2009-04," Department of Mathematics, Royal Holloway, University of London, Feb 17, 2009, 178 pages. Retrieved from: www.ma.rhul.ac.uk/static/techrep/2009/RHUL-MA-2009-04.pdf
	21	SU et al., "The Essence of Command Injection Attacks in Web Applications," Conference record of the 33rd ACM SIGPLAN-SIGACT symposium on Principles of programming languages (POPL '06), 2006, pages 372-382.
	22	Official Action for U.S. Patent Application No. 12/703,074 mailed Sep. 12, 2012 (Attorney Ref. No. 6890-87), 16 pages.
	23	Notice of Allowance for U.S. Patent Application No. 12/703,074 mailed Nov. 21, 2012 (Attorney Ref. No. 6890-87), 5 pages.
	24	Notice of Allowance for U.S. Patent Application No. 13/010,639 mailed Mar. 20, 2013 (Attorney Ref. No. 6890-87-CIP), 15 pages.
	25	Official Action for U.S. Patent Application No. 13/372,433 mailed Apr. 24, 2013 (Attorney Ref. No. 6890-89-2), 6 pages.
	26	Official Action for U.S. Patent Application No. 13/372,439 mailed Apr. 22, 2013 (Attorney Ref. No. 6890-89-3), 6 pages.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.C./

Examiner Signature	/Jason Chiang/	Date Considered	06/04/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1	((roll$3 adj back) near6 time) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:11
L2	7	((roll$3 adj back)) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:12
L3	11	((roll$3 adj back) rollback) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:14
L4	48	((roll$3 adj back) rollback) and ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:18
L5	21	(((roll$3 adj back) rollback) with time) and ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:23
L6	0	((restor$4) near6 time) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 11:40
L7	3	((restor$4) near6 time) and ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 11:41
L11	0	(send provid$3 transmit$4 updat$3) near3 (count near3	US-PGPUB;	OR	ON	2013/06/09

		(threat incident)) near3 (server database)	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			15:01
L12	22	(send provid$3 transmit$4 updat$3) with ((count number) near3 (threat incident)) with (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:02
L13	122	(send provid$3 transmit$4 updat$3 record$4) with ((count number times) with (threat)) with (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:05
L14	635	(send provid$3 transmit$4 updat$3 record$4) with ((count number times) near5 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:08
L15	199	(send provid$3 transmit$4 updat$3 record$4) with ((count number) near5 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:09
L16	11	(send provid$3 transmit$4 updat$3 record$4) with ((count) near5 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:11
L17	43	((count) near2 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:15
L18	9	((count) near2 (threat)) and (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:15
L19	1126	(send provid$3 transmit$4 updat$3) near3 (count) near3 (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2013/06/09 15:18

			IBM_TDB			
L20	15	(send provid$3 transmit$4 updat$3) near3 ((increas$4 add$3) near (count)) near3 (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:20
L21	1816	((increas$4 add$3) near (count)) and (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:22
L22	27	((increas$4 add$3) near (count)) and (malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:23
S1	9	(Melvyn near Morris).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 11:48
S2	3	(Joseph near Jaroch).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 16:51
S3	108	(Webroot).as.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 16:54
S5	0	S3 and cloud and database and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 16:58
S6	2980	(726/23).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/06/04 17:04
S7	72	S6 and cloud and database and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS;	OR	ON	2013/06/04 17:05

			EPO; JPO; DERWENT; IBM_TDB			
S8	54	("20100043072" | "20110197272" | "20090300764" | "20100064368" | "20120017200" | "20060101334" | "20090292791" | "20100306851" | "20110138361" | "8042184" | "20060069912" | "20120260304" | "7707634" | "7343626" | "20070016953" | "20110197177" | "20120266208" | "20060117055" | "20100313183" | "20110083183" | "8146135" | "8307435").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/05 11:39
S9	21	("2006/0069912").URPN.	USPAT	OR	ON	2013/06/05 11:59
S10	17	threat adj server	USPAT	OR	ON	2013/06/05 12:20
S11	2362	cloud and signature	USPAT	OR	ON	2013/06/05 13:23
S12	1181	cloud and signature and layer	USPAT	OR	ON	2013/06/05 13:23
S13	249	cloud and (signature with database)	USPAT	OR	ON	2013/06/05 13:25
S14	78	cloud and (signature with database) and (malware virus)	USPAT	OR	ON	2013/06/05 13:26
S15	143	cloud and (updat$4 near3 (signature database)) and (malware virus)	USPAT	OR	ON	2013/06/05 16:30
S16	65	(updat$4 near3 (signature database) near3 (interval certain period periodic)) and (malware virus)	USPAT	OR	ON	2013/06/05 20:09
S17	1	(09/740294).APP.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/06/05 20:37
S18	0	("(masteradjdatabase)and(virusmalwaresignature)").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/06/07 18:03
S19	1003	(master adj database) and (virus malware signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:04
S20	160	(master adj database) and (virus malware) and signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:05
S21	971	(database) and (virus near signature)	US-PGPUB; USPAT; USOCR; FPRS;	OR	ON	2013/06/07 18:33

			EPO; JPO; DERWENT; IBM_TDB			
S22	639	((stor$4 sav$4 receiv$5) with database) and (virus near signature) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:51
S23	594	((stor$4 sav$4 receiv$5) near5 database) and (virus near signature) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:51
S24	64	((stor$4 sav$4 receiv$5) near5 database) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 10:51
S25	0	((stor$4 sav$4 receiv$5) near3 content near3 database near3 storage) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:02
S26	0	((stor$4 sav$4 receiv$5) near3 database near3 storage) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:03
S27	2	((stor$4 sav$4 receiv$5) near3 content near3 database near3 storage) with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:03
S28	0	((backup) near3 database) with timestamp and (virus malware)and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:05
S29	0	((backup) near3 database) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:06
S30	27	((backup) near3 database) with timestamp and @ad<"20120213"	US-PGPUB; USPAT;	OR	ON	2013/06/08 11:06

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S31	1139	((copy stor$4) near3 database) with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:20
S32	18	((copy stor$4) near3 database) with central with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:21
S33	359	((purg$4 clear$4 remov$4) near3 database near3 (period$6 every)) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:29
S34	0	(master adj database) near2 (virus malware) near2 signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S35	0	(master adj database) near3 (virus malware) near3 signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S36	0	(master adj database) with (virus malware) with signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S37	0	(master adj database) same (virus malware) same signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S38	19	(master adj database) same (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:45

S39	15	((primary secondary) adj database) same (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:54
S40	30	((primary secondary) adj database) with (signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:57
S41	98	(master adj database) same (signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:59
S42	10	(master adj database) same (signature) and (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:59
S43	315	(master adj database) and (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 16:03
S44	18	(virus malware) with definition with (file database) with (cloud community share$2)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 16:21
S45	271	(update refresh recover rebuild) near3 (database) with timestamp	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 20:22
S46	4	(update refresh recover rebuild) near3 (database) with timestamp same (offline off-line (off adj line) disconnect reconnect)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 20:24

EAST Search History (Interference)

<This search history is empty>

6/9/2013 5:06:52 PM

C:\ Users\ jchiang1\ Documents\ EAST\ Workspaces\ 13372375-Malware.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/372,375	02/13/2012	Melvyn Morris	6890-89-1	2918

22442 7590 10/02/2013

Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

EXAMINER	
CHIANG, JASON	
ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
10/02/2013	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

e-docket@sheridanross.com

Applicant-Initiated Interview Summary	Application No.	Applicant(s)	
	13/372,375	MORRIS ET AL.	
	Examiner	Art Unit	
	JASON C. CHIANG	2431	

All participants (applicant, applicant's representative, PTO personnel):

(1) *JASON C. CHIANG*. (3)_____.

(2) *Brent R. Lindon*. (4)_____.

Date of Interview: *24 September 2013*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1*.

Identification of prior art discussed: *Boisjolie et al. and Meyer*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicant's representative and the Examiner discussed the invention and related features in the specification in view of the proposed amendments. The Examiner will reconsider the rejections in light of any newly submitted amendments and/or argument.

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/CAROLYN B KOSOWSKI/ Primary Examiner, Art Unit 2431	/JASON C CHIANG/ Examiner, Art Unit 2431

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.: 13/372,375	)	Confirmation No.: 2918
Applicant: Melvyn MORRIS	)	TC/A.U.: 2413
Filed: February 13, 2012	)	Examiner: CHIANG, JASON
Docket No.: 6890-89-1	)	***Filed Electronically***
For: "METHODS AND APPARATUS FOR DEALING WITH MALWARE"	)	

AMENDMENT AND RESPONSE

Mailstop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Commissioner:

Applicant submits this Amendment and Response to address the Office Action having a mailing date of June 17, 2013. A Petition for a one month Extension of Time along with the requisite fees has been filed concurrently herewith. Although Applicant believes that no additional fees are due in connection with filing this Amendment and Response, please charge any fees deemed necessary to Deposit Account No. 19-1970.

Please amend the above-identified patent application as follows:

Amendments to the Claims are shown in the listing of claims which begins on page **2** of this paper.

Remarks begin on page **6** of this paper.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of classifying a computer object as malware, the method comprising:

at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored or processed;

wherein the base computer comprises plural threat servers arranged to receive the data from the plural remote computers and apply rules or heuristics against the data in real time to determine whether or not the object is malware and to communicate the determination to the remote computers;

the base computer further comprising at least one central server in communication with the threat servers and arranged to receive the data about objects from the threat servers to maintain a master database of data received about objects from all threat servers;

maintaining on at least one of a first of the plural threat servers, a list of objects previously seen at the first threat server and previously forwarded to the central server;

determining whether the computer object has been seen before;

sending the data about the object from the first threat server to the central server when the object has not been seen before; and

increasing a count associated with the number of times that the data about the computer object has been seen, when the data about the computer object has been seen before.

2. (Original) The method according to claim 1, wherein at least one threat server comprises at least one database for holding information received from remote computers to which it is attached, the method comprising:

storing the data in at least one database at the threat server; and

at intervals, storing the contents of the database in storage together with a timestamp and clearing the database.

3. (Original) The method according to claim 2, comprising creating a backup central server by receiving at a central server all of the time-stamped blocks of data and incorporating them into its database.

4. (Original) The method according to claim 2, comprising:

taking a central server off-line for a period of time such that it does not receive updates of data from the threat servers during that period of time;

after the period of time has elapsed, updating the database of the central server with time-stamped blocks of data from the storage that have a timestamp later than the time when the central server went off-line; and

bringing the central server back on line.

5. (Original) The method according to claim 2, comprising:

rolling back the database of a central server to a point of time in the past;

updating the database of the central server with time-stamped blocks of data from storage that have a timestamp later than the past point of time; and

bringing the central server back on line.

6. (Original) The method according to claim 2, wherein the central server has databases including at least one of:

a) object signatures and metadata about that object;

b) object behavior; and

c) information about what objects are present on what remote computers.

7. (Original) The method according to claim 6, wherein the threat and central servers are implemented using cloud computing.

8. (Canceled)

9. (Currently Amended) An apparatus for classifying a computer object as malware, the apparatus comprising:

a base computer arranged to receive data about a computer object from each of plural remote computers on which the object or similar objects are stored or processed;

wherein the base computer comprises plural threat servers arranged to receive the data from the plural remote computers and apply rules or heuristics against that data in real time to determine whether or not the object is malware and to communicate the determination to the remote computers, wherein at least one of a first threat server of the plural threat servers is further arranged to determine whether the data about the computer object has been seen before;

the base computer further comprising at least one central server in communication with the threat servers and arranged to receive the data about objects from the threat servers to maintain a master database of data received about objects from all threat servers, wherein the first threat server is further arranged to (i) maintain a list of objects previously seen at the first threat server and previously forwarded to the central server, (ii) send the data about the object from the first threat server to the central server when the object has not been seen before, and (iii) increase a count associated with the number of times that the data about the computer object has been seen, when the data about the computer object has been seen before.

10. (Original)The apparatus according to claim 9, comprising:

at least one database, the threat servers being arranged to store the data information received from remote computer in the database; and

storage, the threat servers being arranged to, at intervals, store the contents of the database in the storage together with a timestamp and clearing the database.

11. (Original) The apparatus according to claim 10, comprising:

Sophos Ex. 1002
Page 194 of 683

a backup central server having a database, the database of the backup central server being populated by receiving at the backup central server all of the time-stamped blocks of data from the storage and incorporating them into the database.

12. (Original) The apparatus according to claim 10, wherein, in the event that a central server is taken off-line for a period of time such that it does not receive updates of data from the threat servers during that period of time, the central server is arranged to, after the period of time has elapsed, update its database with time-stamped blocks of data from the storage that have a timestamp later than the time when the central server went off-line.

13. (Original) The apparatus according to claim 10, wherein, in the event that the database of a central server is rolled back to a point of time in the past, the central server is arranged to update its database with time-stamped blocks of data from storage that have a timestamp later than the past point of time.

14. (Original) The apparatus according to claim 9, wherein the central server has databases including at least one of:

a) object signatures and metadata about that object;

b) object behavior; and

c) information about what objects are present on what remote computers.

15. (Original) The apparatus according to claim 14, wherein the threat and central servers are implemented using cloud computing.

16-24. (Canceled)

Sophos Ex. 1002
Page 195 of 683

ARGUMENTS/REMARKS

The above-identified patent application has been reviewed in light of the Examiner's Action dated June 17, 2013. Claims 1 and 9 have been amended, and claims 8 and 16 have been canceled, without intending to abandon or to dedicate to the public any patentable subject matter. Accordingly, claims 1-7 and 9-15 are now pending. As set forth herein, reconsideration and withdrawal of the rejections of the claims are respectfully requested.

Examiner Interview

Applicant would like to thank Examiner Chiang for his time during the telephonic interview on September 24, 2013. Examiner Chiang and Applicant's representative, Brent Lindon, discussed the current rejection to clarify the issues at hand, discussed possible additions to the claims, and discussed differences between the cited art and the present claims. The changes discussed are some of the changes included in the current amendments. Again, Applicant appreciates the Examiner's attention and assistance.

Claim Rejection Under 35 U.S.C. § 103

Claims 1, 9, and 14-15 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 8,332,946 to Boisjolie et al. ("Boisjolie") and U.S. Patent Publication No. US 2011/0191341 to Meyer et al. ("Meyer"). Claims 2-3, 6-7 and 10-11 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Boisjolie and Meyer in view of U.S. Patent Publication No. US 2003/0093429 to Nishikawa et al. ("Nishikawa"). Claims 4 and 12 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Boisjolie, Meyer, Nishikawa, and further in view of U.S. Patent Publication No. US 2009/0070304 to Chen et al. ("Chen"). Claims 5 and 13 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Boisjolie, Meyer, Nishikawa, and further in view of U.S. Patent No. 7,814,056 to McGrattan et al. ("*McGrattan*").

To establish a *prima facie* case of obviousness, all claim limitations must first be taught or suggested by the prior art. *See, e.g., DyStar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick Co.*, 464 F.3d 1356, 1360 (Fed. Cir. 2006); 80

Sophos Ex. 1002
Page 196 of 683

U.S.P.Q.2d 1641, 1645 (2006). "All words in a claim must be considered in judging the patentability of that claim against the prior art." MPEP § 2143.03 (citing *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970)). The Examiner must then provide an explicit analysis of the motivation for combining the references. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007); 82 U.S.P.Q.2d 1385, 1396 (2007) ("a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art . . . ."). While the Examiner can choose one of several exemplary rationales from the MPEP to support an obviousness rejection, all the rationales in the MPEP still require the Examiner to demonstrate that all the claim elements are shown in the prior art. *See* MPEP § 2143, Original Eighth Edition, August 2001, Latest Revision July 2008. Applicant respectfully submits that none of the cited references disclose, suggest, or render obvious at least the combination of features as currently claimed.

The Claimed Invention

The claimed invention is generally directed to classifying computer objects as malware utilizing a distributed network. In some embodiments, a base computer comprising plural threat servers and a central server may be arranged to receive data about one or more computer objects located on or otherwise associated with one or more remote computers. In particular, large amounts of data may be used to determine rules used for classifying objects as malware. However, it tends to be impractical to store all data for all the threat servers. Accordingly, a threat server may have one or more databases of objects that have previously been seen and which have already been forwarded to the central server. For data associated with a computer object, the threat server may determine whether the data has already been seen; if the data has been seen, then a count associated with the number of times that the data has been seen is increased and may be forwarded to the central server; otherwise, the data is forwarded to the Central server.

The Boisjolie Reference

Sophos Ex. 1002
Page 197 of 683

Boisjolie is generally directed to a malware-protection method/system for protecting a computer from malware infection by preventing infected files from executing on a computer before they can do harm. *See e.g., Boisjolie,* Abstract. Boisjolie further discloses a malware protection method as illustrated in Figure 1. *See Id,* at Figure 1. In particular, Boisjolie teaches that a new file may enter an endpoint, a fingerprint may be created for the file, and the fingerprint may be verified against a white list. *See e.g., Boisjolie,* col. 4 ln 25- col. 5 ln18. Further, if the fingerprint cannot be verified, the new file is sent from the endpoint to the malware scan servers for scanning. *See Id,* at col. 5 lns 30-40. Boisjolie however, makes no mention of at least sending the data about the object from the first threat server to the central server when the object has not been seen before and increasing a count associated with the number of times that the data about the computer object has been seen, when the data about the computer object has been seen before.

The Meyer Reference

The Meyer reference is generally directed to a computer-implemented method and apparatus for sharing the results of computing operations among related computing system. *See e.g., Meyer,* Abstract. In particular, Meyer teaches a virtualization layer that may abstract hardware into a plurality of local stores for each virtual machine; the shared store may contain or comprise a file-attribute database that may contain, for each of a plurality of files encountered by a group of computing systems, a hash of the file, the results of at least one computing operation, the data of at least one computer operation, and other useful information. *See e.g., Meyer,* ¶ 0028 - ¶ 0029. However, similar to Boisjolie, Meyer fails to teach, suggest, or disclose at least sending the data about the object from the first threat server to the central server when the object has not been seen before and increasing a count associated with the number of times that the data about the computer object has been seen, when the data about the computer object has been seen before. Stated another way, paragraph [0029] of Meyer simply makes no mention of sending the data about the object from the first threat server to the central server when the object has not been seen.

The Quinlan Reference

The Quinlan reference is generally directed to evaluating electronic messages based on probabilistic analysis. *See e.g., Quinlan*, Abstract. In particular, column 6 lines 10-15 of Quinlan states "threat information source 104 generates counts of received messages that have suspicious attachments, and provides the counts to threat information processor 108, or allows an external process to retrieve the counts and store them in a specialized database." *See e.g., Quinlan,* col. 6 lns 10-15. That is, there is no disclosure, teaching, or suggestion in Quinlan of at least sending the data about the object from the first threat server to the central server when the object has not been seen before and increasing a count associated with the number of times that the data about the computer object has been seen, when the data about the computer object has been seen before. This is simply not taught by Quinlan. Accordingly, Applicant respectfully submits that Boisjolie, Meyer, and Quinlan, taken alone, or in any combination, do not teach or render obvious at least the combination of features as recited in independent claim 1 or the combination of features as recited in independent claim 9. Therefore, Applicant respectfully submits that the rejections of claims 1-7 and 9-15 should be reconsidered and withdrawn.

The dependent claims are further distinguishable at least based on the above and the additional feature(s) recited therein.

Sophos Ex. 1002
Page 199 of 683

Conclusion

The application now appearing to be in form for allowance, early notification of same is respectfully requested. Applicant does not acquiesce to any objection, rejection, or argument not specifically addressed herein. Rather, the Applicant believes the amendments and arguments contained herein overcome all objections, rejections, or arguments.

The Examiner is invited to contact the undersigned by telephone if doing so would be of assistance.

Respectfully submitted,

SHERIDAN ROSS P.C.

Date: October 17, 2013

By: /Brent R. Lindon/

Brent R. Lindon
Reg. No. 67,424
1560 Broadway, Suite 1200
Denver, CO 80202
Telephone: 303-863-9700

PTO/SB/22 (03-13)
Approved for use through 3/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): 6890-89-1

Application Number: 13/372,375

Filed: 2012-02-13

For: METHODS AND APPARATUS FOR DEALING WITH MALWARE

Art Unit: 2413

Examiner: Chiang, Jason

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☑ One month (37 CFR 1.17(a)(1))	$200	$100	$50	$ 100.00
☐ Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
☐ Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$
☐ Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐ Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☑ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 191970.

☑ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71. 37 CFR 3.73(b) statement is enclosed (Form PTO/SB/96).

☑ attorney or agent of record. Registration number 67,424.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/Brent R. Lindon/ — Signature

October 17, 2013 — Date

Brent R. Lindon — Typed or printed name

303-863-9700 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☐ * Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	13372375
Filing Date:	13-Feb-2012
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Filer:	Brent Robert Lindon/Kathy Johnston
Attorney Docket Number:	6890-89-1

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 1 month with $0 paid	2251	1	100	100

Sophos Ex. 1002
Page 203 of 683

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**100**

Electronic Acknowledgement Receipt

EFS ID:	17155363
Application Number:	13372375
International Application Number:	
Confirmation Number:	2918
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Customer Number:	22442
Filer:	Brent Robert Lindon
Filer Authorized By:	
Attorney Docket Number:	6890-89-1
Receipt Date:	17-OCT-2013
Filing Date:	13-FEB-2012
Time Stamp:	18:43:17
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$100
RAM confirmation Number	6272
Deposit Account	191970
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		AMEND_01.pdf	151916 fec97582f1f4a55e463b6c983e22ae9d1cd751f1	yes	10

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Claims	2	5
Applicant Arguments/Remarks Made in an Amendment	6	10

Warnings:

Information:

2	Extension of Time	sb0022_EOT_1mo.pdf	186965 f8775fc8d84a6d0090791687363b19db2f140a22	no	2

Warnings:

Information:

3	Fee Worksheet (SB06)	fee-info.pdf	30403 06b8b7ab0da5692db75f689b6493b74523408999	no	2

Warnings:

Information:

Total Files Size (in bytes):	369284

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/372,375	Filing Date 02/13/2012	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT **10/17/2013**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 14	Minus	** 24	= 0	X $80 =	0
Independent (37 CFR 1.16(h))	* 2	Minus	***4	= 0	X $420 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/CORALIA BETANCOURT/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*				Application Number	13/372,375
				Filing Date	February 13, 2012
				First Named Inventor	Melvyn Morris
				Art Unit	2431
				Examiner Name	Jason Chiang
Sheet	1	of	2	Attorney Docket Number	6890-89-1

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No.[1]	Document Number Number-kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	6175869	01/16/2001	Ahuja et al.	
	2	6219786	04/17/2001	Cunningham et al.	
	3	7051365	05/23/2006	Bellovin	
	4	8225218	07/17/2012	Frayman et al.	
	5	2003/0188194	10/02/2003	Currie et al.	
	6	2005/0187740	08/25/2005	Marinescu	
	7	2006/0080637	04/13/2006	Treit et al.	
	8	2006/0272020	11/30/2006	Gardner	
	9	2007/0174429	07/26/2007	Mazzaferri et al.	
	10	2007/0220043	09/20/2007	Oliver et al.	
	11	2008/0115190	05/15/2008	Aaron	
	12	2008/0148381	06/19/2008	Aaron	
	13	2009/0089040	04/02/2009	Monastyrsky et al.	
	14	2009/0172774	07/02/2009	Kot et al.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]; Number[4]; Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

NON-PATENT LITERATURE DOCUMENTS		
Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	15	International Search Report and Written Opinion for International (PCT) Patent Application No. PCT/EP2012/052497 mailed Jul. 13, 2012 (Attorney Ref. No. 6890-89-PCT), 22 pages.
	16	International Preliminary Report on Patentability for International (PCT) Patent Application No. PCT/EP2012/052497 mailed Aug. 29, 2013 (Attorney Ref. No. 6890-89-PCT), 16 pages.
	17	"Network Security Task Manager: Manual - Installation - Configuration," A. & M. Neuber Software GmbH, 2008, 65 pages.

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*				Application Number	13/372,375
				Filing Date	February 13, 2012
				First Named Inventor	Melvyn Morris
				Art Unit	2431
				Examiner Name	Jason Chiang
Sheet	2	of	2	Attorney Docket Number	6890-89-1

	18	CHACKSFIELD, "Facebook apps ask for your permission before data mining," TechRadar.com, Jul. 1, 2010 [retrieved on 6/14/2013], 5 pages. Retrieved from: www.techradar.com/us/news/broadband/web/internet/facebook-apps-ask-for-your-permission-before-data-mining-700540
	19	COGSWELL et al., "RootkitRevealer v1.71," Nov. 1, 2006, [Retrieved on Jun. 29, 2012], 5 pages. Retrieved from: http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx
	20	SRINIVASAN, "Protecting Anti-Virus Software Under Viral Attacks," Master of Science thesis, Arizona State University, Aug. 2007, 82 pages.
	21	Official Action for U.S. Patent Application No. 13/372,433 mailed Aug. 9, 2013 (Attorney Ref. No. 6890-89-2), 18 pages.
	22	Official Action for U.S. Patent Application No. 13/372,439 mailed Jul. 3, 2013 (Attorney Ref. No. 6890-89-3), 16 pages.

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Electronic Patent Application Fee Transmittal

Application Number:	13372375
Filing Date:	13-Feb-2012
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Filer:	Brent Robert Lindon/David Voegtle
Attorney Docket Number:	6890-89-1

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt

EFS ID:	17746278
Application Number:	13372375
International Application Number:	
Confirmation Number:	2918
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Customer Number:	22442
Filer:	Brent Robert Lindon/David Voegtle
Filer Authorized By:	Brent Robert Lindon
Attorney Docket Number:	6890-89-1
Receipt Date:	23-DEC-2013
Filing Date:	13-FEB-2012
Time Stamp:	16:49:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$180
RAM confirmation Number	4667
Deposit Account	191970
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	6890-89-PCT_ISR_WO_07-13-2012.pdf	905907 a429961fab7ae8468f3355672aedffed700f9478	no	22
Warnings:					
Information:					
2	Non Patent Literature	6890-89-PCT_IPRP_08-29-2013.pdf	564330 52f92a2d8a50ba21c66a5aec0418780efbd6a7ca	no	16
Warnings:					
Information:					
3	Non Patent Literature	Network_Security_Task_Manager.pdf	7386820 b2a0f94cba37676baa34fa5425f41afa856fd3c4	no	65
Warnings:					
Information:					
4	Non Patent Literature	CHACKSFIELD_Facebook_apps_ask.pdf	507511 3cc2a6a604be06b79a8d4fbcc525e1793c132943	no	5
Warnings:					
Information:					
5	Non Patent Literature	COGSWELL_RootkitRevealer_v171.pdf	305515 5a73b41744b31289982cdfab23da441148bfea4a	no	5
Warnings:					
Information:					
6	Non Patent Literature	SRINIVASAN_Protecting_Anti-Virus_Software.pdf	2549166 0e5fbceb16694e331bc03aa265e0e1e6509270a9	no	82
Warnings:					
Information:					
7	Non Patent Literature	6890-89-2_OA_08-09-2013.pdf	627333 bd6cd9b0ba17e258060c39a4405f89848eb7ca27	no	18
Warnings:					
Information:					
8	Non Patent Literature	6890-89-3_OA_07-03-2013.pdf	500628 478289ef2cc42de0b135836b9aad7a217c067c3a	no	16
Warnings:					
Information:					

9		IDS_03.pdf	489423 a9b4e6229a2dd6b054af075f2091e55028b0f891	yes	5

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Transmittal Letter	1	3
Information Disclosure Statement (IDS) Form (SB08)	4	5

Warnings:

Information:

10	Fee Worksheet (SB06)	fee-info.pdf	30373 f8366902c0a102ad6169113678a1f838c90248a1	no	2

Warnings:

Information:

Total Files Size (in bytes):	13867006

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

PCT

To:
Bebbington, Nicholas
BECK GREENER
Fulwood House
12 Fulwood Place
London
WC1V 6HR
ROYAUME UNI

16 JUL 2012

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Applicant's or agent's file reference NB2/P17048WO	Date of mailing *(day/month/year)* 13 July 2012 (13-07-2012) **FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/EP2012/052497	International filing date *(day/month/year)* 14 February 2012 (14-02-2012)
Applicant PREVX LIMITED	

1. [X] The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the International Search Report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Fascimile No.: (41-22) 338.82.70

   For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 - 9.011.

2. [ ] The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. [ ] **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   [ ] the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

   [ ] no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

   Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before completion of the technical preparations for international publication (Rules 90*bis*.1 and 90*bis*.3).

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

   For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the *PCT Applicant's Guide*, National Chapters.

Name and mailing address of the International Searching Authority	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040 Fax: (+31-70) 340-3016	SOGNO-PABIS, Elzbieta Tel: +31 (0)70 340-2414

Form PCT/ISA/220 (July 2010)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
NB2/P17048WO		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/EP2012/052497	14/02/2012	15/02/2011
Applicant		
PREVX LIMITED		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 7 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

   a. With regard to the **language,** the international search was carried out on the basis of:

   [X] the international application in the language in which it was filed

   [ ] a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))

   b. [ ] This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).

   c. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. [ ] **Certain claims were found unsearchable** (See Box No. II)

3. [X] **Unity of invention is lacking** (see Box No III)

4. With regard to the **title,**

   [X] the text is approved as submitted by the applicant

   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**

   [X] the text is approved as submitted by the applicant

   [ ] the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings,**

   a. the figure of the **drawings** to be published with the abstract is Figure No. 3

   [X] as suggested by the applicant

   [ ] as selected by this Authority, because the applicant failed to suggest a figure

   [ ] as selected by this Authority, because this figure better characterizes the invention

   b. [ ] none of the figures is to be published with the abstract

Sophos Ex. 1002
Page 217 of 683

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2012/052497

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☒ No protest accompanied the payment of additional search fees.

Sophos Ex. 1002
Page 218 of 683

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2012/052497

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007/016953 A1 (MORRIS MELVYN [GB] ET AL) 18 January 2007 (2007-01-18) cited in the application paragraph [0001] - paragraph [0144]	1-25, 31-35
A	EP 1 315 066 A1 (BRITISH TELECOMM [GB]) 28 May 2003 (2003-05-28) the whole document	1-25, 31-35
X	US 2006/080637 A1 (TREIT RANDAL P [US] ET AL) 13 April 2006 (2006-04-13) paragraph [0008] - paragraph [0012] paragraph [0018] - paragraph [0034] -/--	21, 26-31, 36-40

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 June 2012	13/07/2012

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Pinto, Raúl

3

Form PCT/ISA/210 (second sheet) (April 2005)

Sophos Ex. 1002
Page 219 of 683

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007/220043 A1 (OLIVER IAN [AU] ET AL) 20 September 2007 (2007-09-20) paragraph [0013] - paragraph [0235] -----	21, 26-31, 36-40
X	US 2005/187740 A1 (MARINESCU ADRIAN M [US]) 25 August 2005 (2005-08-25) paragraph [0009] - paragraph [0012] paragraph [0022] - paragraph [0057] -----	41,42
X	US 2009/089040 A1 (MONASTYRSKY ALEXEY V [RU] ET AL) 2 April 2009 (2009-04-02) paragraph [0004] - paragraph [0014] paragraph [0023] - paragraph [0046] -----	41,42
X	Raghunathan Srinivasan: "PROTECTING ANTI-VIRUS SOFTWARE UNDER VIRAL ATTACKS", Arizona State University , August 2007 (2007-08), XP002678947, Retrieved from the Internet: URL:http://www.public.asu.edu/~rsriniv8/Documents/Raghunathan_MS_thesis.pdf [retrieved on 2012-06-29] Chapter 5 -----	43-47
A	Bryce Cogswell and Mark Russinovich: "Rootkit Revealer v1.71", , 1 November 2006 (2006-11-01), XP002678948, Retrieved from the Internet: URL:http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx [retrieved on 2012-06-29] First 2 paragraphs of main text. -----	43-47
X	US 6 175 869 B1 (AHUJA SUDHIR RAMAN [US] ET AL) 16 January 2001 (2001-01-16) column 2, line 15 - column 3, line 20 column 3, line 45 - column 12, line 59 -----	48-56
X	US 2007/174429 A1 (MAZZAFERRI RICHARD JAMES [AU] ET AL) 26 July 2007 (2007-07-26) paragraph [0007] - paragraph [0023] paragraph [0184] paragraph [1163] - paragraph [1166] -----	48-56
X	US 2008/148381 A1 (AARON JEFFREY [US]) 19 June 2008 (2008-06-19) paragraph [0005] - paragraph [0011] paragraph [0015] - paragraph [0047] -----	57-62
	-/--	

International application No
PCT/EP2012/052497

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2008/115190 A1 (AARON JEFFREY [US]) 15 May 2008 (2008-05-15) paragraph [0006] - paragraph [0014] paragraph [0020] - paragraph [0055] -----	57-62
A	US 2006/272020 A1 (GARDNER PHILIP B [US]) 30 November 2006 (2006-11-30) the whole document -----	57-62

3

Sophos Ex. 1002
Page 221 of 683

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2012/052497

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007016953 A1	18-01-2007	CN 101213555 A	02-07-2008
		CN 102096784 A	15-06-2011
		CN 102176224 A	07-09-2011
		EP 1899884 A2	19-03-2008
		JP 2009500706 A	08-01-2009
		US 2007016953 A1	18-01-2007
		WO 2007003916 A2	11-01-2007
EP 1315066 A1	28-05-2003	CA 2467186 A1	05-06-2003
		EP 1315066 A1	28-05-2003
		EP 1446709 A1	18-08-2004
		US 2005022014 A1	27-01-2005
		WO 03046699 A1	05-06-2003
US 2006080637 A1	13-04-2006	NONE	
US 2007220043 A1	20-09-2007	NONE	
US 2005187740 A1	25-08-2005	US 2005187740 A1	25-08-2005
		US 2008141286 A1	12-06-2008
US 2009089040 A1	02-04-2009	US 2009089040 A1	02-04-2009
		US 2009089878 A1	02-04-2009
		US 2009126015 A1	14-05-2009
		US 2009126016 A1	14-05-2009
US 6175869 B1	16-01-2001	NONE	
US 2007174429 A1	26-07-2007	CN 101410803 A	15-04-2009
		US 2007171921 A1	26-07-2007
		US 2007174410 A1	26-07-2007
		US 2007174429 A1	26-07-2007
		US 2007179955 A1	02-08-2007
		US 2007180447 A1	02-08-2007
		US 2007180448 A1	02-08-2007
		US 2007180449 A1	02-08-2007
		US 2007180450 A1	02-08-2007
		US 2007180493 A1	02-08-2007
		US 2007186212 A1	09-08-2007
		US 2007192329 A1	16-08-2007
		US 2007198656 A1	23-08-2007
US 2008148381 A1	19-06-2008	NONE	
US 2008115190 A1	15-05-2008	NONE	
US 2006272020 A1	30-11-2006	NONE	

Sophos Ex. 1002
Page 222 of 683

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-25, 31-35

   Classifying a computer object as malware

   ---

2. claims: 21, 26-31, 36-40

   Identifying malware based on rules

   ---

3. claims: 41, 42

   Monitoring objects running on a computer

   ---

4. claims: 43-47

   Operating security program on computer

   ---

5. claims: 48-56

   Connecting remote computer to a server

   ---

6. claims: 57-62

   Protecting network against malware

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/EP2012/052497	14.02.2012	15.02.2011

International Patent Classification (IPC) or both national classification and IPC
INV. G06F21/00

Applicant
PREVX LIMITED

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☒ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Fax: +31 70 340 - 3016	see form PCT/ISA/210	Pinto, Raúl Telephone No. +31 70 340-0

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

      ☐ on paper

      ☐ in electronic form

   b. (time)

      ☐ in the international application as filed

      ☐ together with the international application in electronic form

      ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. IV Lack of unity of invention

1. ☒ In response to the invitation (Form PCT/ISA/206) to pay additional fees, the applicant has, within the applicable time limit:

   ☒ paid additional fees

   ☐ paid additional fees under protest and, where applicable, the protest fee

   ☐ paid additional fees under protest but the applicable protest fee was not paid

   ☐ not paid additional fees

2. ☐ This Authority found that the requirement of unity of invention is not complied with and chose not to invite the applicant to pay additional fees.

3. This Authority considers that the requirement of unity of invention in accordance with Rule 13.1, 13.2 and 13.3 is

   ☐ complied with

   ☒ not complied with for the following reasons:

   see separate sheet

4. Consequently, this report has been established in respect of the following parts of the international application:

   ☐ all parts.

   ☒ the parts relating to claims Nos. 1-62

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-16, 18, 20-40, 43-62
	No:	Claims	17, 19, 41, 42
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-62
Industrial applicability (IA)	Yes:	Claims	1-62
	No:	Claims	

2. Citations and explanations

see separate sheet

1 . Reference is made to the following documents:

D1 US 2007/016953 A1 (MORRIS MELVYN [GB] ET AL) 18 January 2007 (2007-01-18)cited in the application

D2 EP 1 315 066 A1 (BRITISH TELECOMM [GB]) 28 May 2003 (2003-05-28)

D3 US 2006/080637 A1 (TREIT RANDAL P [US] ET AL) 13 April 2006 (2006-04-13)

D4 US 2007/220043 A1 (OLIVER IAN [AU] ET AL) 20 September 2007 (2007-09-20)

D5 US 2005/187740 A1 (MARINESCU ADRIAN M [US]) 25 August 2005 (2005-08-25)

D6 US 2009/089040 A1 (MONASTYRSKY ALEXEY V [RU] ET AL) 2 April 2009 (2009-04-02)

D7 Raghunathan Srinivasan: "PROTECTING ANTI-VIRUS SOFTWARE UNDER VIRAL ATTACKS", Arizona State University, August 2007 (2007-08), XP002678947, Retrieved from the Internet: URL:http://www.public.asu.edu/~rsriniv8/Documents/Raghunathan_MS_thesis.pdf [retrieved on 2012-06-29]

D8 Bryce Cogswell and Mark Russinovich: "Rootkit Revealer v1.71", , 1 November 2006 (2006-11-01), XP002678948, Retrieved from the Internet: URL:http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx [retrieved on 2012-06-29]

D9 US 6 175 869 B1 (AHUJA SUDHIR RAMAN [US] ET AL) 16 January 2001 (2001-01-16)

D10 US 2007/174429 A1 (MAZZAFERRI RICHARD JAMES [AU] ET AL) 26 July 2007 (2007-07-26)

D11 US 2008/148381 A1 (AARON JEFFREY [US]) 19 June 2008 (2008-06-19)

D12 US 2008/115190 A1 (AARON JEFFREY [US]) 15 May 2008 (2008-05-15)

D13 US 2006/272020 A1 (GARDNER PHILIP B [US]) 30 November 2006 (2006-11-30)

Re Item IV

Unity

2 The separate inventions/groups of inventions are:

1. claims: 1-25, 31-35

   Classifying a computer object as malware

2. claims: 21, 26-31, 36-40

   Identifying malware based on rules

3. claims: 41, 42

   Monitoring objects running on a computer

4. claims: 43-47

   Operating security program on computer

5. claims: 48-56

   Connecting remote computer to a server

6. claims: 57-62

   Protecting network against malware

They are not so linked as to form a single general inventive concept (Rule 13.1 PCT) for the following reasons.

2.1 The prior art as been identified as US 2007/0016953 A1: "Methods and Apparatus for Dealing with Malware" (D1). Document D1 discloses (references in parentheses applying to this document):

A method of classifying a computer object as malware, the method comprising:

at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored and or processed (paragraph 81);

wherein the base computer [...] receives said data from the plural remote computers and apply rules and or heuristics against that data in real time to determine whether or not said object is malware and to communicate said determination to the remote computers (paragraphs 81-83);

-said base computer [...] is arranged to receive said data about objects from [...] [the remote computers] to maintain a master database of data received about objects from all of the [...] [the remote computers] (paragraphs 81-83).

Claim 1 therefore differs from D1 in that the base computer comprises:

-plural threat servers that receive data about objects from the remote computers, and

-one central server in communication with the threat servers where the master database is maintained

The above differences solve the problem of server availability when faced with high number of requests. D1 hints this problem when in paragraphs 20 and 81 it is stated that there may be millions of remote computers connected to the base computer.

When faced with this problem the person skilled in the art (of server load/ availability in a networked environment) would choose from one of the straightforward well known solutions of providing a plurality of servers and include it with the teachings of D1 without the exertion of an inventive step. The functionality at the base computer (in D1)that deals with the reception of the data objects is replaced in a straightforward way with the plurality of threat servers.

Therefore the subject-matter of claim 1 is not inventive (Article 33(3) PCT).

2.2 The subject-matter of the first invention is set out in claims 1-8, 9-16 and 17-18, 19-20 and 21-25, 31-35.

2.2.1 An equivalent reasoning (as for claim 1 above) may be used in the analysis of independent claim 9 which is therefore also considered not inventive (Article 33(3) PCT).

2.2.2 Independent claim 17 is not new (Article 33(2) PCT) for the following reasons. Document D1 discloses (references in parenthesis applying to this document):

A method of classifying a computer object as malware, the method comprising:

at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored and or processed;

(paragraph 81)

counting the number of times in a given time period objects having one or more common attributes or behaviours that have been seen by the remote computers;

comparing the counted number with the expected number based on past observations; and,

if the comparison exceeds some predetermined threshold, flagging the objects as unsafe or as suspicious

(paragraph 101).

2.2.3 An equivalent reasoning (as for claim 17 above) may be used in the analysis of independent claim 19 which is therefore also considered not new (Article 33 (2) PCT).

2.2.4 Independent claim 21 is not inventive (Article 33(3) PCT) for the following reasons. Document D1 discloses (references in parenthesis applying to this document):

A method of classifying a computer object as malware, the method comprising:

at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored and or processed (paragraph 81);

storing said data in a database (paragraph 81).

Claim 21 therefore differs from D1 in that:

-the user is presented with a display of information relating to a group of plural objects and various attributes of those objects, the display being arranged such that commonality is shown between objects, wherein the group of objects displayed correspond to a user query of the database.

This feature is a mere presentation of information (e.g. displaying the result of a database with a grouping clause) that the person skilled in the art would implement when instructed to do so in a straightforward manner. This feature does not therefore contribute to an inventive step.

2.2.5 An equivalent reasoning (as for claim 21 above) may be used in the analysis of independent claim 31 which is therefore also considered not inventive (Article 33(3) PCT).

2.2.6 Dependent claims 2-8, 10-16, 18, 20, 22-25 and 32-35 are either also disclosed in D1 or are considered trivial and well known in the prior art (see D1-D2 and the relevant passages cited in the Search Report). Particularly in what refers to dependent claims 2-5, they define well known features of maintaining backup and/or replication servers.

2.2.7 Therefore no Special Technical Features (STFs) can be seen to make a contribution over D1 (Rule 13.1 PCT).

2.3 The subject-matter of the second invention is set out in claims 21, 26-30 and 31, 36-40.

This differs from D1 by the creation of a rule from a user query if the query identifies malware. These may be considered the Special Technical Features (STFs) of the second invention (Rule 13.1 PCT). These STFs solve the problem of "How to use user knowledge to identify malware".

2.4 The subject-matter of the third invention is set out in claims 41, 42.

This differs from D1 in that a security program is operated to impersonate the operating system. These may be considered the Special Technical Features (STFs) of the third invention (Rule 13.1 PCT). These STFs solve the problem of "How to determine whether objects are malware".

2.5 The subject-matter of the fourth invention is set out in claims 43-44, 45-47.

This differs from D1 in that a program is loaded per component. These may be considered the Special Technical Features (STFs) of the fourth invention (Rule 13.1 PCT). These STFs solve the problem of "How to execute a program if malware prevents loading".

2.6 The subject-matter of the fifth invention is set out in claims 48-51, 52-56.

This differs from D1 in that an agent runs at a remote computer to allocate it to a server. These may be considered the Special Technical Features (STFs) of the fifth invention (Rule 13.1 PCT). These STFs solve the problem of "How to allocate a remote computer to a server".

2.7 The subject-matter of the sixth invention is set out in claims 57-59, 60-62.

This differs from D1 in that an agent running at a remote computer configures a firewall according to a base computer. These may be considered the Special Technical Features (STFs) of the sixth invention (Rule 13.1 PCT). These STFs solve the problem of "Protect network communications against malware".

2.8 The STFs of the six inventions are clearly not the same. Also because they solve different (and unrelated) problems they are not corresponding as required by Rule 13.2 PCT. The application therefore lacks unity.

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

Invention 1

3 Regarding the Examination of claims 1-25, 31-35, see section 1 above.

Invention 2

4 The subject-matter of independent claim 21 is not inventive (Article 33(3) PCT) for the following reasons. Document D3 discloses (references in parenthesis applying to this document).

A method of classifying a computer object as malware, the method comprising:

at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored and or processed;

storing said data in a database (paragraph 8); and,

presenting the user with a display of information relating to a group of plural objects and various attributes of those objects, ~~the display being arranged such that commonality is shown between objects~~, wherein the group of objects displayed correspond to a user query of the database (paragraph 8).

D3 does not disclose "the display being arranged such that commonality is shown between objects". However, if "such that commonality is shown between objects" is interpreted literally this feature is a mere result to be achieved. It interpreted as the data being grouped in some predefined way, this is a well know feature on the state of the art (i.e. grouping data for display). In both cases this feature does not contribute to an inventive step.

5 An equivalent reasoning applies to the subject-matter of equivalent independent claim 31 which therefore is also not considered inventive (Article 33(3) PCT).

6 Dependent claims 26-30 and 36-40 are either also disclosed in the prior art or are considered trivial and well known in the prior art (see D3-D4 and the relevant passages cited in the Search Report). They do not therefore comply with the requirements of Article 33(3) PCT.

Invention 3

7 The subject-matter of independent claim 41 is not new (Article 33(2) PCT) for the following reasons. Document D5 discloses (references in parenthesis applying to this document).

A method of operating a security program on a computer, comprising operating the security program to impersonate or use operating system functions in monitoring objects running on the computer, said monitoring being to determine whether the objects are malware (paragraphs 9-12).

8 An equivalent reasoning applies to the subject-matter of equivalent independent claim 42 which therefore is also not considered new (Article 33(2) PCT).

9 For the sake of completeness it should be said that document D6 is also considered pertinent to the subject-matter of claims 41-42.

Invention 4

10 The subject-matter of independent claim 43 is not inventive (Article 33(3) PCT) for the following reasons. Document D7 discloses (references in parenthesis applying to this document).

A method of operating a security program on a computer, comprising:

loading a first component of the security program on the computer (sections 5.2, 5.3);

dynamically creating a second component of the security program on the computer having different attributes from the first component and which will automatically load in the event that the first component fails to ~~load~~ [run] due to malevolent activity (section 5.4, particularly last 9 lines of first paragraph; the *watch processes* will relaunch the security program).

D7 discloses the launch of another component if the first was stopped (failed to run). Claim 43 defines this action is executed if the component fails to load. This is a straightforward adaptation to a specific situation in the component execution cycle and therefore is not considered to involve an inventive step.

11 An equivalent reasoning applies to the subject-matter of equivalent independent claim 45 which therefore are is not considered inventive (Article 33(3) PCT).

12 Dependent claims 44 and 46-47 are either also disclosed in the prior art or are considered trivial and well known in the prior art (see D7-D8 and the relevant passages cited in the Search Report). They do not therefore comply with the requirements of Article 33(3) PCT.

Invention 5

13 The subject-matter of independent claim 48 is not inventive (Article 33(3) PCT) for the following reasons. Document D9 discloses (references in parenthesis applying to this document).

A method of connecting a remote computer to one of a plurality of servers, the method comprising:

installing an agent program on the remote computer (column 2, lines 21-24, implicitly disclosed);

the agent program having an algorithm for allocating the remote computer to a server ~~determined by the time when the agent program was installed~~; and,

connecting the agent program to the allocated server

(column 2, lines 15-42).

D9 does not disclose allocating the remote computer to a server according to **the time when the agent program was installed**. However D9 does disclose allocating the remote computer to a server according to different rules. The particular rule defined in D9 is a mere administrative decision which the person skilled in the art would implement when instructed to do so without an inventive step.

14 An equivalent reasoning applies to the subject-matter of equivalent independent claim 52 which therefore is also not considered inventive (Article 33(3) PCT).

15 Dependent claims 49-51 and 53-56 are either also disclosed in the prior art or are considered trivial and well known in the prior art (see D9-D10 and the relevant passages cited in the Search Report). They do not therefore comply with the requirements of Article 33(3) PCT.

Invention 6

16 The subject-matter of independent claim 57 is not inventive (Article 33(3) PCT) for the following reasons. Document D11 discloses (references in parenthesis applying to this document).

A method of providing protection against malware, the method comprising:

executing an agent program on a remote computer connected to a network, the agent program being configured to communicate with a base computer via the network (paragraph 10), the agent program ~~including~~ [downloaded to] a firewall arranged to block communications between the remote computer and entities on the network in accordance with predetermined rules (paragraph 10); and,

configuring the firewall in accordance with rules received from the base computer (paragraph 10, 37).

Document D11 does not disclose the agent program **including** a firewall. However no technical advantage can be discerned by this formulation as opposed to the one in D11 disclosing the agent being "in the" firewall.

17 An equivalent reasoning applies to the subject-matter of equivalent independent claim 60 which therefore is also not considered inventive (Article 33(3) PCT).

18 Dependent claims 58-59 and 61-62 are either also disclosed in the prior art or are considered trivial and well known in the prior art (see D11-D13 and the relevant passages cited in the Search Report). They do not therefore comply with the requirements of Article 33(3) PCT.

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING
TRANSMITTAL OF COPY OF INTERNATIONAL
PRELIMINARY REPORT ON PATENTABILITY
(CHAPTER I OF THE PATENT COOPERATION
TREATY)
(PCT Rule 44bis.1(c))

To:

BEBBINGTON, Nicholas
Fulwood House
12 Fulwood Place
London London WC1V 6HR
ROYAUME-UNI

Date of mailing *(day/month/year)* 29 August 2013 (29.08.2013)	
Applicant's or agent's file reference NB2/P17048WO	**IMPORTANT NOTICE**

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/EP2012/052497	14 February 2012 (14.02.2012)	15 February 2011 (15.02.2011)

Applicant
PREVX LIMITED et al

The International Bureau transmits herewith a copy of the international preliminary report on patentability (Chapter I of the Patent Cooperation Treaty)

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. +41 22 338 82 70

Authorized officer
Agnès Wittmann-Regis

e-mail: pt06.pct@wipo.int

Sophos Ex. 1002
Page 238 of 683

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference NB2/P17048WO	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/EP2012/052497	International filing date *(day/month/year)* 14 February 2012 (14.02.2012)	Priority date *(day/month/year)* 15 February 2011 (15.02.2011)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant PREVX LIMITED		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 15 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☒	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 21 August 2013 (21.08.2013)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerlaud Facsimile No. +41 22 338 82 70	Authorized officer Agnès Wittmann-Regis e-mail: pt06.pct@wipo.int

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/EP2012/052497	14.02.2012	15.02.2011

International Patent Classification (IPC) or both national classification and IPC
INV. G06F21/00

Applicant
PREVX LIMITED

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☒ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Fax: +31 70 340 - 3016	see form PCT/ISA/210	Pinto, Raúl Telephone No. +31 70 340-0

Sophos Ex. 1002
Page 240 of 683

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

      ☐ on paper

      ☐ in electronic form

   b. (time)

      ☐ in the international application as filed

      ☐ together with the international application in electronic form

      ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. IV Lack of unity of invention

1. ☒ In response to the invitation (Form PCT/ISA/206) to pay additional fees, the applicant has, within the applicable time limit:

   ☒ paid additional fees

   ☐ paid additional fees under protest and, where applicable, the protest fee

   ☐ paid additional fees under protest but the applicable protest fee was not paid

   ☐ not paid additional fees

2. ☐ This Authority found that the requirement of unity of invention is not complied with and chose not to invite the applicant to pay additional fees.

3. This Authority considers that the requirement of unity of invention in accordance with Rule 13.1, 13.2 and 13.3 is

   ☐ complied with

   ☒ not complied with for the following reasons:

   see separate sheet

4. Consequently, this report has been established in respect of the following parts of the international application:

   ☐ all parts.

   ☒ the parts relating to claims Nos. 1-62

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-16, 18, 20-40, 43-62
	No:	Claims	17, 19, 41, 42
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-62
Industrial applicability (IA)	Yes:	Claims	1-62
	No:	Claims	

2. Citations and explanations

   see separate sheet

1 Reference is made to the following documents:

D1 US 2007/016953 A1 (MORRIS MELVYN [GB] ET AL) 18 January 2007 (2007-01-18)cited in the application

D2 EP 1 315 066 A1 (BRITISH TELECOMM [GB]) 28 May 2003 (2003-05-28)

D3 US 2006/080637 A1 (TREIT RANDAL P [US] ET AL) 13 April 2006 (2006-04-13)

D4 US 2007/220043 A1 (OLIVER IAN [AU] ET AL) 20 September 2007 (2007-09-20)

D5 US 2005/187740 A1 (MARINESCU ADRIAN M [US]) 25 August 2005 (2005-08-25)

D6 US 2009/089040 A1 (MONASTYRSKY ALEXEY V [RU] ET AL) 2 April 2009 (2009-04-02)

D7 Raghunathan Srinivasan: "PROTECTING ANTI-VIRUS SOFTWARE UNDER VIRAL ATTACKS", Arizona State University, August 2007 (2007-08), XP002678947, Retrieved from the Internet: URL:http://www.public.asu.edu/~rsriniv8/Documents/Raghunathan_MS_thesis.pdf [retrieved on 2012-06-29]

D8 Bryce Cogswell and Mark Russinovich: "Rootkit Revealer v1.71", , 1 November 2006 (2006-11-01), XP002678948, Retrieved from the Internet: URL:http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx [retrieved on 2012-06-29]

D9 US 6 175 869 B1 (AHUJA SUDHIR RAMAN [US] ET AL) 16 January 2001 (2001-01-16)

D10 US 2007/174429 A1 (MAZZAFERRI RICHARD JAMES [AU] ET AL) 26 July 2007 (2007-07-26)

D11 US 2008/148381 A1 (AARON JEFFREY [US]) 19 June 2008 (2008-06-19)

D12 US 2008/115190 A1 (AARON JEFFREY [US]) 15 May 2008 (2008-05-15)

D13 US 2006/272020 A1 (GARDNER PHILIP B [US]) 30 November 2006 (2006-11-30)

Re Item IV

Unity

2 The separate inventions/groups of inventions are:

1. claims: 1-25, 31-35

   Classifying a computer object as malware

2. claims: 21, 26-31, 36-40

   Identifying malware based on rules

3. claims: 41, 42

   Monitoring objects running on a computer

4. claims: 43-47

   Operating security program on computer

5. claims: 48-56

   Connecting remote computer to a server

6. claims: 57-62

   Protecting network against malware

They are not so linked as to form a single general inventive concept (Rule 13.1 PCT) for the following reasons.

2.1 The prior art as been identified as US 2007/0016953 A1: "Methods and Apparatus for Dealing with Malware" (D1). Document D1 discloses (references in parentheses applying to this document):

A method of classifying a computer object as malware, the method comprising:

at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored and or processed (paragraph 81);

wherein the base computer [...] receives said data from the plural remote computers and apply rules and or heuristics against that data in real time to determine whether or not said object is malware and to communicate said determination to the remote computers (paragraphs 81-83);

-said base computer [...] is arranged to receive said data about objects from [...] [the remote computers] to maintain a master database of data received about objects from all of the [...] [the remote computers] (paragraphs 81-83).

Claim 1 therefore differs from D1 in that the base computer comprises:

-plural threat servers that receive data about objects from the remote computers, and

-one central server in communication with the threat servers where the master database is maintained

The above differences solve the problem of server availability when faced with high number of requests. D1 hints this problem when in paragraphs 20 and 81 it is stated that there may be millions of remote computers connected to the base computer.

When faced with this problem the person skilled in the art (of server load/ availability in a networked environment) would choose from one of the straightforward well known solutions of providing a plurality of servers and include it with the teachings of D1 without the exertion of an inventive step. The functionality at the base computer (in D1)that deals with the reception of the data objects is replaced in a straightforward way with the plurality of threat servers.

Therefore the subject-matter of claim 1 is not inventive (Article 33(3) PCT).

2.2 The subject-matter of the first invention is set out in claims 1-8, 9-16 and 17-18, 19-20 and 21-25, 31-35.

2.2.1 An equivalent reasoning (as for claim 1 above) may be used in the analysis of independent claim 9 which is therefore also considered not inventive (Article 33(3) PCT).

2.2.2 Independent claim 17 is not new (Article 33(2) PCT) for the following reasons. Document D1 discloses (references in parenthesis applying to this document):

A method of classifying a computer object as malware, the method comprising:

at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored and or processed;

(paragraph 81)

counting the number of times in a given time period objects having one or more common attributes or behaviours that have been seen by the remote computers;

comparing the counted number with the expected number based on past observations; and,

if the comparison exceeds some predetermined threshold, flagging the objects as unsafe or as suspicious

(paragraph 101).

2.2.3 An equivalent reasoning (as for claim 17 above) may be used in the analysis of independent claim 19 which is therefore also considered not new (Article 33 (2) PCT).

2.2.4 Independent claim 21 is not inventive (Article 33(3) PCT) for the following reasons. Document D1 discloses (references in parenthesis applying to this document):

A method of classifying a computer object as malware, the method comprising:

at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored and or processed (paragraph 81);

storing said data in a database (paragraph 81).

Claim 21 therefore differs from D1 in that:

-the user is presented with a display of information relating to a group of plural objects and various attributes of those objects, the display being arranged such that commonality is shown between objects, wherein the group of objects displayed correspond to a user query of the database.

This feature is a mere presentation of information (e.g. displaying the result of a database with a grouping clause) that the person skilled in the art would implement when instructed to do so in a straightforward manner. This feature does not therefore contribute to an inventive step.

2.2.5 An equivalent reasoning (as for claim 21 above) may be used in the analysis of independent claim 31 which is therefore also considered not inventive (Article 33(3) PCT).

2.2.6 Dependent claims 2-8, 10-16, 18, 20, 22-25 and 32-35 are either also disclosed in D1 or are considered trivial and well known in the prior art (see D1-D2 and the relevant passages cited in the Search Report). Particularly in what refers to dependent claims 2-5, they define well known features of maintaining backup and/or replication servers.

2.2.7 Therefore no Special Technical Features (STFs) can be seen to make a contribution over D1 (Rule 13.1 PCT).

2.3 The subject-matter of the second invention is set out in claims 21, 26-30 and 31, 36-40.

This differs from D1 by the creation of a rule from a user query if the query identifies malware. These may be considered the Special Technical Features (STFs) of the second invention (Rule 13.1 PCT). These STFs solve the problem of "How to use user knowledge to identify malware".

2.4 The subject-matter of the third invention is set out in claims 41, 42.

This differs from D1 in that a security program is operated to impersonate the operating system. These may be considered the Special Technical Features (STFs) of the third invention (Rule 13.1 PCT). These STFs solve the problem of "How to determine whether objects are malware".

2.5 The subject-matter of the fourth invention is set out in claims 43-44, 45-47.

This differs from D1 in that a program is loaded per component. These may be considered the Special Technical Features (STFs) of the fourth invention (Rule 13.1 PCT). These STFs solve the problem of "How to execute a program if malware prevents loading".

2.6 The subject-matter of the fifth invention is set out in claims 48-51, 52-56.

This differs from D1 in that an agent runs at a remote computer to allocate it to a server. These may be considered the Special Technical Features (STFs) of the fifth invention (Rule 13.1 PCT). These STFs solve the problem of "How to allocate a remote computer to a server".

2.7 The subject-matter of the sixth invention is set out in claims 57-59, 60-62.

This differs from D1 in that an agent running at a remote computer configures a firewall according to a base computer. These may be considered the Special Technical Features (STFs) of the sixth invention (Rule 13.1 PCT). These STFs solve the problem of "Protect network communications against malware".

2.8 The STFs of the six inventions are clearly not the same. Also because they solve different (and unrelated) problems they are not corresponding as required by Rule 13.2 PCT. The application therefore lacks unity.

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

Invention 1

3 Regarding the Examination of claims 1-25, 31-35, see section 1 above.

Invention 2

4 The subject-matter of independent claim 21 is not inventive (Article 33(3) PCT) for the following reasons. Document D3 discloses (references in parenthesis applying to this document).

A method of classifying a computer object as malware, the method comprising:

at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored and or processed;

storing said data in a database (paragraph 8); and,

presenting the user with a display of information relating to a group of plural objects and various attributes of those objects, ~~the display being arranged such that commonality is shown between objects~~, wherein the group of objects displayed correspond to a user query of the database (paragraph 8).

D3 does not disclose "the display being arranged such that commonality is shown between objects". However, if "such that commonality is shown between objects" is interpreted literally this feature is a mere result to be achieved. It interpreted as the data being grouped in some predefined way, this is a well know feature on the state of the art (i.e. grouping data for display). In both cases this feature does not contribute to an inventive step.

5 An equivalent reasoning applies to the subject-matter of equivalent independent claim 31 which therefore is also not considered inventive (Article 33(3) PCT).

6 Dependent claims 26-30 and 36-40 are either also disclosed in the prior art or are considered trivial and well known in the prior art (see D3-D4 and the relevant passages cited in the Search Report). They do not therefore comply with the requirements of Article 33(3) PCT.

Invention 3

7 The subject-matter of independent claim 41 is not new (Article 33(2) PCT) for the following reasons. Document D5 discloses (references in parenthesis applying to this document).

A method of operating a security program on a computer, comprising operating the security program to impersonate or use operating system functions in monitoring objects running on the computer, said monitoring being to determine whether the objects are malware (paragraphs 9-12).

8 An equivalent reasoning applies to the subject-matter of equivalent independent claim 42 which therefore is also not considered new (Article 33(2) PCT).

9 For the sake of completeness it should be said that document D6 is also considered pertinent to the subject-matter of claims 41-42.

Invention 4

10 The subject-matter of independent claim 43 is not inventive (Article 33(3) PCT) for the following reasons. Document D7 discloses (references in parenthesis applying to this document).

A method of operating a security program on a computer, comprising:

loading a first component of the security program on the computer (sections 5.2, 5.3);

dynamically creating a second component of the security program on the computer having different attributes from the first component and which will automatically load in the event that the first component fails to ~~load~~ [run] due to malevolent activity (section 5.4, particularly last 9 lines of first paragraph; the *watch processes* will relaunch the security program).

D7 discloses the launch of another component if the first was stopped (failed to run). Claim 43 defines this action is executed if the component fails to load. This is a straightforward adaptation to a specific situation in the component execution cycle and therefore is not considered to involve an inventive step.

11 An equivalent reasoning applies to the subject-matter of equivalent independent claim 45 which therefore are is not considered inventive (Article 33(3) PCT).

12 Dependent claims 44 and 46-47 are either also disclosed in the prior art or are considered trivial and well known in the prior art (see D7-D8 and the relevant passages cited in the Search Report). They do not therefore comply with the requirements of Article 33(3) PCT.

Invention 5

13 The subject-matter of independent claim 48 is not inventive (Article 33(3) PCT) for the following reasons. Document D9 discloses (references in parenthesis applying to this document).

A method of connecting a remote computer to one of a plurality of servers, the method comprising:

installing an agent program on the remote computer (column 2, lines 21-24, implicitly disclosed);

the agent program having an algorithm for allocating the remote computer to a server ~~determined by the time when the agent program was installed~~; and,

connecting the agent program to the allocated server

(column 2, lines 15-42).

D9 does not disclose allocating the remote computer to a server according to **the time when the agent program was installed**. However D9 does disclose allocating the remote computer to a server according to different rules. The particular rule defined in D9 is a mere administrative decision which the person skilled in the art would implement when instructed to do so without an inventive step.

14 An equivalent reasoning applies to the subject-matter of equivalent independent claim 52 which therefore is also not considered inventive (Article 33(3) PCT).

15 Dependent claims 49-51 and 53-56 are either also disclosed in the prior art or are considered trivial and well known in the prior art (see D9-D10 and the relevant passages cited in the Search Report). They do not therefore comply with the requirements of Article 33(3) PCT.

Invention 6

16 The subject-matter of independent claim 57 is not inventive (Article 33(3) PCT) for the following reasons. Document D11 discloses (references in parenthesis applying to this document).

A method of providing protection against malware, the method comprising:

executing an agent program on a remote computer connected to a network, the agent program being configured to communicate with a base computer via the network (paragraph 10), the agent program ~~including~~ [downloaded to] a firewall arranged to block communications between the remote computer and entities on the network in accordance with predetermined rules (paragraph 10); and,

configuring the firewall in accordance with rules received from the base computer (paragraph 10, 37).

Document D11 does not disclose the agent program **including** a firewall. However no technical advantage can be discerned by this formulation as opposed to the one in D11 disclosing the agent being "in the" firewall.

17 An equivalent reasoning applies to the subject-matter of equivalent independent claim 60 which therefore is also not considered inventive (Article 33(3) PCT).

18 Dependent claims 58-59 and 61-62 are either also disclosed in the prior art or are considered trivial and well known in the prior art (see D11-D13 and the relevant passages cited in the Search Report). They do not therefore comply with the requirements of Article 33(3) PCT.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of:	)	Group Art Unit: 2431
Melvyn Morris	)	Confirmation No.: 2918
Serial No.: 13/372,375	)	Examiner: Jason Chiang
Filed: February 13, 2012	)	SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT
Atty. File No.: 6890-89-1	)	
Entitled: "Methods and Apparatus for Dealing with Malware"	)	*Electronically Submitted*

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

The references cited on attached Form PTO/SB08 are being called to the attention of the Examiner.

☒ Copies of the cited non-patent and/or foreign references are enclosed herewith.

☐ Copies of the cited U.S. patents and/or patent applications are enclosed herewith.

☒ Copies of the cited U.S. patents/patent application publications are not enclosed in accordance with 37 C.F.R. § 1.98(a).

☐ Copies of the cited references are not enclosed, in accordance with 37 C.F.R. § 1.98(d), because the references were cited by or submitted to the U.S. Patent and Trademark Office in prior application Serial No. _____ filed _____, which is relied upon for an earlier filing date under 35 U.S.C. § 120.

☐ To the best of applicants' belief, the pertinence of the foreign-language references is believed to be summarized in the attached English abstracts and/or in the figures, although applicants do not necessarily vouch for the accuracy of the translation.

☐ Examiner's attention is drawn to the following related applications:

Serial No. _____ filed _____ (Attorney Ref. No. _____)

Serial No. _____ filed _____ (Attorney Ref. No. _____)

☐ Other:_____

Submission of the above information is not intended as an admission that any item is citable under the statutes or rules to support a rejection, that any item disclosed represents analogous art, or that those skilled in the art would refer to or recognize the pertinence of any reference without the benefit of hindsight, nor should an inference be drawn as to the pertinence

Sophos Ex. 1002
Page 254 of 683

of the references based on the order in which they are presented. Submission of this statement should not be taken as an indication that a search has been conducted, or that no better art exists.

It is respectfully requested that the cited information be expressly considered during the prosecution of this application and the references made of record therein.

FEES

☐	**37 CFR 1.97(b)**: No fee is believed due in connection with this submission, because the information disclosure statement submitted herewith is satisfied by one of the following conditions ("X" indicates satisfaction): ☐ Within three months of the filing date of a national application other than a continued prosecution application under 37 CFR 1.53(d), or ☐ Within three months of the date of entry of the national stage as set forth in § 1.491 in an international application, or ☐ Before the mailing date of a first Office Action on the merits, or ☐ Before the mailing of a first Office action after the filing of a request for continued examination under 37 CFR 1.114. Although no fee is believed due, if any fee is deemed due in connection with this submission, please charge such fee to Deposit Account 19-1970.
☒	**37 CFR 1.97(c)**: The information disclosure statement transmitted herewith is being filed after all the above conditions (37 CFR 1.97(b)), but before the mailing date of any one of the following conditions: (1) a final action under 37 C.F.R. 1.113, or (2) a notice of allowance under 37 C.F.R. 1.311, or (3) an action that otherwise closes prosecution in the application. This Information Disclosure Statement is accompanied by: ☐ A Certification (below) as specified by 37 C.F.R. 1.97(e). Although no fee is believed due, if any fee is deemed due in connection with this submission, please charge such fee to Deposit Account 19-1970. OR ☒ Please charge Deposit Account 19-1970 in the amount of $180.00 for the fee set forth in 37 C.F.R. 1.17(p) for submission of an information disclosure statement. Please credit any overpayment or charge any underpayment to Deposit Account 19-1970.
☐	**37 CFR 1.97(d)**: This Information Disclosure Statement is being submitted after the period specified in 37 CFR 1.97(c). ☐ This information Disclosure Statement includes a Certification (below) as specified by 37 C.F.R. 1.97(e) AND ☐ Applicants hereby requests consideration of the reference(s) disclosed herein. Please charge Deposit Account 19-1970 in the amount of $180.00 under 37 C.F.R. 1.17(p). Please credit any overpayment or charge any underpayment to Deposit Account 19-1970. Election to pay the fee should not be taken as an indication that applicant(s) cannot execute a certification.

Sophos Ex. 1002
Page 255 of 683

Certification (37 C.F.R. 1.97(e))
(Applicable only if checked)

☐ The undersigned certifies that:

☐ Each item of information contained in this information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this statement. 37 C.F.R. 1.97(e)(1).

☐ A copy of the communication from the foreign patent office is enclosed.

OR

☐ No item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned after making reasonable inquiry, no item of information contained in this Information Disclosure Statement was known to any individual designated in 37 C.F.R. 1.56(c) more than three months prior to the filing of this statement. 37 C.F.R. 1.97(e)(2).

Respectfully submitted,

SHERIDAN ROSS P.C.

By: /Brent R. Lindon/ BL

Brent R. Lindon
Registration No. 67424
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: 12/23/2013

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/372,375	02/13/2012	Melvyn Morris	6890-89-1	2918

22442 7590 01/06/2014

Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

EXAMINER	
CHIANG, JASON	
ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
01/06/2014	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

e-docket@sheridanross.com

Office Action Summary	Application No. 13/372,375	Applicant(s) MORRIS ET AL.	
	Examiner JASON C. CHIANG	Art Unit 2431	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/17/2013*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-7 and 9-15* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-7 and 9-15* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

1. The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

2. This action is in response to the Amendment filed on 10/17/2013.

3. Claims 1-7 and 9-15 are under examination. Claims 8 and 16 have been cancelled. Claims 1 and 9 have been amended.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1, 9, 14-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boisjolie et al. (US 8,332,946 B1), Meyer et al. (US 2011/0191341 A1) and Quinlan (US 7921063 B1).

Regarding claim 1, Boisjolie et al. discloses:

A method of classifying a computer object as malware **[Abstract, "The malware-protection method employs a number of techniques and relies on multiple layers of protection to identify trusted files, prevent execution of untrustworthy files, accurately detect corrupted files, analyze questionable files, and quarantine files"]**, the method comprising:

at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored or processed **[Col. 4, lines 53-64, "At STEP 2, a new file from an external source enters the endpoint 102. One of ordinary skill in the art will recognize that the new file may be of a variety of types, including, for example, audio, video, multi-media, text, executable, archives, HTML, and the like. Other types for the new file, other than those listed herein, will be apparent to one of ordinary skill in the art. From STEP 2, the method 100 proceeds to STEP 3. At STEP 3, a fingerprint for the new file (i.e., a new-file fingerprint) is created by the endpoint 102 and the new-file fingerprint is sent to application-verification servers 104 for verification"]**;

wherein the base computer comprises plural threat servers arranged to receive the data from the plural remote computers and apply rules or heuristics against the data in real time to determine whether or not the object is malware and to communicate the determination to the remote computers **[Col. 5, lines 4-7, "At STEP 4, the application verification servers 104 attempt to verify the new-file fingerprint against an application-data-signature whitelist in data communication with the application-verification servers 104", lines 30-37, "At STEP 5, if the verification of the new-file**

fingerprint in STEP 4 returns that the new file cannot be identified as either good or bad (i.e., is unknown), the new file is sent from the endpoint 102 to malware-scan servers 106 for scanning Various scanning techniques are typically used to detect malware such as, for example, traditional virus-signature-based definition comparison, heuristics, sandbox emulation, analysis, and prediction, and the like.", Fig. 1, Backend identifies threat and notifies client];

maintaining on at least one of a first of the threat servers, a list of objects previously seen at the first threat server and previous forwarded to the central server **[Col. 5, lines 19-21, "In a typical embodiment, the application-verification servers 104 list a disposition for the new-file fingerprint that includes, for example, good, bad/not good, and unknown"]**.

determining whether the computer object has been seen before **[Col. 5, lines 4-7, "At STEP 4, the application verification servers 104 attempt to verify the new-file fingerprint against an application-data -signature whitelist in data communication with the application-verification servers 104"]**; sending the data about the object from the first threat server to the central server when the object has not been seen before **[Col. 5, lines 30-33, "At STEP 5, if the verification of the new-file fingerprint in STEP 4 returns that the new file cannot be identified as either good or bad (i.e., is unknown), the new file is sent from the endpoint 102 to malware-scan servers 106 for scanning"]**;

Boisjolie et al. does not explicitly disclose the base computer further comprising at least one central server in communication with the threat servers and arranged to

receive the data about objects from the threat servers to maintain a master database of data received about objects from all threat servers.

However, Meyer et al. in the field relates to systems and methods for sharing the results of computing operations (such as malware or data-loss-prevention scans) performed on shared or common files among related computing systems teaches the base computer further comprising at least one central server in communication with the threat servers and arranged to receive the data about objects from the threat servers to maintain a master database of data received about objects from all threat servers **[Paragraph 0029, "Shared store 216 generally represents any type or form of physical or virtualized storage that may be shared or accessed by a group of related computing systems, such as virtual machines 202(1)-(N) in FIG. 2. In some examples, shared store 216 may contain or comprise a file-attribute database (such as file-attribute database 120 in FIGS. 1 and 5) that may contain, for each of a plurality of files encountered by a group of computing systems (such as virtual machines 202(1)-(N)): 1) a hash of the file, 2) the results of at least one computing operation performed in connection with the file (such as a classification assigned to the file during a malware analysis, at least one rationale for the classification assigned to the file during the malware analysis, at least one virus definition set or heuristic used when performing the malware analysis, or the like), 3) the date of at least one computing operation performed in connection with the file (such as the date of the most-recent malware scan performed on the file), and/or 4) any**

other potentially useful information that may be shared among related computing systems"].

At the time of the invention, it would have been obvious to a person having ordinary skill in the art to incorporate the teaching of Meyer et al. into the teaching of Boisjolie et al. with the motivation of sharing the results of computing operations among related computing systems as taught by Meyer et al. **[Meyer et al.: abstract]**.

Both Boisjolie et al. and Meyer et al. do not teach increasing a count associated with the number of times that the data about the computer object has been seen, when the data about the computer object has been seen before.

However, Quinlan in the field relates to network data communications teaches increasing a count associated with the number of times that the data about the computer object has been seen, when the data about the computer object has been seen before **[Col. 6, lines 10-15, "threat information source 104 generates counts of received messages that have suspicious attachments, and provides the counts to threat information processor 108, or allows an external process to retrieve the counts and store them in a specialized database"]**.

At the time of the invention, it would have been obvious to a person having ordinary skill in the art to incorporate the teaching of Quinlan into the teaching of Boisjolie et al., and Meyer et al. with the motivation for use in managing computer virus outbreaks as taught by Quinlan **[Quinlan: col. 6, lines 6-15]**.

Regarding claim 9, it recites similar limitations as of claim 1. The reasons for the rejection of claim 1 are incorporated herein.

Regarding claim 14, the rejection of claim 9 is incorporated.

Boisjolie et al. discloses a method of classifying a computer object as malware.

Meyer et al. further discloses the central server has databases including at least one of a) object signatures and metadata about that object; b) object behavior; and c) information about what objects are present on what remote computers **[Paragraph 0029, "Shared store 216 generally represents any type or form of physical or virtualized storage that may be shared or accessed by a group of related computing systems, such as virtual machines 202(1)-(N) in FIG. 2. In some examples, shared store 216 may contain or comprise a file-attribute database (such as file-attribute database 120 in FIGS. 1 and 5) that may contain, for each of a plurality of files encountered by a group of computing systems (such as virtual machines 202(1)-(N)): 1) a hash of the file, 2) the results of at least one computing operation performed in connection with the file (such as a classification assigned to the file during a malware analysis, at least one rationale for the classification assigned to the file during the malware analysis, at least one virus definition set or heuristic used when performing the malware analysis, or the like), 3) the date of at least one computing operation performed in connection with the file (such as the date of the most-recent malware scan performed on the file), and/or 4) any other potentially useful information that may be shared among related computing systems"]**.

At the time of the invention, it would have been obvious to a person having ordinary skill in the art to incorporate the teaching of Meyer et al. into the teaching of

Boisjolie et al. with the motivation of sharing the results of computing operations among related computing systems as taught by Meyer et al. **[Meyer et al.: abstract]**.

Regarding claim 15, the rejection of claim 14 is incorporated.

Boisjolie et al. further discloses the threat and central servers are implemented using cloud computing **[Col. 2, lines 28-30, "Responsive to a determined status of unknown in response to a malware scan, the new file is sent to a cloud-based malware-scanning engine"]**.

6. Claims 2-3, 6-7 and 10-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boisjolie et al. (US 8,332,946 B1), Meyer et al. (US 2011/0191341 A1) and Quinlan (US 7921063 B1) as applied to claims 1, 9, 14-15, and in view of Nishikawa et al. (US 2003/0093429 A1).

Regarding claim 2, the rejection of claim 1 is incorporated.

Boisjolie et al. further discloses at least one threat server comprises at least one database for holding information received from remote computers to which it is attached, the method comprising storing the data in at least one database at the threat server **[Col. 4, lines 61-64, "At STEP 3, a fingerprint for the new file (i.e., a new-file fingerprint) is created by the endpoint 102 and the new-file fingerprint is sent to application-verification servers 104 for verification", Fig. 1, Application database]**;

Meyer et al. discloses the server in communication with the threat servers and arranged to receive the data about objects from the threat servers to maintain a master database of data received about objects from all threat servers with timestamp **[Fig. 5]**.

Quinlan discloses a count associated with the number of times that the data about the computer object has been seen.

They do not teach at intervals, storing the contents of the database in storage and clearing the database.

Nishikawa et al. in the field relates to a data storage system teaches at intervals, storing the contents of the database in storage and clearing the database **[Paragraph 0030, "The server 102 is referred to as a "dynamic database server," in part, because it is updated with new data or records that have been inputted into the saving job DB 118 since the last batch process. Accordingly, the server 102 has more current data than the DWH server 105 that receives data periodically from the batch extraction step 119. As used herein, the term "dynamic database" is a database that is stored with data more recent than the DWH. In the present embodiment, the dynamic database is a temporarily database that is periodically purged of redundant or old data that have been copied into the DWH"]**.

At the time of the invention, it would have been obvious to a person having ordinary skill in the art to incorporate the teaching of Nishikawa et al. into the teaching of Boisjolie et al., Meyer et al. and Quinlan with motivation to allow the system to delete old data and save new records **[Nishikawa et al.: Paragraph 0033]**.

Regarding claim 3, the rejection of claim 2 is incorporated.

Boisjolie et al. discloses a method of classifying a computer object as malware.

Meyer et al. further discloses the method according to claim 2 comprising creating a backup central server by receiving at a central server all of the time-stamped

blocks of data and incorporating them into its database **[Paragraph 0029, "Shared store 216 generally represents any type or form of physical or virtualized storage that may be shared or accessed by a group of related computing systems, such as virtual machines 202(1)-(N) in FIG. 2. In some examples, shared store 216 may contain or comprise a file-attribute database (such as file-attribute database 120 in FIGS. 1 and 5) that may contain, for each of a plurality of files encountered by a group of computing systems (such as virtual machines 202(1)-(N)): 1) a hash of the file, 2) the results of at least one computing operation performed in connection with the file (such as a classification assigned to the file during a malware analysis, at least one rationale for the classification assigned to the file during the malware analysis, at least one virus definition set or heuristic used when performing the malware analysis, or the like), 3) the date of at least one computing operation performed in connection with the file (such as the date of the most-recent malware scan performed on the file), and/or 4) any other potentially useful information that may be shared among related computing systems", Fig. 5]**.

At the time of the invention, it would have been obvious to a person having ordinary skill in the art to incorporate the teaching of Meyer et al. into the teaching of Boisjolie et al. with the motivation of sharing the results of computing operations among related computing systems as taught by Meyer et al. **[Meyer et al.: abstract]**.

Regarding claim 6, the rejection of claim 2 is incorporated.

Boisjolie et al. discloses a method of classifying a computer object as malware.

Meyer et al. further discloses the central server has databases including at least one of a) object signatures and metadata about that object; b) object behavior; and c) information about what objects are present on what remote computers **[Paragraph 0029, "Shared store 216 generally represents any type or form of physical or virtualized storage that may be shared or accessed by a group of related computing systems, such as virtual machines 202(1)-(N) in FIG. 2. In some examples, shared store 216 may contain or comprise a file-attribute database (such as file-attribute database 120 in FIGS. 1 and 5) that may contain, for each of a plurality of files encountered by a group of computing systems (such as virtual machines 202(1)-(N)): 1) a hash of the file, 2) the results of at least one computing operation performed in connection with the file (such as a classification assigned to the file during a malware analysis, at least one rationale for the classification assigned to the file during the malware analysis, at least one virus definition set or heuristic used when performing the malware analysis, or the like), 3) the date of at least one computing operation performed in connection with the file (such as the date of the most-recent malware scan performed on the file), and/or 4) any other potentially useful information that may be shared among related computing systems"]**.

At the time of the invention, it would have been obvious to a person having ordinary skill in the art to incorporate the teaching of Meyer et al. into the teaching of Boisjolie et al. with the motivation of sharing the results of computing operations among related computing systems as taught by Meyer et al. **[Meyer et al.: abstract]**.

Regarding claim 7, the rejection of claim 2 is incorporated.

Boisjolie et al. further discloses the threat and central servers are implemented using cloud computing **[Col. 2, lines 28-30, "Responsive to a determined status of unknown in response to a malware scan, the new file is sent to a cloud-based malware-scanning engine"]**.

Regarding claim 10, it recites similar limitations as of claim 2. The reasons for the rejection of claim 2 are incorporated herein.

Regarding claim 11, it recites similar limitations as of claim 3. The reasons for the rejection of claim 3 are incorporated herein.

7. Claims 4 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boisjolie et al. (US 8,332,946 B1), Meyer et al. (US 2011/0191341 A1), Quinlan (US 7921063 B1) and Nishikawa et al. (US 2003/0093429 A1) as applied to claims 2-3, 6-7 and 10-11, and in view of Chen et al. (US 2009/0070304).

Regarding claim 4, the rejection of claim 2 is incorporated.

Boisjolie et al. discloses a method of classifying a computer object as malware.

Meyer et al. discloses creating a backup central server by receiving at a central server all of the time-stamped blocks of data and incorporating them into its database.

Quinlan discloses a count associated with the number of times that the data about the computer object has been seen.

Nishikawa et al. teaches at intervals, storing the contents of the database in storage and clearing the database.

They do not teach taking a central server off-line for a period of time such that it does not receive updates of data from the threat servers during that period of time; after the period of time has elapsed, updating the database of the central server with time-stamped blocks of data from the storage that have a timestamp later than the time when the central server went off-line; and bringing the central server back on line.

However, Chen in the field relates to database systems teaches taking a central server off-line for a period of time such that it does not receive updates of data from the threat servers during that period of time; after the period of time has elapsed, updating the database of the central server with time-stamped blocks of data from the storage that have a timestamp later than the time when the central server went off-line; and bringing the central server back on line **[Paragraph 0004, "Applications commonly use this timestamp column for controlling optimistic locking schemes as follows: the application retrieves one or more rows from the table, including the timestamp column; the application logically or physically disconnects from the database system; the application makes updates to the rows that were retrieved from the database; and sometime later, the application reconnects to the database so that it can record the updates in the database"]**.

At the time of the invention, it would have been obvious to a person having ordinary skill in the art to incorporate the teaching of Chen et al. into the teaching of Boisjolie et al., Meyer et al., Quinlan and Nishikawa et al. with the motivation of ensuring data consistency **[Chen et al.: paragraph 0003]**.

Regarding claim 12, it recites similar limitations as of claim 4. The reasons for the rejection of claim 4 are incorporated herein.

8. Claims 5 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boisjolie et al. (US 8,332,946 B1), Meyer et al. (US 2011/0191341 A1), Quinlan (US 7921063 B1) and Nishikawa et al. (US 2003/0093429 A1) as applied to claims 2-3, 6-7 and 10-11, and in view of McGrattan et al. (US 7814056 B2).

Regarding claim 5, the rejection of claim 2 is incorporated.

Boisjolie et al. discloses a method of classifying a computer object as malware.

Meyer et al. further discloses creating a backup central server by receiving at a central server all of the time-stamped blocks of data and incorporating them into its database.

Quinlan discloses a count associated with the number of times that the data about the computer object has been seen.

Nishikawa et al. teaches at intervals, storing the contents of the database in storage and clearing the database.

They do not teach rolling back the database of a central server to a point of time in the past; updating the database of the central server with time-stamped blocks of data from storage that have a timestamp later than the past point of time; and bringing the central server back on line.

However McGrattan et al. in the field relates to storage backup teaches rolling back the database of a central server to a point of time in the past **[Col. 5, lines 1-13,**

"A method for restoring backup data from a database, according to one embodiment, will be described with reference to FIG. 2. The backup data is stored in the database as a plurality of data blocks. Each data block is typically stored with associated timestamp information in the database. A specification of a time to which data restoration is desired is received (step S21). The specified time is compared to timestamp information stored (step S23) for each of the data blocks of the backup data in the database. A selected data block of the backup data is retrieved if the selected data block has a timestamp at or earlier than the specified time and no other data blocks of the backup data which correspond to the selected data block have more contemporaneous timestamps between the specified time and the associated timestamp of the selected data block (step S25)"]; updating the database of the central server with time-stamped blocks of data from storage that have a timestamp later than the past point of time; and bringing the central server back on line **[Col. 9, lines 4-34, "When a request for the operation "refresh object" is received, process software 602 collects the latest timestamps associated with the objects in the specified object set and correlates them to the data block digests for each data block in each of the objects of the object set (step S1). A list of the data block digests for the entire specified object set 901 is compiled and sorted in order of an object system directories walk-through (for example, data block digests are collected block-by-block for each object in the object set, and the collected data block digests are sorted) and is then sent to object system agent 601 (step S91). Object attributes are then read from Object**

system 600 for the object to be "refreshed" (step S92). The modification date of the object to be "refreshed" is compared to the timestamp information for the stored objects. If the modification date is higher than the latest timestamp for the object, then the object is read (step S92). For every block of size n in the object, a new data block digest is generated and compared against the ones in the list received by object system agent 601 at step 91 (step S93). If the data block digests are not equivalent, then the data block and the generated data block digest are both sent to process software 602 (step S94). If the data block digests are equivalent, then the data block is dropped and the system proceeds to the next block (step S94). Once process software 602 receives the new data blocks, it sends the metadata for the data blocks to database server 603 to be cataloged in database catalog 604 (step S95b) and the data block and data block digest are forwarded to media server 605 to be stored in database 609 (step S95b)", Col. 1, lines 21-43, "Enterprises and individuals who use computers that contain critical data, need disaster recovery plans in place in the event of a disaster, in order to safeguard vital information stored on the computers. Even in non-disaster situations, in which users may just want to archive their information, it is beneficial to implement "backup" and recovery plans", "A partial backup can be either differential, in which all of the files that were changed since the last complete backup are considered, or incremental, in which all of the files that were changed since the last backup are considered, or user-defined, in which only sets of files specified by a user are considered"].

At the time of the invention, it would have been obvious to a person having ordinary skill in the art to incorporate the teaching of McGrattan et al. into the teaching of Boisjolie et al., Meyer et al., Quinlan and Nishikawa et al. with the motivation of able to restoring backup data from a database by using the timestamp as taught by McGrattan et al. **[McGrattan et al.: abstract]**.

Regarding claim 13, it recites similar limitations as of claim 5. The reasons for the rejection of claim 5 are incorporated herein.

Response to Arguments

9. Applicant's arguments, filed on 10/17/2013, with respect to rejection under 35 USC § 103(a) have been fully considered but they are not persuasive.

Independent claims 1 and 9 have been amended with additional limitations: "maintaining on at least one of a first of the threat servers, a list of objects previously seen at the first threat server and previous forwarded to the central server; determining whether the computer object has been seen before; sending the data about the object from the first threat server to the central server when the object has not been seen before; and increasing a count associated with the number of times that the data about the computer object has been seen, when the data about the computer object has been seen before ."

Applicant argues that Boisjolie, Meyer, and Quinlan, taken alone, or in any combination, do not teach or render these features.

In response, the Examiner respectfully disagrees. Boisjolie discloses the application verification server (threat server) maintaining a list of known objects identified as good or bad. When a new object is sent to application verification server for verification, the application verification server verifies the object against with that list. It will forward the object to the malware scan server if the object cannot be identified as either good or bad. The list is updated with threat information after the malware scan server determines whether a malware threat exists (Col. 5, line 4-37, Fig. 1). Meyer et al. discloses a central server comprising a database which contain objects related to malware analysis (Paragraph 0029). Quinlan discloses generating counts of received messages that have suspicious attachments (Col. 6, lines 10-15). At the time of the invention, it would have been obvious to a person having ordinary skill in the art to incorporate the teaching of Quinlan into the teaching of Boisjolie et al., and Meyer et al. with the motivation of managing computer virus outbreaks as taught by Quinlan (Quinlan: col. 6, lines 6-15).

Therefore, the Examiner respectfully submits that the combination of Boisjolie, Meyer et al. and Quinlan teach/suggest these features.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to Applicant's disclosure:

US 8195938 B2 Cloud-based application whitelisting

US 8296178 B2 Services using globally distributed infrastructure for secure content management

US 7231440 B1 System and method for distributing portable computer virus definition records with binary file conversion

US 8347386 B2 System and method for server-coupled malware prevention

US 8448243 B1 Systems and methods for detecting unknown malware in an executable file

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JASON C. CHIANG whose telephone number is (571)270-3393. The examiner can normally be reached on 9AM to 6PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, CORDELIA P. ZECHER can be reached on (571)272-7771. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/J. C. C./
Examiner, Art Unit 2431

/CAROLYN B KOSOWSKI/
Primary Examiner, Art Unit 2431

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L4	9	(Melvyn near Morris).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:29
L5	3	(Joseph near Jaroch).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:30
L6	813	((increas$4 add$3 generat$4) near (count)) and (malware threat)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:31
L7	742	((increas$4 add$3 generat$4) near (count)) and (malware threat) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:32
L8	0	(((seen identified) near (before previous)) with (increas$4 add$3 generat$4) near (count)) and (malware threat) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:33
L9	0	(((seen identified) near (before previous)) same ((increas$4 add$3 generat$4) near (count))) and (malware threat) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:33
L10	48	(((seen identified)) same ((increas$4 add$3 generat$4) near (count))) and (malware threat) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:33
S1	9	(Melvyn near Morris).in.	US-PGPUB;	OR	ON	2013/06/04

			USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			11:48
S2	3	(Joseph near Jaroch).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 16:51
S3	108	(Webroot).as.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 16:54
S5	0	S3 and cloud and database and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 16:58
S6	2980	(726/23).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/06/04 17:04
S7	72	S6 and cloud and database and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 17:05
S8	54	("20100043072" | "20110197272" | "20090300764" | "20100064368" | "20120017200" | "20060101334" | "20090292791" | "20100306851" | "20110138361" | "8042184" | "20060069912" | "20120260304" | "7707634" | "7343626" | "20070016953" | "20110197177" | "20120266208" | "20060117055" | "20100313183" | "20110083183" | "8146135" | "8307435").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/05 11:39
S9	21	("2006/0069912").URPN.	USPAT	OR	ON	2013/06/05 11:59
S10	17	threat adj server	USPAT	OR	ON	2013/06/05 12:20
S11	2362	cloud and signature	USPAT	OR	ON	2013/06/05 13:23
S12	1181	cloud and signature and layer	USPAT	OR	ON	2013/06/05 13:23
S13	249	cloud and (signature with database)	USPAT	OR	ON	2013/06/05 13:25
S14	78	cloud and (signature with database) and (malware	USPAT	OR	ON	2013/06/05

		virus)				13:26
S15	143	cloud and (updat$4 near3 (signature database)) and (malware virus)	USPAT	OR	ON	2013/06/05 16:30
S16	65	(updat$4 near3 (signature database) near3 (interval certain period periodic)) and (malware virus)	USPAT	OR	ON	2013/06/05 20:09
S17	1	(09/740294).APP.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/06/05 20:37
S18	0	("(masteradjdatabase)and(virusmalwaresignature)").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/06/07 18:03
S19	1003	(master adj database) and (virus malware signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:04
S20	160	(master adj database) and (virus malware) and signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:05
S21	971	(database) and (virus near signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:33
S22	639	((stor$4 sav$4 receiv$5) with database) and (virus near signature) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:51
S23	594	((stor$4 sav$4 receiv$5) near5 database) and (virus near signature) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:51
S24	64	((stor$4 sav$4 receiv$5) near5 database) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2013/06/08 10:51

			IBM_TDB			
S25	0	((stor$4 sav$4 receiv$5) near3 content near3 database near3 storage) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:02
S26	0	((stor$4 sav$4 receiv$5) near3 database near3 storage) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:03
S27	2	((stor$4 sav$4 receiv$5) near3 content near3 database near3 storage) with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:03
S28	0	((backup) near3 database) with timestamp and (virus malware)and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:05
S29	0	((backup) near3 database) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:06
S30	27	((backup) near3 database) with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:06
S31	1139	((copy stor$4) near3 database) with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:20
S32	18	((copy stor$4) near3 database) with central with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:21
S33	359	((purg$4 clear$4 remov$4) near3 database near3 (period$6 every)) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS;	OR	ON	2013/06/08 11:29

			EPO; JPO; DERWENT; IBM_TDB			
S34	0	(master adj database) near2 (virus malware) near2 signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S35	0	(master adj database) near3 (virus malware) near3 signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S36	0	(master adj database) with (virus malware) with signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S37	0	(master adj database) same (virus malware) same signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S38	19	(master adj database) same (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:45
S39	15	((primary secondary) adj database) same (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:54
S40	30	((primary secondary) adj database) with (signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:57
S41	98	(master adj database) same (signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:59
S42	10	(master adj database) same (signature) and (virus malware)	US-PGPUB; USPAT;	OR	ON	2013/06/08 15:59

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S43	315	(master adj database) and (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 16:03
S44	18	(virus malware) with definition with (file database) with (cloud community share$2)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 16:21
S45	271	(update refresh recover rebuild) near3 (database) with timestamp	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 20:22
S46	4	(update refresh recover rebuild) near3 (database) with timestamp same (offline off-line (off adj line) disconnect reconnect)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 20:24
S47	1	((roll$3 adj back) near6 time) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:11
S48	7	((roll$3 adj back)) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:12
S49	11	((roll$3 adj back) rollback) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:14
S50	48	((roll$3 adj back) rollback) and ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:18

S51	21	(((roll$3 adj back) rollback) with time) and ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:23
S52	0	((restor$4) near6 time) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 11:40
S53	3	((restor$4) near6 time) and ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 11:41
S54	0	(send provid$3 transmit$4 updat$3) near3 (count near3 (threat incident)) near3 (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:01
S55	22	(send provid$3 transmit$4 updat$3) with ((count number) near3 (threat incident)) with (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:02
S56	122	(send provid$3 transmit$4 updat$3 record$4) with ((count number times) with (threat)) with (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:05
S57	635	(send provid$3 transmit$4 updat$3 record$4) with ((count number times) near5 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:08
S58	199	(send provid$3 transmit$4 updat$3 record$4) with ((count number) near5 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:09
S59	11	(send provid$3 transmit$4 updat$3 record$4) with ((count) near5 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2013/06/09 15:11

			DERWENT; IBM_TDB			
S60	43	((count) near2 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:15
S61	9	((count) near2 (threat)) and (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:15
S62	1126	(send provid$3 transmit$4 updat$3) near3 (count) near3 (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:18
S63	15	(send provid$3 transmit$4 updat$3) near3 ((increas$4 add$3) near (count)) near3 (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:20
S64	1816	((increas$4 add$3) near (count)) and (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:22
S65	27	((increas$4 add$3) near (count)) and (malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:23

EAST Search History (Interference)

< This search history is empty>

12/ 14/ 2013 4:35:35 PM
C:\ Users\ jchiang1\ Documents\ EAST\ Workspaces\ 13372375-Malware.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13372375	MORRIS ET AL.
	Examiner	Art Unit
	JASON C CHIANG	2431

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	23	06/04/2013	JC

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor search in East	06/04/2013	JC
Text search in East of USPGPUB, USPAT, USOCR, FPRS, EPO, JPO, DERWENT, IBM_TDB	06/05/2013	JC
Inventor search in East	12/14/2013	JC
Text search in East of USPGPUB, USPAT, USOCR, FPRS, EPO, JPO, DERWENT, IBM_TDB	12/14/2013	JC

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/JASON C CHIANG/ Examiner.Art Unit 2431	

Sophos Ex. 1002
Page 287 of 683

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13372375	MORRIS ET AL.
	Examiner	**Art Unit**
	JASON C CHIANG	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/09/2013	12/14/2013							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	-							
	9	✓	✓							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16	✓	-							
	17	N	N							
	18	N	N							
	19	N	N							
	20	N	N							
	21	N	N							
	22	N	N							
	23	N	N							
	24	N	N							

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/372,375	02/13/2012	Melvyn Morris	6890-89-1	2918

22442 7590 04/04/2014

Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

EXAMINER	
CHIANG, JASON	
ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
04/04/2014	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

e-docket@sheridanross.com

Applicant-Initiated Interview Summary	Application No.	Applicant(s)	
	13/372,375	MORRIS ET AL.	
	Examiner	Art Unit	
	JASON C. CHIANG	2431	

All participants (applicant, applicant's representative, PTO personnel):

(1) *JASON C. CHIANG*. (3)_____.

(2) *Brent R. Lindon*. (4)_____.

Date of Interview: *24 March 2014*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1*.

Identification of prior art discussed: *Boisjolie, Meyer, Quinlan, etc.,*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicant's representative and Examiner discussed the differences between the invention and the prior arts. The Examiner will reconsider the rejection in light of any newly submitted RCE with amendments to further clarify the claimed invention.

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/JASON C CHIANG/ Examiner, Art Unit 2431	

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	13/372,375	Filing Date	2012-02-13	Docket Number (if applicable)	6890-89-1	Art Unit	2413
First Named Inventor	Melvyn MORRIS			Examiner Name	CHIANG, JASON		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☐ Other _____

☒ Enclosed

- ☒ Amendment/Reply
- ☐ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☒ Other Petition for Extension of Time - 1 month

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____ (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 191970

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

☐ Applicant Signature

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/Brent R. Lindon/	Date (YYYY-MM-DD)	2014-05-06
Name	Brent R. Lindon	Registration Number	67424

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.: 13/372,375	)	Confirmation No.: 2918
Applicant: Melvyn MORRIS	)	TC/A.U.: 2413
Filed: February 13, 2012	)	Examiner: CHIANG, JASON
Docket No.: 6890-89-1	)	***Filed Electronically***
For: "METHODS AND APPARATUS FOR DEALING WITH MALWARE"	)	

AMENDMENT AND RESPONSE

Mailstop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Commissioner:

Applicant submits this Amendment and Response to address the Office Action having a mailing date of June 17, 2013. Submitted herewith is a Request for Continued Examination and a Petition for a one month Extension of Time along with the requisite fees. Although Applicant believes that no additional fees are due in connection with filing this Amendment and Response, please charge any fees deemed necessary to Deposit Account No. 19-1970.

Please amend the above-identified patent application as follows:

Amendments to the Claims are shown in the listing of claims which begins on page **2** of this paper.

Remarks begin on page **7** of this paper.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of classifying a computer object as malware, the method comprising:

~~at a base computer,~~ receiving, at a first threat server, details of ~~data about~~ a first computer object from ~~each of plural~~a first remote computer~~computers~~, wherein the details of ~~on which~~ the first computer object include data uniquely identifying the ~~or similar objects are stored or processed~~first computer object;

determining, by the first threat server, whether the first computer object has been previously seen by comparing the data uniquely identifying the first computer object to a plurality of data uniquely identifying plural computer objects in a first database associated with the first threat server;

receiving additional information about the first computer object from the first remote computer when the first computer object has not been previously seen;

storing the details of the first computer object and the received additional information about the first computer object in a second database associated with the first threat server when the first computer object has not been previously seen;

providing contents of the second database to at least one database associated with a central server;~~wherein the base computer comprises plural threat servers arranged to receive the data from the plural remote computers and apply rules or heuristics against the data in real time to determine whether or not the object is malware and to communicate the determination to the remote computers;~~

~~the base computer further comprising at least one central server in communication with the threat servers and arranged to receive the data about objects from the threat servers to maintain a master database of data received about objects from all threat servers;~~

~~maintaining on at least one of a first of the plural threat servers, a list of objects previously seen at the first threat server and previously forwarded to the central server;~~

~~determining whether the computer object has been seen before;~~

~~sending the data about the object from the first threat server to the central server when the object has not been seen before; and~~

increasing a count associated with ~~the~~ a number of times that the first computer object ~~data about the computer object~~ has been seen~~, when the data about the computer object has been seen before~~ and providing the increased count associated with the number of times that the first computer object has been seen to a central server; and

receiving, at a second threat server, at least a portion of the contents of the at least one database associated with the central server, wherein the at least a portion of the contents of the at least one database associated with the central server include a subset of the details of the first computer object stored in the second database.

2. (Currently Amended) The method according to claim 1, ~~wherein at least one threat server comprises at least one database for holding information received from remote computers to which it is attached, the method~~further comprising~~:~~

storing ~~the data in at least one database at the threat server; and~~ at intervals, ~~storing~~ the contents of the second database in storage together with a timestamp and clearing the second database.

3. (Currently Amended) The method according to claim 2, further comprising creating a backup central server by receiving at a second central server, all of the time-stamped blocks of data from the second database and incorporating all of the time-stamped blocks of data~~them~~ into ~~its~~ at least one database associated with the second central server.

4. (Currently Amended) The method according to claim 2, further comprising:

taking ~~a~~ the central server off-line for a period of time such that ~~it~~ the central server does not receive ~~updates of~~ data from the first and second threat servers during that period of time;

after the period of time has elapsed, updating at least one ~~the~~ database associated with ~~of~~ the central server with time-stamped blocks of data from the storage that have a timestamp later than the time when the central server went off-line; and

bringing the central server back on line.

5. (Currently Amended) The method according to claim 2, comprising:

rolling back ~~the~~ at least one database ~~of a~~associated with the central server to a point of time in the past;

updating the at least one database ~~of the~~associated with the central server with time-stamped blocks of data from storage that have a timestamp later than the past point of time; and

bringing the central server back on line.

6. (Currently Amended) The method according to claim 2, wherein the central server has one or more databases including at least one of:

a) object signatures and metadata about that object;

b) object behavior; and

c) information about what objects are present on what remote computers.

7. (Original) The method according to claim 6, wherein the threat and central servers are implemented using cloud computing.

8. (Canceled)

9. (Currently Amended) An apparatus for classifying a computer object as malware, the apparatus comprising:

a ~~base computer~~ first threat server arranged to receive ~~data~~ details~~about~~ of a computer object from ~~each of~~a first ~~plural~~ remote ~~computers~~computer, wherein the details of the first computer object include data uniquely identifying ~~on which~~ the first computer object ~~or similar objects are stored or processed,~~;

wherein the ~~base computer comprises~~ first ~~plural~~ threat ~~servers~~server is further arranged to receive the ~~data~~ details of the computer object from the first remote computer and determine whether~~from the plural remote computers and apply rules or heuristics against that data in real time to determine whether or not the object is malware and to communicate the determination to the remote computers, wherein at least one of a first threat server of the plural threat servers is further arranged to determine whether the data about~~ the first computer object has been previously seen ~~before~~by comparing the data uniquely identifying the first computer object to a plurality of data uniquely identifying plural computer objects in a first database associated with the first threat server, wherein the first threat server is further arranged to receive additional information about the first computer object from the first remote computer when the first computer object has not been previously seen, store the details of the first computer object and the received additional information about the first computer object in a second database associated with the first threat server when the first computer object has not been previously seen, provide contents of the second database to at least one database associated with a central server,~~;~~ and increase a count associated with a number of times that the first computer object has been seen;

a central server arranged to receive the increased count associated with the number of times that the first computer object has been seen; and

a second threat server arranged to receive at least a portion of the contents of the at least one database associated with the central server, wherein the at least a portion of the contents of the at least one database associated with the central server include a subset of the details of the first computer object stored in the second database

~~the base computer further comprising at least one central server in communication with the threat servers and arranged to receive the data about objects from the threat servers to maintain a master database of data received about objects from all threat servers, wherein the first threat server is further arranged to (i) maintain a list of objects~~

~~previously seen at the first threat server and previously forwarded to the central server, (ii) send the data about the object from the first threat server to the central server when the object has not been seen before, and (iii) increase a count associated with the number of times that the data about the computer object has been seen, when the data about the computer object has been seen before~~.

10. (Currently Amended) The apparatus according to claim 9, ~~comprising:~~wherein

~~at least one database, the threat servers being arranged to store the data information received from remote computer in the database; and~~

~~storage,~~ the first and second threat servers ~~being~~are arranged to store, at intervals, ~~store~~ the contents of the second database in ~~the~~ storage together with a timestamp and ~~clearing~~ clear the database.

11. (Currently Amended) The apparatus according to claim 10, further comprising:

a backup central server having a database, the database of the backup central server being populated by receiving at the backup central server all of the time-stamped blocks of data from the storage and incorporating them into the database of the backup central server.

12. (Currently Amended) The apparatus according to claim 10, wherein, in the event that ~~a~~ the central server is taken off-line for a period of time such that it does not receive updates of data from the first and second threat servers during that period of time, the central server is arranged to, after the period of time has elapsed, update ~~its~~at least one database with time-stamped blocks of data from the storage that have a timestamp later than the time when the central server went off-line.

13. (Currently Amended) The apparatus according to claim 10, wherein, in the event that at least one ~~the~~ database of a central server is rolled back to a point of time in the past, the central server is arranged to update the at least one~~its~~ database with time-

Sophos Ex. 1002
Page 300 of 683

stamped blocks of data from storage that have a timestamp later than the ~~past~~ point of time in the past.

14. (Currently Amended) The apparatus according to claim 9, wherein the central server has one or more databases that include ~~including~~ at least one of:

a) object signatures and metadata about that object;

b) object behavior; and

c) information about what objects are present on what remote computers.

15. (Currently Amended) The apparatus according to claim 14, wherein the first and second threat servers and the central ~~servers~~server are implemented using cloud computing.

16-24. (Canceled)

25. (New) The method according to claim 1, further comprising:

receiving, at the second threat server, details of a second computer object from a second remote computer, wherein the details of the second computer object include data uniquely identifying the second computer object;

determining, by the second threat server, whether the second computer object has been previously seen by comparing the data uniquely identifying the second computer object to a plurality of data uniquely identifying plural computer objects in a third database associated with the second threat server;

determining that the second computer object has been seen before;

increasing a count associated with a number of times that the second computer object has been seen and providing the increased count associated with the number of times that the second computer object has been seen to the at least one central server; and

receiving, at the first threat server, a count associated with the number of times that the second computer object has been seen.

ARGUMENTS/REMARKS

The above-identified patent application has been reviewed in light of the Examiner's Action dated January 06, 2014. Claims 1-6, and 9-15 have been amended, without intending to abandon or to dedicate to the public any patentable subject matter. Claim 25 has been added. Accordingly, claims 1-7, 9-15 and 25 are now pending. As set forth herein, reconsideration and withdrawal of the rejections of the claims are respectfully requested.

Examiner Interview

Applicant would like to thank Examiner Chiang for his time during the telephonic interview on March 24, 2014. Examiner Chiang and Applicant's representative, Brent Lindon, discussed the current rejection to clarify the issues at hand, discussed possible additions to the claims, and discussed differences between the cited art and the present claims. The changes discussed are some of the changes included in the current amendments. Again, Applicant appreciates the Examiner's attention and assistance.

Claim Rejection Under 35 U.S.C. § 103

Claims 1, 9, and 14-15 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 8,332,946 to Boisjolie et al. ("Boisjolie") and U.S. Patent Publication No. US 2011/0191341 to Meyer et al. ("Meyer") and U.S. Patent Publication No. 7,921,063 to Quinlan ("Quinlan"). Claims 2-3, 6-7 and 10-11 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Boisjolie, Meyer, and Quinlan, in view of U.S. Patent Publication No. US 2003/0093429 to Nishikawa et al. ("Nishikawa"). Claims 4 and 12 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Boisjolie, Meyer, Quinlan, Nishikawa, and further in view of U.S. Patent Publication No. US 2009/0070304 to Chen et al. ("Chen"). Claims 5 and 13 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Boisjolie, Meyer, Quinlan, Nishikawa, and further in view of U.S. Patent No. 7,814,056 to McGrattan et al. ("McGrattan").

To establish a *prima facie* case of obviousness, all claim limitations must first be taught or suggested by the prior art. *See, e.g., DyStar Textilfarben GmbH & Co.*

Deutschland KG v. C.H. Patrick Co., 464 F.3d 1356, 1360 (Fed. Cir. 2006); 80 U.S.P.Q.2d 1641, 1645 (2006). "All words in a claim must be considered in judging the patentability of that claim against the prior art." MPEP § 2143.03 (citing *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970)). The Examiner must then provide an explicit analysis of the motivation for combining the references. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007); 82 U.S.P.Q.2d 1385, 1396 (2007) ("a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art . . . ."). While the Examiner can choose one of several exemplary rationales from the MPEP to support an obviousness rejection, all the rationales in the MPEP still require the Examiner to demonstrate that all the claim elements are shown in the prior art. *See* MPEP § 2143, Original Eighth Edition, August 2001, Revision July 2008. Applicant respectfully submits that none of the cited references disclose, suggest, or render obvious at least the combination of features as currently claimed.

The Claimed Invention

The claimed invention is generally directed to classifying computer objects as malware utilizing a distributed network. In some embodiments, a threat server and a central server may be arranged to receive data about one or more computer objects located on or otherwise associated with one or more remote computers. In particular, the servers will be dealing with huge amounts of data and there will be a large amount of commonality in the data which can be used for determining rules on what objects are malware. *See e.g., Applicant's specification as published,* ¶ 0092. However, it is generally impractical to store all data on one or more servers located in all regions because this presents a problem with regard to determining whether or not the data is common in real-time. *See e.g., Id.*

Moreover, in a backup environment, it would be equally impractical to post to databases at a single server which is designated a master server and to propagate data from the master server to other servers in a community because a single server does most of the work whilst other servers, such as backup servers, are underutilized. *See e.g., Id* at ¶ 0101. Thus, a single server must be more powerful than the backup servers. *See e.g.,*

Sophos Ex. 1002
Page 303 of 683

Id. This tends to be wasteful and inefficient of resources. *See e.g., Id.* In comparison, the exemplary embodiment, shares the workload around the servers equally. *See e.g., Id.*

Accordingly, to address these issues, an exemplary embodiment adopts the following scheme: each threat server examines an incoming packet of data from a remote computer about an object seen on that remote computer. *See e.g., Id.,* at ¶ 0093. The threat server has a database of objects that have previously been seen and which have already been sent to a central server. *See e.g., Id.* The threat server checks its database for the checksum of the incoming data; if the checksum is found, then the data has already been seen by the central server. *See e.g., Id.* In this case, the threat server increases the count associated with that checksum in its database of the number of times that data has been seen to assist in determining the popularity of a piece of software or the frequency of the occurrence of a specific event. *See e.g., Id.,* This information can then be forwarded to the central server. *See e.g., Id.* If the checksum is not found in the threat database, then the threat server requests the full data packet from the remote computer and then forwards this to the central server. *See e.g., Id.* The central server then stores this data in the appropriate databases and keeps a master list of all data objects seen on all of the remote computers. *See e.g., Id.* This master list is propagated back to the threat servers in each of the geographical locations. *See e.g., Id.* Thus, all threat servers are updated with information about which objects have been seen by the community. *See e.g., Id.*

Such a scheme has been found to reduce workload and traffic in the network by a factor of about 50 compared with a conventional scheme where typically each piece of data on being received by a web server would immediately be propagated to all other servers in the system. *See e.g.., Id.,* at ¶ 0094. Moreover, such architecture allows vast amounts of data to be managed across multiple locations and servers. *See e.g., Id.,* at ¶ 0107. The architecture can be scaled and servers copied without incurring extra work or affecting the running of the system. *See e.g., Id.*

The Boisjolie Reference

Boisjolie is generally directed to a malware-protection method/system for protecting a computer from malware infection by preventing infected files from

Sophos Ex. 1002
Page 304 of 683

executing on a computer before they can do harm. *See e.g., Boisjolie,* Abstract. Boisjolie further discloses a malware protection method as illustrated in Figure 1. *See e.g., Boisjolie* at Figure 1. In particular, Boisjolie teaches that a new file may enter an endpoint, a fingerprint may be created for the file, and the fingerprint may be verified against a white list. *See e.g., Boisjolie,* col. 4 ln 25- col. 5 ln18. Further, if the fingerprint cannot be verified, the new file is sent from the endpoint to the malware scan servers for scanning. *See Id,* at col. 5 lns 30-40. Boisjolie however, makes no mention of at least receiving additional information about the first computer object from a first remote computer when the first computer object has not been previously seen; storing the details of the first computer object and the received additional information about the first computer object in a second database associated with a first threat server when the first computer object has not been previously seen; providing contents of the second database to at least one database associated with a central server; increasing a count associated with a number of times that the first computer object has been seen and providing the increased count associated with the number of times that the first computer object has been seen to a central server; and receiving, at a second threat server, at least a portion of the contents of the at least one database associated with the central server, wherein the at least a portion of the contents of the at least one database associated with the central server include a subset of the details of the first computer object stored in the second database. As previously discussed, such a scheme reduces workload and network traffic. Applicant respectfully submits that Boisjolie provides no disclosure related to such an implementation and further does not operate in this manner.

The Meyer Reference

The Meyer reference is generally directed to a computer-implemented method and apparatus for sharing the results of computing operations among related computing system. *See e.g., Meyer,* Abstract. In particular, Meyer teaches a virtualization layer that may abstract hardware into a plurality of local stores for each virtual machine; the shared store may contain or comprise a file-attribute database that may contain, for each of a plurality of files encountered by a group of computing systems, a hash of the file, the results of at least one computing operation, the data of at least one computer operation,

and other useful information. *See e.g., Meyer,* ¶ 0028 - ¶ 0029. However, similar to Boisjolie, Meyer fails to teach, suggest, or disclose at least the method as claimed. In particular, Meyer fails to teach, suggest, or render obvious at least receiving additional information about the first computer object from a first remote computer when the first computer object has not been previously seen; storing the details of the first computer object and the received additional information about the first computer object in a second database associated with a first threat server when the first computer object has not been previously seen; providing contents of the second database to at least one database associated with a central server; increasing a count associated with a number of times that the first computer object has been seen and providing the increased count associated with the number of times that the first computer object has been seen to a central server; and receiving, at a second threat server, at least a portion of the contents of the at least one database associated with the central server, wherein the at least a portion of the contents of the at least one database associated with the central server include a subset of the details of the first computer object stored in the second database. As previously discussed, such a scheme reduces workload and network traffic and Applicant respectfully submits that Meyer provides no such teaching as claimed.

The Quinlan Reference

The Quinlan reference is generally directed to evaluating electronic messages based on probabilistic analysis. *See e.g., Quinlan*, Abstract. In particular, column 6 lines 10-15 of Quinlan states "threat information source 104 generates counts of received messages that have suspicious attachments, and provides the counts to threat information processor 108, or allows an external process to retrieve the counts and store them in a specialized database." *See e.g., Quinlan,* col. 6 lns 10-15. However, nowhere does Quinlan teach or suggest at least the method as claimed or how/why the counts are relevant to the overall system. That is, Quinlan merely teaches providing a count relating to a number of received messages that have suspicious attachments. Accordingly, Applicant respectfully submits that Quinlan is deficient for at least not teaching least receiving additional information about the first computer object from a first remote computer when the first computer object has not been previously seen; storing the details

of the first computer object and the received additional information about the first computer object in a second database associated with a first threat server when the first computer object has not been previously seen; providing contents of the second database to at least one database associated with a central server; increasing a count associated with a number of times that the first computer object has been seen and providing the increased count associated with the number of times that the first computer object has been seen to a central server; and receiving, at a second threat server, at least a portion of the contents of the at least one database associated with the central server, wherein the at least a portion of the contents of the at least one database associated with the central server include a subset of the details of the first computer object stored in the second database. This is simply not taught by Quinlan. Accordingly, Applicant respectfully submits that Boisjolie, Meyer, and Quinlan, taken alone, or in any combination, do not teach or render obvious at least the combination of features as recited in independent claim 1 or the combination of features as recited in independent claim 9. Therefore, Applicant respectfully submits that the rejections of claims 1-7 and 9-15 should be reconsidered and withdrawn.

The dependent claims are further distinguishable at least based on the above and the additional feature(s) recited therein.

Conclusion

The application now appearing to be in form for allowance, early notification of same is respectfully requested. Applicant does not acquiesce to any objection, rejection, or argument not specifically addressed herein. Rather, the Applicant believes the amendments and arguments contained herein overcome all objections, rejections, or arguments.

The Examiner is invited to contact the undersigned by telephone if doing so would be of assistance.

Respectfully submitted,

SHERIDAN ROSS P.C.

Date: May 6, 2014

By: /Brent R. Lindon/

Brent R. Lindon
Reg. No. 67,424
1560 Broadway, Suite 1200
Denver, CO 80202
Telephone: 303-863-9700

PTO/SB/22 (03-13)
Approved for use through 3/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): 6890-89-1

Application Number: 13/372,375

Filed: 2012-02-13

For: METHODS AND APPARATUS FOR DEALING WITH MALWARE

Art Unit: 2413

Examiner: CHIANG, JASON

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☑ One month (37 CFR 1.17(a)(1))	$200	$100	$50	$ 100.00
☐ Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
☐ Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$
☐ Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐ Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 191970.

☑ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71. 37 CFR 3.73(b) statement is enclosed (Form PTO/SB/96).

☑ attorney or agent of record. Registration number 67424.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/Brent R. Lindon/ — Signature

2014-05-06 — Date

Brent R. Lindon — Typed or printed name

303-863-9700 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☐ * Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	13372375
Filing Date:	13-Feb-2012
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Filer:	Brent Robert Lindon/Kathy Johnston
Attorney Docket Number:	6890-89-1

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 1 month with $0 paid	2251	1	100	100

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Request for Continued Examination	2801	1	600	600
		Total in USD ($)		**700**

Electronic Acknowledgement Receipt

EFS ID:	18956874
Application Number:	13372375
International Application Number:	
Confirmation Number:	2918
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Customer Number:	22442
Filer:	Brent Robert Lindon
Filer Authorized By:	
Attorney Docket Number:	6890-89-1
Receipt Date:	06-MAY-2014
Filing Date:	13-FEB-2012
Time Stamp:	16:11:49
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$700
RAM confirmation Number	2657
Deposit Account	191970
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	sb0030e_RCE.pdf	697477 05c62ff04f5ebf27c0a8a86f4cb107c51cc7251f	no	3
Warnings:					
Information:					
2		AMEND_02.pdf	166429 2cf3b36d574717579b31d5ff293ce40e89b54e21	yes	14

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment Submitted/Entered with Filing of CPA/RCE	1	1
Claims	2	7
Applicant Arguments/Remarks Made in an Amendment	8	14

Warnings:					
Information:					
3	Extension of Time	sb0022_EOT_1-month.pdf	186844 a6cb2d362d9f09976b9885109ea9e02097783cb7	no	2
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	32356 de03e242134cc0f5f44cffe707b440dcd303dd26	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1083106		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/372,375	Filing Date 02/13/2012	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT **05/06/2014**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 14	Minus	** 24	= 0	X $80 =	0
Independent (37 CFR 1.16(h))	* 2	Minus	***4	= 0	X $420 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/PEARLIE A. FENNELL/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	13/372,375
Filing Date	02-13-2012
First Named Inventor	Melvyn Morris
Title	METHODS AND APPARATUS FOR DEALING WITH MALWARE
Art Unit	2431
Examiner Name	CHIANG, JASON
Attorney Docket Number	04584.0012USU1

SIGNATURE of Applicant or Patent Practitioner

Signature	/Andrew T. Pouzeshi/	Date (Optional)	May 29, 2014
Name	Andrew T. Pouzeshi	Registration Number	67672
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ *Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☐ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 23552

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

WEBROOT INC.

☐ Inventor or Joint Inventor (title not required below)

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature		Date (Optional)	May 12, 2014
Name	Ryan Howe		
Title	Associate General Counsel		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ Total of forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office;U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of1995, no persons arerequired to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: Webroot Inc.

Application No./Patent No.: 13/372,375 Filed/Issue Date: 02-13-2012

Titled: METHODS AND APPARATUS FOR DEALING WITH MALWARE

Webroot Inc., a corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☑ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 028443, Frame 0609, or for which a copy thereof is attached.

B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

   1. From: _____ To: _____

      The document was recorded in the United States Patent and Trademark Office at

      Reel _____, Frame _____, or for which a copy thereof is attached.

   2. From: _____ To: _____

      The document was recorded in the United States Patent and Trademark Office at

      Reel _____, Frame _____, or for which a copy thereof is attached.

This collection of information is required by37 CFR3.73(b). The information is required toobtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentialityis governed by35 U.S.C. 122and 37 CFR1.11 and1.14. Thiscollection is estimated to take 12 minutes to complete, including gathering, preparing, and submittingthe completed application form to the USPTO.Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent tothe Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.**SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☑ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Andrew T. Pouzeshi/	May 29, 2014
Signature	Date
Andrew T. Pouzeshi	67672
Printed or Typed Name	Title or Registration Number

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that yoube given certain informationin connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, pleasebe advised that: (1) the general authority forthe collection of thisinformation is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and(3) the principal purpose forwhich the information isused by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent applicationor patent. If you do not furnish the requested information,the U.S. Patent and Trademark Office may not be able to process and/or examineyour submission,which may result in termination of proceedings or abandonment of the applicationor expiration of the patent.

The informationprovided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the informationin order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an InternationalApplication filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, arecord may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from thissystem of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	19158576
Application Number:	13372375
International Application Number:	
Confirmation Number:	2918
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Customer Number:	22442
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate
Filer Authorized By:	Andrew T. Pouzeshi
Attorney Docket Number:	6890-89-1
Receipt Date:	29-MAY-2014
Filing Date:	13-FEB-2012
Time Stamp:	14:24:04
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	2014_05_29_POA_04584_0012 USU1.pdf	271418 fa4695b9756db2e39dd0a88151f76c6bdd915c32	no	2

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
2	Assignee showing of ownership per 37 CFR 3.73.	2014_05_29_373c_04584_0012USU1.pdf	118088 d8a3deb3bb54be8cf4d5573977d0055610a5845c	no	3
Warnings:					
Information:					
			Total Files Size (in bytes):	389506	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/372,375	02/13/2012	Melvyn Morris	04584.0012USU1

CONFIRMATION NO. 2918

23552
MERCHANT & GOULD PC
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

POA ACCEPTANCE LETTER

OC000000068802478

Date Mailed: 06/05/2014

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 05/29/2014.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/kgebremichael/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/372,375	02/13/2012	Melvyn Morris	6890-89-1

CONFIRMATION NO. 2918

POWER OF ATTORNEY NOTICE

22442
Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

OC000000068802449

Date Mailed: 06/05/2014

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 05/29/2014.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/kgebremichael/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13372375
Filing Date	2012-02-13
First Named Inventor	Melvyn Morris
Art Unit	2431
Examiner Name	CHIANG, JASON
Attorney Docket Number	04584.0012USU1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20060272020		2006-11-30	Gardner	
	2	20080115190		2008-05-15	Aaron	
	3	20080148381		2008-06-19	Aaron	
	4	20070220043		2007-09-20	Oliver et al.	
	5	20060080637		2006-04-13	Treit et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13372375
	Filing Date	2012-02-13
	First Named Inventor	Melvyn Morris
	Art Unit	2431
	Examiner Name	CHIANG, JASON
	Attorney Docket Number	04584.0012USU1

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Extended European Search Report for EP Application No. 14161844.7, mailed July 25, 2014, 5 pages.	☐
	2	Extended European Search Report for EP Application No. 14161847.0, mailed July 25, 2014, 5 pages.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13372375
Filing Date	2012-02-13
First Named Inventor	Melvyn Morris
Art Unit	2431
Examiner Name	CHIANG, JASON
Attorney Docket Number	04584.0012USU1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Andrew T. Pouzeshi/	Date (YYYY-MM-DD)	2014-08-25
Name/Print	Andrew T. Pouzeshi	Registration Number	67672

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	19953040
Application Number:	13372375
International Application Number:	
Confirmation Number:	2918
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Customer Number:	23552
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate
Filer Authorized By:	Andrew T. Pouzeshi
Attorney Docket Number:	04584.0012USU1
Receipt Date:	25-AUG-2014
Filing Date:	13-FEB-2012
Time Stamp:	14:00:21
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	2014_08_25_SIDS_TransLtr_04584_0012USU1.pdf	73885 62ecb898a774eee5679e219f39ec408566122d44	no	2

Warnings:	
Information:	

2	Non Patent Literature	EP141618447_EESR_072514_5 pgs.PDF	165021 3115db0899398b40aeeea24e110f45f200e96e6f	no	5
Warnings:					
Information:					
3	Non Patent Literature	EP141618470_EESR_072514_5 pgs.PDF	146729 4825df135a23f25f48425087085b75916e541c54	no	5
Warnings:					
Information:					
4	Information Disclosure Statement (IDS) Form (SB08)	2014_08_25_SIDS_1449_04584_0012USU1.PDF	612254 5d497bc9a03ab02c21d1154c150dc7d7e3a4c90a	no	4
Warnings:					
Information:					
		Total Files Size (in bytes):	997889		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Morris, et al.	Examiner:	Chiang, Jason
Serial No.:	13/372,375	Group Art Unit:	2431
Filed:	February 13, 2012	Docket No.:	04584.0012USU1
Title:	METHODS AND APPARATUS FOR DEALING WITH MALWARE		

Filed via EFS-Web

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT (37 C.F.R. § 1.97(b))

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Attention: Commissioner for Patents

With regard to the above-identified application, the items of information listed on the enclosed Form 1449 are brought to the attention of the Examiner.

This statement should be considered because it is submitted before the mailing of a first Office Action after the filing of a Request for Continued Examination under 37 C.F.R. § 1.114 or a CPA under 37 C.F.R. § 1.53(d). Accordingly, no fee is due for consideration of the items listed on the enclosed Form 1449.

In accordance with 37 C.F.R. §1.98(a)(2), a copy of each foreign patent and/or a copy of each publication, other than U.S. patents and U.S. patent application publications, listed on the accompanying Form 1449 is enclosed.

No representation is made that a reference is "prior art" within the meaning of 35 U.S.C. §§ 102 and 103 and Applicants reserve the right, pursuant to 37 C.F.R. § 1.131 or otherwise, to establish that the reference(s) are not "prior art." Moreover, Applicants do not represent that a reference has been thoroughly reviewed or that any relevance of any portion of a reference is intended.

Consideration of the items listed is respectfully requested. Pursuant to the provisions of M.P.E.P. 609, it is requested that the Examiner return a copy of the attached Form 1449, marked

as being considered and initialed by the Examiner, to the undersigned with the next official communication.

Please charge any additional fees or credit any overpayment to Deposit Account No. 13-2725.

Respectfully submitted,

Dated: August 25, 2014

/Andrew T. Pouzeshi/

Andrew T. Pouzeshi, Reg. No. 67,672
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1639

23552
PATENT TRADEMARK OFFICE

Sophos Ex. 1002
Page 333 of 683

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/372,375	02/13/2012	Melvyn Morris	04584.0012USU1	2918

23552 7590 12/22/2014

MERCHANT & GOULD PC
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
CHIANG, JASON	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
12/22/2014	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPTO23552@merchantgould.com

Office Action Summary	Application No. 13/372,375	Applicant(s) MORRIS ET AL.	
	Examiner JASON C. CHIANG	Art Unit 2431	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05/06/2014*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-7,9-15 and 25* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-7,9-15 and 25* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *12/23/2013 and 08/25/2014*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

1. The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 05/06/2014 has been entered.

3. Claims 1-7, 9-15 and 25 are under examination. Claims 1-6 and 9-15 have been amended. Claim 25 is newly added claim.

Claim Objections

4. Claims 1 and 9 are objected to because of the following informalities: Claims 1 and 9 recite “providing contents of the second database to at least one database associated with a central server” and “providing the increased count associated with the number of times that the first computer object has been seen to a central server”, the Examiner assumes these two “central server” are the same central server. Appropriate correction is required.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 9, 14-15 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boisjolie et al. (US 8,332,946 B1) and Brennan (US 2007/0028304 A1).

Regarding claim 1, Boisjolie et al. discloses:

A method of classifying a computer object as malware **[Abstract, "The malware-protection method employs a number of techniques and relies on multiple layers of protection to identify trusted files, prevent execution of untrustworthy files, accurately detect corrupted files, analyze questionable files, and quarantine files"]**, the method comprising:

receiving, at a first threat server, details of a first computer object from a first remote computer, wherein the details of the first computer object include data uniquely identifying the first computer object **[Col. 4, lines 53-64, "At STEP 2, a new file from an external source enters the endpoint 102…At STEP 3, a fingerprint for the new**

file (i.e., a new-file fingerprint) is created by the endpoint 102 and the new-file fingerprint is sent to application-verification servers 104 for verification"];;

determining, by the first threat server, whether the first computer object has been previous seen by comparing the data uniquely identifying the first computer object to a plurality of data uniquely identifying plurality computer objects in a first database associated with the first threat server **[col. 5, lines 4-7, "At STEP 4, the application verification servers 104 attempt to verify the new-file fingerprint against an application-data-signature whitelist in data communication with the application-verification servers 104", col. 5, lines 19-21, "In a typical embodiment, the application-verification servers 104 list a disposition for the new-file fingerprint that includes, for example, good, bad/not good, and unknown"]**;

receiving additional information about the first computer object from the first remote computer when the first computer object has not been previously seen **[col. 7, line 66 – col. 8, line 3, "However, responsive to a determination of unknown at STEP 236, the flow 200 proceeds to STEP 242. At STEP 242, the new file is scanned against a malware-definition file in data communication with the application-verification servers 104." (Send the new file to application-verification server for scanning when the fingerprint of the new file is unknown)]**; and

receiving, at a second threat server, at least a portion of the contents of the at least one database associated with the central server, wherein the at least a portion of the contents of the at least one database associated with the central server include a subset of the details of the first computer object stored in the second database **[col. 9,**

lines 7-14, "From STEP 262, the flow 200 proceeds to STEP 264. At STEP 264, the application-data-signature whitelist on the endpoint 102, as well as any other endpoints, are updated to reflect that the new file is not good. From STEP 264, the flow 200 proceeds to STEP 266. At STEP 266, a request is made for the endpoint 102, as well as any other endpoints, to update their malware definition file in order to be able to detect the new file"].

Boisjolie et al. does not explicitly disclose storing the details of the first computer object and the received additional information about the first computer object in a second database associated with the first threat server when the first computer object has not been previously seen; providing contents of the second database to at least one database associated with a central server; increasing a count associated with a number of times that the first computer object has been seen and providing the increased count associated with the number of times that the first computer object has been seen to a central server;

However, Brennan in the same field relates to network security system teaches:

storing the details of the first computer object and the received additional information about the first computer object in a second database associated with the first threat server when the first computer object has not been previously seen **[par 0030, "A single server can support many hosts 12, e.g., hundreds or thousands of hosts. The server also maintains a database of metadata relating to analyses, such as scan histories and approval states, with respect to files and programs. This metadata is referred to as an "antibody" for each of the files and programs",**

par. 0041, “In another aspect, all copies of new files are kept in a special directory in a server 42”, fig. 1, files pool 34];

providing contents of the second database to at least one database associated with a central server **[par. 0115, "A server has an antibody database 34 of generally every unique hash that has ever been reported by any of its hosts, and a super server (if there is one) has an antibody database of generally every unique hash which has been seen on any of its servers", par. 0116, “new files propagate from the host to the server to super server in response to "New File" or "Dirty File" events, and the newly computed antibody state propagates in reverse from super server to server to host user to host kernel in the form of antibody updates”]**;

increasing a count associated with a number of times that the first computer object has been seen and providing the increased count associated with the number of times that the first computer object has been seen to a central server **[par 0131, “When an antibody changes state on the server, an incrementing counter value is written to the antibody”, par 0201, “Along with the statistics for each category, the user can view "top ten lists" of an item, highlighting the most frequently seen instances of each across all hosts managed by the server” (server and super server keep track of count)]**;

At the time of the invention, it would have been obvious to a person having ordinary skill in the art to incorporate the teaching of Brennan into the teaching of Boisjolie et al. with the motivation of providing a defense from known and unknown viruses, worms, spyware, hackers, unapproved/unwanted software and social

engineering attacks. Administrators can access detailed information and statistics on new executables, scripts, and embedded scripts as they appear and propagate to networked systems as taught by Brennan **[Brennan: par. 0008]**.

Regarding claim 9, it recites similar limitations as of claim 1. The reasons for the rejection of claim 1 are incorporated herein.

Regarding claim 14, the rejection of claim 9 is incorporated.

Boisjolie et al. discloses a method of classifying a computer object as malware.

Boisjolie et al. does not discloses the central server has one or more database that include at least one of a) object signatures and metadata about that object; b) object behavior; and c) information about what objects are present on what remote computers.

However, Brennan teaches the central server has databases including at least one of a) object signatures and metadata about that object; b) object behavior; and c) information about what objects are present on what remote computers **[par 0030, "The server also maintains a database of metadata relating to analyses, such as scan histories and approval states, with respect to files and programs. This metadata is referred to as an "antibody" for each of the files and programs", par. 0115, "A server has an antibody database 34 of generally every unique hash that has ever been reported by any of its hosts, and a super server (if there is one) has an antibody database of generally every unique hash which has been seen on any of its servers"]**.

At the time of the invention, it would have been obvious to a person having ordinary skill in the art to incorporate the teaching of Brennan into the teaching of Boisjolie et al. with the motivation of providing a defense from known and unknown viruses, worms, spyware, hackers, unapproved/unwanted software and social engineering attacks as taught by Brennan **[Brennan: par. 0008]**.

Regarding claim 15, the rejection of claim 14 is incorporated.

Boisjolie et al. further discloses the first and second threat servers and the central server are implemented using cloud computing **[Col. 2, lines 28-30, "Responsive to a determined status of unknown in response to a malware scan, the new file is sent to a cloud-based malware-scanning engine"]**.

Regarding claim 25, claim 25 has limitations similar to claim 1 and it recites same features of claim 1 but apply to second threat server, second computer object and second remote computer.

Boisjolie et al. further discloses second threat server, second computer object and second remote computer **[col. 4, lines 37-40, "In a typical embodiment, the malware-protection method 100 interfaces with a plurality of endpoints", col. 2, lines 6-9, "A malware-protection method responsive to an access request for a new file from an endpoint computer of a plurality of endpoint computers, verifies as safe an access location of the new file"]**.

Brennan teaches the second threat server **[par. 0009, "The system architecture preferably includes agent software that runs on each protected host, and a server, referred to as a "server"… The server can be implemented as an**

appliance (which generally suggests a more limited functionality device). A single appliance can support many hosts, e.g. 10,000 hosts. A further server or appliance, sometimes referred to as a "super server," can monitor multiple appliances"].

At the time of the invention, it would have been obvious to a person having ordinary skill in the art to incorporate the teaching of Brennan into the teaching of Boisjolie et al. with the motivation of providing a defense from known and unknown viruses, worms, spyware, hackers, unapproved/unwanted software and social engineering attacks as taught by Brennan **[Brennan: par. 0008]**.

7. Claims 2, 6-7 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boisjolie et al. (US 8,332,946 B1), Brennan (US 2007/0028304 A1) as applied to claims 1, 9, 14-15, 25 and in view of Nishikawa et al. (US 2003/0093429 A1).

Regarding claim 2, the rejection of claim 1 is incorporated.

Boisjolie et al. further discloses at least one threat server comprises at least one database for holding information received from remote computers to which it is attached, the method comprising storing the data in at least one database at the threat server **[Col. 4, lines 61-64, "At STEP 3, a fingerprint for the new file (i.e., a new-file fingerprint) is created by the endpoint 102 and the new-file fingerprint is sent to application-verification servers 104 for verification", Fig. 1, Application database]**;

Brennan discloses storing the contents of the second database in storage with a timestamp and clearing the second database **[par. 0315, "Backup. Backs and**

restores the configuration to removable media (and also to the network). Save configuration and database. Save the configuration and antibody database (e.g., via XML)", par, 0199, "A network status interface provides an overview of the running system, including: recent events and associated information, including unique file identifier, event time stamp"].

They do not teach clearing the database.

Nishikawa et al. in the field relates to a data storage system teaches at intervals, storing the contents of the database in storage and clearing the database **[Paragraph 0030, "The server 102 is referred to as a "dynamic database server," in part, because it is updated with new data or records that have been inputted into the saving job DB 118 since the last batch process. Accordingly, the server 102 has more current data than the DWH server 105 that receives data periodically from the batch extraction step 119. As used herein, the term "dynamic database" is a database that is stored with data more recent than the DWH. In the present embodiment, the dynamic database is a temporarily database that is periodically purged of redundant or old data that have been copied into the DWH"]**.

At the time of the invention, it would have been obvious to a person having ordinary skill in the art to incorporate the teaching of Nishikawa et al. into the teaching of Boisjolie et al. and Brennan with motivation to allow the system to delete old data and save new records **[Nishikawa et al.: Paragraph 0033]**.

Regarding claim 6, the rejection of claim 2 is incorporated.

Boisjolie et al. discloses a method of classifying a computer object as malware.

Boisjolie et al. does not discloses the central server has one or more database that include at least one of a) object signatures and metadata about that object; b) object behavior; and c) information about what objects are present on what remote computers.

However, Brennan teaches the central server has databases including at least one of a) object signatures and metadata about that object; b) object behavior; and c) information about what objects are present on what remote computers **[par 0030, "The server also maintains a database of metadata relating to analyses, such as scan histories and approval states, with respect to files and programs. This metadata is referred to as an "antibody" for each of the files and programs", par. 0115, "A server has an antibody database 34 of generally every unique hash that has ever been reported by any of its hosts, and a super server (if there is one) has an antibody database of generally every unique hash which has been seen on any of its servers"]**.

At the time of the invention, it would have been obvious to a person having ordinary skill in the art to incorporate the teaching of Brennan into the teaching of Boisjolie et al. with the motivation of providing a defense from known and unknown viruses, worms, spyware, hackers, unapproved/unwanted software and social engineering attacks as taught by Brennan **[Brennan: par. 0008]**.

Regarding claim 7, the rejection of claim 2 is incorporated.

Boisjolie et al. further discloses the threat and central servers are implemented using cloud computing **[Col. 2, lines 28-30, "Responsive to a determined status of**

unknown in response to a malware scan, the new file is sent to a cloud-based malware-scanning engine"].

Regarding claim 10, it recites similar limitations as of claim 2. The reasons for the rejection of claim 2 are incorporated herein.

8. Claims 3 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boisjolie et al., Brennan (US 2007/0028304 A1) and Nishikawa et al. (US 2003/0093429 A1) as applied to claims 2, 6-7 and 10, and in view of Meyer et al. (US 2011/0191341 A1).

Regarding claim 3, the rejection of claim 2 is incorporated.

Boisjolie et al. discloses a method of classifying a computer object as malware.

Brennan discloses storing the contents of the second database in storage with a timestamp and clearing the second database.

Nishikawa et al. discloses at intervals, storing the contents of the database in storage and clearing the database.

They do not disclose creating a backup central server by receiving at a second central server all of the time-stamped blocks of data from the second database and incorporating all of the time-stamped blocks of data into at least one database associated with the second central server.

Meyer et al. discloses the method according to claim 2 comprising creating a backup central server by receiving at a central server all of the time-stamped blocks of data and incorporating them into its database **[Paragraph 0029, "Shared store 216**

generally represents any type or form of physical or virtualized storage that may be shared or accessed by a group of related computing systems, such as virtual machines 202(1)-(N) in FIG. 2. In some examples, shared store 216 may contain or comprise a file-attribute database (such as file-attribute database 120 in FIGS. 1 and 5) that may contain, for each of a plurality of files encountered by a group of computing systems (such as virtual machines 202(1)-(N)): 1) a hash of the file, 2) the results of at least one computing operation performed in connection with the file (such as a classification assigned to the file during a malware analysis, at least one rationale for the classification assigned to the file during the malware analysis, at least one virus definition set or heuristic used when performing the malware analysis, or the like), 3) the date of at least one computing operation performed in connection with the file (such as the date of the most-recent malware scan performed on the file), and/or 4) any other potentially useful information that may be shared among related computing systems", Fig. 5].

At the time of the invention, it would have been obvious to a person having ordinary skill in the art to incorporate the teaching of Meyer et al. into the teaching of Boisjolie et al., Brennan, and Nishikawa et al. with the motivation of sharing the results of computing operations among related computing systems as taught by Meyer et al. **[Meyer et al.: abstract]**.

Regarding claim 11, it recites similar limitations as of claim 3. The reasons for the rejection of claim 3 are incorporated herein.

9. Claims 4 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boisjolie et al., Brennan (US 2007/0028304 A1) and Nishikawa et al. (US 2003/0093429 A1) as applied to claims 2, 6-7 and 10, and in view of Chen et al. (US 2009/0070304).

Regarding claim 4, the rejection of claim 2 is incorporated.

Boisjolie et al. discloses a method of classifying a computer object as malware.

Brennan discloses storing the contents of the second database in storage with a timestamp and clearing the second database.

Nishikawa et al. discloses at intervals, storing the contents of the database in storage and clearing the database.

They do not teach taking the central server off-line for a period of time such that the central server does not receive data from the first and second threat servers during that period of time; after the period of time has elapsed, updating at least one database associated with the central server with time-stamped blocks of data from the storage that have a timestamp later than the time when the central server went off-line; and bringing the central server back on line.

However, Chen in the field relates to database systems teaches taking a central server off-line for a period of time such that it does not receive updates of data from the threat servers during that period of time; after the period of time has elapsed, updating the database of the central server with time-stamped blocks of data from the storage that have a timestamp later than the time when the central server went off-line; and bringing the central server back on line **[Paragraph 0004, "Applications commonly use this timestamp column for controlling optimistic locking schemes as follows:**

the application retrieves one or more rows from the table, including the timestamp column; the application logically or physically disconnects from the database system; the application makes updates to the rows that were retrieved from the database; and sometime later, the application reconnects to the database so that it can record the updates in the database"].

At the time of the invention, it would have been obvious to a person having ordinary skill in the art to incorporate the teaching of Chen et al. into the teaching of Boisjolie et al., Brennan and Nishikawa et al. with the motivation of ensuring data consistency **[Chen et al.: paragraph 0003]**.

Regarding claim 12, it recites similar limitations as of claim 4. The reasons for the rejection of claim 4 are incorporated herein.

10. Claims 5 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boisjolie et al., Brennan (US 2007/0028304 A1) and Nishikawa et al. (US 2003/0093429 A1) as applied to claims 2, 6-7 and 10, and in view of McGrattan et al. (US 7814056 B2).

Regarding claim 5, the rejection of claim 2 is incorporated.

Boisjolie et al. discloses a method of classifying a computer object as malware.

Brennan discloses storing the contents of the second database in storage with a timestamp and clearing the second database.

Nishikawa et al. discloses at intervals, storing the contents of the database in storage and clearing the database.

They do not teach rolling back at least one database associated with the central server to a point of time in the past; updating the at least one database associated with the central server with time-stamped blocks of data from storage that have a timestamp later than the past point of time; and bringing the central server back on line.

However McGrattan et al. in the field relates to storage backup teaches rolling back the database of a central server to a point of time in the past **[Col. 5, lines 1-13, "A method for restoring backup data from a database, according to one embodiment, will be described with reference to FIG. 2. The backup data is stored in the database as a plurality of data blocks. Each data block is typically stored with associated timestamp information in the database. A specification of a time to which data restoration is desired is received (step S21). The specified time is compared to timestamp information stored (step S23) for each of the data blocks of the backup data in the database. A selected data block of the backup data is retrieved if the selected data block has a timestamp at or earlier than the specified time and no other data blocks of the backup data which correspond to the selected data block have more contemporaneous timestamps between the specified time and the associated timestamp of the selected data block (step S25)"]**; updating the database of the central server with time-stamped blocks of data from storage that have a timestamp later than the past point of time; and bringing the central server back on line **[Col. 9, lines 4-34, "When a request for the operation "refresh object" is received, process software 602 collects the latest timestamps associated with the objects in the specified object set and correlates them to the**

data block digests for each data block in each of the objects of the object set (step S1). A list of the data block digests for the entire specified object set 901 is compiled and sorted in order of an object system directories walk-through (for example, data block digests are collected block-by-block for each object in the object set, and the collected data block digests are sorted) and is then sent to object system agent 601 (step S91). Object attributes are then read from Object system 600 for the object to be "refreshed" (step S92). The modification date of the object to be "refreshed" is compared to the timestamp information for the stored objects. If the modification date is higher than the latest timestamp for the object, then the object is read (step S92). For every block of size n in the object, a new data block digest is generated and compared against the ones in the list received by object system agent 601 at step 91 (step S93). If the data block digests are not equivalent, then the data block and the generated data block digest are both sent to process software 602 (step S94). If the data block digests are equivalent, then the data block is dropped and the system proceeds to the next block (step S94). Once process software 602 receives the new data blocks, it sends the metadata for the data blocks to database server 603 to be cataloged in database catalog 604 (step S95b) and the data block and data block digest are forwarded to media server 605 to be stored in database 609 (step S95b)", Col. 1, lines 21-43, "Enterprises and individuals who use computers that contain critical data, need disaster recovery plans in place in the event of a disaster, in order to safeguard vital information stored on the computers. Even in non-disaster

situations, in which users may just want to archive their information, it is beneficial to implement "backup" and recovery plans", "A partial backup can be either differential, in which all of the files that were changed since the last complete backup are considered, or incremental, in which all of the files that were changed since the last backup are considered, or user-defined, in which only sets of files specified by a user are considered"].

At the time of the invention, it would have been obvious to a person having ordinary skill in the art to incorporate the teaching of McGrattan et al. into the teaching of Boisjolie et al., Brennan, and Nishikawa et al. with the motivation of able to restoring backup data from a database by using the timestamp as taught by McGrattan et al. **[McGrattan et al.: abstract]**.

Regarding claim 13, it recites similar limitations as of claim 5. The reasons for the rejection of claim 5 are incorporated herein.

Response to Arguments

11. Applicant's arguments, filed on 08/12/2013, with respect to rejection under 35 USC § 103(a) have been fully considered but are moot in view of the new ground(s) of rejection.

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to Applicant's disclosure:

US 8195938 B2 Cloud-based application whitelisting

US 8296178 B2 Services using globally distributed infrastructure for secure content management

US 7231440 B1 System and method for distributing portable computer virus definition records with binary file conversion

US 8347386 B2 System and method for server-coupled malware prevention

US 8448243 B1 Systems and methods for detecting unknown malware in an executable file

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JASON C. CHIANG whose telephone number is (571)270-3393. The examiner can normally be reached on 9AM to 6PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, CORDELIA P. ZECHER can be reached on (571)272-7771. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/J.C./
Examiner, Art Unit 2431

/CORDELIA ZECHER/
Supervisory Patent Examiner, Art Unit 2431

Notice of References Cited	Application/Control No. 13/372,375	Applicant(s)/Patent Under Reexamination MORRIS ET AL.	
	Examiner JASON C. CHIANG	Art Unit 2431	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2007/0028304 A1	02-2007	Brennan, Todd	726/024
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13372375	MORRIS ET AL.
	Examiner	Art Unit
	JASON C CHIANG	2431

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	23	06/04/2013	JC

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor search in East	06/04/2013	JC
Text search in East of USPGPUB, USPAT, USOCR, FPRS, EPO, JPO, DERWENT, IBM_TDB	06/05/2013	JC
Inventor search in East	12/14/2013	JC
Text search in East of USPGPUB, USPAT, USOCR, FPRS, EPO, JPO, DERWENT, IBM_TDB	12/14/2013	JC
Inventor search in East	12/11/2014	JC
Text search in East of USPGPUB, USPAT, USOCR, FPRS, EPO, JPO, DERWENT, IBM_TDB	12/11/2014	JC

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/JASON C CHIANG/ Examiner.Art Unit 2431	

Sophos Ex. 1002
Page 356 of 683

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13372375
Filing Date	2012-02-13
First Named Inventor	Melvyn Morris
Art Unit	2431
Examiner Name	CHIANG, JASON
Attorney Docket Number	04584.0012USU1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/J.C./	1	20060272020		2006-11-30	Gardner	
/J.C./	2	20080115190		2008-05-15	Aaron	
/J.C./	3	20080148381		2008-06-19	Aaron	
/J.C./	4	20070220043		2007-09-20	Oliver et al.	
/J.C./	5	20060080637		2006-04-13	Treit et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13372375
Filing Date	2012-02-13
First Named Inventor	Melvyn Morris
Art Unit	2431
Examiner Name	CHIANG, JASON
Attorney Docket Number	04584.0012USU1

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
/J.C./	1	Extended European Search Report for EP Application No. 14161844.7, mailed July 25, 2014, 5 pages.	☐
/J.C./	2	Extended European Search Report for EP Application No. 14161847.0, mailed July 25, 2014, 5 pages.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Jason Chiang/	Date Considered	12/13/2014

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13372375
Filing Date	2012-02-13
First Named Inventor	Melvyn Morris
Art Unit	2431
Examiner Name	CHIANG, JASON
Attorney Docket Number	04584.0012USU1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Andrew T. Pouzeshi/	Date (YYYY-MM-DD)	2014-08-25
Name/Print	Andrew T. Pouzeshi	Registration Number	67672

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	1	of	2

Complete if Known	
Application Number	13/372,375
Filing Date	February 13, 2012
First Named Inventor	Melvyn Morris
Art Unit	2431
Examiner Name	Jason Chiang
Attorney Docket Number	6890-89-1

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/J.C./	1	6175869	01/16/2001	Ahuja et al.	
/J.C./	2	6219786	04/17/2001	Cunningham et al.	
/J.C./	3	7051365	05/23/2006	Bellovin	
/J.C./	4	8225218	07/17/2012	Frayman et al.	
/J.C./	5	2003/0188194	10/02/2003	Currie et al.	
/J.C./	6	2005/0187740	08/25/2005	Marinescu	
/J.C./	7	2006/0080637	04/13/2006	Treit et al.	
/J.C./	8	2006/0272020	11/30/2006	Gardner	
/J.C./	9	2007/0174429	07/26/2007	Mazzaferri et al.	
/J.C./	10	2007/0220043	09/20/2007	Oliver et al.	
/J.C./	11	2008/0115190	05/15/2008	Aaron	
/J.C./	12	2008/0148381	06/19/2008	Aaron	
/J.C./	13	2009/0089040	04/02/2009	Monastyrsky et al.	
/J.C./	14	2009/0172774	07/02/2009	Kot et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]; Number[4]; Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
/J.C./	15	International Search Report and Written Opinion for International (PCT) Patent Application No. PCT/EP2012/052497 mailed Jul. 13, 2012 (Attorney Ref. No. 6890-89-PCT), 22 pages.
/J.C./	16	International Preliminary Report on Patentability for International (PCT) Patent Application No. PCT/EP2012/052497 mailed Aug. 29, 2013 (Attorney Ref. No. 6890-89-PCT), 16 pages.
/J.C./	17	"Network Security Task Manager: Manual - Installation - Configuration," A. & M. Neuber Software GmbH, 2008, 65 pages.

Examiner Signature	/Jason Chiang/	Date Considered	12/13/2014

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*				Application Number	13/372,375
				Filing Date	February 13, 2012
				First Named Inventor	Melvyn Morris
				Art Unit	2431
				Examiner Name	Jason Chiang
Sheet	2	of	2	Attorney Docket Number	6890-89-1

/J.C./	18	CHACKSFIELD, "Facebook apps ask for your permission before data mining," TechRadar.com, Jul. 1, 2010 [retrieved on 6/14/2013], 5 pages. Retrieved from: www.techradar.com/us/news/broadband/web/internet/facebook-apps-ask-for-your-permission-before-data-mining-700540
/J.C./	19	COGSWELL et al., "RootkitRevealer v1.71," Nov. 1, 2006, [Retrieved on Jun. 29, 2012], 5 pages. Retrieved from: http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx
/J.C./	20	SRINIVASAN, "Protecting Anti-Virus Software Under Viral Attacks," Master of Science thesis, Arizona State University, Aug. 2007, 82 pages.
/J.C./	21	Official Action for U.S. Patent Application No. 13/372,433 mailed Aug. 9, 2013 (Attorney Ref. No. 6890-89-2), 18 pages.
/J.C./	22	Official Action for U.S. Patent Application No. 13/372,439 mailed Jul. 3, 2013 (Attorney Ref. No. 6890-89-3), 16 pages.

Examiner Signature	/Jason Chiang/	Date Considered	12/13/2014

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13372375	MORRIS ET AL.
	Examiner	**Art Unit**
	JASON C CHIANG	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/09/2013	12/14/2013	12/13/2014						
	1	✓	✓	✓						
	2	✓	✓	✓						
	3	✓	✓	✓						
	4	✓	✓	✓						
	5	✓	✓	✓						
	6	✓	✓	✓						
	7	✓	✓	✓						
	8	✓	-	-						
	9	✓	✓	✓						
	10	✓	✓	✓						
	11	✓	✓	✓						
	12	✓	✓	✓						
	13	✓	✓	✓						
	14	✓	✓	✓						
	15	✓	✓	✓						
	16	✓	-	-						
	17	N	N	N						
	18	N	N	N						
	19	N	N	N						
	20	N	N	N						
	21	N	N	N						
	22	N	N	N						
	23	N	N	N						
	24	N	N	N						

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	190	("20100043072" | "20100332593" | "8453244" | "7051365" | "20110197272" | "20090300764" | "20100064368" | "20120017200" | "8301904" | "8347386" | "8352484" | "20060080637" | "20090172774" | "20060101334" | "20090292791" | "20100306851" | "20110138361" | "8042184" | "7231440" | "8321944" | "20090089040" | "20060272020" | "20060069912" | "20120260304" | "7707634" | "20110191299" | "20110191341" | "7814056" | "7921063" | "8116732" | "20070220043" | "20080115190" | "7343626" | "20030093429" | "20090070304" | "7188173" | "8234709" | "8296178" | "8321540" | "8332946" | "8448243" | "20070174429" | "6175869" | "20080148381" | "20070016953" | "20110197177" | "20120266208" | "8336100" | "8347375" | "20060080637" | "20060117055" | "20100313183" | "20110083183" | "8146135" | "8307435" | "8195938" | "8443447" | "20060272020" | "8225218" | "8276202" | "20030188194" | "20050187740" | "20080115190" | "20080148381" | "6219786" | "20070220043").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/13 20:26
L2	6016	(726/23).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/12/13 20:27
L3	173	L1 NOT L2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/13 20:27
L4	70	("20100043072" | "20110197272" | "20090300764" | "20100064368" | "20120017200" | "20060101334" | "20090292791" | "20100306851" | "20110138361" | "8042184" | "20060069912" | "20120260304" | "7707634" | "7343626" | "20070016953" | "20110197177" | "20120266208" | "20060117055" | "20100313183" | "20110083183" | "8146135" | "8307435").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/13 20:27
L5	120	L1 NOT L4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/13 20:27
S1	9	(Melvyn near Morris).in.	US-PGPUB;	OR	ON	2013/06/04

			USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			11:48
S2	3	(Joseph near Jaroch).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 16:51
S3	108	(Webroot).as.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 16:54
S5	0	S3 and cloud and database and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 16:58
S6	2980	(726/23).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/06/04 17:04
S7	72	S6 and cloud and database and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 17:05
S8	54	("20100043072" | "20110197272" | "20090300764" | "20100064368" | "20120017200" | "20060101334" | "20090292791" | "20100306851" | "20110138361" | "8042184" | "20060069912" | "20120260304" | "7707634" | "7343626" | "20070016953" | "20110197177" | "20120266208" | "20060117055" | "20100313183" | "20110083183" | "8146135" | "8307435").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/05 11:39
S9	21	("2006/0069912").URPN.	USPAT	OR	ON	2013/06/05 11:59
S10	17	threat adj server	USPAT	OR	ON	2013/06/05 12:20
S11	2362	cloud and signature	USPAT	OR	ON	2013/06/05 13:23
S12	1181	cloud and signature and layer	USPAT	OR	ON	2013/06/05 13:23
S13	249	cloud and (signature with database)	USPAT	OR	ON	2013/06/05 13:25
S14	78	cloud and (signature with database) and (malware	USPAT	OR	ON	2013/06/05

		virus)				13:26
S15	143	cloud and (updat$4 near3 (signature database)) and (malware virus)	USPAT	OR	ON	2013/06/05 16:30
S16	65	(updat$4 near3 (signature database) near3 (interval certain period periodic)) and (malware virus)	USPAT	OR	ON	2013/06/05 20:09
S17	1	(09/740294).APP.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/06/05 20:37
S18	0	("(masteradjdatabase)and(virusmalwaresignature)").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/06/07 18:03
S19	1003	(master adj database) and (virus malware signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:04
S20	160	(master adj database) and (virus malware) and signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:05
S21	971	(database) and (virus near signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:33
S22	639	((stor$4 sav$4 receiv$5) with database) and (virus near signature) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:51
S23	594	((stor$4 sav$4 receiv$5) near5 database) and (virus near signature) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:51
S24	64	((stor$4 sav$4 receiv$5) near5 database) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2013/06/08 10:51

			IBM_TDB			
S25	0	((stor$4 sav$4 receiv$5) near3 content near3 database near3 storage) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:02
S26	0	((stor$4 sav$4 receiv$5) near3 database near3 storage) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:03
S27	2	((stor$4 sav$4 receiv$5) near3 content near3 database near3 storage) with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:03
S28	0	((backup) near3 database) with timestamp and (virus malware)and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:05
S29	0	((backup) near3 database) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:06
S30	27	((backup) near3 database) with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:06
S31	1139	((copy stor$4) near3 database) with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:20
S32	18	((copy stor$4) near3 database) with central with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:21
S33	359	((purg$4 clear$4 remov$4) near3 database near3 (period$6 every)) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS;	OR	ON	2013/06/08 11:29

			EPO; JPO; DERWENT; IBM_TDB			
S34	0	(master adj database) near2 (virus malware) near2 signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S35	0	(master adj database) near3 (virus malware) near3 signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S36	0	(master adj database) with (virus malware) with signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S37	0	(master adj database) same (virus malware) same signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S38	19	(master adj database) same (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:45
S39	15	((primary secondary) adj database) same (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:54
S40	30	((primary secondary) adj database) with (signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:57
S41	98	(master adj database) same (signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:59
S42	10	(master adj database) same (signature) and (virus malware)	US-PGPUB; USPAT;	OR	ON	2013/06/08 15:59

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S43	315	(master adj database) and (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 16:03
S44	18	(virus malware) with definition with (file database) with (cloud community share$2)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 16:21
S45	271	(update refresh recover rebuild) near3 (database) with timestamp	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 20:22
S46	4	(update refresh recover rebuild) near3 (database) with timestamp same (offline off-line (off adj line) disconnect reconnect)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 20:24
S47	1	((roll$3 adj back) near6 time) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:11
S48	7	((roll$3 adj back)) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:12
S49	11	((roll$3 adj back) rollback) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:14
S50	48	((roll$3 adj back) rollback) and ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:18

S51	21	(((roll$3 adj back) rollback) with time) and ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:23
S52	0	((restor$4) near6 time) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 11:40
S53	3	((restor$4) near6 time) and ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 11:41
S54	0	(send provid$3 transmit$4 updat$3) near3 (count near3 (threat incident)) near3 (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:01
S55	22	(send provid$3 transmit$4 updat$3) with ((count number) near3 (threat incident)) with (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:02
S56	122	(send provid$3 transmit$4 updat$3 record$4) with ((count number times) with (threat)) with (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:05
S57	635	(send provid$3 transmit$4 updat$3 record$4) with ((count number times) near5 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:08
S58	199	(send provid$3 transmit$4 updat$3 record$4) with ((count number) near5 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:09
S59	11	(send provid$3 transmit$4 updat$3 record$4) with ((count) near5 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2013/06/09 15:11

			DERWENT; IBM_TDB			
S60	43	((count) near2 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:15
S61	9	((count) near2 (threat)) and (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:15
S62	1126	(send provid$3 transmit$4 updat$3) near3 (count) near3 (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:18
S63	15	(send provid$3 transmit$4 updat$3) near3 ((increas$4 add$3) near (count)) near3 (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:20
S64	1816	((increas$4 add$3) near (count)) and (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:22
S65	27	((increas$4 add$3) near (count)) and (malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:23
S66	9	(Melvyn near Morris).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:29
S67	3	(Joseph near Jaroch).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:30
S68	813	((increas$4 add$3 generat$4) near (count)) and (malware threat)	US-PGPUB; USPAT; USOCR;	OR	ON	2013/12/14 16:31

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S69	742	((increas$4 add$3 generat$4) near (count)) and (malware threat) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:32
S70	0	(((seen identified) near (before previous)) with (increas$4 add$3 generat$4) near (count)) and (malware threat) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:33
S71	0	(((seen identified) near (before previous)) same ((increas$4 add$3 generat$4) near (count))) and (malware threat) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:33
S72	48	(((seen identified)) same ((increas$4 add$3 generat$4) near (count))) and (malware threat) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:33
S73	347	(master central primary global) near2 (server database) same (signature) and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/11 22:30
S74	609	(provid$4 send$4 transmit$4) near2 (master central primary global) near2 (server database) and (virus malware spyware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/11 22:35
S75	586	(provid$4 send$4 transmit$4 submit$4 post$4 report$4) adj2 (master central primary global) adj2 (server database) and (virus malware spyware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/11 22:36
S76	39	(Melvyn near Morris).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/11 23:33
S77	10	S76 and (malware).clm.	US-PGPUB;	OR	ON	2014/12/11

			USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB				23:34

EAST Search History (Interference)

<This search history is empty>

12/13/2014 8:37:04 PM
C:\Users\jchiang1\Documents\EAST\Workspaces\13372375-Malware.wsp

PATENT
Conf. No. 2918

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Morris, et al.	Examiner:	CHIANG, JASON
Serial No.:	13/372,375	Group Art Unit:	2431
Filed:	February 13, 2012	Docket No.:	04584.0012USU1
Title:	METHODS AND APPARATUS FOR DEALING WITH MALWARE		

Filed Via EFS-Web on June 22, 2015

AMENDMENT & RESPONSE TO NON-FINAL OFFICE ACTION

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Commissioner:

In response to the Non-Final Office Action mailed December 22, 2014, please amend the above-identified application as follows:

Amendments to the Claims are reflected in the listing of claims that begins on page 2 of this paper.

Remarks/Arguments begin on page 7 of this paper.

Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (Currently Amended) A method of classifying a computer object as malware, the method comprising:

receiving, at a first threat server, details of a first computer object from a first remote computer, wherein the details of the first computer object include data uniquely identifying the first computer object;

determining, by the first threat server, whether the first computer object has been previously seen by comparing the data uniquely identifying the first computer object to a plurality of data uniquely identifying plural computer objects in a first database associated with the first threat server;

receiving additional information about the first computer object from the first remote computer when the first computer object has not been previously seen;

storing the details of the first computer object and the received additional information about the first computer object in a second database associated with the first threat server when the first computer object has not been previously seen;

providing contents of the second database to at least one database associated with a central server, wherein the contents comprise a signature of the first computer object, behavior information about the first computer object, and information about the first remote computer;

increasing a count associated with a number of times that the first computer object has been seen, and providing the increased count associated with the number of times that the first computer object has been seen to [[a]] the central server; and

receiving, at a second threat server, at least a portion of the contents of the at least one database associated with the central server, wherein the at least a portion of the contents of the at least one database associated with the central server include a subset of the details of the first computer object stored in the second database.

2. (Previously Presented) The method according to claim 1, further comprising storing at intervals, the contents of the second database in storage together with a timestamp and clearing the second database.

3. (Previously Presented) The method according to claim 2, further comprising creating a backup central server by receiving at a second central server, all of the time-stamped blocks of data from the second database and incorporating all of the time-stamped blocks of data into at least one database associated with the second central server.

4. (Previously Presented) The method according to claim 2, further comprising:

taking the central server off-line for a period of time such that the central server does not receive data from the first and second threat servers during that period of time;

after the period of time has elapsed, updating at least one database associated with the central server with time-stamped blocks of data from the storage that have a timestamp later than the time when the central server went off-line; and

bringing the central server back on line.

5. (Previously Presented) The method according to claim 2, comprising:

rolling back at least one database associated with the central server to a point of time in the past;

updating the at least one database associated with the central server with time-stamped blocks of data from storage that have a timestamp later than the past point of time; and

bringing the central server back on line.

6. (Currently Amended) The method according to claim 2, wherein the central server ~~has one or more databases including at least one of~~ comprises:

a) an object database storing object signatures and metadata about [[that]] objects;

b) a behavior database storing object behavior information; and

c) a computer-object database storing information about what objects are present on what remote computers.

7. (Original) The method according to claim 6, wherein the threat and central servers are implemented using cloud computing.

8. (Canceled)

9. (Currently Amended) A system ~~An apparatus~~ for classifying a computer object as malware, the system ~~apparatus~~ comprising:

a first threat server arranged to receive details of a computer object from a first remote computer, wherein the details of the first computer object include data uniquely identifying the first computer object, wherein the first threat server is further arranged to receive the details of the computer object from the first remote computer and determine whether the first computer object has been previously seen by comparing the data uniquely identifying the first computer object to a plurality of data uniquely identifying plural computer objects in a first database associated with the first threat server, wherein the first threat server is further arranged to receive additional information about the first computer object from the first remote computer when the first computer object has not been previously seen, store the details of the first computer object and the received additional information about the first computer object in a second database associated with the first threat server when the first computer object has not been previously seen, provide contents of the second database to at least one database associated with a central server wherein the contents comprise a signature of the first computer object, behavior information about the first computer object, and information about the first remote computer, and increase a count associated with a number of times that the first computer object has been seen;

the [[a]] central server arranged to receive the increased count associated with the number of times that the first computer object has been seen; and

a second threat server arranged to receive at least a portion of the contents of the at least one database associated with the central server, wherein the at least a portion of the contents of the at least one database associated with the central server include a subset of the details of the first computer object stored in the second database.

Sophos Ex. 1002
Page 377 of 683

10. (Currently Amended) The system ~~apparatus~~ according to claim 9, wherein the first and second threat servers are arranged to store, at intervals, the contents of the second database in storage together with a timestamp and clear the database.

11. (Currently Amended) The system ~~apparatus~~ according to claim 10, further comprising:

a backup central server having a database, the database of the backup central server being populated by receiving at the backup central server all of the time-stamped blocks of data from the storage and incorporating them into the database of the backup central server.

12. (Currently Amended) The system ~~apparatus~~ according to claim 10, wherein, in the event that the central server is taken off-line for a period of time such that it does not receive updates of data from the first and second threat servers during that period of time, the central server is arranged to, after the period of time has elapsed, update at least one database with time-stamped blocks of data from the storage that have a timestamp later than the time when the central server went off-line.

13. (Currently Amended) The system ~~apparatus~~ according to claim 10, wherein, in the event that at least one database of a central server is rolled back to a point of time in the past, the central server is arranged to update the at least one database with time-stamped blocks of data from storage that have a timestamp later than the point of time in the past.

14. (Currently Amended) The system ~~apparatus~~ according to claim 9, wherein the central server ~~has one or more databases that include at least one of~~ comprises:

a) an object database storing object signatures and metadata about [[that]] objects;

b) a behavior database storing object behavior information; and

c) a computer-object database storing information about what objects are present on what remote computers.

15. (Currently Amended) The system ~~apparatus~~ according to claim 14, wherein the first and second threat servers and the central server are implemented using cloud computing.

16-24. (Canceled)

25. (Previously Presented) The method according to claim 1, further comprising:

receiving, at the second threat server, details of a second computer object from a second remote computer, wherein the details of the second computer object include data uniquely identifying the second computer object;

determining, by the second threat server, whether the second computer object has been previously seen by comparing the data uniquely identifying the second computer object to a plurality of data uniquely identifying plural computer objects in a third database associated with the second threat server;

determining that the second computer object has been seen before;

increasing a count associated with a number of times that the second computer object has been seen and providing the increased count associated with the number of times that the second computer object has been seen to the at least one central server; and

receiving, at the first threat server, a count associated with the number of times that the second computer object has been seen.

REMARKS/ARGUMENTS

This Amendment and the following remarks are intended to fully respond to the non-final Office Action dated December 22, 2014, hereinafter "Office Action." In that Office Action, claims 1-7, 9-15 and 25 were examined and all claims were rejected. Specifically, claims 1 and 9 were objected to for various informalities. Claims 1, 9, 14-15 and 25 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Boisjolie et al. (U.S. Pat. No. 8,332,946; hereinafter "Boisjolie") and Brennan (U.S. Publ. No. 2007/0028304; hereinafter "Brennan"). Claims 2, 6-7 and 10 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Boisjolie, Brennan as applied to claims 1, 9, 14-15, and 25, and in view of Nishikawa et al. (U.S. Publ. No. 2003/0093429; hereinafter "Nishikawa"). Claims 3 and 11 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Boisjolie, Brennan and Nishikawa as applied to claims 2, 6-7 and 10, and in view of Meyer et al. (U.S. Publ. No. 2011/0191341; hereinafter "Meyer"). Claims 4 and 12 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Boisjolie, Brennan and Nishikawa as applied to claims 2, 6-7 and 10, and in view of Chen et al. (U.S. Publ. No. 2009/0070304; hereinafter "Chen"). Claims 5 and 13 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Boisjolie, Brennan and Nishikawa as applied to claims 2, 6-7 and 10, and in view of McGrattan et al. (U.S. Pat. No. 7,814,056; hereinafter "McGrattan").

Reconsideration of these rejections, as they might apply to the original and amended claims in view of these remarks, is respectfully requested. In this Amendment, claims 1, 6, and 9-15 have been amended and no claims have been cancelled or added. Therefore, claims 1-7, 9-15 and 25 remain present for examination.

Claim Objections:

Claims 1 and 9 were objected to for various informalities. Claims 1 and 9 have been amended to recite "the central server." In light of these amendments, Applicants respectfully request that the Examiner withdraw the objections of claims 1 and 9 and allow the claims at the Examiner's earliest convenience.

Claim Rejections Under § 103:

Claims 1, 9, 14-15 and 25

Claims 1, 9, 14-15 and 25 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Boisjolie and Brennan. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

Aspects of the present disclosure relate to systems and methods for classifying a computer object as malware. A threat server may receive information about a computer object from a remote computer. The threat server may determine whether or not the first computer object has been previously seen. If the first object has not been previously seen, the threat server may receive additional information about the first computer object from the remote computer. The information about the computer object may be stored in a database associated with a central server. The information stored at the database associated with the central server can include a signature of the first computer object, behavior information about the first computer object, and information about the first remote computer.

Boisjolie generally discloses a malware protection method that prevents infected files form executing. *See* Boisjolie, Abstract. A file is compared against a whitelist. If the file is unknown, e.g., not on the whitelist, the file is scanned against a malware definition file. *See id.*, col. 2, ll. 40-67. If the file is determined to be good, then the whitelist is updated to include the file and the file is allowed to execute. *See* col. 7, ll. 51-67.

Turning now to the claims, Boisjolie fails to teach or suggest at least "providing contents of the second database to at least one database associated with a central server, wherein the contents comprise a signature of the first computer object, behavior information about the first

computer object, and information about the first remote computer," as recited in independent claim 1. Indeed, the Office Action admits that Boisjolie does not teach providing the contents of the second database to at least one database associated with a central server at all. *See* Office Action, p. 5. To be sure, Boisjolie cannot teach providing "a signature of the first computer object, behavior information about the first computer object, and information about the first remote computer" to a database associated with a central server when the reference fails to teach providing any information to a database associated with a central server.

Brennan fails to compensate for Boisjolie's deficiencies. Brennan generally discloses a digital antibody system that allows an administrator to monitor and control files installed on a large network of computers. The antibody system can also be used to provide defense from known an unknown viruses, works, spyware, hackers and social engineering attacks. Brennan teaches that a server maintains a database of metadata, referred to as antibodies, relating to analyses, such as scan histories. *See* Brennan, para. [0030]. The results of a scan history, however, does not teach providing "a signature of the first computer object, behavior information about the first computer object, and information about the first remote computer" to a database associated with a central server. Indeed, paragraphs [0085]-[0100] identify the different types of antibody data which can be stored, none of which include at least "a signature of the first computer object, behavior information about the first computer object, and information about the first remote computer." Thus, also fails to teach or suggest at least "providing contents of the second database to at least one database associated with a central server, wherein the contents comprise a signature of the first computer object, behavior information about the first computer object, and information about the first remote computer," as recited in independent claim 1, and therefore fails to compensate for the deficiencies of Boisjolie. Thus, claim 1 is allowable over the combination of the references.

For at least similar reasons, independent claim 9 is also allowable over the combination of Boisjolie and Brennan. Claim 9 recites, *inter alia*, "provide contents of the second database to at least one database associated with a central server wherein the contents comprise a signature of the first computer object, behavior information about the first computer object, and

information about the first remote computer." Thus, claim 9 is allowable for at least similar reasons as discussed with respect to independent claim 1.

For at least the foregoing reasons, independent claims 1 and 9 are allowable over the combination of Boisjolie and Brennan. All other claims, i.e., claims 14-15 and 25, depend from one of claims 1 or 9 and, thus, are also allowable. Applicants respectfully request that the Examiner issue a Notice of Allowance for claims 1, 9, 14-15 and 25.

Claims 2, 6-7 and 10

Claims 2, 6-7 and 10 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Boisjolie, Brennan as applied to claims 1, 9, 14-15, and 25, and in view of Nishikawa. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

Claims 2 and 6-7 depend from claim 1. For at least the reasons previously discussed, independent claim 1 is allowable over the combination of Boisjolie and Brennan. Furthermore, Nishikawa fails to compensate for their deficiencies. Nishikawa generally discloses,

> a data warehouse system includes a first database configured to receive first data from a first client, a data warehouse configured to receive second data corresponding to the first data from the first database after an interval to enable a second client to access the second data, and a dynamic database configured to receive third data corresponding to the first data from the first database prior to receipt of the second data by the data warehouse in order to provide the second client with access to the third data prior to the availability of the second data to the second client.

Nishikawa, para. [0007]. Nishikawa, however, fails to teach or suggest at least "providing contents of the second database to at least one database associated with a central server, wherein the contents comprise a signature of the first computer object, behavior information about the

first computer object, and information about the first remote computer," as recited in independent claim 1. To be sure, there is no teaching of "providing contents of the second database to at least one database associated with a central server" whatsoever, let alone the specific type of content recited in independent claim 1. Thus, claim 1 is allowable over the combination of Boisjolie, Brennan, and Nishikawa.

For at least similar reasons, independent claim 9 is also allowable over the combination of Boisjolie, Brennan, and Nishikawa. Claim 9 recites, *inter alia*, "provide contents of the second database to at least one database associated with a central server wherein the contents comprise a signature of the first computer object, behavior information about the first computer object, and information about the first remote computer." Thus, claim 9 is allowable for at least similar reasons as discussed with respect to independent claim 1.

For at least the foregoing reasons, independent claims 1 and 9 are allowable over the combination of Boisjolie, Brennan, and Nishikawa. All other claims, i.e., claims 2, 6-7, and 10, depend from one of claims 1 or 9 and, thus, are also allowable. Applicants respectfully request that the Examiner issue a Notice of Allowance for claims 2, 6-7, and 10.

Claims 3 and 11

Claims 3 and 11 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Boisjolie, Brennan and Nishikawa as applied to claims 2, 6-7 and 10, and in view of Meyer. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Further, under *KSR Int'l Co. v. Teleflex, Inc.*, there "must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." 127 S. Ct. 1727, 1741 (2007). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

Claim 3 depends from claim 1. For at least the reasons previously discussed, claim 1 is allowable over the combination of Boisjolie, Brennan, and Nishikawa. Meyer fails to compensate for their deficiencies. Meyer generally discloses,

> sharing the results of computing operations among related computing systems may include: 1) identifying a need to perform a computing operation on a file, 2) identifying a unique identifier associated with the file, 3) determining, by using the unique identifier to query a shared store that is shared by a group of related computing systems, that at least one computing system within the group of related computing systems has previously performed the computing operation on an instance of the file, and then 4) retrieving the results of the computing operation from the shared store instead of performing the computing operation.

Meyer, Abstract. Meyer, however, fails to teach or suggest at least "providing contents of the second database to at least one database associated with a central server, wherein the contents comprise a signature of the first computer object, behavior information about the first computer object, and information about the first remote computer," as recited in independent claim 1. Thus, claim 1 is allowable over the combination of Boisjolie, Brennan, Nishikawa, and Meyer.

For at least similar reasons, independent claim 9 is also allowable over the combination of Boisjolie, Brennan, Nishikawa, and Meyer. Claim 9 recites, *inter alia*, "provide contents of the second database to at least one database associated with a central server wherein the contents comprise a signature of the first computer object, behavior information about the first computer object, and information about the first remote computer." Thus, claim 9 is allowable for at least similar reasons as discussed with respect to independent claim 1.

For at least the foregoing reasons, independent claims 1 and 9 are allowable over the combination of Boisjolie, Brennan, Nishikawa, and Meyer. All other claims, i.e., claims 3 and 11, depend from one of claims 1 or 9 and, thus, are also allowable. Applicants respectfully request that the Examiner issue a Notice of Allowance for claims 3 and 11.

Claims 4 and 12

Claims 4 and 12 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Boisjolie, Brennan and Nishikawa as applied to claims 2, 6-7 and 10, and in view of Chen. Applicants respectfully traverse the § 103 rejection because the Office Action has not established

a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Further, under *KSR Int'l Co. v. Teleflex, Inc.*, there "must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." 127 S. Ct. 1727, 1741 (2007). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

Claim 4 depends from claim 1. For at least the reasons previously discussed, claim 1 is allowable over the combination of Boisjolie, Brennan, and Nishikawa. Chen fails to compensate for their deficiencies. Chen generally discloses an "improved automatically updated timestamp for database systems is disclosed. The automatically updated timestamp can be provided in a hidden timestamp column for a table, where the value of the timestamp column can be retrieved with a query that calls the column by name." Chen, Abstract. Chen, however, fails to teach or suggest at least "providing contents of the second database to at least one database associated with a central server, wherein the contents comprise a signature of the first computer object, behavior information about the first computer object, and information about the first remote computer," as recited in independent claim 1. Thus, claim 1 is allowable over the combination of Boisjolie, Brennan, Nishikawa, and Chen.

For at least similar reasons, independent claim 9 is also allowable over the combination of Boisjolie, Brennan, Nishikawa, and Chen. Claim 9 recites, *inter alia*, "provide contents of the second database to at least one database associated with a central server wherein the contents comprise a signature of the first computer object, behavior information about the first computer object, and information about the first remote computer." Thus, claim 9 is allowable for at least similar reasons as discussed with respect to independent claim 1.

For at least the foregoing reasons, independent claims 1 and 9 are allowable over the combination of Boisjolie, Brennan, Nishikawa, and Chen. All other claims, i.e., claims 4 and 12, depend from one of claims 1 or 9 and, thus, are also allowable. Applicants respectfully request that the Examiner issue a Notice of Allowance for claims 4 and 12.

Sophos Ex. 1002
Page 386 of 683

Claims 5 and 13

Claims 5 and 13 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Boisjolie, Brennan and Nishikawa as applied to claims 2, 6-7 and 10, and in view of McGrattan. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

Claim 5 depends from claim 1. For at least the reasons previously discussed, claim 1 is allowable over the combination of Boisjolie, Brennan, and Nishikawa. McGrattan fails to compensate for their deficiencies. McGrattan generally discloses "backing up data to a database are provided. A specified data set to be backed up is broken down into a plurality of data blocks, each data block is associated with a data block digest, and the data blocks and associated data block digests are stored in the database." McGrattan, Abstract. McGrattan, however, fails to teach or suggest at least "providing contents of the second database to at least one database associated with a central server, wherein the contents comprise a signature of the first computer object, behavior information about the first computer object, and information about the first remote computer," as recited in independent claim 1. Thus, claim 1 is allowable over the combination of Boisjolie, Brennan, Nishikawa, and McGrattan.

For at least similar reasons, independent claim 9 is also allowable over the combination of Boisjolie, Brennan, Nishikawa, and McGrattan. Claim 9 recites, *inter alia*, "provide contents of the second database to at least one database associated with a central server wherein the contents comprise a signature of the first computer object, behavior information about the first computer object, and information about the first remote computer." Thus, claim 9 is allowable for at least similar reasons as discussed with respect to independent claim 1.

For at least the foregoing reasons, independent claims 1 and 9 are allowable over the combination of Boisjolie, Brennan, Nishikawa, and McGrattan. All other claims, i.e., claims 5 and 13, depend from one of claims 1 or 9 and, thus, are also allowable. Applicants respectfully request that the Examiner issue a Notice of Allowance for claims 5 and 13.

Sophos Ex. 1002
Page 388 of 683

CONCLUSION

This Amendment fully responds to the Office Action mailed on December 22, 2014. Still, that Office Action may contain arguments and rejections that are not directly addressed by this Amendment due to the fact that they are rendered moot in light of the preceding arguments in favor of patentability. Hence, failure of this Amendment to directly address an argument raised in the Office Action should not be taken as an indication that the Applicants believe the argument has merit. Furthermore, the claims of the present application may include other elements, not discussed in this Amendment, which are not shown, taught, or otherwise suggested by the references of record. Accordingly, the preceding arguments in favor of patentability are advanced without prejudice to other bases of patentability.

This Amendment is filed concurrently with a Petition for Extension of Time. It is believed that no further fees are due with this Response. However, the Commissioner is hereby authorized to charge any deficiencies or credit any overpayment with respect to this patent application to deposit account number 13-2725.

In light of the above remarks and amendments, it is believed that the application is now in condition for allowance and such action is respectfully requested. Should any additional issues need to be resolved, the Examiner is requested to telephone the undersigned to attempt to resolve those issues.

Respectfully submitted,

Dated: June 22, 2015

/Andrew T. Pouzeshi/
Andrew T. Pouzeshi, Reg. No. 67,672
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1639

23552
PATENT TRADEMARK OFFICE

Electronic Patent Application Fee Transmittal

Application Number:	13372375
Filing Date:	13-Feb-2012
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate
Attorney Docket Number:	04584.0012USU1

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $0 paid	2253	1	700	700
Miscellaneous:				
			Total in USD ($)	**700**

Electronic Acknowledgement Receipt

EFS ID:	22703320
Application Number:	13372375
International Application Number:	
Confirmation Number:	2918
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Customer Number:	23552
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate
Filer Authorized By:	Andrew T. Pouzeshi
Attorney Docket Number:	04584.0012USU1
Receipt Date:	22-JUN-2015
Filing Date:	13-FEB-2012
Time Stamp:	17:24:16
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$700
RAM confirmation Number	4391
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Extension of Time	2015_06_22_EOT_04584_0012USU1.PDF	194541 d9471d9e2acb25e712bd62bcb0c228b6585a1416	no	2
Warnings:					
Information:					
2		2015_06_22_RespNFOA_of_122214_04584_0012USU1.pdf	151192 459795f40f04e77a58c7c6f0ea38ed35d5f76d64	yes	16

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Claims	2	6
Applicant Arguments/Remarks Made in an Amendment	7	16

Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30749 9791ff222bc3f645c9ecd05cb497f0a914423fda	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	376482	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/22 (03-13)
Approved for use through 3/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): 04584.0012USU1

Application Number: 13/372,375

Filed: February 13, 2012

For: METHODS AND APPARATUS FOR DEALING WITH MALWARE

Art Unit: 2431

Examiner: CHIANG, JASON

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☐ Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
☑ Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$ 700.00
☐ Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐ Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☑ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 132725.

☑ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71. 37 CFR 3.73(b) statement is enclosed (Form PTO/SB/96).

☑ attorney or agent of record. Registration number 67672.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/Andrew T. Pouzeshi/ — Signature

June 22, 2015 — Date

Andrew T. Pouzeshi — Typed or printed name

303-357-1639 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☐ * Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/372,375	Filing Date 02/13/2012	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT **06/22/2015**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 15	Minus	** 24	= 0	X $80 =	0
Independent (37 CFR 1.16(h))	* 2	Minus	***4	= 0	X $420 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/Kelley Dantzler/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

23552 7590 08/05/2015

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER
CHIANG, JASON

ART UNIT	PAPER NUMBER
2431	

DATE MAILED: 08/05/2015

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/372,375	02/13/2012	Melvyn Morris	04584.0012USU1	2918

TITLE OF INVENTION: METHODS AND APPARATUS FOR DEALING WITH MALWARE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	11/05/2015

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

23552 7590 08/05/2015
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/372,375	02/13/2012	Melvyn Morris	04584.0012USU1	2918

TITLE OF INVENTION: METHODS AND APPARATUS FOR DEALING WITH MALWARE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	11/05/2015

EXAMINER	ART UNIT	CLASS-SUBCLASS
CHIANG, JASON	2431	726-023000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ❑ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ❑ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

Sophos Ex. 1002
Page 399 of 683

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/372,375	02/13/2012	Melvyn Morris	04584.0012USU1	2918

23552 7590 08/05/2015

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
CHIANG, JASON	
ART UNIT	PAPER NUMBER
2431	

DATE MAILED: 08/05/2015

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 13/372,375	Applicant(s) MORRIS ET AL.	
	Examiner JASON C. CHIANG	Art Unit 2431	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *06/22/2015*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1-7, 9-15 and 25*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☐ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/JASON C CHIANG/
Examiner, Art Unit 2431

1. The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

Notice to Applicants

2. This communication is in response to the Amendment filed on 06/22/2015.

3. Claims 1-7, 9-15 and 25 are under examination.

Allowable Subject Matter

4. Claims 1-7, 9-15 and 25 are allowed.

5. This communication warrants No Examiner's Reason for Allowance, applicant's reply make evident the reasons for allowance, satisfying the “record as a whole” proviso of the rule 37 CFR 1.104(e). Specifically, applicant’s arguments filed on 06/22/2015 are persuasive, as such the reasons for allowance are in all probability evident from the record and no statement is deemed necessary (see MPEP 1302.14).

6. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to Applicant's disclosure:

US 8195938 B2 Cloud-based application whitelisting

US 8296178 B2 Services using globally distributed infrastructure for secure content management

US 7231440 B1 System and method for distributing portable computer virus definition records with binary file conversion

US 8347386 B2 System and method for server-coupled malware prevention

US 8448243 B1 Systems and methods for detecting unknown malware in an executable file

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JASON C. CHIANG whose telephone number is (571)270-3393. The examiner can normally be reached on 9AM to 6PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, CORDELIA P. ZECHER can be reached on (571) 272-7771. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/J. C. C./
Examiner, Art Unit 2431

/CORDELIA ZECHER/
Supervisory Patent Examiner, Art Unit 2431

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13372375	MORRIS ET AL.
	Examiner	Art Unit
	JASON C CHIANG	2431

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	23	06/04/2013	JC

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor search in East	06/04/2013	JC
Text search in East of USPGPUB, USPAT, USOCR, FPRS, EPO, JPO, DERWENT, IBM_TDB	06/05/2013	JC
Inventor search in East	12/14/2013	JC
Text search in East of USPGPUB, USPAT, USOCR, FPRS, EPO, JPO, DERWENT, IBM_TDB	12/14/2013	JC
Inventor search in East	12/11/2014	JC
Text search in East of USPGPUB, USPAT, USOCR, FPRS, EPO, JPO, DERWENT, IBM_TDB	12/11/2014	JC
Inventor search in East	7/30/2015	JC
Text search in East of USPGPUB, USPAT, USOCR, FPRS, EPO, JPO, DERWENT, IBM_TDB	7/30/2015	JC

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/JASON C CHIANG/ Examiner.Art Unit 2431	

INTERFERENCE SEARCH			
US Class/ CPC Symbol	**US Subclass / CPC Group**	**Date**	**Examiner**
H04L	63/14	7/30/2015	JC
G06F	21/56	7/30/2015	JC

/JASON C CHIANG/ Examiner.Art Unit 2431	

Sophos Ex. 1002
Page 407 of 683

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13372375	MORRIS ET AL.
	Examiner	**Art Unit**
	JASON C CHIANG	2431

CPC								
Symbol							**Type**	**Version**
H04L		63	/	0263			F	2013-01-01
H04L		63	/	14			I	2013-01-01
G06F		21	/	56			I	2013-01-01
G06F		21	/	566			I	2013-01-01
H04L		63	/	145			I	2013-01-01
			/					
			/					
			/					
			/					
			/					
			/					
			/					
			/					
			/					
			/					

CPC Combination Sets								
Symbol						**Type**	**Set**	**Ranking**	**Version**
			/						
			/						

/JASON C CHIANG/ Examiner.Art Unit 2431	07/30/2015	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	15	
		O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13372375	MORRIS ET AL.
	Examiner	**Art Unit**
	JASON C CHIANG	2431

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION									
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED				
726	23	H	0	4	L	29 / 06 (2006.01.01)	H	0	4	L	29 / 06 (2006.01.01)
		G	0	6	F	21 / 56 (2013.01.01)	G	0	6	F	21 / 56 (2013.01.01)

CROSS REFERENCE(S)																					
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)																				

/JASON C CHIANG/ Examiner.Art Unit 2431	07/30/2015	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	15	
		O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13372375	MORRIS ET AL.
	Examiner	**Art Unit**
	JASON C CHIANG	2431

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1		17												
2	2		18												
3	3		19												
4	4		20												
5	5		21												
6	6		22												
7	7		23												
	8		24												
9	9	8	25												
10	10														
11	11														
12	12														
13	13														
14	14														
15	15														
	16														

/JASON C CHIANG/ Examiner.Art Unit 2431	07/30/2015	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	15	
		O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	544	(virus malware) and signature same behavior same (identifier ID IP computer) and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 19:55
L2	134	(virus malware) and signature same behavior same (identifier ID) and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 19:56
L3	64	(virus malware) and signature same behavior same (identifier) and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 19:57
L6	130	(virus malware) and signature same behavior same (infected) and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 20:27
L7	47	(virus malware) and (stor$4 receiv$4 send$4 provid$4) same signature same behavior same (infected) and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 20:28
L8	58	(virus malware) and (stor$4 receiv$4 send$4 provid$4) same signature same behavior same (list) and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 20:32
L9	41	(Melvyn near Morris).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 20:53
L10	20	(Joseph near Jaroch).in.	US-PGPUB;	OR	ON	2015/07/30

			USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			20:54
S1	9	(Melvyn near Morris).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 11:48
S2	3	(Joseph near Jaroch).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 16:51
S3	108	(Webroot).as.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 16:54
S5	0	S3 and cloud and database and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 16:58
S6	2980	(726/23).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/06/04 17:04
S7	72	S6 and cloud and database and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 17:05
S8	54	("20100043072" | "20110197272" | "20090300764" | "20100064368" | "20120017200" | "20060101334" | "20090292791" | "20100306851" | "20110138361" | "8042184" | "20060069912" | "20120260304" | "7707634" | "7343626" | "20070016953" | "20110197177" | "20120266208" | "20060117055" | "20100313183" | "20110083183" | "8146135" | "8307435").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/05 11:39
S9	21	("2006/0069912").URPN.	USPAT	OR	ON	2013/06/05 11:59
S10	17	threat adj server	USPAT	OR	ON	2013/06/05 12:20

S11	2362	cloud and signature	USPAT	OR	ON	2013/06/05 13:23
S12	1181	cloud and signature and layer	USPAT	OR	ON	2013/06/05 13:23
S13	249	cloud and (signature with database)	USPAT	OR	ON	2013/06/05 13:25
S14	78	cloud and (signature with database) and (malware virus)	USPAT	OR	ON	2013/06/05 13:26
S15	143	cloud and (updat$4 near3 (signature database)) and (malware virus)	USPAT	OR	ON	2013/06/05 16:30
S16	65	(updat$4 near3 (signature database) near3 (interval certain period periodic)) and (malware virus)	USPAT	OR	ON	2013/06/05 20:09
S17	1	(09/740294).APP.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/06/05 20:37
S18	0	("(masteradjdatabase)and(virusmalwaresignature)").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/06/07 18:03
S19	1003	(master adj database) and (virus malware signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:04
S20	160	(master adj database) and (virus malware) and signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:05
S21	971	(database) and (virus near signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:33
S22	639	((stor$4 sav$4 receiv$5) with database) and (virus near signature) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:51
S23	594	((stor$4 sav$4 receiv$5) near5 database) and (virus near signature) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	OR	ON	2013/06/07 18:51

			IBM_TDB			
S24	64	((stor$4 sav$4 receiv$5) near5 database) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 10:51
S25	0	((stor$4 sav$4 receiv$5) near3 content near3 database near3 storage) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:02
S26	0	((stor$4 sav$4 receiv$5) near3 database near3 storage) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:03
S27	2	((stor$4 sav$4 receiv$5) near3 content near3 database near3 storage) with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:03
S28	0	((backup) near3 database) with timestamp and (virus malware)and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:05
S29	0	((backup) near3 database) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:06
S30	27	((backup) near3 database) with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:06
S31	1139	((copy stor$4) near3 database) with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:20
S32	18	((copy stor$4) near3 database) with central with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS;	OR	ON	2013/06/08 11:21

			EPO; JPO; DERWENT; IBM_TDB			
S33	359	((purg$4 clear$4 remov$4) near3 database near3 (period$6 every)) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:29
S34	0	(master adj database) near2 (virus malware) near2 signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S35	0	(master adj database) near3 (virus malware) near3 signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S36	0	(master adj database) with (virus malware) with signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S37	0	(master adj database) same (virus malware) same signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S38	19	(master adj database) same (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:45
S39	15	((primary secondary) adj database) same (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:54
S40	30	((primary secondary) adj database) with (signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:57
S41	98	(master adj database) same (signature)	US-PGPUB; USPAT;	OR	ON	2013/06/08 15:59

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S42	10	(master adj database) same (signature) and (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:59
S43	315	(master adj database) and (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 16:03
S44	18	(virus malware) with definition with (file database) with (cloud community share$2)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 16:21
S45	271	(update refresh recover rebuild) near3 (database) with timestamp	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 20:22
S46	4	(update refresh recover rebuild) near3 (database) with timestamp same (offline off-line (off adj line) disconnect reconnect)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 20:24
S47	1	((roll$3 adj back) near6 time) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:11
S48	7	((roll$3 adj back)) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:12
S49	11	((roll$3 adj back) rollback) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:14

S50	48	((roll$3 adj back) rollback) and ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:18
S51	21	(((roll$3 adj back) rollback) with time) and ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:23
S52	0	((restor$4) near6 time) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 11:40
S53	3	((restor$4) near6 time) and ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 11:41
S54	0	(send provid$3 transmit$4 updat$3) near3 (count near3 (threat incident)) near3 (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:01
S55	22	(send provid$3 transmit$4 updat$3) with ((count number) near3 (threat incident)) with (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:02
S56	122	(send provid$3 transmit$4 updat$3 record$4) with ((count number times) with (threat)) with (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:05
S57	635	(send provid$3 transmit$4 updat$3 record$4) with ((count number times) near5 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:08
S58	199	(send provid$3 transmit$4 updat$3 record$4) with ((count number) near5 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2013/06/09 15:09

			DERWENT; IBM_TDB			
S59	11	(send provid$3 transmit$4 updat$3 record$4) with ((count) near5 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:11
S60	43	((count) near2 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:15
S61	9	((count) near2 (threat)) and (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:15
S62	1126	(send provid$3 transmit$4 updat$3) near3 (count) near3 (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:18
S63	15	(send provid$3 transmit$4 updat$3) near3 ((increas$4 add$3) near (count)) near3 (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:20
S64	1816	((increas$4 add$3) near (count)) and (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:22
S65	27	((increas$4 add$3) near (count)) and (malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:23
S66	9	(Melvyn near Morris).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:29
S67	3	(Joseph near Jaroch).in.	US-PGPUB; USPAT; USOCR;	OR	ON	2013/12/14 16:30

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S68	813	((increas$4 add$3 generat$4) near (count)) and (malware threat)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:31
S69	742	((increas$4 add$3 generat$4) near (count)) and (malware threat) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:32
S70	0	(((seen identified) near (before previous)) with (increas$4 add$3 generat$4) near (count)) and (malware threat) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:33
S71	0	(((seen identified) near (before previous)) same ((increas$4 add$3 generat$4) near (count))) and (malware threat) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:33
S72	48	(((seen identified)) same ((increas$4 add$3 generat$4) near (count))) and (malware threat) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:33
S73	347	(master central primary global) near2 (server database) same (signature) and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/11 22:30
S74	609	(provid$4 send$4 transmit$4) near2 (master central primary global) near2 (server database) and (virus malware spyware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/11 22:35
S75	586	(provid$4 send$4 transmit$4 submit$4 post$4 report$4) adj2 (master central primary global) adj2 (server database) and (virus malware spyware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/11 22:36
S76	39	(Melvyn near Morris).in.	US-PGPUB;	OR	ON	2014/12/11

			USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			23:33
S77	10	S76 and (malware).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/11 23:34
S78	190	("20100043072" | "20100332593" | "8453244" | "7051365" | "20110197272" | "20090300764" | "20100064368" | "20120017200" | "8301904" | "8347386" | "8352484" | "20060080637" | "20090172774" | "20060101334" | "20090292791" | "20100306851" | "20110138361" | "8042184" | "7231440" | "8321944" | "20090089040" | "20060272020" | "20060069912" | "20120260304" | "7707634" | "20110191299" | "20110191341" | "7814056" | "7921063" | "8116732" | "20070220043" | "20080115190" | "7343626" | "20030093429" | "20090070304" | "7188173" | "8234709" | "8296178" | "8321540" | "8332946" | "8448243" | "20070174429" | "6175869" | "20080148381" | "20070016953" | "20110197177" | "20120266208" | "8336100" | "8347375" | "20060080637" | "20060117055" | "20100313183" | "20110083183" | "8146135" | "8307435" | "8195938" | "8443447" | "20060272020" | "8225218" | "8276202" | "20030188194" | "20050187740" | "20080115190" | "20080148381" | "6219786" | "20070220043").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/13 20:26
S79	6016	(726/23).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/12/13 20:27
S80	173	S78 NOT S79	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/13 20:27
S81	70	("20100043072" | "20110197272" | "20090300764" | "20100064368" | "20120017200" | "20060101334" | "20090292791" | "20100306851" | "20110138361" | "8042184" | "20060069912" | "20120260304" | "7707634" | "7343626" | "20070016953" | "20110197177" | "20120266208" | "20060117055" | "20100313183" | "20110083183" | "8146135" | "8307435").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/13 20:27
S82	120	S78 NOT S81	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	OR	ON	2014/12/13 20:27

			IBM_TDB			

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L4	2722	(H04L63/14 G06F21/56).CPC.	US-PGPUB; USPAT; UPAD	OR	ON	2015/07/30 20:11
L5	20	L4 and (signature).clm. and (behavior).clm. and (database).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2015/07/30 20:13

7/ 30/ 2015 9:03:58 PM
C:\ Users\ jchiang1\ Documents\ EAST\ Workspaces\ 13372375-Malware.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13372375	MORRIS ET AL.
	Examiner	**Art Unit**
	JASON C CHIANG	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/09/2013	12/14/2013	12/13/2014	07/30/2015					
1	1	✓	✓	✓	=					
2	2	✓	✓	✓	=					
3	3	✓	✓	✓	=					
4	4	✓	✓	✓	=					
5	5	✓	✓	✓	=					
6	6	✓	✓	✓	=					
7	7	✓	✓	✓	=					
	8	✓	-	-	-					
9	9	✓	✓	✓	=					
10	10	✓	✓	✓	=					
11	11	✓	✓	✓	=					
12	12	✓	✓	✓	=					
13	13	✓	✓	✓	=					
14	14	✓	✓	✓	=					
15	15	✓	✓	✓	=					
	16	✓	-	-	-					
	17	N	N	N	N					
	18	N	N	N	N					
	19	N	N	N	N					
	20	N	N	N	N					
	21	N	N	N	N					
	22	N	N	N	N					
	23	N	N	N	N					
	24	N	N	N	N					
8	25			✓	=					

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/372,375	02/13/2012	Melvyn Morris	04584.0012USU1	2918

23552 7590 08/18/2015

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
CHIANG, JASON	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
08/18/2015	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPTO23552@merchantgould.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

Application No. : 13372375
Applicant : Morris
Filing Date : 02/13/2012
Date Mailed : 08/18/2015

NOTICE TO FILE CORRECTED APPLICATION PAPERS

Notice of Allowance Mailed

This application has been accorded an Allowance Date and is being prepared for issuance. The application, however, is incomplete for the reasons below.

Applicant is given two (2) months from the mail date of this Notice within which to respond. This time period for reply is extendable under 37 CFR 1.136(a) for only TWO additional MONTHS.

The informalities requiring correction are indicated in the attachment(s). If the informality pertains to the abstract, specification (including claims) or drawings, the informality must be corrected with an amendment in compliance with 37 CFR 1.121 (or, if the application is a reissue application, 37 CFR 1.173). Such an amendment may be filed after payment of the issue fee if limited to correction of informalities noted herein. See Waiver of 37 CFR 1.312 for Documents Required by the Office of Patent Publication, 1280 Off. Gaz. Patent Office 918 (March 23, 2004). In addition, if the informality is not corrected until after payment of the issue fee, for purposes of 35 U.S.C. 154(b)(1)(iv), "all outstanding requirements" will be considered to have been satisfied when the informality has been corrected. A failure to respond within the above-identified time period will result in the application being ABANDONED.

See attachment(s).

A copy of this notice MUST be returned with the reply. Please address response to "Mail Stop Issue Fee, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450".

/Joseph Boris/
Publication Branch
Office of Data Management
(571) 272-4200

Application No. 13372375

IDENTIFICATION OF APPLICATION DEFICIENCIES IN APPLICATION FILED BEFORE SEPTEMBER 16, 2012

☐ Applicant must provide legible text for the following item(s).

- ☐ Specification filed , page(s) .
- ☐ Claims filed , claim(s) .
- ☐ Other:

☐ Applicant must provide missing information on the following page(s) of the specification by amending the specification to add the missing text. No new matter may be added.
Page/line no(s).

☒ The specification refers to one or more applications by attorney docket number and does not show the U.S. application number(s). Applicant must supply the U.S. application number in place of each attorney docket number.
Page/line no(s). 1, paragraph 0002

☐ Applicant must provide an Abstract of the Disclosure.

☐ The Application Data Sheet (ADS dated) did not show the inventor's residence at all, or did not show both a city and state in the U.S. inventor's residence, or did not show both a city and country in the non-U.S. inventor's residence. Applicant must supply a Supplemental Application Data Sheet (ADS) that shows each U.S. inventor's city and state of residence and each non-U.S. inventor's city and country of residence. To be in compliance with 37 CFR 1.76, the Supplemental Application Data Sheet must identify the information being changed by using underlining for additions and strikethroughs or brackets for deletions.

☐ Other:

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Morris, et al.	Examiner:	Chiang, Jason
Serial No.:	13/372,375	Group Art Unit:	2431
Filed:	February 13, 2012	Docket No.:	04584.0012USU1
Title:	METHODS AND APPARATUS FOR DEALING WITH MALWARE		

Filed Via EFS-Web on October 19, 2015

AMENDMENT UNDER 37 C.F.R. § 1.312

Mail Stop Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Commissioner:

In response to the Notice to File Corrected Application Papers mailed August 18, 2015, please amend the above-identified application pursuant to 37 C.F.R. 1.312 as follows:

Amendments to the Specification begin on page 2 of this paper.

Remarks begin on page 3 of this paper.

Amendments to the Specification

Please amend the Specification, at page 1, paragraph [0002], as follows:

Reference to Co-Pending Applications for Patent

[0002] The present Application for Patent is related to the following ~~co-pending~~ U.S. Patent Applications: co-pending U.S. Patent Application Serial No. 13/372,433, entitled "METHODS AND APPARATUS FOR MALWARE THREAT RESEARCH," ~~having Attorney Docket No. 9400.004.03, filed concurrently herewith,~~ assigned to the assignee hereof, and expressly incorporated by reference herein; and U.S. Patent Application Serial No. 13/372,439, entitled "METHODS AND APPARATUS FOR AGENT-BASED MALWARE MANAGEMENT" ~~having Attorney Docket No. 9400.004.04~~, now abandoned, ~~filed concurrently herewith,~~ assigned to the assignee hereof, and expressly incorporated by reference herein.

Sophos Ex. 1002
Page 427 of 683

Remarks

In this Amendment under 37 C.F.R. § 1.312, the specification has been amended to update the related applications. No new matter has been added. Applicants respectfully request that the Examiner enter this Amendment under 37 C.F.R. § 1.312.

Submitted herewith is a copy of the Notice to File Corrected Application Papers, as requested. It is believed that no further fees are due with this Response. However, the Commissioner is hereby authorized to charge any deficiencies or credit any overpayment with respect to this patent application to deposit account number 13-2725.

Respectfully submitted,

Dated: October 19, 2015

/Andrew T. Pouzeshi/
Andrew T. Pouzeshi, Reg. No. 67,672
Merchant & Gould P.C.
PO Box 2903
Minneapolis, MN 55402-0903
303.357.1639

23552
PATENT TRADEMARK OFFICE

Sophos Ex. 1002
Page 428 of 683

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/372,375	02/13/2012	Melvyn Morris	04584.0012USU1	2918

23552 7590 08/18/2015

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
CHIANG, JASON	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
08/18/2015	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPTO23552@merchantgould.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

Application No. : 13372375
Applicant : Morris
Filing Date : 02/13/2012
Date Mailed : 08/18/2015

NOTICE TO FILE CORRECTED APPLICATION PAPERS

Notice of Allowance Mailed

This application has been accorded an Allowance Date and is being prepared for issuance. The application, however, is incomplete for the reasons below.

Applicant is given two (2) months from the mail date of this Notice within which to respond. This time period for reply is extendable under 37 CFR 1.136(a) for only TWO additional MONTHS.

The informalities requiring correction are indicated in the attachment(s). If the informality pertains to the abstract, specification (including claims) or drawings, the informality must be corrected with an amendment in compliance with 37 CFR 1.121 (or, if the application is a reissue application, 37 CFR 1.173). Such an amendment may be filed after payment of the issue fee if limited to correction of informalities noted herein. See Waiver of 37 CFR 1.312 for Documents Required by the Office of Patent Publication, 1280 Off. Gaz. Patent Office 918 (March 23, 2004). In addition, if the informality is not corrected until after payment of the issue fee, for purposes of 35 U.S.C. 154(b)(1)(iv), "all outstanding requirements" will be considered to have been satisfied when the informality has been corrected. A failure to respond within the above-identified time period will result in the application being ABANDONED.

See attachment(s).

A copy of this notice MUST be returned with the reply. Please address response to "Mail Stop Issue Fee, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450".

/Joseph Boris/
Publication Branch
Office of Data Management
(571) 272-4200

Application No. 13372375

IDENTIFICATION OF APPLICATION DEFICIENCIES IN APPLICATION FILED BEFORE SEPTEMBER 16, 2012

☐ Applicant must provide legible text for the following item(s).

- ☐ Specification filed , page(s) .
- ☐ Claims filed , claim(s) .
- ☐ Other:

☐ Applicant must provide missing information on the following page(s) of the specification by amending the specification to add the missing text. No new matter may be added.
Page/line no(s).

☒ The specification refers to one or more applications by attorney docket number and does not show the U.S. application number(s). Applicant must supply the U.S. application number in place of each attorney docket number.
Page/line no(s). 1, paragraph 0002

☐ Applicant must provide an Abstract of the Disclosure.

☐ The Application Data Sheet (ADS dated) did not show the inventor's residence at all, or did not show both a city and state in the U.S. inventor's residence, or did not show both a city and country in the non-U.S. inventor's residence. Applicant must supply a Supplemental Application Data Sheet (ADS) that shows each U.S. inventor's city and state of residence and each non-U.S. inventor's city and country of residence. To be in compliance with 37 CFR 1.76, the Supplemental Application Data Sheet must identify the information being changed by using underlining for additions and strikethroughs or brackets for deletions.

☐ Other:

Electronic Acknowledgement Receipt

EFS ID:	23821804
Application Number:	13372375
International Application Number:	
Confirmation Number:	2918
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Customer Number:	23552
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate
Filer Authorized By:	Andrew T. Pouzeshi
Attorney Docket Number:	04584.0012USU1
Receipt Date:	19-OCT-2015
Filing Date:	13-FEB-2012
Time Stamp:	14:43:59
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		2015-10-19_312Amdt_04584_0012USU1.PDF	197261 a9e311097194ad2fa7fe6bf659f74739a3f354f4	yes	6

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment after Notice of Allowance (Rule 312)	1	1
	Specification	2	2
	Applicant Arguments/Remarks Made in an Amendment	3	6
Warnings:			
Information:			
	Total Files Size (in bytes):	197261	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/372,375	02/13/2012	Melvyn Morris	04584.0012USU1	2918

23552 7590 10/23/2015
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER
CHIANG, JASON

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
10/23/2015	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPTO23552@merchantgould.com

Response to Rule 312 Communication	Application No. 13/372,375	Applicant(s)
	Examiner	Art Unit

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address –

1. ☒ The amendment filed on *19 October 2015* under 37 CFR 1.312 has been considered, and has been:

a) ☒ entered.

b) ☐ entered as directed to matters of form not affecting the scope of the invention.

c) ☐ disapproved because the amendment was filed after the payment of the issue fee.
Any amendment filed after the date the issue fee is paid must be accompanied by a petition under 37 CFR 1.313(c)(1) and the required fee to withdraw the application from issue.

d) ☐ disapproved. See explanation below.

e) ☐ entered in part. See explanation below.

L.HILL

PUBLISHING DIVISION

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	13372375	Filing Date	2012-02-13	Docket Number (if applicable)	04584.0012USU1	Art Unit	2431
First Named Inventor	Melvyn Morris			Examiner Name	CHIANG, JASON		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☐ Other _____

☒ Enclosed

- ☐ Amendment/Reply
- ☒ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____ (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 132725

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

☐ Applicant Signature

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/Andrew T. Pouzeshi/	Date (YYYY-MM-DD)	2015-11-05
Name	Andrew T. Pouzeshi	Registration Number	67672

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PATENT
Conf. No. 2918

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Morris, et al.	Examiner:	CHIANG, JASON
Serial No.:	13/372375	Group Art Unit:	2431
Filed:	February 13, 2012	Docket No.:	04584.0012USU1
Title:	METHODS AND APPARATUS FOR DEALING WITH MALWARE		

Filed via EFS-Web

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT (37 C.F.R. § 1.97(b))

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Attention: Commissioner for Patents

With regard to the above-identified application, the items of information listed on the enclosed Form 1449 are brought to the attention of the Examiner.

This statement should be considered because it is submitted before the mailing of a first Office Action after the filing of a Request for Continued Examination under 37 C.F.R. § 1.114 or a CPA under 37 C.F.R. § 1.53(d). Accordingly, no fee is due for consideration of the items listed on the enclosed Form 1449.

In accordance with 37 C.F.R. §1.98(a)(2), a copy of each foreign patent and/or a copy of each publication, other than U.S. patents and U.S. patent application publications, listed on the accompanying Form 1449 is enclosed.

No representation is made that a reference is "prior art" within the meaning of 35 U.S.C. §§ 102 and 103 and Applicants reserve the right, pursuant to 37 C.F.R. § 1.131 or otherwise, to establish that the reference(s) are not "prior art." Moreover, Applicants do not represent that a reference has been thoroughly reviewed or that any relevance of any portion of a reference is intended.

Consideration of the items listed is respectfully requested. Pursuant to the provisions of M.P.E.P. 609, it is requested that the Examiner return a copy of the attached Form 1449, marked

as being considered and initialed by the Examiner, to the undersigned with the next official communication.

Please charge any additional fees or credit any overpayment to Deposit Account No. 13-2725.

Respectfully submitted,

Dated: November 5, 2015

/Andrew T. Pouzeshi/

Andrew T. Pouzeshi, Reg. No. 67,672
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1639

23552
PATENT TRADEMARK OFFICE

Sophos Ex. 1002
Page 440 of 683

PATENT
Conf. No. 2918

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Morris, et al.	Examiner:	CHIANG, JASON
Serial No.:	13/372,375	Group Art Unit:	2431
Filed:	February 13, 2012	Docket No.:	04584.0012USU1
Title:	METHODS AND APPARATUS FOR DEALING WITH MALWARE		

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

ASSERTION OF SMALL ENTITY STATUS PURSUANT TO 37 C.F.R. §1.27 (c)(1)

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Commissioner:

The assignee of the above-identified application, Webroot Inc., hereby asserts that it is entitled to small entity status as defined in 37 C.F.R. 1.27.

Respectfully submitted,

Dated: November 5, 2015

/Andrew T. Pouzeshi/
Andrew T. Pouzeshi, Reg. No. 67,672
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1639

23552
PATENT TRADEMARK OFFICE

FORM 1449* INFORMATION DISCLOSURE STATEMENT IN AN APPLICATION (Use several sheets if necessary)	Docket Number: 04584.0012USU1	Application Number: 13/372,375
	Inventor: Melvyn Morris	
	Filing Date: 02-13-2012	Group Art Unit: 2431

U.S. PATENT DOCUMENTS						
EXAMINER INITIAL	DOCUMENT NO.	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	6,842,878	01/11/2005	Johnson et al.			
	7,555,476	06/30/2009	Holbrook			
	7,921,459	04/05/2011	Houston et al.			
	8,347,375	01/01/2013	Graham et al.			
	8,543,694	09/24/2013	Petersen et al.			
	2004/0103315	05/27/2004	Cooper et al.			
	2005/0131959	06/16/2005	Thorman et al.			

FOREIGN PATENT DOCUMENTS							
	DOCUMENT NO.	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
						YES	NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)		
		Dietrich (2003) Code Project "Event Logging, Part I: XEventLog - Basic NT Event Logging," 10 pages. Available at: http://www.codeproject.com/Articles/3995/Event-Logging-Part-I-XEventLog-Basic-NT-Event-Logg
		Wikipedia as crawled by Wayback Machine on March 1, 2010 "Event Viewer" 6 pages.

23552
PATENT TRADEMARK OFFICE

EXAMINER	DATE CONSIDERED

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form for next communication to the Applicant.

Electronic Patent Application Fee Transmittal

Application Number:	13372375
Filing Date:	13-Feb-2012
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate
Attorney Docket Number:	04584.0012USU1

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
RCE- 2nd and Subsequent Request	2820	1	850	850
		Total in USD ($)		**850**

Electronic Acknowledgement Receipt

EFS ID:	24003599
Application Number:	13372375
International Application Number:	
Confirmation Number:	2918
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Customer Number:	23552
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate
Filer Authorized By:	Andrew T. Pouzeshi
Attorney Docket Number:	04584.0012USU1
Receipt Date:	05-NOV-2015
Filing Date:	13-FEB-2012
Time Stamp:	18:21:40
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$850
RAM confirmation Number	5084
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Assertion of entitlement to small entity status	2015-11-05_SmallEntityAssert_04584_0012USU1.PDF	69658 2f07217e1704a965bfb7351d8b633c01ec269668	no	1
Warnings:					
Information:					
2	Request for Continued Examination (RCE)	2015-11-05_RCE_04584_0012USU1.PDF	697609 4d6db8527a666fca1042fa0d9c591714f762e27c	no	3
Warnings:					
Information:					
3	Transmittal Letter	2015-11-05_4thSIDS_TransLtr_04584_0012USU1.PDF	75389 9c74e08b3318dc72fa2023500b9b30eef4059a62	no	2
Warnings:					
Information:					
4	Information Disclosure Statement (IDS) Form (SB08)	2015-11-05_4thSIDS_1449_04584_0012USu1.PDF	132479 909562ad776b74b7baacefdf2ca853c031fa3e08	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
5	Non Patent Literature	Dietrich_Event_Logging.PDF	1143838 a5a2be79649e8d977357107dd9fdb91bdc0a4264	no	10
Warnings:					
Information:					
6	Non Patent Literature	Event_Viewer.PDF	478217 32c549d783e17ba3d69d3c8c8598509435ab81c4	no	6
Warnings:					
Information:					
7	Fee Worksheet (SB06)	fee-info.pdf	30573 8b67cd3b2af81baa3466342eb2ed05cfb67b2fcb	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	2627763		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

23552 7590 11/24/2015

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER
CHIANG, JASON

ART UNIT	PAPER NUMBER
2431	

DATE MAILED: 11/24/2015

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/372,375	02/13/2012	Melvyn Morris	04584.0012USU1	2918

TITLE OF INVENTION: METHODS AND APPARATUS FOR DEALING WITH MALWARE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	02/24/2016

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

23552 7590 11/24/2015
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/372,375	02/13/2012	Melvyn Morris	04584.0012USU1	2918

TITLE OF INVENTION: METHODS AND APPARATUS FOR DEALING WITH MALWARE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	02/24/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
CHIANG, JASON	2431	726-023000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ❑ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ❑ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

Sophos Ex. 1002
Page 449 of 683

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/372,375	02/13/2012	Melvyn Morris	04584.0012USU1	2918

23552 7590 11/24/2015

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
CHIANG, JASON	
ART UNIT	PAPER NUMBER
2431	

DATE MAILED: 11/24/2015

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 13/372,375	Applicant(s) MORRIS ET AL.	
	Examiner JASON C. CHIANG	Art Unit 2431	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *11/05/2015*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1-7, 9-15 and 25*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 11/05/2015
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☐ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/JASON C CHIANG/ Examiner, Art Unit 2431	/CORDELIA ZECHER/ Supervisory Patent Examiner, Art Unit 2431

1. The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/05/2015 has been entered.

Information Disclosure Statement

3. The Information Disclosure Statement filed on October 5, 2015 has been entered and considered, it does not change the reasons for allowance.

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JASON C. CHIANG whose telephone number is (571)270-3393. The examiner can normally be reached on 9AM to 6PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, CORDELIA P. ZECHER can be reached on (571)272-7771. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/J. C. C./
Examiner, Art Unit 2431

/CORDELIA ZECHER/
Supervisory Patent Examiner, Art Unit 2431

FORM 1449* INFORMATION DISCLOSURE STATEMENT IN AN APPLICATION (Use several sheets if necessary)	Docket Number: 04584.0012USU1	Application Number: 13/372,375
	Inventor: Melvyn Morris	
	Filing Date: 02-13-2012	Group Art Unit: 2431

U.S. PATENT DOCUMENTS

EXAMINER INITIAL	DOCUMENT NO.	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
/J.C./	6,842,878	01/11/2005	Johnson et al.			
/J.C./	7,555,476	06/30/2009	Holbrook			
/J.C./	7,921,459	04/05/2011	Houston et al.			
/J.C./	8,347,375	01/01/2013	Graham et al.			
/J.C./	8,543,694	09/24/2013	Petersen et al.			
/J.C./	2004/0103315	05/27/2004	Cooper et al.			
/J.C./	2005/0131959	06/16/2005	Thorman et al.			

FOREIGN PATENT DOCUMENTS

	DOCUMENT NO.	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
						YES	NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

/J.C./		Dietrich (2003) Code Project "Event Logging, Part I: XEventLog - Basic NT Event Logging," 10 pages. Available at: http://www.codeproject.com/Articles/3995/Event-Logging-Part-I-XEventLog-Basic-NT-Event-Logg
/J.C./		Wikipedia as crawled by Wayback Machine on March 1, 2010 "Event Viewer" 6 pages.

23552
PATENT TRADEMARK OFFICE

EXAMINER /Jason Chiang/	DATE CONSIDERED 11/13/2015

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form for next communication to the Applicant.

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13372375	MORRIS ET AL.
	Examiner	**Art Unit**
	JASON C CHIANG	2431

CPC								
Symbol							**Type**	**Version**
H04L		63	/	0263			F	2013-01-01
H04L		63	/	14			I	2013-01-01
G06F		21	/	56			I	2013-01-01
G06F		21	/	566			I	2013-01-01
H04L		63	/	145			I	2013-01-01
			/					
			/					
			/					
			/					
			/					
			/					
			/					
			/					
			/					
			/					

CPC Combination Sets								
Symbol							**Type**	**Set**	**Ranking**	**Version**
			/							
			/							

/JASON C CHIANG/ Examiner.Art Unit 2431	11/13/2015	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	15	
/DEDE ZECHER/ Supervisory Patent Examiner.Art Unit 2431	11/16/2015	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13372375	MORRIS ET AL.
	Examiner	**Art Unit**
	JASON C CHIANG	2431

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION									
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED				
726	23	H	0	4	L	29 / 06 (2006.0)	H	0	4	L	29 / 06 (2006.0)
CROSS REFERENCE(S)		G	0	6	F	21 / 56 (2013.0)	G	0	6	F	21 / 56 (2013.0)

CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				

/JASON C CHIANG/ Examiner.Art Unit 2431	11/13/2015	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	15	
/DEDE ZECHER/ Supervisory Patent Examiner.Art Unit 2431	11/16/2015	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13372375	MORRIS ET AL.
	Examiner	**Art Unit**
	JASON C CHIANG	2431

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1		17												
2	2		18												
3	3		19												
4	4		20												
5	5		21												
6	6		22												
7	7		23												
	8		24												
9	9	8	25												
10	10														
11	11														
12	12														
13	13														
14	14														
15	15														
	16														

/JASON C CHIANG/ Examiner.Art Unit 2431	11/13/2015	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	15	
/DEDE ZECHER/ Supervisory Patent Examiner.Art Unit 2431	11/16/2015	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13372375	MORRIS ET AL.
	Examiner	**Art Unit**
	JASON C CHIANG	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/09/2013	12/14/2013	12/13/2014	07/30/2015	11/13/2015				
1	1	✓	✓	✓	=	=				
2	2	✓	✓	✓	=	=				
3	3	✓	✓	✓	=	=				
4	4	✓	✓	✓	=	=				
5	5	✓	✓	✓	=	=				
6	6	✓	✓	✓	=	=				
7	7	✓	✓	✓	=	=				
	8	✓	-	-	-	-				
9	9	✓	✓	✓	=	=				
10	10	✓	✓	✓	=	=				
11	11	✓	✓	✓	=	=				
12	12	✓	✓	✓	=	=				
13	13	✓	✓	✓	=	=				
14	14	✓	✓	✓	=	=				
15	15	✓	✓	✓	=	=				
	16	✓	-	-	-	-				
	17	N	N	N	N	N				
	18	N	N	N	N	N				
	19	N	N	N	N	N				
	20	N	N	N	N	N				
	21	N	N	N	N	N				
	22	N	N	N	N	N				
	23	N	N	N	N	N				
	24	N	N	N	N	N				
8	25			✓	=	=				

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Morris, et al.	Examiner:	Chiang, Jason
Serial No.:	13/372,375	Group Art Unit:	2431
Filed:	February 13, 2012	Docket No.:	04584.0012USU1
Title:	METHODS AND APPARATUS FOR DEALING WITH MALWARE		

Filed Via EFS-Web on October 19, 2015

AMENDMENT UNDER 37 C.F.R. § 1.312

Mail Stop Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Commissioner:

In response to the Notice to File Corrected Application Papers mailed August 18, 2015, please amend the above-identified application pursuant to 37 C.F.R. 1.312 as follows:

Amendments to the Specification begin on page 2 of this paper.

Remarks begin on page 3 of this paper.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13372375	MORRIS ET AL.
	Examiner	Art Unit
	JASON C CHIANG	2431

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	23	06/04/2013	JC

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor search in East	06/04/2013	JC
Text search in East of USPGPUB, USPAT, USOCR, FPRS, EPO, JPO, DERWENT, IBM_TDB	06/05/2013	JC
Inventor search in East	12/14/2013	JC
Text search in East of USPGPUB, USPAT, USOCR, FPRS, EPO, JPO, DERWENT, IBM_TDB	12/14/2013	JC
Inventor search in East	12/11/2014	JC
Text search in East of USPGPUB, USPAT, USOCR, FPRS, EPO, JPO, DERWENT, IBM_TDB	12/11/2014	JC
Inventor search in East	7/30/2015	JC
Text search in East of USPGPUB, USPAT, USOCR, FPRS, EPO, JPO, DERWENT, IBM_TDB	7/30/2015	JC
Search in East of USPGPUB, USPAT, USOCR, FPRS, EPO, JPO, DERWENT, IBM_TDB	11/13/2015	JC

INTERFERENCE SEARCH

/JASON C CHIANG/ Examiner.Art Unit 2431	

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
H04L	63/14	7/30/2015	JC
G06F	21/56	7/30/2015	JC
H04L	63/14	11/13/2015	JC
G06F	21/56	11/13/2015	JC

/JASON C CHIANG/ Examiner.Art Unit 2431	

Sophos Ex. 1002
Page 462 of 683

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	9	(Melvyn near Morris).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 11:48
S2	3	(Joseph near Jaroch).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 16:51
S3	108	(Webroot).as.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 16:54
S5	0	S3 and cloud and database and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 16:58
S6	2980	(726/23).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/06/04 17:04
S7	72	S6 and cloud and database and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 17:05
S8	54	("20100043072" | "20110197272" | "20090300764" | "20100064368" | "20120017200" | "20060101334" | "20090292791" | "20100306851" | "20110138361" | "8042184" | "20060069912" | "20120260304" | "7707634" | "7343626" | "20070016953" | "20110197177" | "20120266208" | "20060117055" | "20100313183" | "20110083183" | "8146135" | "8307435").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/05 11:39

S9	21	("2006/0069912").URPN.	USPAT	OR	ON	2013/06/05 11:59
S10	17	threat adj server	USPAT	OR	ON	2013/06/05 12:20
S11	2362	cloud and signature	USPAT	OR	ON	2013/06/05 13:23
S12	1181	cloud and signature and layer	USPAT	OR	ON	2013/06/05 13:23
S13	249	cloud and (signature with database)	USPAT	OR	ON	2013/06/05 13:25
S14	78	cloud and (signature with database) and (malware virus)	USPAT	OR	ON	2013/06/05 13:26
S15	143	cloud and (updat$4 near3 (signature database)) and (malware virus)	USPAT	OR	ON	2013/06/05 16:30
S16	65	(updat$4 near3 (signature database) near3 (interval certain period periodic)) and (malware virus)	USPAT	OR	ON	2013/06/05 20:09
S17	1	(09/740294).APP.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/06/05 20:37
S18	0	("(masteradjdatabase)and(virusmalwaresignature)").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/06/07 18:03
S19	1003	(master adj database) and (virus malware signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:04
S20	160	(master adj database) and (virus malware) and signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:05
S21	971	(database) and (virus near signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:33
S22	639	((stor$4 sav$4 receiv$5) with database) and (virus near signature) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:51
S23	594	((stor$4 sav$4 receiv$5) near5 database) and (virus	US-PGPUB;	OR	ON	2013/06/07

		near signature) and @ad<"20120213"	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			18:51
S24	64	((stor$4 sav$4 receiv$5) near5 database) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 10:51
S25	0	((stor$4 sav$4 receiv$5) near3 content near3 database near3 storage) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:02
S26	0	((stor$4 sav$4 receiv$5) near3 database near3 storage) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:03
S27	2	((stor$4 sav$4 receiv$5) near3 content near3 database near3 storage) with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:03
S28	0	((backup) near3 database) with timestamp and (virus malware)and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:05
S29	0	((backup) near3 database) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:06
S30	27	((backup) near3 database) with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:06
S31	1139	((copy stor$4) near3 database) with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2013/06/08 11:20

			IBM_TDB			
S32	18	((copy stor$4) near3 database) with central with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:21
S33	359	((purg$4 clear$4 remov$4) near3 database near3 (period$6 every)) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:29
S34	0	(master adj database) near2 (virus malware) near2 signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S35	0	(master adj database) near3 (virus malware) near3 signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S36	0	(master adj database) with (virus malware) with signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S37	0	(master adj database) same (virus malware) same signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S38	19	(master adj database) same (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:45
S39	15	((primary secondary) adj database) same (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:54
S40	30	((primary secondary) adj database) with (signature)	US-PGPUB; USPAT; USOCR; FPRS;	OR	ON	2013/06/08 15:57

			EPO; JPO; DERWENT; IBM_TDB			
S41	98	(master adj database) same (signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:59
S42	10	(master adj database) same (signature) and (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:59
S43	315	(master adj database) and (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 16:03
S44	18	(virus malware) with definition with (file database) with (cloud community share$2)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 16:21
S45	271	(update refresh recover rebuild) near3 (database) with timestamp	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 20:22
S46	4	(update refresh recover rebuild) near3 (database) with timestamp same (offline off-line (off adj line) disconnect reconnect)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 20:24
S47	1	((roll$3 adj back) near6 time) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:11
S48	7	((roll$3 adj back)) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:12
S49	11	((roll$3 adj back) rollback) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT;	OR	ON	2013/06/09 10:14

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S50	48	((roll$3 adj back) rollback) and ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:18
S51	21	(((roll$3 adj back) rollback) with time) and ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:23
S52	0	((restor$4) near6 time) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 11:40
S53	3	((restor$4) near6 time) and ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 11:41
S54	0	(send provid$3 transmit$4 updat$3) near3 (count near3 (threat incident)) near3 (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:01
S55	22	(send provid$3 transmit$4 updat$3) with ((count number) near3 (threat incident)) with (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:02
S56	122	(send provid$3 transmit$4 updat$3 record$4) with ((count number times) with (threat)) with (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:05
S57	635	(send provid$3 transmit$4 updat$3 record$4) with ((count number times) near5 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:08

S58	199	(send provid$3 transmit$4 updat$3 record$4) with ((count number) near5 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:09
S59	11	(send provid$3 transmit$4 updat$3 record$4) with ((count) near5 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:11
S60	43	((count) near2 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:15
S61	9	((count) near2 (threat)) and (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:15
S62	1126	(send provid$3 transmit$4 updat$3) near3 (count) near3 (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:18
S63	15	(send provid$3 transmit$4 updat$3) near3 ((increas$4 add$3) near (count)) near3 (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:20
S64	1816	((increas$4 add$3) near (count)) and (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:22
S65	27	((increas$4 add$3) near (count)) and (malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:23
S66	9	(Melvyn near Morris).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2013/12/14 16:29

			DERWENT; IBM_TDB			
S67	3	(Joseph near Jaroch).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:30
S68	813	((increas$4 add$3 generat$4) near (count)) and (malware threat)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:31
S69	742	((increas$4 add$3 generat$4) near (count)) and (malware threat) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:32
S70	0	(((seen identified) near (before previous)) with (increas$4 add$3 generat$4) near (count)) and (malware threat) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:33
S71	0	(((seen identified) near (before previous)) same ((increas$4 add$3 generat$4) near (count))) and (malware threat) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:33
S72	48	(((seen identified)) same ((increas$4 add$3 generat$4) near (count))) and (malware threat) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:33
S73	347	(master central primary global) near2 (server database) same (signature) and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/11 22:30
S74	609	(provid$4 send$4 transmit$4) near2 (master central primary global) near2 (server database) and (virus malware spyware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/11 22:35
S75	586	(provid$4 send$4 transmit$4 submit$4 post$4 report$4) adj2 (master central primary global) adj2 (server database) and (virus malware spyware) and	US-PGPUB; USPAT; USOCR;	OR	ON	2014/12/11 22:36

		@ad<"20120213"	FPRS; EPO; JPO; DERWENT; IBM_TDB			
S76	39	(Melvyn near Morris).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/11 23:33
S77	10	S76 and (malware).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/11 23:34
S78	190	("20100043072" | "20100332593" | "8453244" | "7051365" | "20110197272" | "20090300764" | "20100064368" | "20120017200" | "8301904" | "8347386" | "8352484" | "20060080637" | "20090172774" | "20060101334" | "20090292791" | "20100306851" | "20110138361" | "8042184" | "7231440" | "8321944" | "20090089040" | "20060272020" | "20060069912" | "20120260304" | "7707634" | "20110191299" | "20110191341" | "7814056" | "7921063" | "8116732" | "20070220043" | "20080115190" | "7343626" | "20030093429" | "20090070304" | "7188173" | "8234709" | "8296178" | "8321540" | "8332946" | "8448243" | "20070174429" | "6175869" | "20080148381" | "20070016953" | "20110197177" | "20120266208" | "8336100" | "8347375" | "20060080637" | "20060117055" | "20100313183" | "20110083183" | "8146135" | "8307435" | "8195938" | "8443447" | "20060272020" | "8225218" | "8276202" | "20030188194" | "20050187740" | "20080115190" | "20080148381" | "6219786" | "20070220043").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/13 20:26
S79	6016	(726/23).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/12/13 20:27
S80	173	S78 NOT S79	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/13 20:27
S81	70	("20100043072" | "20110197272" | "20090300764" | "20100064368" | "20120017200" | "20060101334" | "20090292791" | "20100306851" | "20110138361" | "8042184" | "20060069912" | "20120260304" | "7707634" | "7343626" | "20070016953" | "20110197177" | "20120266208" | "20060117055" | "20100313183" | "20110083183" | "8146135" | "8307435").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/13 20:27
S82	120	S78 NOT S81	US-PGPUB;	OR	ON	2014/12/13

			USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			20:27
S83	544	(virus malware) and signature same behavior same (identifier ID IP computer) and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 19:55
S84	134	(virus malware) and signature same behavior same (identifier ID) and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 19:56
S85	64	(virus malware) and signature same behavior same (identifier) and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 19:57
S86	130	(virus malware) and signature same behavior same (infected) and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 20:27
S87	47	(virus malware) and (stor$4 receiv$4 send$4 provid$4) same signature same behavior same (infected) and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 20:28
S88	58	(virus malware) and (stor$4 receiv$4 send$4 provid$4) same signature same behavior same (list) and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 20:32
S89	41	(Melvyn near Morris).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 20:53
S90	20	(Joseph near Jaroch).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	OR	ON	2015/07/30 20:54

			IBM_TDB			
S93	18	("20040103315" | "20050131959" | "6842878" | "7555476" | "7921459" | "8347375" | "8543694").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/11/13 11:19

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	2997	(H04L63/14 G06F21/56).CPC.	US-PGPUB; USPAT	OR	ON	2015/11/13 13:45
L2	20	L1 and (signature).clm. and (behavior).clm. and (database).clm.	US-PGPUB; USPAT	OR	ON	2015/11/13 13:45
S91	2722	(H04L63/14 G06F21/56).CPC.	US-PGPUB; USPAT	OR	ON	2015/07/30 20:11
S92	20	S91 and (signature).clm. and (behavior).clm. and (database).clm.	US-PGPUB; USPAT	OR	ON	2015/07/30 20:13

11/13/2015 1:46:21 PM
C:\Users\jchiang1\Documents\EAST\Workspaces\13372375-Malware.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY.DOCKET NO./TITLE	REQUEST ID
13/372,375	02/13/2012	Melvyn Morris	04584.0012USU1	12740

Acknowledgement of Loss of Entitlement to Entity Status Discount

The entity status change request below filed through Private PAIR on 02/24/2016 has been accepted.

CERTIFICATIONS:

Change of Entity Status:

X Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be notification of loss of entitlement to small or micro entity status, as applicable.

This portion must be completed by the signatory or signatories making the entity status change in accordance with 37 CFR 1.4(d)(4).

Signature:	/Andrew T. Pouzeshi/
Name:	Andrew T. Pouzeshi
Registration Number:	67672

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	13372375	Filing Date	2012-02-13	Docket Number (if applicable)	04584.0012USU1	Art Unit	2431
First Named Inventor	Melvyn Morris			Examiner Name	CHIANG, JASON		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☐ Other _____

☒ Enclosed

- ☐ Amendment/Reply
- ☒ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____ (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 132725

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

Applicant Signature

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature		Date (YYYY-MM-DD)	2016-02-24
Name	Andrew T. Pouzeshi	Registration Number	67672

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	13372375
Filing Date:	13-Feb-2012
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate
Attorney Docket Number:	04584.0012USU1

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
RCE- 2nd and Subsequent Request	1820	1	1700	1700
		Total in USD ($)		**1700**

Electronic Acknowledgement Receipt

EFS ID:	25012743
Application Number:	13372375
International Application Number:	
Confirmation Number:	2918
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Customer Number:	23552
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate
Filer Authorized By:	Andrew T. Pouzeshi
Attorney Docket Number:	04584.0012USU1
Receipt Date:	24-FEB-2016
Filing Date:	13-FEB-2012
Time Stamp:	18:18:29
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$1700
RAM confirmation Number	4785
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	2016-02-24-5thSIDS-SB08-04584-0012USU1.PDF	612814 06acfa0e076289fea0e64d643b90d4701cf6f906	no	5
Warnings:					
Information:					
2	Foreign Reference	JP-2009-500706.PDF	15109904 823b7e09618c60a9e31e4ecf698af7f700b741c8	no	77
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
3	Foreign Reference	JP-H08-44677.PDF	12426768 624409ee30c9248a107dc720912f1f9d9803b559	no	30
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
4	Non Patent Literature	CN_OA_2012200183069_02_06_15_26pgs.pdf	5544802 8b05c2c4ea20530aa6f087cb7833a24fd9e9a7b8	no	26
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
5	Non Patent Literature	12703074_AMEND_11_06_12_8PGS.PDF	309337 54a183d7d9d4e49fb537679efbd7db566e96d161	no	8
Warnings:					
Information:					
6	Non Patent Literature	12703074_AMEND_12_07_12_7pgs.PDF	259887 bd505e33f15bfb79d37c1d604e29895ecbfde787	no	7
Warnings:					
Information:					

7	Non Patent Literature	13372433_AMEND_01_06_14_13pgs.PDF	524212 319810c79e0b05c581225006d28e2e7a03184032	no	13
Warnings:					
Information:					
8	Non Patent Literature	13372433_FOA_05_09_14_22pgs.PDF	740975 a438c541649ba5d7436ba36e1ff7659abbb04c43	no	22
Warnings:					
Information:					
9	Non Patent Literature	13372433_AMEND_10_09_14_14pgs.PDF	598239 912f25dbc05de609dfea515dc6c53cfa6105dd88	no	14
Warnings:					
Information:					
10	Non Patent Literature	13372433_NFOA_09_10_15_16pgs.PDF	536257 b7b1914b774666d9daba8afadd07c692a85c05c9	no	16
Warnings:					
Information:					
11	Non Patent Literature	13372439_FOA_02_24_14_15pgs.PDF	514816 e143e192fd2652c3689c49e0b0f7c41d19454561	no	15
Warnings:					
Information:					
12	Non Patent Literature	13372439_AMEND_11_04_13_12pgs.PDF	530397 c3b49c0a25bd9b79431a5d0a76e0ac6986474b5f	no	12
Warnings:					
Information:					
13	Non Patent Literature	13372433-AMEND-021016-18pgs.PDF	795192 d6a12dc29400a2c0769e263e29a53ce7b03f6a70	no	18
Warnings:					
Information:					
14	Non Patent Literature	JP-OA-2013-553909-01-26-16-6pgs.PDF	1985306 6b26b56b6e957c5a92170b37a5ccc8dfa58e811c	no	6
Warnings:					
Information:					
15	Non Patent Literature	CN_2ndOA_2012800183069_01_11_16_11pgs.PDF	478186 e770bb5b62c518fc0742eb61911272bed040a9a3	no	11
Warnings:					
Information:					

16	Request for Continued Examination (RCE)	2016-02-24-RCE-04584-0012USU1.PDF	705293 bc5770d5810e0b6c8a254b754091bbb74953b860	no	3
Warnings:					
Information:					
17	Fee Worksheet (SB06)	fee-info.pdf	30485 1af86407c3960d24bf2c54c7413e43581adf385e	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	41702870		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13372375
Filing Date	2012-02-13
First Named Inventor	Melvyn Morris
Art Unit	2431
Examiner Name	CHIANG, JASON
Attorney Docket Number	04584.0012USU1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7761912		2010-07-20	Yee et al.	
	2	8407790		2013-03-26	Mony	
	3	8499283		2013-07-30	Mony	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20050172338		2005-08-04	Sandu et al.	
	2	20060161856		2006-07-20	Heir	
	3	20080229422		2008-09-18	Hudis et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13372375
	Filing Date	2012-02-13
	First Named Inventor	Melvyn Morris
	Art Unit	2431
	Examiner Name	CHIANG, JASON
	Attorney Docket Number	04584.0012USU1

	4	20110047594		2011-02-24	Mahaffey et al.			

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	JP 2009-500706	JP		2009-01-08			
	2	JP H08-44677	JP		1996-02-16			

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Chinese Patent Application No. 201280018306.9, First Office Action mailed June 2, 2015, 26 pages. (No English translation available)	
	2	U.S. Patent Application No. 12/703,074, Amendment and Response dated November 6, 2012, 8 pages.	
	3	U.S. Patent Application No. 12/703,074, Amendment after Allowance dated December 7, 2012, 7 pages.	
	4	U.S. Patent Application No. 13/372,433, Amendment and Response dated January 6, 2014, 13 pages.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13372375
	Filing Date	2012-02-13
	First Named Inventor	Melvyn Morris
	Art Unit	2431
	Examiner Name	CHIANG, JASON
	Attorney Docket Number	04584.0012USU1

	5	U.S. Patent Application No. 13/372,433, Final Rejection mailed May 9, 2014, 22 pages.	
	6	U.S. Patent Application No. 13/372,433, Amendment and Response dated October 9, 2014, 14 pages.	
	7	U.S. Patent Application No. 13/372,433, Non-Final Rejection mailed September 10, 2015, 16 pages.	
	8	U.S. Patent Application No. 13/372,439, Amendment and Response dated November 4, 2013, 12 pages.	
	9	U.S. Patent Application No. 13/372,439, Final Rejection mailed February 24, 2014, 15 pages.	
	10	U.S. Patent Application No. 13/372,433, Amendment and Response filed February 10, 2016, 18 pages.	
	11	Japanese Patent Application No. 2013-553909, Office Action mailed January 26, 2016, 6 pages (English Translation).	
	12	Chinese Patent Application No. 201280018306.9, Second Office Action mailed January 11, 2016, 11 pages (English Translation).	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13372375
Filing Date	2012-02-13
First Named Inventor	Melvyn Morris
Art Unit	2431
Examiner Name	CHIANG, JASON
Attorney Docket Number	04584.0012USU1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Andrew T. Pouzeshi/	Date (YYYY-MM-DD)	2016-02-24
Name/Print	Andrew T. Pouzeshi	Registration Number	67672

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2009-500706
(P2009-500706A)
(43)公表日　平成21年1月8日(2009.1.8)

(51)Int.Cl.	F I	テーマコード（参考）
G06F 21/22 (2006.01)	G06F 9/06 660N	5B276

審査請求 未請求　予備審査請求 未請求　（全 35 頁）

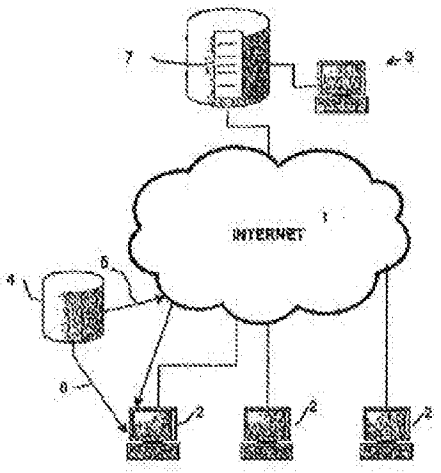
(21)出願番号　特願2008-518975 (P2008-518975)
(86)(22)出願日　平成18年6月30日 (2006.6.30)
(85)翻訳文提出日　平成20年2月27日 (2008.2.27)
(86)国際出願番号　PCT/GB2006/002439
(87)国際公開番号　WO2007/003916
(87)国際公開日　平成19年1月11日 (2007.1.11)
(31)優先権主張番号　0513375.6
(32)優先日　平成17年6月30日 (2005.6.30)
(33)優先権主張国　英国 (GB)

(71)出願人　508000052
プレヴィクス リミテッド
PREVX LIMITED
イギリス国、ディー24 8ディーゼット ダービー、プライド パーク、ニュー パーク プレイス 3
3 New Park Place, Pride Park, Derby DE24 8DZ, United Kingdom
(74)代理人　100104765
弁理士 江上 達夫
(74)代理人　100107331
弁理士 中村 聡延

最終頁に続く

(54)【発明の名称】マルウェアに対処する方法及び装置

(57)【要約】
一の態様では、一のコンピュータオブジェクトをマルウェアとして分類する方法は、ベースコンピュークにおいて、前記オブジェクト又は類似の複数のオブジェクトを記憶する複数のリモートコンピュークの夫々からのコンピュータオブジェクトに関するデータを受信する工程を含む。前記複数のコンピュータから受信したコンピュータオブジェクトに関するデータは、前記ベースコンピュータにおいて比較される。前記コンピュータオブジェクトは、前記比較に基づいてマルウェアとして分類される。一の実施例では、前記コンピュータオブジェクトに関するデータは、前記オブジェクト内に含まれる又は前記オブジェクトにより構成される複数の実行可能命令と、前記オブジェクトのサイズと、前記オブジェクトの現在の名称と、各リモートコンピュータ上における前記オブジェクトの物理的格納位置又はパスと、前記オブジェクトの業者、前記オブジェクトに関するソフトウェア製品及びバージョン、並びに前記オブジェクトを作成、構成、又は夫々のリモートコンピュータ上で実行する際に前記オブジェクトにより開始された又は前記オブジェクト



Sophos Ex. 1002
Page 489 of 683

【特許請求の範囲】
【請求項1】
一のコンピュータオブジェクトをマルウェアとして分類する方法であって、
ベースコンピュータにおいて、前記オブジェクト又は類似の複数のオブジェクトを記憶する複数のリモートコンピュータの夫々からのコンピュータオブジェクトに関するデータを受信する工程と、
前記複数のコンピュータから受信した前記コンピュータオブジェクトに関する前記データを、前記ベースコンピュータにおいて比較する工程と、
前記比較に基づいて前記コンピュータオブジェクトをマルウェアとして分類する工程と
を備えることを特徴とする分類方法。
【請求項2】
前記複数のリモートコンピュータから前記ベースコンピュータに送信され且つ前記比較において用いられた、前記コンピュータオブジェクトに関する前記データは、前記オブジェクト内に含まれる又は前記オブジェクトにより構成される複数の実行可能命令と、前記オブジェクトのサイズと、前記オブジェクトの現在の名称と、前記オブジェクトのディスク上での物理的およびフォルダ位置と、前記オブジェクトの本来の名称と、前記オブジェクトの作成及び変更日時と、前記オブジェクト内に記憶された業者、製品、バージョン、及び他の情報と、前記オブジェクトヘッダ又は前記リモートコンピュータにより保持されたヘッダと、前記オブジェクトを夫々のリモートコンピュータ上で実行する、構成する又は作成する際に、前記オブジェクトにより開始された又は前記オブジェクトを含むイベントと、のうちの一以上を含むことを特徴とする請求項1に記載の方法。
【請求項3】
前記比較により、前記オブジェクトと他の複数のオブジェクトとの関係が識別されることを特徴とする請求項1又は2に記載の方法。
【請求項4】
前記オブジェクトが関連する少なくとも一の他のオブジェクトが、マルウェアとして分類される場合に、前記オブジェクトをマルウェアとして分類することを特徴とする請求項3に記載の方法。
【請求項5】
前記他の複数のオブジェクトは、前記複数のリモートコンピュータのうちの少なくともいくつかに記憶された前記オブジェクト又は類似の複数のオブジェクトを含むことを特徴とする請求項3又は4に記載の方法。
【請求項6】
前記他の複数のオブジェクトは、親若しくは子オブジェクト、又は前記オブジェクトに対してプロセス関連オブジェクトである、他の複数のオブジェクトを含むことを特徴とする請求項3から5のいずれか一項に記載の方法。
【請求項7】
前記データは、前記夫々のリモートコンピュータ上の複数のオブジェクトについて実行されたハッシングプロセスによって取得される鍵の形態で送信されることを特徴とする請求項1から6のいずれか一項に記載の方法。
【請求項8】
前記鍵は、前記オブジェクト内に含まれる又は前記オブジェクトにより構成される実行可能命令を表す少なくとも一の要素を有することを特徴とする請求項7に記載の方法。
【請求項9】
前記鍵は、前記オブジェクトに関するデータを表す少なくとも一の要素を有することを特徴とする請求項7又は8に記載の方法。
【請求項10】
前記オブジェクトに関する前記データは、前記オブジェクトの現在の名称と、前記オブジェクトのディスク上での物理的およびフォルダ位置と、前記オブジェクトの本来の名称

と、前記オブジェクトの作成及び変更日時と、前記オブジェクト内に記憶された業者、製品、バージョン、及び他の情報と、前記オブジェクトヘッダ又は前記リモートコンピュータにより保持されたヘッダと、前記オブジェクトを夫々のリモートコンピュータ上で実行する、構成する又は作成する際に前記オブジェクトにより開始された又は前記オブジェクトを含むイベントと、のうちの少なくとも一つを含むことを特徴とする請求項９に記載の方法。

【請求項11】

前記鍵は、前記オブジェクトの物理的サイズを表す少なくとも一の要素を有することを特徴とする請求項７から１０のいずれか一項に記載の方法。

【請求項12】

先ず一のオブジェクトを非マルウェアとして分類する工程と、前記オブジェクトについての許容される振る舞いを規定する前記オブジェクトのマスクを生成する工程と、少なくとも一の前記リモートコンピュータ上で前記オブジェクトの動作を監視する工程と、実際に監視された前記振る舞いが前記マスクによって許可されたものを逸脱する場合に、前記オブジェクトをマルウェアとして分類する工程とを備えることを特徴とする請求項１から１１のいずれか一項に記載の方法。

【請求項13】

一のコンピュータオブジェクトをマルウェアとして分類する装置であって、

前記オブジェクト又は類似の複数のオブジェクトを記憶する複数のリモートコンピュータの夫々からのコンピュータオブジェクトに関するデータを受信するように構成及び配置された一のベースコンピュータを備え、

前記ベースコンピュータは、前記複数のコンピュークから受信した前記コンピュータオブジェクトに関する前記データを、比較するように構成及び配置され、

前記ベースコンピュータは、前記比較に基づいて前記コンピュータオブジェクトをマルウェアとして分類するように構成及び配置されることを特徴とする分類装置。

【請求項14】

前記ベースコンピュータは、前記オブジェクト内に含まれる又は前記オブジェクトにより構成される複数の実行可能命令と、前記オブジェクトのサイズと、前記オブジェクトの現在の名称と、前記オブジェクトのディスク上での物理的およびフォルダ位置と、前記オブジェクトの本来の名称と、前記オブジェクトの作成及び変更日時と、前記オブジェクト内に記憶された業者、製品、バージョン、及び他の情報と、前記オブジェクトヘッダ又は前記リモートコンピュータにより保持されたヘッダと、前記オブジェクトを夫々のリモートコンピュータ上で実行する、構成する又は作成する際に前記オブジェクトにより開始された又は前記オブジェクトを含むイベントと、のうちの一以上を含む前記データを、比較するように構成及び配置されることを特徴とする請求項１３に記載の装置。

【請求項15】

前記ベースコンピュータは、前記比較により、前記オブジェクトと他の複数のオブジェクトとの関係が識別されるように構成及び配置されることを特徴とする請求項１３又は１４に記載の装置。

【請求項16】

前記ベースコンピュータは、前記オブジェクトが関連する少なくとも一の他のオブジェクトが、マルウェアとして分類される場合に、前記オブジェクトをマルウェアとして分類するように構成及び配置されることを特徴とする請求項１５に記載の装置。

【請求項17】

前記ベースコンピュータは、前記他の複数のオブジェクトが、前記複数のリモートコンピュータのうちの少なくともいくつかに記憶された前記オブジェクト又は類似の複数のオブジェクトを含むように構成及び配置されることを特徴とする請求項１５又は１６に記載の装置。

【請求項18】

前記ベースコンピュータは、前記他の複数のオブジェクトが、親若しくは子オブジェク

Sophos Ex. 1002
Page 491 of 683

ト、又は前記オブジェクトに対してプロセス関連オブジェクトである他の複数のオブジェクトを含むように構成及び配置ことを特徴とする請求項１５から１７のいずれか一項に記載の装置。

【請求項19】

前記ベースコンピュータは、前記夫々のリモートコンピュータ上の複数のオブジェクトについて実行されたハッシングプロセスによって取得される鍵の形態で送信されたデータを処理できるように構成及び配置されることを特徴とする請求項１３から１８のいずれか一項に記載の装置。

【請求項20】

前記鍵は、前記オブジェクト内に含まれる又は前記オブジェクトにより構成される実行可能命令を表す少なくとも一の要素を有することを特徴とする請求項１９に記載の装置。

【請求項21】

前記鍵は、前記オブジェクトに関するデータを表す少なくとも一の要素を有することを特徴とする請求項１９又は２０に記載の装置。

【請求項22】

前記オブジェクトに関する前記データは、前記オブジェクトの現在の名称と、前記オブジェクトのディスク上での物理的およびフォルダ位置と、前記オブジェクトの本来の名称と、前記オブジェクトの作成及び変更日時と、前記オブジェクト内に記憶された業者、製品、バージョン、及び他の情報と、前記オブジェクトヘッダ又は前記リモートコンピュータにより保持されたヘッダと、前記オブジェクトを夫々のリモートコンピュータ上で実行する、構成する又は作成する際に前記オブジェクトにより開始された又は前記オブジェクトを含むイベントと、のうちの少なくとも一つを含むことを特徴とする請求項２１に記載の装置。

【請求項23】

前記鍵は、前記オブジェクトの物理的サイズを表す少なくとも一の要素を有することを特徴とする請求項１９から２２のいずれか一項に記載の装置。

【請求項24】

前記ベースコンピュータは、先ず非マルウェアとして分類された一のオブジェクトについての許容される振る舞いを規定するマスクを生成するように構成及び配置され、また前記ベースコンピュータは、少なくとも一の前記リモートコンピュータ上で前記オブジェクトの動作を監視し、実際に監視された前記振る舞いが前記マスクによって許可されたものを逸脱する場合に、前記オブジェクトをマルウェアとして分類するように構成及び配置されることを特徴とする請求項１９から２３のいずれか一項に記載の装置。

【請求項25】

一のコンピュータオブジェクトに関するデータを、一のリモートコンピュータから一のベースコンピュータに、前記ベースコンピュータにおいて他の複数のリモートコンピュータから受信した類似データと比較を行えるように提供する方法であって、

前記リモートコンピュータに記憶された一のコンピュータオブジェクトに関するデータを、一のリモートコンピュータから一のベースコンピュータに提供する工程を備え、

前記データは、前記オブジェクト内に含まれる又は前記オブジェクトにより構成される複数の実行可能命令と、前記オブジェクトのサイズと、前記オブジェクトの現在の名称と、前記オブジェクトのディスク上での物理的およびフォルダ位置と、前記オブジェクトの本来の名称と、前記オブジェクトの作成及び変更日時と、前記オブジェクト内に記憶された業者、製品、バージョン、及び他の情報と、前記オブジェクトヘッダ又は前記リモートコンピュータにより保持されたヘッダと、前記オブジェクトを夫々のリモートコンピュータ上で実行する、構成する又は作成する際に前記オブジェクトにより開始された又は前記オブジェクトを含むイベントと、のうちの一以上を含み、

前記データは、前記リモートコンピュータ上の前記オブジェクトについて実行されたハッシングプロセスによって取得された鍵の形態で送信されることを特徴とする提供方法。

【請求項26】

Sophos Ex. 1002
Page 492 of 683

前記鍵は、前記オブジェクト内に含まれる又は前記オブジェクトにより構成される実行可能命令を表す少なくとも一の要素を有することを特徴とする請求項２５に記載の提供方法。

【請求項27】

前記鍵は、前記オブジェクトに関するデータを表す少なくとも一の要素を有することを特徴とする請求項２５又は２６に記載の提供方法。

【請求項28】

前記オブジェクトに関する前記データは、前記オブジェクトの現在の名称と、前記オブジェクトのディスク上での物理的およびフォルダ位置と、前記オブジェクトの本来の名称と、前記オブジェクトの作成及び変更日時と、前記オブジェクト内に記憶された業者、製品、バージョン、及び他の情報と、前記オブジェクトヘッダ又は前記リモートコンピュータにより保持されたヘッダと、並びに前記オブジェクトを夫々のリモートコンピュータ上で実行する、構成する又は作成する際に前記オブジェクトにより開始された又は前記オブジェクトを含むイベントと、のうちの少なくとも一つを含むことを特徴とする請求項２７に記載の方法。

【請求項29】

前記鍵は、前記オブジェクトの物理的サイズを表す少なくとも一の要素を有することを特徴とする請求項２５から２８のいずれか一項に記載の方法。

【請求項30】

コンピュータに請求項２５から２９のいずれか一項に記載の方法を実行させるプログラム命令を備えるコンピュータプログラム。

【請求項31】

一のリモートコンピュータが有するマルウェアからの保護を決定する方法であって、

一のベースコンピュータにおいて、前記リモートコンピュータ上である時点で動作しているセキュリティ製品のうちの全て又は選択された製品の詳細を、受信する工程と、

前記ベースコンピュータに接続された他の複数のリモートコンピュータから類似の情報を受信する工程と、

特定の組み合わせのセキュリティ製品を有している前記他の複数のリモートコンピュータによって識別されなかった任意のマルウェアプロセスを識別する工程と

を備えることを特徴とする決定方法。

【請求項32】

前記一のリモートコンピュータは、前記識別に基づいて前記マルウェアプロセスによる攻撃の影響を受けやすい可能性があるという情報を、前記一のリモートコンピュータのユーザに提供する工程を備えることを特徴とする請求項３１に記載の方法。

【請求項33】

前記全て又は選択されたセキュリティ製品の詳細は、当該セキュリティ製品の名称と、バージョンと、ロードされたシグネチャファイルとを含むことを特徴とする請求項３１又は３２に記載の方法。

【請求項34】

一のリモートコンピュータが有するマルウェアからの保護を決定する装置であって、

前記リモートコンピュータ上である時点で動作しているセキュリティ製品のうちの全て又は選択された製品の詳細を受信するように構成及び配置された一のベースコンピュータを備え、

当該ベースコンピュータは、前記ベースコンピュータに接続された他の複数のリモートコンピュータから類似の情報を受信するように構成及び配置され、

前記ベースコンピュータは、特定の組み合わせのセキュリティ製品を有している前記他の複数のリモートコンピュータによって識別されなかった任意のマルウェアプロセスを識別するように構成及び配置されることを特徴とする決定装置。

【請求項35】

前記ベースコンピュータは、前記一のリモートコンピュータが、前記識別に基づいて前

Sophos Ex. 1002
Page 493 of 683

記マルウェアプロセスによる攻撃の影響を受けやすい可能性があるという情報を、前記一のリモートコンピュータのユーザに提供するように構成及び配置されることを特徴とする請求項３４に記載の装置。

【請求項36】

前記全て又は選択されたセキュリティ製品の詳細は、当該セキュリティ製品の名称と、バージョンと、ロードされたシグネチャファイルとを含むことを特徴とする請求項３４又は３５に記載の装置。

【請求項37】

第１のコンピュータオブジェクトの子孫であるか又は関連オブジェクトである一のコンピュータオブジェクトを、マルウェア又は安全として分類する方法であって、

第１のコンピュータオブジェクトをマルウェア又は安全として分類する工程と、

前記第１のコンピュータオブジェクトを一意的に識別する一要素であって、前記第１のコンピュータオブジェクトの子孫又は他の関連コンピュータオブジェクトの鍵において受け継がれたか若しくは存在する前記一要素を、前記第１のコンピュータオブジェクトに関連する鍵において識別する工程と、

前記コンピュータオブジェクトの鍵に存在する一意的な識別子要素に基づいて、前記コンピュータオブジェクトを、場合によってマルウェア又は安全として分類する工程と

を備えることを特徴とする分類方法。

【請求項38】

前記第１のコンピュータオブジェクトの活動を監視する工程と、前記第１のコンピュータオブジェクトが安全として先ず分類されてその後マルウェアであると判断された場合に、前記第１のコンピュータオブジェクトをマルウェアとして再分類する工程とを備え、更に、前記一意的な識別子要素が存在する鍵を備えた任意のコンピュータオブジェクトを、マルウェアとして自動的に分類する工程を備えることを特徴とする請求項３７に記載の方法。

【請求項39】

コンピュータに請求項３８又は３９に記載の方法を実行させるプログラム命令を備えるコンピュータプログラム。

【請求項40】

第１のコンピュータオブジェクトの子孫であるか又は関連オブジェクトである一のコンピュータオブジェクトを、マルウェア又は安全として分類する装置であって、

第１のコンピュータオブジェクトをマルウェア又は安全として分類するように構成及び配置された一のコンピュータを備え、

当該コンピュータは、前記第１のコンピュータオブジェクトを一意的に識別する一要素であって、前記第１のコンピュータオブジェクトの子孫又は他の関連コンピュータオブジェクトの鍵において受け継がれたか若しくは存在する前記一要素を、前記第１のコンピュータオブジェクトに関連する鍵において識別するように構成及び配置され、

前記コンピュータは、前記コンピュータオブジェクトの鍵に存在する一意的な識別子要素に基づいて、前記コンピュータオブジェクトを、場合によってマルウェア又は安全として分類するように構成及び配置されることを特徴とする分類装置。

【請求項41】

前記コンピュータは、前記第１のコンピュータオブジェクトの活動を監視し、前記第１のコンピュータオブジェクトが安全として先ず分類されてその後マルウェアであると判断された場合に、前記第１のコンピュータオブジェクトをマルウェアとして再分類するように構成及び配置され、更に、前記コンピュータは、前記一意的な識別子要素が存在する鍵を備えた任意のコンピュータオブジェクトを、マルウェアとして自動的に分類するように構成及び配置されることを特徴とする請求項４０に記載の装置。

【請求項42】

一のコンピュータにソフトウェアをインストールする方法であって、

一のコンピュータへのソフトウェアのインストール開始時に、ユーザが前記インスト―

ルを認証したかを確認するための前記コンピュータ上のコンピュータ生成プロンプトを、前記ユーザに提供する工程と、
ユーザ認証が受信されない場合に前記インストールを中止する工程と、そのほか、
前記コンピュータにおいて、前記インストールを進めるための前記ユーザ認証を受信する工程と、
前記インストールを進める工程と、
前記インストール中に作成又は使用された複数のコンピュータオブジェクトに関するデータを取得する工程と、
前記データを前記ローカルコンピュータに記憶する工程と
を備えたことを特徴とするインストール方法。
【請求項43】
前記ローカルに記憶されたデータは、前記インストール中に作成又は使用された全てのオブジェクトが前記インストールプロセスの一部であることを確認するために、前記インストール中に参照され、前記インストール中に作成又は使用された全てのオブジェクトが前記インストールプロセスの一部でない場合には、（１）前記インストールを中止する工程、及び（１１）前記コンピュータ上のコンピュータ生成プロンプトを適宜前記ユーザに提供する工程のうち少なくとも一方を備えることを特徴とする請求項４２に記載の方法。
【請求項44】
複数のコンピュータに接続可能であるコミュニティデータベースに前記コンピュータを接続する工程と、前記記憶されたデータを、他のコンピュータによって提供された類似のデータと比較するために前記コミュニティデータベースにアップロードする工程とを備えることを特徴とする請求項４２又は４３に記載の方法。
【請求項45】
複数の信頼できるインストーラに関するデータを前記コンピュータにダウンロードする工程を備え、前記複数の信頼できるインストーラに関するデータは、前記信頼できるインストーラに関連する又は前記信頼できるインストーラによって作成された任意のオブジェクトを自動的に認証して先に進むように、前記インストール中に参照されることを特徴とする請求項４２から４４のいずれか一項に記載の方法。
【請求項46】
前記複数の信頼できるインストーラに関するデータは、前記コンピュータにおける前記インストールを進めるための前記ユーザ認証の受理に続く所定の時間のみ参照されることを特徴とする請求項４５に記載の方法。
【請求項47】
コンピュータに請求項４２から４６のいずれか一項に記載の方法を実行させるプログラム命令を備えるコンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【0001】
本発明は、一般的にはマルウェアに対処する方法及び装置に関する。一の態様では、本発明は、マルウェアとしてコンピュータオブジェクトを分類する方法及び装置に関する。他の態様では、本発明は、マルウェアからのリモートコンピュータが有する保護を決定する方法及び装置に関する。他の態様では、本発明は、マルウェア又は安全としてコンピュータオブジェクトを分類する方法及び装置に関する。他の態様では、本発明は、コンピュータにソフトウェアをインストールする方法に関する。
【背景技術】
【0002】
用語「マルウェア」は、ここでは、悪質なコードである又は悪質なコードを含む、一般的には任意の実行可能なコンピュータファイル又はより一般的には「オブジェクト」を指すことに用いられる。マルウェアは、従って、ウイルス、トロイの木馬（Trojan）、ワーム、スパイウェア、アドウェア等を含む。
【0003】

アンチウイルススキャンソフトウェア等の典型的なアンチマルウェア製品は、複数のオブジェクト、又は該オブジェクト若しくはその一部に適用されたアルゴリズムの複数の結果をスキャンして、ウイルスの存在を示すことが知られているオブジェクトのシグネチャ（Signature）を探す。一般にはマルウェアに対処する方法は、新型のマルウェアが例えばインターネットを介して放出された際、これらはいずれ検出される。新型のマルウェアが一旦検出されると、この分野のサービスプロバイダは、これらに対処することを目的とするシグネチャを作成し、次にこれらのシグネチャが、アンチマルウェアプログラムを更新する形で公開或いはリリース（release）される。発見的方法も採用されている。

【0004】

これらのシステムは、公知の悪質オブジェクトに対し保護することに非常に有効である。しかしながら、これらのシステムは、シグネチャファイルの作成及び／又は更新に依存する。このため、出現する又は公開される新たなマルウェアと、当該マルウェアが作成又は更新されることに対抗してユーザへ供給されるシグネチャとの間に、必然的に遅延が生じる。従ってユーザは、一週間又はそれ以上にもなりうる、ある一定の期間、新たなマルウェアからの危険にさらされている。更に、アンチウイルス製品に打ち勝つために、マルウェアライターは、難読化（Obfuscation）技術を用いて、検出からウイルスコードのシグネチャ基本データ又はシグネチャを隠そうとする。典型的には、難読化はウイルスに関するコードを暗号化又はパッキングすることを含む。

【0005】

WO-A-2004/097602は、ローカルコンピュータにより受信又は作成されたコンピュータファイルを解析し、これらを公知のファイルのデータベースと比較して、特定のファイルが公知であるかを決定し、そうである場合に、特定のファイルが「安全」であるとみなせるほど十分長く知られているかを決定するシステムについて記載している。しかしながら、実際には、そのままではこれは十分な保護を提供しそうにない。なぜなら、例えば、ウイルス又はトロイの木馬のアクティブペイロード（即ち、データの本体）は、ある特定の日時に、若しくはローカル又はリモートシステム又はプロセスからのメッセージ若しくは命令を受信する際に、或いはそのプロセスが最初に実行又は公開されてから何カ月若しくは何年か後の特定のイベントが行われた時に、活性化するようにプログラムされるだけであるからである。よって、単にファイル年齢を見るだけでは、それが安全であり且つ安全のままでいられるかについて決定するのに十分ではない。

【0006】

WO-A-2004/083408における システムでは、コンピュータ上で作動している特定のファイルによってなされる接続の試みを調べることで、ファイル中のワームを検出する。

【0007】

US-A-6944772、US-A-6772346、EP-A-1549012、及びGB-A-2390040は全て、複数の「ローカル」コンピュータの全てがネットワーク（例えば、ＬＡＮ又はインターネットであってよい）を介して中央コンピュータに接続している「コミュニティベース（community-based）」アンチマルウェアシステムを開示する。それらのローカルコンピュータに知られていないファイルに出会った際には、それらのローカルコンピュータは、そのファイルの実行許可の要求を中央コンピュータに送信する。もし、そのファイルが中央コンピュータにおいて認識されると、中央コンピュータは、そのファイルが安全であると知られている場合に、ローカルコンピュータがそのファイルを実行する許可を送信できる。或いは、そのファイルが悪質であると知られている場合には、「否認」命令を送信できる。しかしながら、これら先行技術における各提案では、ファイルが中央コンピュータで知られていない場合、全ファイルは中央コンピュータに送信され、そこで安全としてみなされるべきかマルウェアとしてみなされるべきかを決定するために解析される。このような解析は、ファイルを詳細な解析にかけることによって、典型的には手動で、又は「半手動で」実行される。詳細な解析は、例えばエミュレーション又は解読であり、通常要求される人の関与を考えると、多くの日数を要しうる。従って、新たなファイルを安全又はマルウェアとして分類するまでには、かなりの期間がかかる。これらの先行技術におけるシステムでは、ロ

Sophos Ex. 1002
Page 496 of 683

ーカルコンピュータによって中央コンピュータに送信されるファイルの実行許可の要求は、そのファイルを特異的に表す「鍵」又は「シグネチャ」又はチェックサムの送信を含んでよい。

【0008】

類似のコミュニティベースアンチマルウェアシステムが、WO-A-02/33525に開示されている。このシステムでは、安全か又はマルウェアであるかが中央コンピュータに知られていないファイルを実行するためにローカルコンピュータが許可を求めている場合、他のローカルコンピュータ上のファイルの普及に関する何らかの限定された監査情報を、そのファイルの実行許可を求めているローカルコンピュータに関連した人的システム管理者に送信できる。従って、人的システム管理者は、ファイルが安全に実行できるか否かについて、「手動」による決定ではあるが、十分な情報を得た上で決定できる。

【0009】

US-A-2004/0073810におけるシステムでは、添付又は他の送信ファイルに関するデータを含むメタファイルが、中央コンピュータに送信される。そのファイルに関するデータを解析し、送信ファイルがマルウェアである可能性を決定する。送信ファイルが少なくともある一定数のサーバを介して送信された場合にマルウェアとして取り扱われるという具体例が与えられている。

【0010】

US-A-2005/0021994及びUS-A-2004/0153644に開示されたシステムでは、例えばファイルに関連するソフトウェアベンダーにより安全として認定を受けた、事前承認されたファイルは、更なる検査を行わずに実行することが常に許可されていてよい。US-A-2004/0153644におけるシステムの一の実施例では、監視（モニクリング）を実行し、そのファイルによる異常に多数の要求が、複数のローカルコンピュータからある期間に中央管理部において受信され、又は単一のコンピュータ上のファイルによる異常に多数の要求が、その単一コンピュータからある期間に中央管理部において受信された場合に、ファイルが悪質であると決定する。

【0011】

US-A-2004/0006704におけるシステムでは、ソフトウェアバージョンのデータベースを備えたコンピュータ上におけるインストールされたソフトウェアのバージョンとそれらの公知の脆弱性とが比較される。従って、コンピュータのユーザは、既存のソフトウェアを更新する又は新しいソフトウェアをインストールすることにより、特定リスク及びこれらのリスクを最小限にする方法を知ることができる。

【0012】

WO-A-03/021402におけるシステムでは、中央データベースは、複数のローカルコンピュータの夫々に記憶された全ファイルの仮想イメージを保持する。一のローカルコンピュータにおける脅威が識別されると、類似の構成を備えた他のローカルコンピュータはそのリスクについて知らされる。

【0013】

【特許文献1】WO-A-2004/097602
【特許文献2】WO-A-2004/0083408
【特許文献3】US-A-6944772
【特許文献4】US-A-6772346
【特許文献5】EP-A-1549012
【特許文献6】EP-A-1280040
【特許文献7】WO-A-02/33525
【特許文献8】US-A-2004/0073810
【特許文献9】US-A-2005/0021994
【特許文献10】US-A-2004/0153644
【特許文献11】US-A-2004/0006704
【特許文献12】WO-A-03/021402

【発明の開示】
【発明が解決しようとする課題】
【0014】
よって先行技術のシステムは、新しいオブジェクトが悪質であるか否かを決定するために、当該オブジェクトの綿密な解析に依存する。これが遅延を引き起こし、その結果、そのファイルが解析され、新たなアンチマルウェアシグネチャが配布されるまでの間において、ユーザへのリスクを引き起こす。或いは、先行技術のシステムは、特定オブジェクトの動作の限定的な解析に依存する。若しくは、先行技術のシステムにおけるコンピュータへの送信方法は、当該オブジェクトが悪質である可能性を決定するために実行される。
【課題を解決するための手段】
【0015】
本発明の第１の態様によれば、一のコンピュータオブジェクトをマルウェアとして分類する方法であって、ベースコンピュータにおいて、前記オブジェクト又は類似の複数のオブジェクトを記憶する複数のリモートコンピュータの夫々からのコンピュータオブジェクトに関するデータを受信する工程と、前記複数のコンピュータから受信した前記コンピュータオブジェクトに関する前記データを、前記ベースコンピュータにおいて比較する工程と、前記比較に基づいて前記コンピュータオブジェクトをマルウェアとして分類する工程とを備える分類方法が提供される。
【0016】
単にシグネチャマッチングに依存する先行技術と比較すると、この態様は、複数のオブジェクト及び／又はそれらの異なるリモートコンピュータに対する影響間の比較を行い、ある特定のオブジェクトが良好又はマルウェアとして分類されるべきか否かを決定できる、高度なパターン解析を行うことができる。これにより、マルウェアであるかを決定するようなオブジェクト自体の詳細な解析をせずに、オブジェクトの性質について迅速な決定ができる。また、従来技術におけるアンチウイルスソフトウェアのような、シグネチャマッチングに用いるべき新たなシグネチャを生成する必要性は避けられる。
【0017】
好適な実施例では、前記複数のリモートコンピュータから前記ベースコンピュータに送信され、且つ前記比較において用いられた前記コンピュータオブジェクトに関する前記データは、前記オブジェクト内に含まれる又は前記オブジェクトにより構成される複数の実行可能命令と、前記オブジェクトのサイズと、前記オブジェクトの現在の名称と、前記オブジェクトのディスク上での物理的およびフォルダ位置と、前記オブジェクトの本来の名称と、前記オブジェクトの作成及び変更日時と、前記オブジェクト内に記憶された業者、製品、バージョン、及び他の情報と、前記オブジェクトヘッダ又は前記リモートコンピュータにより保持されたヘッダと、前記オブジェクトを夫々のリモートコンピュータ上で実行する、構成する又は作成する際に前記オブジェクトにより開始された又は前記オブジェクトを含むイベントと、のうちの一以上を含む。
【0018】
好ましくは、前記比較により、前記オブジェクトと他の複数のオブジェクトとの関係が識別される。一の例では、このオブジェクト又は親若しくは他の関連オブジェクトが不良（又は良好）である場合に、これを迅速及び自動的に用いて、子オブジェクトを不良（又は良好）と印付（即ち、マーク或いはマーキング）できる。よって、前記オブジェクトが関連する少なくとも一の他のオブジェクトが、マルウェアとして分類される場合に、前記オブジェクトをマルウェアとして分類する。前記他の複数のオブジェクトは、前記複数のリモートコンピュータのうちの少なくともいくつかに記憶された前記オブジェクト又は類似の複数のオブジェクトを含む。前記他の複数のオブジェクトは、親若しくは子オブジェクト、又は前記オブジェクトに対してプロセス関連オブジェクトである他の複数のオブジェクトを含む。
【0019】
最も好適な実施例では、前記データは、前記夫々のリモートコンピュータ上の複数のオ

Sophos Ex. 1002
Page 498 of 683

ブジェクトについて実行されたハッシングプロセスによって取得される鍵の形態で送信される。このような鍵を用いる主な利点は、ベースコンピュータに送信する必要のあるデータの量を低く抑えておくことである。数千又は何百万ものリモートコンピュータが接続されて存在し、更に夫々が非常に多数のオブジェクトの詳細を送信してよい場合は、これは重要な利点となりうる。

【0020】

前記鍵は、前記オブジェクト内に含まれる又は前記オブジェクトにより構成される実行可能命令を表す少なくとも一の要素を有する。この重要且つ好ましい特徴により、ベースコンピュータにおいてオブジェクトの実行可能命令についてのみ比較ができる。これは、例えば、大抵の場合オブジェクトがマルウェアであることのインジケータとなる、基本的に同じ実行可能命令を有する異なる名称のオブジェクトが、それにもかかわらずこの目的において「同じ」オブジェクトとしてみなすことができることを意味する。他の例として、ベースコンピュータに既に知られた先のバージョンと比べてわずかに改定されており、且つ、少なくとも実質上、実行可能命令の点で、先のバージョンと同じとみなされうる新たなバージョンのプログラムが公開されてよい。この場合、わずかな差を無視でき、オブジェクトは同じであるとみなされる。これは、マルウェアと、例えば先のソフトウェアの修正バージョンとを区別する際に有用であるだけでなく、データ送信及び記憶の要求が低く抑えられる。なぜなら、ベースコンピュータは、リモートコンピュータに、明らかに新しいオブジェクトがこの目的において先に知られたオブジェクトと同じであると知らせることができ、従って、リモートコンピュータに、オブジェクトの詳細やオブジェクト自体をベースコンピュータに送信することを回避させることができるからである。

【0021】

前記鍵は、前記オブジェクトに関するデータを表す少なくとも一の要素を有する。前記オブジェクトに関する前記データは、前記オブジェクトの現在の名称と、前記オブジェクトのディスク上での物理的およびフォルダ位置と、前記オブジェクトの本来の名称と、前記オブジェクトの作成及び変更日時と、前記オブジェクト内に記憶された業者、製品、バージョン、及び他の情報と、前記オブジェクトヘッダ又は前記リモートコンピュータにより保持されたヘッダと、前記オブジェクトを夫々のリモートコンピュータ上で実行する、構成する又は作成する際に前記オブジェクトにより開始された又は前記オブジェクトを含むイベントと、のうちの少なくとも一つを含んでよい。

【0022】

前記鍵は、前記オブジェクトの物理的サイズを表す少なくとも一の要素を有することが好ましい。

【0023】

この鍵に一より多いこれらの要素が存在する場合、その複数の要素は分離可能であることが好ましい。

【0024】

先ず一のオブジェクトを非マルウェアとして分類する工程と、前記オブジェクトについての許容される振る舞いを規定する前記オブジェクトのマスクを生成する工程と、少なくとも一の前記リモートコンピュータ上で前記オブジェクトの動作を監視する工程と、実際に監視された前記振る舞いが前記マスクによって許可されたものを逸脱する場合に前記オブジェクトをマルウェアとして分類する工程とを備えてよい。これにより、良好と分類又はみなされた一のオブジェクトの振る舞いを監視する効率的且つ効果的方法が提供される。またこのオブジェクトの振る舞いがマルウェアであることの理由となる場合は、当該オブジェクトを迅速にマルウェアとして再分類することができる。

【0025】

本発明の第２の態様によれば、一のコンピュータオブジェクトをマルウェアとして分類する装置であって、前記オブジェクト又は類似の複数のオブジェクトを記憶する複数のリモートコンピュータの夫々からのコンピュータオブジェクトに関するデータを受信するように構成及び配置された一のベースコンピュータを備え、前記ベースコンピュータは、前

Sophos Ex. 1002
Page 499 of 683

記複数のコンピュータから受信した前記コンピュータオブジェクトに関する前記データを、比較するように構成及び配置され、前記ベースコンピュータは、前記比較に基づいて前記コンピュータオブジェクトをマルウェアとして分類するように構成及び配置される分類装置が提供される。

【0026】

本発明の第３の態様によれば、一のコンピュータオブジェクトに関するデータを一のリモートコンピュータから一のベースコンピュータに、前記ベースコンピュータにおいて他の複数のリモートコンピュータから受信した類似データと比較を行えるように提供する方法であって、前記リモートコンピュータに記憶された一のコンピュータオブジェクトに関するデータを一のリモートコンピュータから一のベースコンピュータに提供する工程を備え、前記データは、前記オブジェクト内に含まれる又は前記オブジェクトにより構成される複数の実行可能命令と、前記オブジェクトのサイズと、前記オブジェクトの現在の名称と、前記オブジェクトのディスク上での物理的およびフォルダ位置と、前記オブジェクトの本来の名称と、前記オブジェクトの作成及び変更日時と、前記オブジェクト内に記憶された業者、製品、バージョン、及び他の情報と、前記オブジェクトヘッダ又は前記リモートコンピュータにより保持されたヘッダと、並びに前記オブジェクトを作成、構成、又は夫々のリモートコンピュータ上で実行する際に前記オブジェクトにより開始された又は前記オブジェクトを含むイベントのうちの一以上を含み、前記データは、前記リモートコンピュータ上のオブジェクトについて実行されたハッシングプロセスによって取得された鍵の形態で送信される提供方法が提供される。

【0027】

リモートコンピュータ上で実行しているいわゆるエージェントソフトウェアによって実行されるこの方法により、ベースコンピュータへの効率的なデータ送信が可能となり、データ送信及び記憶の要求が最小限となり、またベースコンピュータにおいて迅速な解析を行うことができる。

【0028】

前記鍵は、前記オブジェクト内に含まれる又は前記オブジェクトにより構成される実行可能命令を表す少なくとも一の要素を有することが好ましい。

【0029】

前記鍵は、前記オブジェクトに関するデータを表す少なくとも一の要素を有することが好ましい。前記オブジェクトに関する前記データは、前記オブジェクトの現在の名称と、前記オブジェクトのディスク上での物理的およびフォルダ位置と、前記オブジェクトの本来の名称と、前記オブジェクトの作成及び変更日時と、前記オブジェクト内に記憶された業者、製品、バージョン、及び他の情報と、前記オブジェクトヘッダ又は前記リモートコンピュータにより保持されたヘッダと、並びに前記オブジェクトを夫々のリモートコンピュータ上で実行する、構成する又は作成する際に前記オブジェクトにより開始された又は前記オブジェクトを含むイベントと、のうちの少なくとも一つを含んでよい。

【0030】

前記鍵は、前記オブジェクトの物理的サイズを表す少なくとも一の要素を有することが好ましい。

【0031】

本発明の第４の態様によれば、一のリモートコンピュータが有するマルウェアからの保護を決定する方法であって、一のベースコンピュータにおいて、前記リモートコンピュータ上である時点で動作しているセキュリティ製品のうちの全て又は選択された製品の詳細を受信する工程と、前記ベースコンピュータに接続された他の複数のリモートコンピュータから類似の情報を受信する工程と、特定の組み合わせのセキュリティ製品を有している前記他の複数のリモートコンピュータによって識別されなかった任意のマルウェアプロセスを識別する工程と、を備える決定方法が提供される。

【0032】

このように、ベースコンピュータは、例えばある時点で存在する設定及びシグネチャフ

Sophos Ex. 1002
Page 500 of 683

ァイルを含んだオペレーティングシステムと各種セキュリティ製品との特定の特異な組み合わせによって、ある特定のコンピュータがある特定のマルウェアオブジェクトに感染しやすい又は脆弱なこれらの製品及び設定を有する状態になるかに関する情報を取得するために、用いられることができる。ユーザは、適宜助言を受け、例えばこの状況を改善する提言が受けることができる。

【0033】

従って、前記一のリモートコンピュータは、前記識別に基づいて前記マルウェアプロセスによる攻撃の影響を受けやすい可能性があるという情報を前記一のリモートコンピュータのユーザに提供する工程を備えてよい。

【0034】

前記全て又は選択されたセキュリティ製品の詳細は、当該セキュリティ製品の名称と、バージョンと、ロードされたシグネチャファイルとを含むことが好ましい。

【0035】

本発明の第５の態様によれば、一のリモートコンピュータが有するマルウェアからの保護を決定する装置であって、前記リモートコンピュータ上である時点で動作しているセキュリティ製品のうちの全て又は選択された製品の詳細を受信するように構成及び配置された一のベースコンピュータを備え、当該ベースコンピュータは、前記ベースコンピュータに接続された他の複数のリモートコンピュータから類似の情報を受信するように構成及び配置され、前記ベースコンピュータは、特定の組み合わせのセキュリティ製品を有している前記他の複数のリモートコンピュータによって識別されなかった任意のマルウェアプロセスを識別するように構成及び配置される決定装置が提供される。

【0036】

本発明の第６の態様によれば、第１のコンピュータオブジェクトの子孫であるか又は関連オブジェクトである一のコンピュータオブジェクトを、マルウェア又は安全として分類する方法であって、第１のコンピュータオブジェクトをマルウェア又は安全として分類する工程と、前記第１のコンピュータオブジェクトを一意的に識別する一要素であって前記第１のコンピュークオブジェクトの子孫又は他の関連コンピュータオブジェクトの鍵において受け継がれたか若しくは存在する前記一要素を、前記第１のコンピュータオブジェクトに関連する鍵において識別する工程と、前記コンピュータオブジェクトの鍵に存在する一意的な識別子要素に基づいて、前記コンピュータオブジェクトを、場合によってマルウェア又は安全として分類する工程と、を備える分類方法が提供される。

【0037】

この態様は、系図の概念を用いてオブジェクトをマルウェアとして印付（即ち、マーク或いはマーキング）できる。例えば、ある特定のプロセスは、子プロセスを発生させて良く、故に関連している。第１のオブジェクトに関連する鍵を検査して、第１のオブジェクトを一意的に識別する要素であって且つ受け継がれる或いは第１のオブジェクトの子孫又は他の関連オブジェクトにおける鍵に存在する前記要素を、識別してよい。

【0038】

この方法は、前記第１のコンピュータオブジェクトの活動を監視する工程と、前記第１のコンピュータオブジェクトが安全として先ず分類されてその後マルウェアであると判断された場合に、前記第１のコンピュータオブジェクトをマルウェアとして再分類する工程と、を備え、更に、前記一意的な識別子要素が存在する鍵を備えた任意のコンピュータオブジェクトを、マルウェアとして自動的に分類する工程を備えてよい。

【0039】

本発明の第７の態様によれば、第１のコンピュータオブジェクトの子孫であるか又は関連オブジェクトである一のコンピュータオブジェクトを、マルウェア又は安全として分類する装置であって、第１のコンピュータオブジェクトをマルウェア又は安全として分類するように構成及び配置された一のコンピュータを備え、当該コンピュータは、前記第１のコンピュータオブジェクトを一意的に識別する一要素であって前記第１のコンピュータオブジェクトの子孫又は他の関連コンピュータオブジェクトの鍵において受け継がれたか若

Sophos Ex. 1002
Page 501 of 683

しくは存在する前記一要素を、前記第１のコンピュータオブジェクトに関連する鍵において識別するように構成及び配置され、前記コンピュータは、前記コンピュータオブジェクトの鍵に存在する一意的な識別子要素に基づいて、前記コンピュータオブジェクトを、場合によってマルウェア又は安全として分類するように構成及び配置される分類装置が提供される。

【0040】

本発明の第８の態様によれば、一のコンピュータにソフトウェアをインストールする方法であって、一のコンピュータへのソフトウェアのインストール開始時に、ユーザが前記インストールを認証したかを確認するための前記コンピュータ上のコンピュータ生成プロンプトを、前記ユーザに提供する工程と、ユーザ認証が受信されない場合に前記インストールを中止する工程と、そのほか、前記コンピュータにおいて、前記インストールを進めるための前記ユーザ認証を受信する工程と、前記インストールを進める工程と、前記インストール中に作成又は使用された複数のコンピュータオブジェクトに関するデータを取得する工程と、前記データを前記ローカルコンピュータに記憶する工程と、を備えたインストール方法が提供される。

【0041】

これは、ユーザが新たなソフトウェアをインストールしていて、例えば上述した種類のコミュニティデータベースを備えたベースコンピュータに接続されていない際の安全性を提供する。この場合、ローカルコンピュータ上で実行しているエージェントソフトウェアで実行されるこの方法により、ユーザは、インストール中に作成されたオブジェクトに関するデータ（例えば、プロセス、新たなファイル等）を同時に収集しながらインストールを進めることが可能となる。

【0042】

前記ローカルに記憶されたデータは、前記インストール中に作成又は使用された全てのオブジェクトが前記インストールプロセスの一部であることを確認するために前記インストール中に参照され、前記インストール中に作成又は使用された全てのオブジェクトが前記インストールプロセスの一部でない場合には、（ｉ）前記インストールを中止する工程、及び（ｉｉ）前記コンピュータ上のコンピュータ生成プロンプトを適宜前記ユーザに提供する工程のうち少なくとも一方を備えることが好ましい。これにより、インストールが要求されたオブジェクトのみの作成又は使用を許可し、よって（マルウェアが、新たなソフトウェアの通常インストールの一部であるとは予期されないオブジェクトをしばしば作成すること条件下で）無意識にマルウェアをインストールしてしまわないようにすることがこの方法で確保される。

【0043】

好適な実施例では、複数のコンピュータに接続可能であるコミュニティデータベースに前記コンピュータを接続する工程と、前記記憶されたデータを、他のコンピュータによって提供された類似のデータと比較するために前記コミュニティデータベースにアップロードする工程とを備える。

【0044】

この方法は、複数の信頼できるインストーラに関するデータを前記コンピュータにダウンロードする工程を備え、前記複数の信頼できるインストーラに関するデータは、前記信頼できるインストーラに関連する又は前記信頼できるインストーラによって作成された任意のオブジェクトを自動的に認証して先に進むように、前記インストール中に参照されてよい。これにより、先験的に信頼できると知られたソフトウェアのインストールが容易になる。

【0045】

前記複数の信頼できるインストーラに関するデータは、前記コンピュータにおける前記インストールを進めるための前記ユーザ認証の受理に続く所定の時間のみ参照されてよい。

【0046】

Sophos Ex. 1002
Page 502 of 683

本発明は、コンピュータに上記の方法のうちのいずれか一つを実行させるプログラム命令を備えるコンピュータプログラムも含む。

【0047】

図面を参照して記述される本発明の実施例は、コンピュータ装置において実行されるコンピュータプロセスと、コンピュータ装置自体とを含むが、本発明はコンピュータプログラムにまで及ぶ。特に、本発明を実施するのに適したキャリア上又はキャリア内のコンピュータプログラムである。このプログラムは、ソースコード、オブジェクトコード、コード中間ソース、及び部分コンパイル型等のオブジェクトコードの形態であってよい、或いは、本発明に係るプロセスの実施において好適なその他の形態であってよい。キャリアは、プログラムを伝送できる任意の実体又は装置であってよい。例えば、キャリアは、例えばＣＤ－ＲＯＭ又は半導体ＲＯＭ等のＲＯＭ、又は例えばフロッピーディスク又はハードディスク等の磁気記録媒体等の記憶媒体を備えてよい。更にキャリアは、電気又は光ケーブルを介して、若しくは無線通信又は他の手段により伝えられる電気又は光信号等の、伝送可能なキャリアであってよい。

【発明を実施するための最良の形態】

【0048】

添付の図面を参照して、本発明の実施例を一例として説明する。

【0049】

図１を参照すると、コンピュータネットワークは、一般にインターネット１等の分散型ネットワークのようなものに基づくものとして示される。しかしながら、本発明は、ＬＡＮ等の他の種類のネットワークを用いて、又はその全域で実行されてよい。複数のローカル又は「リモート」コンピュータ２は、インターネット１を介して「中央」又は「ベース」コンピュータ３に接続される。コンピュータ２は、夫々様々に、パソコン、任意の種類のサーバ、ＰＤＡ、携帯電話、双方向テレビ、又はコンピュータオブジェクトを取り込んで動作させる他の装置であってよい。この意味でのオブジェクトは、コンピュータファイル、ファイルの一部若しくはサブプログラム、マクロ、又はコンピュータにより若しくはコンピュータ上で動作するウェブページ若しくは他のコード、或いは他の実行、エミュレート、シミュレーション、又は解釈されたイベントであってよい。オブジェクト４が図に模式的に示されているが、例えばライン５で示すようにインターネット１を介してリモートコンピュータ２にダウンロードされてよいし、又はライン６で示すように直接適用されてもよい。

【0050】

一の好適な実施例では、ベースコンピュータ３はデータベース７を保持する。リモートコンピュータ２がオブジェクト４を実行してオブジェクト４が安全か否かを決定する際に、リモートコンピュータ２は、このデータベース７と作用する。コミュニティデータベース７は、接続された全リモートコンピュータ２上で実行される各オブジェクトに関連する情報によって、時間とともに増められてゆく。以下に更に説明するように、各オブジェクト４の代表データは、オブジェクト、及びその効果に関連するいわゆるシグネチャ（signature）又は鍵（key）の形態をとることが好ましい。以下に更に説明するように、データベース７は、オブジェクトの性能及び動作のパラメータを設定するオブジェクト４用のマスクを更に含んでよい。

【0051】

ここで図２を参照すると、開始点２１において、一のプロセス等のコンピュータオブジェクト４をリモートコンピュータ２において実行する。ステップ２２において、リモートコンピュータ２上で実行されているローカル「エージェント」ソフトウェアの動作により、そのプロセスの動作がフックされ、エージェントソフトウェアがリモートコンピュータ２に記憶されたローカスデータベースを検索して、その特定のプロセス、その関連オブジェクト、及び／又はイベントを表すシグネチャ若しくは鍵を検索できる。もし、そのローカルシグネチャが存在する場合は、そのプロセスが安全とみなされることを示すか、又は安全でないとみなされることを示す。危険なプロセスとは、マルウェアであると発覚した

Sophos Ex. 1002
Page 503 of 683

プロセスかもしれないし、その実行から生じた、危険若しくは悪質な結果を予測しなかった又は知ったことが発覚したプロセスかもしれない。もしシグネチャがそのプロセスは安全であると示す場合は、そのプロセス又はイベントは、ステップ２３において実行するリモートコンピュータ２上のローカルエージェントソフトウェアにより許可される。もしシグネチャが、そのプロセスは安全でないと示す場合は、そのプロセス又はイベントはステップ２４において中止される。

【0052】

当然のことながら、「安全である」又は「安全でない」の２つよりも多い状態が存在してよく、選択がユーザに与えられてよい。例えば、一のオブジェクトが局所的に安全でないとみなされる場合、それにもかかわらずに関連プロセスを実行できる選択肢がユーザに与えられてよい。各リモートコンピュータ２に対して複数の異なる状態が与えられてもよい。この状態は、時間枠又はリモートコンピュータの位置、状態、又は所有権を考慮する、中央システムによって、変更可能である。

【0053】

オブジェクトが局所的に知られていない場合、そのオブジェクトの詳細は、インターネット１又は他のネットワークを通って、コミュニティデータベース７に蓄積するための、また好ましくはベースコンピュータ３において更なる解析を行うためのベースコンピュータ３に送られる。この場合、次にコミュニティデータベース７は、ステップ２５において、コミュニティデータベース７に既に記憶されているオブジェクトのシグネチャを求めて検索される。コミュニティデータベース７には、夫々監視されたリモートコンピュータ２により実行されるプログラム又はプロセス等のオブジェクトを代表するシグネチャが供給される。この分野における典型的な実施では、ベースコンピュータ３に接続又は接続可能な数千又は何百万ものリモートコンピュータ２が存在してよい。そのため、インターネット１に新たに公開された、又はそうでなければこれらのリモートコンピュータ２のうちのいずれかで見つかる任意のオブジェクトが、すぐに見つけられる。またシグネチャが作成され、夫々のリモートコンピュータ２によってベースコンピュータ３に送信されるであろう。

【0054】

コミュニティデータベース７が、関与しているリモートコンピュータ２において予め知られていなかったオブジェクトのシグネチャを求めて検索される際に、そのシグネチャが発見され、且つシグネチャがオブジェクトは安全であると示す場合は、シグネチャのコピー、又は少なくともそのオブジェクトが安全であるというメッセージが、ステップ２６において関与するリモートコンピュータ２のローカルデータベースに送信され、ローカルデータベースに書えられる。このようにして、リモートコンピュータ２は、この情報を、そのオブジェクト４に出会う次の機会へと即時に手渡す。別のメッセージも、現在のインスタンスでオブジェクトを実行させるために、リモートコンピュータ２に戻される。

【0055】

もしシグネチャがコミュニティデータベース７で発見され、これが何らかの理由でオブジェクトは安全ではないと示す場合、シグネチャは再びコピーされてローカルデータベースに戻され、ステップ２７において「安全でない」と、印付（即ち、マーク或いはマーキング）される、並びに／或いは、メッセージがリモートコンピュータ２に送信されて、オブジェクトの実行が中止される（又は実行できなくなる）、及び／又はユーザにオブジェクトを実行するか否かについての、納得した上での選択肢（インフォームドチョイス）が与えられる。

【0056】

もし、全コミュニティデータベース７を検索後もオブジェクトがまだ知られない場合は、このオブジェクトは、この分野において今までに見られたことのない完全に新しいオブジェクトであることが仮定される。従って、シグネチャはステップ２８において、そのオブジェクトを表すものとして作成される、或いは、リモートコンピュータ２により送信されたシグネチャは、この目的で用いられ、このシグネチャが、ステップ２９において不良

Sophos Ex. 1002
Page 504 of 683

である、又は安全でないようなコミュニティデータベース７として、先ずは印付される。そのシグネチャは、ステップ３０において最初にオブジェクトを実行したリモートコンピュータ２のローカルデータベースにコピーされる。次に、メッセージがリモートコンピュータ２に送られ、リモートコンピュータ２にオブジェクトを実行しないように命令してよい、或いは、オブジェクトが実行可能であるか否かについてのインフォームドコンセントを、ユーザに与えてもよい。加えて、ステップ３１において、オブジェクト自体のコピーをリモートコンピュータ２からコミュニティデータベース７により要求されてよい。

【００５７】

もし、リモートコンピュータ２におけるユーザが、新しすぎるので安全でないとみなされたプロセスを実行する、と選択する場合、そのプロセスはリモートコンピュータ２及び／又はコミュニティデータベース７により監視されてよい。また、例えばｎ日間後にも何の悪影響も起きない又は示されない場合は、安全であるとみなされてよい、或いは、コミュニティデータベース７は、ネットワークの一部を形成する多数のリモートコンピュータ２により求められたプロセスの各インスタンスのログ（記録）を保持してよい。特定数のインスタンスが記録され、他の特定数のインスタンス又はプロセスが実行を許可され安全に実行された後には、コミュニティデータベース７におけるシグネチャは、安全でないというよりはむしろ安全であると印付されてよい。安全性の監視における他の多くの変更は、この概念の範囲内で行われてよい。

【００５８】

ベースコンピュータ３に送られるオブジェクト４の詳細は、オブジェクト４を一意的に識別するシグネチャ又は「鍵」の形態であることが好ましい。これは主にデータ格納及び送信要求の量を制限するためである。この鍵は、リモートコンピュータ２においてオブジェクトに作用しているハッシング関数により形成されてよい。

【００５９】

好適な実施例における鍵は、少なくとも三つの分離可能な要素を有するように特別に配置される。第１の要素は、オブジェクト内に含まれる又はオブジェクトにより構成される実行可能命令を表す、第２の要素は、当該オブジェクトに関するデータを表す。第３の要素は、オブジェクトの物理的なサイズを表す。第２の要素におけるオブジェクトに関するデータは、ファイル名と、そのディスク上での物理的及びフォルダ位置と、その本来のファイル名と、その作成及び変更日時と、業者、製品及びバージョン、並びにオブジェクト内に記憶された他のいかなる情報と、そのファイルヘッダ又はそれについてリモートコンピュータ２により保持されたヘッダと、またオブジェクトを作成、構成、又は夫々のリモートコンピュータ上で実行する際にオブジェクトにより開始された又は前記オブジェクトを含むイベント等の、任意又は全ての他の識別形態であってよい。一般に、鍵に備わった情報は、少なくともこれらの要素のうちの一つ、またはこれらのうち任意の組み合わせにおける任意の二以上の要素を含んでよい。

【００６０】

一の好適な実施例では、タイプＰＥ（マイクロソフト（Microsoft）により規定されたPortable Executableファイル）の.exe及び.dllファイル等（しかしこれらには制限されない）の全ての実行ファイルについて、チェックサムを作成する。三種類のチェックサムが、ファイルの性質に応じて生成される、即ち、

タイプ１：ファイルにおける５つの異なるセクションをチェックサムする。これらは、インポートテーブル、コードセクションにおける開始セクション及び終了セクション、並びに全ファイルの開始セクション及び終了セクションを含む。このタイプは、解析される大部分のファイルに対して適用される。

【００６１】

タイプ２：旧ＤＯＳ又は１６ビット実行ファイルに対して、全ファイルをチェックサムする。

【００６２】

タイプ３：ある所定サイズを超えるファイルに対して、ファイルを大きな塊毎にサンプ

Sophos Ex. 1002
Page 505 of 683

リングして、その後チェックサムする。ある所定サイズより小さいファイルに対しては、全ファイルをチェックサムする。

【0063】

チェックサムプロセスに対して、原理上は任意の技術が可能である。ＭＤ５（Message Digestアルゴリズム５）は、この目的で広く用いられる暗号ハッシュ関数である。

【0064】

これにより、チェックサムの実行可能要素のみを参照し、共通の実行可能コードを共有する二つの実行可能要素を比較することにより、コアチェックサムを生成することができる。

【0065】

上記のタイプ１チェックサムに対して、三つのシグネチャプロセスが用いられてよい。第１のシグネチャは、全ファイルを規定し、殆どいずれのファイルの内容に対する変化とともに変化する。第２のシグネチャは、変化が少ないプロセスの処理命令の規定のみを図る。第３のシグネチャは、ファイルサイズを用いており、これにより異なるサイズのオブジェクトが衝突する可能性が非常に減少する。異なる対応物を伴って頻々に現れる全てのシグネチャの発生を追跡或いは探知することにより、変更された又は共通点から作成されたけれども、新たな、場合によっては悪質な機能性を実行するように編集されたプロセスを識別することができる。

【0066】

この「メタデータ」は、現在の及び新たに派生したヒューリスティクス（発見的問題解決法）を、コミュニティデータベース７のデータ上で実行させることができる。

【0067】

コミュニティデータベース７に記憶されたデータは、必然的に一のオブジェクトの作成、配置、実施、行動（挙動）（behavior）、識別、並びに、他の複数のオブジェクトであってそれに作用する又はそれにより作用される該他の複数のオブジェクトに対する関係を提供することになる。

【0068】

好適な中央ヒューリスティクスは、一のオブジェクトが安全か、安全でないか、又は疑わしいかをはっきりさせるために、５つの特異的なプロセスを用いる。

【0069】

これらのうちの第１のプロセスは、オブジェクトを見ているすべてのリモートコンピュータ２から獲得した又は相関した一又は複数の名称、位置、業者、製品、バージョン情報を用いる。単一のオブジェクトに対してこれら複数の情報を考慮することによって、オブジェクトの信憑性及び／又は信頼性の程度として用いられるスコアを決定できる。大抵の安全なオブジェクトは、多数の識別情報又は位置を用いない傾向がある。オブジェクトの種類及びその位置については、この情報を考慮して規則を定めることができる。例えば、テンポラリファイルは、同一のオブジェクトについて各リモートコンピュータ上では異なる可能性のある複数のシステム生成ファイル名を頻繁に用いる。オブジェクトが少数しか存在しない場合には、先にその識別情報を用いた他のオブジェクトの既知の振る舞い（又は挙動若しくは行動）と比較して、その振る舞いを考慮するための参照点を提供する。例えば、notepad.exeのバージョンという趣旨の新たなオブジェクトは、notepad.exeとしても知られる一以上の他のオブジェクトの振る舞いと比べて、その振る舞いを有することができる。この比較は、同一又は類似の識別情報を用いる単一の他のオブジェクト又は複数の他のオブジェクトに対して行われてよい。このようにして、新たなパターンの振る舞いが、新たなオブジェクト用に識別される、またそれにより、好適な実施例は、オブジェクトの振る舞いを時間の経過とともに取り纏まり、先に安全とみなされたオブジェクトの状態を再考させてしまうような新たな振る舞いパターンを識別することができる。或いは、識別に基づくスコアを、他のオブジェクトのスコア、又は複数の組み合わせで考慮すべきこのオブジェクト上の他のプロセスにより作成されたスコアとともに考慮してよい。

【0070】

Sophos Ex. 1002
Page 506 of 683

第２のプロセスは、一のオブジェクトの、当該オブジェクトに作用する又は当該オブジェクトが作用する他の複数のオブジェクトに対する関係を用いる。例えば、どのオブジェクトがこのオブジェクトを作成したか、どの複数のオブジェクトがこのオブジェクトを作成したか、どの複数のオブジェクトがこのオブジェクトを実行又は構成する一のレジストリキーを作成したか、どの複数のオブジェクトがこのオブジェクトにより作成された複数のレジストリキーによって構成されたか又は当該複数のレジストリキーを備えているか、等について解析できる。この点では、オブジェクトは、当該オブジェクトにより他のオブジェクトに対して、又は他のオブジェクトにより当該オブジェクトに対して実行されたイベントに基づく関係を有していると考えられる。この単純な１対１関係の連鎖は、複雑な一連の点相関を与える。これにより、受け継がれた関係が、任意のオブジェクト、イベントによるその前身、又はイベントによるその子孫（即ち、子及びサブチャイルドプロセス）に対して考慮できる。これにより、既知の、未知の、安全と知られた、又は不良と知られたオブジェクト、若しくはこれらの組み合わせとの関係及び関連付けについて記述するスコアを展開できる。一又は他の種類に対する特異な関係、多くの関係、又は混じりあった関係を有するオブジェクトは、安全か否かを判断されてよい、或いは、安全か否かの決定に達するために、関係に基づくスコアを他のスコアとともに考慮してよい。このデータは、直接又は他のオブジェクトを介して関連するオブジェクト、及びそれらの振る舞い（或いは行動若しくは挙動）に関する多くの因子を推定するために用いることもできる。例えば、一のオブジェクトの振る舞いが、どのように他のオブジェクトとの関連性又はつながりによって影響又は変更されるかについて推定できる。例えば、マイクロソフトによりウィンドウズシリーズのオペレーティングシステムが供給されたnotepad．exeについて考える。これは、限られた範囲の機能性しか有しておらず、従って、データを他のコンピュータに送信したり、他のプログラムを実行したりする等の幅広いイベントを実行するとは期待されない。しかしながら、notepad．exeの振る舞いは、ダイナミックリンクライブラリ導入（ＤＬＬ導入）等、それに新たなコードを導入することにより変更され得る。この場合、notepad．exeは、コード導入又は他のオブジェクトとのつながりによって取得された新たな性能を有するであろう。オブジェクト間の関係を規定するデータを用いることで、プログラムの新たな振る舞いは、他のオブジェクトとの関連性に起因すると推定できる。もし、その新たな振る舞いが悪意ある場合、プロセスのいずれか又は全ては、必要に応じて安全でないと印付することができる。

【0071】

取得された振る舞いの組み合わせは、オブジェクトが安全か否かを決定する基準を提供する。典型的には、マルウェアは、ある振る舞い及び特徴を示す。例えばマルウェアは、しばしば自己存続の必要性がある。これは、あるイベント又はシステムの再起動を自動的に再始動する必要がある場合に、明らかとなる。特異な位置で自動再始動又は実行を引き起こすオブジェクトを作成することが、マルウェアの典型的な特徴である。ウィンドウズシステム環境のコアオブジェクトの入れ替えは、マルウェアの典型的な特徴の他の例である。振る舞いのパターンを提供することにより、オブジェクトが安全でないか安全かの決定を自動化できる。コミュニティデータベース７におけるコミュニティデータの集中化は、オブジェクトの振る舞いを迅速に取り入れる能力をもたらし、マルウェアの迅速な識別及び決定を可能にする。オブジェクトは、スコアを導く際に考慮され得るイベントを、自動的に実行してもよい。

【0072】

第３のプロセスは、時間及びボリュームを含む。関連するデータは、オブジェクトが最初に見られたのはいつか、最後に見られたのはいつか、何回見られたか、所与の時間間隔で何回見られたか、オブジェクトにおける加速の増加又は減少は見られたかを含む。この情報は、複数のリモートコンピュータのコミュニティにおいて一のオブジェクトの普及を決定するのに非常に密接に関係している。スコアは、一のオブジェクトが安全か、安全でないか、若しくは流行しすぎて非常に徹底的な調査無しに実行又は伝播させることができないか、を決定するために用いることができる。これらのメトリクス（metrics）に基づ

Sophos Ex. 1002
Page 507 of 683

いて展開される。この場合、オブジェクトは、その振る舞い又は関係についての未解決の更なる情報の実行を一時的に控える、又は阻止することができる。このスコアは、他のプロセスからのスコアと組み合わせて用いられてもよい、時間に関しても、振る舞い及び識別性を含むけれどもこれらに制限されない他の情報との組み合わせで、非常に意味がある。例えば、多形性又は無作為に指名されたオブジェクトの場合、時間は強力な限定子である。（多形性ウイルスは、一のコンピュータから他のコンピュータに複製する度にその暗号化アルゴリズム及び対応する暗号鍵を変化させるので、従来の手法で検出するのは困難である。）他の複数のプログラムを作成する一のプログラムは、時間の経過に伴う活動に基づき、しばしば正常又は異常であるとみなされる。

【0073】

第４のプロセスは、一のオブジェクトの振る舞いを考慮する。これにより、スコアは、一のオブジェクトにより実行されたイベント、若しくは当該オブジェクト自体又は他のオブジェクトにより当該オブジェクトに対して実行されたイベントの種類に基づいて、展開できる。コミュニティデータベース７の集中型システムは、イベントの種類を無限にでき、イベントを実行するオブジェクト、又はそれに対して行われたイベントを備えたオブジェクト、若しくは両方を考慮できる。幾つかのイベントの種類も、オブジェクト以外の外部情報、例えばイベントを実行してインターネットチャットリレーサイトに接続するプログラム、又はウインドウズホストファイル等の非実行ファイルを変更するプログラムに関連する。一のオブジェクトにおける行動イベントは、任意のイベントの「行為者（actor）」（即ち、オブジェクトが他のオブジェクトに対して何かを行う）又は「被性者（victim）」（即ち、オブジェクトが他のオブジェクトにより何かされる）として、組み合わせて、順番に、大量に、存在又は非存在下で、又はこれらの任意の組み合わせで等、いろいろな方法で考え得る。好適な実施例における行動イベントは、リモートコンピュータ２により、又は他の外部源から供給されてよい。このプロセスは、これらを孤立させて又は組み合わせて考慮できる。更に、オブジェクトが作用する又はオブジェクトに作用する他のオブジェクトの状態と組み合わせて行動イベントが考慮されることは、好適な実施例の特徴である。例えば、プログラムの作成は、そのプログラムの作成が安全か否か、新しいか、知られていないか、又は疑わしいかによって、異なるスコアを有してよい。同様に、不良と知られたプログラムにより作成されたプログラムは、それを作成するオブジェクトの状態に応じてその作成イベントに起因した異なるスコアを有する可能性がある。

【0074】

第５のプロセスは、ウェブページ又はスクリプトの振る舞いを考慮する。この点に関して、ウェブページ及びＵＲＬの組み合わせには、あたかも他の実行ファイルのようなオブジェクトであるかのように振る舞いが追跡或いは探知されるという特性が与えられている。この例において、ウェブページは、通常ウェブブラウザ（例えば、IExplore.exe又はFirefox.exe）によって実行されるイベントとして見られるイベントを実行してよい。好適な実施例は、ウェブブラウザの識別の詳細及びシグネチャを、ブラウザ内に表示されている又は実行しているウェブページに関連する「疑似」オブジェクト識別に代えて使う。この点に関して、関連するウェブページ及び／又はウェブサイトの状態が安全か、安全でないか、知られていないか、疑わしいかについて、他のオブジェクトと同様に決定されてよい。ウェブページの「疑似」オブジェクト識別により、好適な実施例は、潜在的に非安全な行動の一部又は全てを防ぐように、若しくはリモートユーザに警告情報を与えてウェブサイト、ウェブページ又はそれらの内容の安全性について案内するように、そのウェブページ又はウェブサイトの機能性を阻止、妨害（interject）又は制限することもできる。

【0075】

他の種類のうち、取得されたメタデータの種類は以下の通りであってよい。即ち、

「イベント」：これらは、他のオブジェクト又は他の実体（entity）に作用するオブジェクトの活動（actions）、又は振る舞い若しくは行動（behaviors）を規定する。イベントは、三つの主要要素を有している。即ち、行為を実行するオブジェクトの鍵（「行為者」）、実行された行為（「イベントタイプ」）、並びに、行為が実行されている他の実態

Sophos Ex. 1002
Page 508 of 683

の識別又はオブジェクトの鍵（「属性者」）である。単純でありながら、この構造により、無限の一連の行動及び関係を規定することができる。一のイベントにおける三要素の例は、以下の通りであってよい。

【0076】

【表1】

行為者（actor）	イベントタイプ	受動体(victim)
オブジェクト１	プログラム作成	オブジェクト２
オブジェクト１	データ送信	ＩＰアドレス３
オブジェクト１	プログラム消去	オブジェクト４
オブジェクト１	実行	オブジェクト２
オブジェクト２	レジストリキー作成	オブジェクト４

【0077】

「識別」：これらは、一のオブジェクトの属性を規定する。これらは、ファイル名、ディスク上又はメモリ内におけるその物理的位置、ファイルシステム（パス）内におけるディスク上の論理的位置、ファイルが作成されたのはいつか、最後にアクセスされたのはいつか、最後に変更されたのはいつか、業者として記憶された情報、ファイル及びその内容の一部及びバージョン番号である製品、その本来のファイル名、並びにファイルサイズ等を含むファイルヘッダ詳細などの、各種アイテムを含む。

【0078】

「起源行為者（genesisactor）」：イベントの直接の行為者ではないが、実行されているイベントの最終的な親である一のオブジェクトの鍵。例えば、ソフトウェアのインストールの場合、これはユーザ又はシステムが最初に実行し、且つソフトウェアのインストールプロセス、例えばSetup.exeを開始したオブジェクトの鍵であろう。

【0079】

「補助データ（ancillary data）」：多数のイベントは、補助データ、例えばレジストリ実行キーの作成を記録するために用いられたイベント等のイベントを要求してよい。この状況において、「イベント」は、レジストリ実行キーを作成する行為者オブジェクト、イベントタイプ自体（例えば、「レグランキー（regrunkey）」）、並びにレジストリ実行キーの被性者若しくは対象を、識別する。この場合の補助データは、実行キーエントリ自体を規定する。即ち、ハイブ、キーの名称、バリューである。

【0080】

「イベントチェックサム」：イベントデータは、単一のイベント、行為者、属性者及び任意の補助データに対するその識別に対する情報が数百バイトに至るほど非常に大きくなりうるので、システムはこのデータ自体をイベントチェックサムによってまとめることができる。二つのイベントチェックサムは、ＣＲＣ及びＡｄｌｅｒ等の様々なアルゴリズムを利用して用いられる。チェックサムは、イベントのコアデータのものである。これにより、リモートコンピュータ２は、既にこれらの記憶されたチェックサムに関連するデータを有する可能性がある中央コンピュータ３に、データのチェックサムを送信できる。この場合、リモートコンピュータ２に要なる情報を要求しない、中央コンピュータ３が、そのチェックサムを一度も受信したことがない場合のみ、関連データをリモートコンピュータ２に要求する。これにより、リモートコンピュータ２及び中央コンピュータ３の両者のパーフォーマンスがかなり改善され、より効果的なスケーリングが可能となる。

【0081】

よって、コミュニティデータベース７において、リモートコンピュータ２から取得されたメタデータを用いて、コミュニティ全域におけるプロセスの振る舞い（或いは行動若しくは挙動）を規定することができる。上述のように、このデータは上記の複数の要素（ファイルサイズ、位置等）のうちの少なくとも一の要素、若しくは二、三、四、五、又は六

の要素、或いは七の全ての要素（又はここで具体的に述べなかったより多くの要素）を含んでよい。これは適宜、コミュニティデータベース７で利用するための新たな自動化ルールのモデル化、テスト、及び生成を行うために用いてよく、更にリモートコンピュータ２のローカルデータベースに保持され利用されたこれらに追加されるルールとして用いて、新たな又は進のプロセス及びプロセス活動に対するリモートコンピュータ２の応答の識別及び決定を行ってよい。

【００８２】

また、同質の実体としての任意のサブプロセスとともにプロセスを監視でき、全コミュニティにわたってトップレベルプロセスの活動を比較できる。また、確実且つ潜在的に悪意のある実行は、一以上の具体的なサブプロセスがロードされる場合に起こるのみである。これにより、言うまでもなく今日悪意のあるコードの主要源であるインターネットからユーザが取得する、ダウンロード可能な任意のコードにより、機能性を容易に変更できるInternet Explorer又は他のブラウザ等の、プログラムの効果的な監視（不必要な遮断無しに）が可能となる。

【００８３】

頻繁に利用する複数のユーザのうち潜在的にかなりの部分は、そのうちの少なくとも一人が新たなマルウェアに感染しているという高い確率を示す。伝播速度を検出及び記録して、マルウェアの伝播を検出できる。マルウェアは、ファイルサイズ、位置、及び名称等の上述した他の因子と随意に併用した、この伝播速度に基づいて、悪質或いは不良と特定できる。感染のシンプルボリュームをトリガーとして用いることもできる。更なる実施例では、コミュニティ内でコードを実行する最初の試みの進行に相まって、名称以外では同一のコードの一部分における名称の違いにより、それ以外は同様に署名されるコードの一部分を悪質として表すパターンマッチングが可能になる。

【００８４】

この特徴は、ある実施例において、「私たちのコミュニティにおいて、ロックされずにＸよりも速く伝播するものはない」状態を可能とするので、任意のプロセス又はイベントが所与の期間を超えてより迅速に伝播する場合、悪質として印付される。これは、例えば一のオブジェクトが十分迅速に伝播している場合には、それがマルウェアか否かを決定する解析を行う前にコンピュータを感染させてしまう可能性があることを考えれば、安全性のためである。

【００８５】

このプロセスは、コミュニティにおける伝播業者（即ち、伝播種類の源）の識別により、コミュニティデータベースに保持されたタイムスタンプデータ及びこれらの属性を悪質として有するコードの一部分のマーキング（印付）から自動化できる。比較すると、全ての他のアンチマルウェアプロバイダは、単純に悪質として知られたモデルに頼っており、従って、実際に終端部で生じており報告されるマルウェア感染に主に依存していると考えられている。

【００８６】

よって、コミュニティデータベース７を用いて早期診断、又は単純に予防措置をとることができ、従って、潜在的に迅速に伝播するワームや他のマルウェアをそれらのライフサイクルの非常に遅い段階で停止させることが可能である。インターネットに接続されたすべてのコンピュータを数分以内に感染可能なワームが生成可能であるとすると、この特徴は非常に望ましいものである。

【００８７】

新たなソフトウェアの伝播速度を規定するデータを、エージェントソフトウェアによりリモートコンピュータ２から集めてコミュニティデータベース７に供給したメタデータと組み合わせることにより、より迅速な決定さえなされてよい。これは、リモートコンピュータ２上でランダムに名称及び／又は位置を変更することによりそれら自体をユーザから隠そうとするプロセスの監視を含む。また、コンピュータ上で完全同一（即ち、同一のコード内容を備える）であるけれども異なる名称の同一コピーを作成するプロセスの試みも

Sophos Ex. 1002
Page 510 of 683

含む、これは、ワームの伝統的な特質である。

【0088】

一のオブジェクトのシグネチャは、そのオブジェクトを用いて作ることができ、且つそのオブジェクトから想定される振る舞いの特定タイプを示すマスクを備えるか又は該マスクに関連してよい。一のオブジェクトがリモートコンピュータ２上で実行可能である場合、初期のシグネチャ検索２２がオブジェクトは安全であると示していても、そのオブジェクトの動作はマスクのパラメータ内で監視されてよい。マスクは、例えばオブジェクトの想定される振る舞いと、通信を可能にするためにオープンにすることが要求された任意のポート又はインターフェースの詳細を含めて、オブジェクトによって合法的にリモートコンピュータ２に作成させた、又は当該作成が要求された任意の外部要求、又はインターネット接続と、そのオブジェクトから問い合わせがなされると予測されるローカル、又はローカルエリアネットワークを超えたネットワーク、ワイドエリアネットワーク、又はインターネット等の、任意のデータベースと、等を示してよい。よって、マスクは、そのオブジェクトの想定される「正常な」振る舞いの全体像を与えることができる。

【0089】

従って、実際には、一の実施例において、オブジェクトの振る舞いは一（又は複数）のリモートコンピュータ２により継続的に監視され、またそのオブジェクトに関連する情報がコミュニティデータベース７とやり取りされ、オブジェクトがその想定されるマスク内で実行しているかが決定される。マスクを逸脱する任意の振る舞いは、識別され、オブジェクトが安全のままであるか否かについて、継続的に評価することに用いることができる。従って、例えば定期的に（例えば毎月又は毎年）オブジェクトが新たなポートを開いて更新する、又は定期的なデータを取得する場合、この情報にフラグが立てられる。もし、オブジェクトがこれを他のリモートコンピュータに対して行い、何の悪影響も受けなかった場合、或いはこの振る舞いが他のオブジェクトから安全であると知らされている場合は、この振る舞いは安全な振る舞いとしてみなされてよく、そしてマスクは、これを許可するように変更される。仮に、この新たな行動が実際は安全でない又は悪意のある結果をもたらすと事前に分かっていた場合は、そのオブジェクトは、たとえ先に安全であるとみなされていたとしても、安全でないものと印付される。同様に、オブジェクトが、安全でないと知られたウェブサイトやデータベースに接続しようとする、又は一般に安全でないプログラムによりのみ行われるアクションであると知られたアクションを起こそうとする場合は、再度、オブジェクトは安全でないとみなされてよい。

【0090】

これは図３に模式的に示される。図３は、任意のオブジェクトが、例えば、主要なソフトウェア会社、照合の権威、政府機関等の信頼できる相手によって事前に許可されうるという概念も示す。事前許可により、以前は発売されていなかった新たなオブジェクトの供給者は、そのオブジェクトの事前許可を取得でき、またそのオブジェクトの想定されており且つ許容されている振る舞いを詳述するマスクの供給者による供給を随意に含む。

【0091】

例えば図３を参照すると、一のプロセスが実行される際に、ローカル及び／又はコミュニティデータベースはステップ３１以前として検索される。このプロセスが事前許可されたものでない場合、図２の複数のステップが行われ、このプロセスは、ステップ３２で、実行を許可されるか又はされない。このプロセスがステップ３３で決定されるように事前許可される場合、ステップ３４において、すぐに実行可能とされる。これにより、この方法の動作が終了してよい。しかしながら、好適なバリエーションにおいては、このプロセスは実行中に監視され、監視状態のステップ３５で将来実行されるたびに監視されて、その行動がその事前許可されたマスク３６の範囲内にあるかが決定される。この行動が事前許可されたマスク３６の範囲内にある場合、プロセス実行の継続が許可される。もし、この行動が、事前許可されていないプロセス又は接続を更に開始すること等により、事前許可されたマスク３６を逸脱する場合、この行動は、警告ステップ３７においてフラグ立てされる。様々なアクションがこの段階でとられうる。プロセスは、単純に実行が許可され

ないというものでもよい。或いは、この行動は許容できるか否かを確認することのできる初期に事前許可を可能とした信頼できる権威に連絡がとられてもよい。もし許容できる場合、マスクは適宜変更されてよい。もし許容できない場合、そのプロセスは安全でないと印付される。他の多くのアクションは、そのような警告状態を通知する際に行われてよい。

【００９２】

もしプロセスが、ステップ３３において事前許可されていないと見つかったけれども実行を許可されている場合、そのプロセスはそのプロセスの正常な振る舞いを代表するマスク３９を生成するためにステップ３８で監視される。このマスクを代表するデータは、他のコンピュータがこのプロセスを実行する際のスキャンするコミュニティデータベース７に送信されてよい。プロセスを実行する度に又はプロセスの実行中に継続して当該プロセスを監視することにより、そのプロセスの先の振る舞いとは異なる任意の振る舞いを知ることができ、マスクを変更できる。或いはこの振る舞いを用いて、一度安全であるとみなされたプロセスを現在は安全でないとみなすべきであると決定してもよい。

【００９３】

他の実施例では、コンピュータ２は、コミュニティデータベース７に周期的に又は要求に応じて情報を提供し、当該コンピュータ２上にロードされた又は利用可能なソフトウェア製品の全て又は選択された製品を代表する、インストールされたエージェントソフトウェアを備えてよい。特にこれは、局所的にロードされたセキュリティ製品（アンチウイルスソフトウェア、アンチスパイウェア、アンチアドウェア等を含むアンチマルウェアシステムなど）、ファイアウォール製品、どのシグネチャファイルが現在ロードされているかの具体的な設定及び詳細、オペレーティングシステム及び他のソフトウェアのバージョン詳細、並びにどのファイルが動作しているか、または任意の時点での特定のバージョン及びソフトウェア設定等の情報のうちの、一つ又はそれ以上の項目に関する情報であってよい。（当然のことながら、より多くの項目に対して一致しているかを監査及び検査することにより、コンピュータが非常に類似して配置される可能性が増加し、従って、一致検索中における検索漏れ及び誤検出の割合が減少する。）

これらのソフトウェア製品等に関する情報は、コミュニティデータベースに個別に提供されてよい。しかしながら、再度データの記憶量及び送信量の理由から、その情報は、その情報を（例えば、コンピュータ２においてハッシュ又は圧縮関数により）代表するシグネチャ又は鍵として提供されることが好ましい。図４は、ローカルセキュリティ製品、バージョン、シグネチャファイル、ファイアウォール設定等の全ての詳細をどのように用いて、鍵４１を作成するかについて模式的に示す。鍵は、コミュニティデータベース７に送信される。コミュニティデータベース７は、多数の、場合によっては何百万人のユーザのコンピュータ２からこのような情報を供給されているので、対応する情報を、同一又は類似の構成のセキュリティ製品等を有する他のコンピュータ２のために保持することになろう。従って、コミュニティデータベース７は、同一の設定やロードされたシグネチャファイル等を含む同一又は類似の組み合わせのセキュリティ製品を有する他のコンピュータ２を求めてステップ４２で検索できる。

【００９４】

この実施例のコミュニティデータベース７は、エージェントソフトウェアにより、全コンピュータ２により実行された複数のプロセスの詳細を供給されてよく、これにより、一のプロセスが各コンピュータ２により検出されたか否かを知ることになる。

【００９５】

このようにして、コミュニティデータベース７は、例えば、ある時点において存在する設定及びシグネチャファイルを含んだ、オペレーティングシステムと各種セキュリティ製品とのある特異な組み合わせにより、ある特定のコンピュータ２がある特定のマルウェアオブジェクトに感染しやすい又は脆弱なこれらの製品及び設定を有する状態になるかに関する情報を取得するために用いられ得る。

【００９６】

Sophos Ex. 1002
Page 512 of 683

単純な例では、例えばデータベースが、コンピュータが過去に、ダウンロードシグネチャ最新版Ｃを備えたバージョンＡのアンチウイルス製品Ｂを有し、特定の設定Ｅを備えたファイアウォールＤと、またシグネチャ最新版Ｇを備えたアンチスパイウェアソフトウェアＦを有したことを知っているけれども、特定のマルウェアプロセスＰが、その時点でこの組み合わせのプログラムによって検出されなかったことを知らなかった場合、この情報は、そのセキュリティ製品／設定の組み合わせを有することが知られているコンピュータ２に提供することができ、またこれを用いて、コンピュータ２が、その特定のマルウェアプロセスによる攻撃に対して短期的には弱いということを示すことができる。この情報は、ウィンドウ４３をコンピュータ２のスクリーンディスプレイに表示するか、又はユーザに、より詳細にその位置を説明する特定のウェブサイトを案内することによりユーザに提示できる。例えばこれらのセキュリティ製品等の特定の組み合わせは、コンピュータをＳｏｂｉｇウイルスの感染という危険にさらしており、そのウイルスはコンピュータで検出不可能であることをユーザに知らしてよい。ユーザは、具体的な助言（例えば、特定のシグネチャファイルを備えた特定のアンチウイルスプログラムを更新する）、或いはソフトウェアをダウンロード及びインストールしてこの危険性を取り除くように求められてよい。

【0097】

よって、コミュニティデータベース７は、ある特定の時間にある特定のコンピュータ上の全セキュリティ製品等に関する情報を供給された際に、セキュリティ製品の特定の組み合わせと共にコンピュータ上で生じ且つ局所的には検出されなかった「悪質或いは不良」と印付されたプロセスのイベントを求めて検索される。そしてこの情報は、その特定のコンピュータのユーザに、例えば直接又はユーザにウェブサイトを案内することにより、フィードバックできる。この情報は、事実上リアルタイムに供給でき、よって新たなユーザ又は新たなコンピュータはコンピュータの効果的な安全性を非常に迅速に向上させることが可能となる。

【0098】

また好適な方法はどのオブジェクトが相互に関連しあうかを探知し、系図の概念を用いてオブジェクトをマルウェアとして印付できる。例えば、何らかの特定のプロセスは、子プロセスを発生させてよく、故にそれらは関連している。第１のオブジェクトに関連する鍵を検査して、第１のオブジェクトを一意的に識別する要素であって且つ受け継がれる或いは第１のオブジェクトの子孫又は他の関連オブジェクトにおける鍵に存在する要素を、識別してよい。この要素は、ここでは「遺伝子（gene）」と称する。この一般的技術は、多くの方法で用いられてよい。

【0099】

ａ）公知の信頼できる親プロセスは、ローカルコンピュータ上の実行が安全であると自動的に印付される子プロセスを作成する能力を与えられている。この「受け継がれた」特性は、孫プロセス等に伝えられてよい。この安全な状態は、その親の子プロセスに伝えられ、場合によってはこの子プロセスを介して更なる子プロセス（ここでは「子孫（issue）」と称する）、この子孫のシグネチャはすべて自動的にローカルデータベースに良好と記録できる。これにより、コミュニティデータベース７への接続が利用不可能であっても、子孫プロセスは迅速に良好と印付できる。

【0100】

ｂ）親プロセスの活動を監視することにより、親プロセスがマルウェアであると後にわかった場合に、子孫プロセスの全てを自動的にローカルデータベースに不良或いは悪質と記録することができる。

【0101】

ｃ）同様に、この子孫プロセスの活動を監視することにより、もし子孫プロセスのうちの一つがマルウェアであると後にわかった場合に、一以上の親プロセス及び他の子孫プロセスの全て（すなわち、この内容における関連プロセスの全て）を自動的にローカルデータベースに不良或いは悪質と記録することができる。

Sophos Ex. 1002
Page 513 of 683

【0102】
ｄ）親によって行われた、一以上の子に対する能力を含めた一以上の子に対するシグネチャの作成は、親の振る舞い及び決定に応じて、良好か不良かを自動的に印付できる。いくつかの実施例では、その製品は、子プロセスの誕生を「観察」又は監視することができ、到着時に自動的にシグネチャを作成することができる。これは、他の不良プログラムによる一の不良プログラムの作成を監視する能力をもたらす。従って、一のプログラムの家系を監視することができるので、例えば、祖父が一のプログラム（父）を作成し、これが順に一の不良プログラム（息子）を作成する場合には、自動的に父は不良プログラムであると決定できる。
【0103】
ｅ）子が親として既に不良な子孫を生成したので、更なる誕生に対するシグネチャの自動的な作成をトリガーするという子の受け継いだ能力を、自動的に喪失させる特徴が含まれてよい。ルールとして、もしファイルが一の不良な子孫を有する場合には、受け継いだ能力は自動的に削除できることが好ましい。
【0104】
ｆ）クローン又は一卵性双生児のオブジェクト（例えば、コミュニティ内の他のシステム上で実行している同一プロセス）を観察し、それらの子孫のパターンを比較し、ある特定のプロセスをマルウェアとして取り扱うか否かに関する決定を行う能力。
【0105】
これらの特徴ａ）からｆ）のうちの一以上を用いて、しばしば非実践なインターネットへの永久接続に必ずしも１００％依存することなく効率的に用いることができる、セキュリティ製品を製造する問題に対する解決策を提供することができる。この例は、ワールドワイドウェブ中に自動的に製品最新版を展開可能にしたいと望む生産業者によってますます用いられているWindows Update及び他のプロセスである。
【0106】
伝統的なソフトウェアに比べての、これらのタイプの特徴において考えられる利益は、以下の通りである。アンチウイルスソフトウェアは、公知の不良シグネチャのキャッシュを有する傾向がある。問題であるのは、これを常に最新の状態にしておくことである。誰かが新しいコンピュータを購入するという簡単な例をあげてみよう。コンピュータには、シグネチャキャッシュとともに予めロードされたアンチウイルス製品がついてくる。ＰＣが構築され、店頭に出荷され、ユーザによって購入される間に、数日又は数週間経過するであろう。ユーザはＰＣを起動し、ＰＣが構築された後に生成された任意の新たなウイルス又はマルウェアにさらす。完全な保護のためには、ユーザがインターネットに接続し、最新版をダウンロードすることが求められる。これは、インターネット上のユーザによる他の活動の先に起こることを保障できない（保障することは物理的にはほぼ不可能である）。公知の良好プロセスのローカルキャッシュとともに、本発明の実施例と同様に、コンピュータ製造者によって予めロードされた全ての良好（欠点のない（clean））なソフトウェアに対する予め生成されたシグネチャのキャッシュを予めロードしたコンピュータ／ターミナルを出荷できる。この場合、ユーザは、任意の新たな又は最新のプログラムがすぐに検出及び照合されることを知りつつ、インターネットに接続できる。また、いかなる自動更新されるソフトウエアも、シグネチャが強制的に、その子供や更に遠縁の子孫（即ち、孫、ひ孫など）のために自動的に構築されるように機能し得る。
【0107】
ここで、「Virus Bulletin Conference October 2005」に発表されたマイクロソフト会社のAdrian Stepanによる「Defeating Polymorphism: Beyond Emulation」と、2006年4月５日に出願されたUS 60/789156とを参照する。これらの全内容は、参照文献として組み込まれる。その論文及び特許出願では、ファイルを解析して当該ファイルが実際にマルウェアであるか否かを決定することができるように、ファイルを復号する方法が開示されている。US 60/789156は特に、ホストコンピュータを用いて実行可能コンピュータファイルを解凍／復号する方法であって、前記実行可能コンピュータファイルを複数の基本コード

ブロックに分割する工程と、前記基本コードブロックのうちの少なくともいくつかを前記ホストコンピュータによって実行可能である翻訳基本コードブロックに翻訳する工程と、前記基本コードブロックのうちの少なくともいくつかを前記ホストコンピュータのメモリにリンクさせる工程と、前記ホストコンピュータ上の前記基本コードブロックのうちの少なくともいくつかを、前記実行可能コンピュータファイルが解凍又は復号できるように実行する工程とを備え、前記解凍又は復号された実行可能コンピュータファイルを解析して、前記実行可能コンピュータファイルがマルウェアとして分類される又はされるべきであるかについて決定できる解凍／復号方法を開示する。また、US 60/789156は、実行可能コンピュータファイルを解凍／復号する方法であって、前記実行可能コンピュータファイルを複数の基本コードブロックに分割する工程と、前記複数の基本ブロックのうちの少なくともいくつかに対して、各基本ブロックの読取及びキャッシュされた仮想メモリアドレスに対応する読取及びキャッシュされたリアルアドレスを記憶するキャッシュメモリの少なくとも一の読取ページを作成し、且つ前記複数の基本ブロックのうちの少なくともいくつかに対して、各基本ブロックの書込み及びキャッシュされた仮想メモリアドレスに対応する書込み及びキャッシュされたリアルアドレスを記憶するキャッシュメモリの少なくとも一の書込みページを作成する工程と、前記基本コードブロックのうちの少なくともいくつかを前記実行可能コンピュータファイルが解凍又は復号できるように実行することにより前記実行可能ファイルをエミュレートする工程とを備え、前記解凍又は復号された実行可能コンピュータファイルを解析して、前記実行可能コンピュータファイルがマルウェアとして分類される又はされるべきであるかについて決定でき、一の基本ブロックの実行中に、前記キャッシュメモリの読取ページおよび書込みページのうちの少なくとも一つは、前記基本ブロックにアクセスしている前記仮想アドレスに対応するキャッシュされたリアルアドレスの検査を受ける、解凍／復号方法を開示する。

【0108】

これらの文献に開示された技術は、詳細なファイルの解析が望まれる際に本内容において用いることができる。しかしながら、より一般的には、これらの文献で開示された技術、特にUS 60/789156に開示された改良技術を用いて、コンピュータ上で実行される際のファイルの活動に関する情報を提供できる。なぜなら、これらの文献で開示された技術によりファイルの実行がエミュレートされ、これによりファイルの活動を解釈できるからである。

【0109】

ユーザがオフライン時にソフトウェアのインストールを望む際に、更なる状況が生じる。好適な実施例では、ユーザが新たなソフトウェアをオフラインでインストールしようとする際に、ユーザのコンピュータ２で実行中のエージェントソフトウェアは、インストールの実行自体がユーザによって「認証」されるようにインストールプロセスを進めるために、ユーザに認証を促す。このユーザによる認証は、「起源（Genesis）」イベントとして取り扱われる。以下そのように称する。しかしながら、インストール装置上の他の既存プログラムとやりとりするソフトウェアのインストール時に、共通に用いられるプロセスがある。例えば、マイクロソフトのMSIEXECである。

【0110】

起源手法は、ユーザのコンピュータ２のユーザ認証の結果として、シグネチャを生成するプロセスを含む。これらのシグネチャは、ユーザのコンピュータ２のローカルデータベースに記憶される。一の実施例では、これらの局所的に記憶されたシグネチャは、インストールを進めるように、必要に応じてインストールプロセス中にエージェントソフトウェアによって参照される、或いは、エージェントソフトウェアによって行われたセキュリティチェックをインストールプロセス中にＯＦＦすることができる。このＯＦＦは、制限された期間にのみ行われ、例えば大抵のソフトウェアをインストールするには十分である数分間等であり、このＯＦＦ時間は、随意にユーザの設定で変更可能である。

【0111】

いずれにしても、一旦インストールが完了し、ユーザのコンピュータ２がコミュニティ

Sophos Ex. 1002
Page 515 of 683

データベース７に接続されると、ユーザのコンピュータ２上のエージェントソフトウェアは、インストールに関連するシグネチャをユーザのローカルデータベースからコミュニティデータベース７にアップロードできる。そして、他のユーザのコンピュータ２からの対応データとともに、コミュニティデータベース７を用いて、この特定のソフトウェアのインストールが両性であるという迅速な決定を行うことができる。

【0112】

この実施例の変形として、ユーザのコンピュータ２がある時点でオンラインである場合に、ユーザのコンピュータ２上のエージェントソフトウェアは、いわゆる「信頼できるインストーラ」又は「ライセンスインストーラ」のシグネチャをダウンロードしてよい。これにより、「ライセンスインストーラ」及び当該ライセンスインストーラの任意の子プロセスが、起源イベントが「現在」である間、例えばユーザからの認証の後数分の間に、実行の許可を受ける方法を動作できる。ライセンスインストーラのシグネチャは、コミュニティデータベース７に付与されるにつれて及び付与される際に、オンラインでリモートコンピュータ２に常にダウンロードされることが好ましい。

【0113】

この方法に対して、起源イベントの最中にメディアの変化が起きた場合にはライセンスインストーラを実行させることを防止するような、更なる改良があってよい。しかしながら、マルウェアであるかもしれない任意の未知のプロセスは、さらに検出及び遮断されてよい。少数のライセンスインストーラを備えることにより、最小データが必要とされるので、特にウイルスシグネチャファイルのダウンロードと比較すると、ダウンロードが容易になる。別の例として、例えば「Windows Update」等の非常に信頼されるインストーラを採用して、その非常に信頼されるインストーラによって作成された新しいプロセスの全てを、迅速に安全であると特徴づけてもよい。

【0114】

リモートコンピュータ２をコミュニティデータベース７に接続させる際に起きるインストールの場合、別の選択肢として、インストールをしようとしているソフトウェアがコミュニティデータベース７に知られていない場合に、システムがそのインストールを遮断又はユーザに警告することがあげられる。例えば、「ソフトウェアをインストールしようとしています。このソフトウェアは「コミュニティ」に知られていません。次に進みますか？」という程度のメッセージが、ユーザのコンピュータ２に表示されてよい。

【0115】

本発明の実施例は、特に説明した例を参照して記述した。しかし当然のことながら、上述の例は、本発明の範囲内で変形及び変更されてよい。

【図面の簡単な説明】

【0116】

【図１】本発明の実施例が実行される装置を模式的に示す図である。

【図２】本発明の実施例に係る方法における一例の動作を模式的に示すフローチャートである。

【図３】本発明の実施例に係る方法における他の例の動作を模式的に示すフローチャートである。

【図４】情報取得段階を模式的に示すフローチャートである。

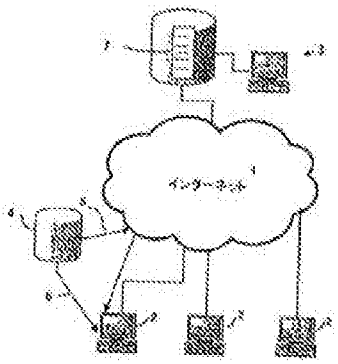
【符号の説明】

【0117】

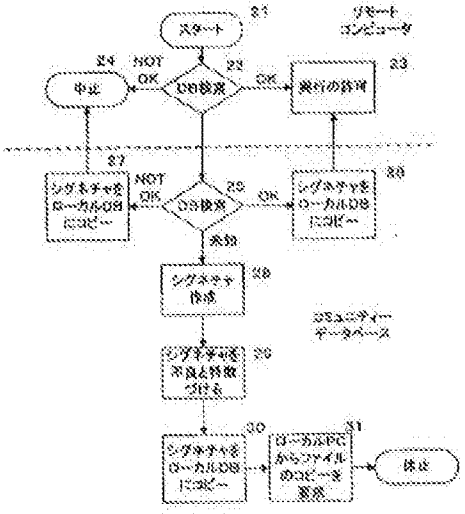
１　インターネット
２　リモートコンピュータ
３　ベースコンピュータ
４　オブジェクト
５　ライン
６　ライン
７　コミュニティデータベース

Sophos Ex. 1002
Page 516 of 683

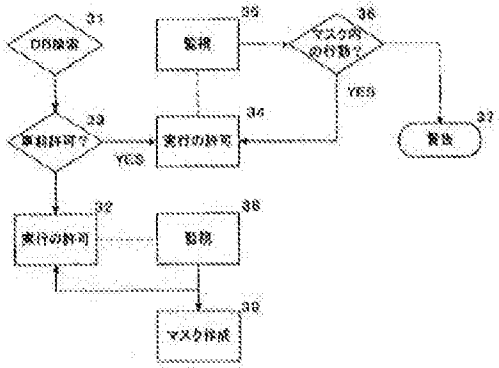
【図１】


インターネット

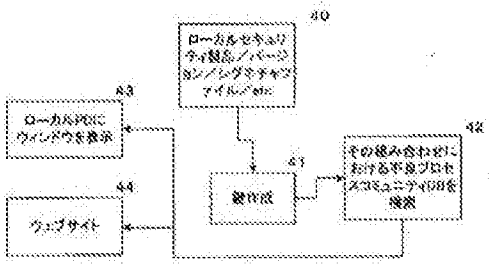
【図２】


スタート
リモートコンピュータ
中止
NOT OK
DB検索
OK
実行の許可
シグネチャをローカルDBにコピー
シグネチャ待ち
セキュリティーデータベース
ローカルPCからファイルのコピー要求
終了

【図３】


DB検索
監視
マスク例の作製
YES
実行の許可
終了
マスク作成

【図４】


ローカルセキュリティ製品／パーソナルファイアウォール等
ローカルPCにウィンドウを表示
実行部
その組み合わせにおける不足コンポーネントDBを検索
ウェブサイト

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2006/002439

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 549 012 A (DATACENTERTECHNOLOGIES N.V) 29 June 2005 (2005-06-29) cited in the application page 2, paragraphs 6,7 page 3, paragraphs 17,18 page 6, paragraph 48 - paragraph 49 page 8, paragraph 58 - paragraph 61 page 10, paragraph 68 - paragraph 72	1-13, 13-23, 25-38, 37,39,40
Y		12,24, 38,41
X	US 2004/153644 A1 (MCCORKENDALE BRUCE ET AL) 5 August 2004 (2004-08-05) cited in the application page 2, paragraphs 21,25 page 4, paragraph 43 - page 5, paragraph 53	1-11, 13-23, 25-38, 37,39,40

-/--

[X] Further documents are listed in the continuation of Box C.　　[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 October 2006	15/01/2007
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Arbutina, Ljiljana

Form PCT/ISA/210 (second sheet) (April 2005)

Sophos Ex. 1002
Page 518 of 683

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2005/002439

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 315 066 A (BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY) 28 May 2003 (2003-05-28) page 3, paragraph 8 page 6, paragraph 36 - page 7, paragraph 48 abstract	1,13,25, 30,37, 39,40
X	US 2004/039921 A1 (CHUANG SHYNE-SONG) 26 February 2004 (2004-02-26) cited in the application page 2, paragraph 33 - page 4, paragraph 51	1,13,25, 30,37, 39,40
Y	US 2005/086508 A1 (ALBORNOZ JORDI A) 21 April 2005 (2005-04-21) page 1, paragraph 8	12,24, 38,41
A	ZENKIN D: "Fighting Against the Invisible Enemy - Methods for detecting an unknown virus" COMPUTERS & SECURITY, ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, NL, vol. 20, no. 4, 31 July 2001 (2001-07-31), pages 316-321, XP004254268 ISSN: 0167-4048	

3

Sophos Ex. 1002
Page 519 of 683

INTERNATIONAL SEARCH REPORT

International application No.
PCT/GB2006/002439

Box II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-30, 37-41

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

Form PCT/ISA/210 (continuation of first sheet (2)) (January 2004)

International Application No. PCT/GB2006/002439

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-30,37-41

Method and apparatus for classifying a computer object as malware

---

2. claims: 31-36

Method and apparatus for determining the protection that a remote computer has from a malware

---

3. claims: 42-47

Method of installing a software on a computer

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/GB2006/002439

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1549012 A	29-06-2005	NONE	
US 2004153644 A1	05-08-2004	NONE	
EP 1315068 A	28-05-2003	CA 2467186 A1 WO 03046699 A1 US 2005022014 A1	05-06-2003 05-06-2003 27-01-2005
US 2004039921 A1	26-02-2004	AU 9620501 A WO 0233525 A2	29-04-2002 25-04-2002
US 2005086500 A1	21-04-2005	NONE	

(81)指定国　　AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IS,IT,LT,LU,LV,MC,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LV,LY,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）
１．フロッピー
２．ＷＩＮＤＯＷＳ

(72)発明者　モリス，メルヴィン
イギリス国，ディーイー５６　２エルユー　ダービーシャー，ターンディッチ，インテイク　レイン，レッドマイヤー　ギャップ（番地なし）
(72)発明者　スタッブス，ポール
イギリス国，エムケー４４　３エイエックス　ベッドフォードシャー，ウィボストン，ルカリー　ロード　７
(72)発明者　ハートウィグ，マーカス
イギリス国，エムケー９　２イーエイ　バッキンガムシャー，ミルトン　ケインズ，ミッドサマー　ブールヴァード　４９４，イクスチェンジ　ハウス
(72)発明者　ハーター，ダレン
イギリス国，ジーエル４　３ジェイゼット　グロスターシャー，グロスター，ハックルコウト，バーンウッド　ロード　１７８
Ｆターム(参考) 5B276 FD08

【要約の続き】
を含むイベントのうちの一以上を含む。

Sophos Ex. 1002
Page 523 of 683

Patent Translate
Powered by EPO and Google

Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

DESCRIPTION JP4936294

Method and apparatus for dealing with malware

[0001]

[0001] The present invention relates generally to a method and apparatus for dealing with malware. In one aspect, the present invention relates to a method and apparatus for classifying a computer object as malware. In another aspect, the present invention relates to a method and apparatus for determining the protection that a remote computer from malware. In another aspect, the present invention relates to a method and apparatus for classifying a computer object as malware or safety. In another aspect, the present invention relates to a method for installing software on the computer.

[0002]

[0002] The term "malware" is used herein includes a certain or malicious code with malicious code is used to refer to "objects" are typically from a computer file or any executable generally . Malware is, therefore, including viruses, Trojan horses (Trojan), worms, spyware, adware, etc.,

[0003]

[0003] Exemplary anti-malware products anti-virus scanning software, etc., a plurality of objects, or the object or by scanning a plurality of results of the applied algorithms in a part thereof, may indicate the presence of a virus known is looking for signatures (signature) of the object is. General methods for dealing with malware, the when released new malware for example through the Internet, which are all detected. When new malware is detected once, the service provider in this field is to create a signature that aims to address these, then these signatures, public or release in a manner that updates the anti-malware programs (release) is being. Heuristic methods have also been employed.

[0004]

[0004] These systems are highly effective in protecting against known malicious objects. However, these systems rely on the creation and / or updated signature files. Therefore, a new malware that are emerging or public, between the signature supplied against that the malware is created or updated to the user, is inevitably a delay occurs. Therefore, the user may also be a one week or more, a certain period of time, are at risk from a new malware. In addition, in order to overcome the anti-virus product, malware writers, using the obfuscation (Obfuscation) technology, to try to hide the signature basic data or the signature of the virus code from detection. Typically, obfuscation includes encrypting or packing the code for the virus.

[0005]

[0005] WO-A-2004/097602 analyzes the computer files received or created by the local computer, these are compared to a database of known files, a particular file determines either known If so, it describes a system for determining whether a particular file is known sufficiently long regarded as "safe". However, in practice, it is intact it is unlikely to provide adequate protection. This is because, for example, a virus or Trojan horse of active payload (ie, data of the body) is, to a certain date and time, or when you receive a message or instructions from the local or remote system or process, or when the process first when certain events of many months or years later from being executed or published is performed, since only be programmed to activate. Therefore, the simply looking at file age, it is not sufficient to determine whether it can remain safe and and safe.

Sophos Ex. 1002
Page 525 of 683

[0006]

[0006] In the system of WO-A-2004/0083408, by examining the connection attempts made by a particular file that is run on a computer, detects a worm in the file.

[0007]

[0007] US-A-6944772, US-A-6772346, EP-A-1549012, and all EP-A-1280040, the network all of the plurality of "local" computer (for example, be a LAN or the Internet) discloses a "community-based (community-based)" anti-malware system connected to a central computer via a. If you are experiencing those files that are not known to the local computer, their local computer sends a request for execution permissions of that file to a central computer. If the file is recognized in the central computer, the central computer, if the file is known to be safe, it transmits a permission to the local computer to execute the file. Alternatively, if the file is known to be malicious, it can send a "denial" instruction. However, in the proposals in these prior art, if the file is not known at the central computer, all files are sent to the central computer where it is analyzed to determine what should be regarded as malware should be regarded as safe that. Such analysis is, by applying a file to detailed analysis, typically manually, or "semi-manual" is executed. Detailed analysis, for example emulation or decryption, given the involvement of the person that is normally required, can take many days. Therefore, by the time to classify a new file as a safety or malware, it takes a considerable period of time. In the system in these prior art, it requests for files executable permissions to be sent to the central computer by the local computer may include a transmission of the file specifically expressed "key" or "signature" or checksum.

[0008]

[0008] Similar community-based anti-malware system is disclosed in WO-A-02/33525. In this system, if it is safe or malware local computer to run the file that is not known to the central computer is seeking permission, it has been some sort of limitation on the dissemination of the files on other local computer audit information, can be transmitted to the human system administrator associated with the local computer seeking permission to run the file. Therefore, the human system administrator, whether or not the file can be safely executed, but it is a decision by the "manual", can be determined upon obtaining sufficient information.

[0009]

Sophos Ex. 1002
Page 526 of 683

[0009] In the system of US-A-2004/0073810, a metafile containing data about the attachments or other transmission file is transmitted to the central computer. It analyzes data about the file, determining the likelihood transmission file is malware. Examples are given that are treated as malware if the transmission file is transmitted over a certain number of servers at least some.

[0010]

[0010] US-A-2005/0021994 and in US-A-2004/0153644 to the disclosed system, have been certified as safe by the software vendor that is associated, for example, files, pre-approved files, further inspection always it may have been allowed to run without. In one embodiment of the system in the US-A-2004/0153644, to perform monitoring (monitoring), an unusually large number of requests by the file is received in the central management section in a certain period of time from a number of local computer, or many requests abnormality by the file on a single computer, when it is received at the central control unit a period of time from the single computer, the file is determined to be malicious.

[0011]

[0011] in the system in the US-A-2004/0006704 is, and software version that is installed on a computer equipped with the software version of the database and their known vulnerabilities are compared. Thus, the user's computer, by installing a new software or to update existing software, it is possible to know how to minimize the specific risks and their risks.

[0012]

[0012] In the system of WO-A-03/021402, a central database maintains a virtual image of all the files stored in each of the plurality of local computers. When the threat in one of the local computer is identified, other local computer with a similar configuration are informed about the risk.

[0013]

Sophos Ex. 1002
Page 527 of 683

[0013] WO-A-2004/097602 WO-A-2004/0083408 US-A-6944772 US-A-6772346 EP-A-1549012 EP-A-1280040 WO-A-02/33525 US-A-2004 / 0073810 US-A-2005/0021994 US-A-2004/0153644 US-A-2004/0006704 WO-A-03/021402

[0014]

[0014] Thus the prior art systems, because the new object to determine whether malicious, is dependent on in-depth analysis of the object. This causes a delay, as a result, during the period until the file is parsed, a new anti-malware signatures are distributed, causing a risk to the user. Alternatively, prior art systems rely on limited analysis of the operation of a particular object. Alternatively, the transmission method to a computer in the prior art systems, is performed to determine the likelihood the object is malicious.

[0015]

According to a first aspect of the [0015] present invention, one of the computer object to a method of classifying as malware, the base computer, from each of the plurality of remote computers to store the objects or similar plurality of objects a step of receiving data about the computer object, the data about the computer object received from said plurality of computers, the steps of comparing in the base computer, and a step of classifying as malware the computer object based on the comparison classification method with a is provided.

[0016]

[0016] If simply compared with the prior art that rely on signature matching, this embodiment performs a comparison between the effects on the plurality of objects and / or remote computers having different them a particular object is classified as good or malware It can determine whether or not to. It is possible to perform sophisticated pattern analysis. Thus, without a detailed analysis of the object itself, such as to determine whether a malware, it is quick decision about the nature of the object. Also, like the anti-virus software in the prior art, the need to generate a new signature to be used for signature matching is avoided.

[0017]

Sophos Ex. 1002
Page 528 of 683

[0017] In a preferred embodiment constructed, transmitted from the plurality of remote computers to the base computer, and the data about the computer object that is used in the comparison, or by the objects included in said object multiple and executable instructions, and the size of the object, and the current name of the object, and the physical and folder location on the disk of the object, and the original name of the object, create and change the date and time of the object If, skilled stored in the object, executes product, version, and other information, the header held by the object header or the remote computer, the objects on the respective remote computers, constituting or including and events, including that have been or the object initiated by the object when you create, one or more of the.

[0018]

[0018] Preferably, the said comparison, the relationship between the object and several other objects are identified. In one example, if this object or a parent or other related object is bad (or good), and it used to quickly and automatically, bad child objects (or good) and with a sign (ie, mark or marking) can be. Therefore, at least one other object said object is associated is, if it is classified as malware, classifying the object as malware. It said other of the plurality of objects include at least the object or similar plurality of objects stored in some of the plurality of remote computers. It said other of the plurality of objects includes a plurality of other objects is a process-related object parent or child object, or with respect to said object.

[0019]

[0019] In a most preferred embodiment, the data is transmitted in the form of a key that is acquired by a plurality of executed hashing process for objects on the respective remote computers. The main advantage of using such a key is to keep down the amount of data that needs to be transmitted to the base computer. Thousands or millions there is also the remote computer connection, even if you may send the details of each of a very large number of objects, this can be an important advantage.

[0020]

[0020] The key has at least one of the elements representing the executable instructions

Sophos Ex. 1002
Page 529 of 683

configured by or said object included in the object. This important and preferred feature, only can be compared for the executable instructions of the object at the base computer. This, for example, the indicator of that in most cases the object is malware, objects fundamentally different names have the same executable instructions, nevertheless it can be regarded as the "same" object for this purpose It means. As another example, which is slightly revised compared with previously known prior versions based computer, and, at least substantially, in terms of executable instructions, a new version that can be considered the same as the previous version the program may be published. In this case, negligible slight differences, are considered the object are the same. This is because the malware, not only for example be useful in distinguishing the modified version of the previous software, request for data transmission and storage is kept low. Because the base computer, the remote computer apparently new object can notify to be the same as the object previously known for this purpose, therefore, the remote computer details and object itself object based computer This is because it is possible to avoid sending.

[0021]

[0021] The key has at least one of the elements representing the data related to the object. The data relating to the object, and the current name of the object, and the physical and folder position on the disk of the object, and the original name of the object, and create and modify date and time of the object, to the object stored skilled in the art, the product, version, and other information and, the object at the time said the header, which is held by the object header or the remote computer, you run the object on each of the remote computer, to be or create configuration it may include an event containing initiated or said object, at least one of the.

[0022]

[0022] The key preferably has at least one of the elements representing the physical size of the object.

[0023]

[0023] When these elements are present more than one in this key, it is preferable that the plurality of elements are separable.

Sophos Ex. 1002
Page 530 of 683

[0024]

[0024] First a step of classifying an object as a non-malware, generating a mask for said object that defines the acceptable behavior for the object, the operation of said object on at least one of said remote computer a step of monitoring, actually monitored the behavior may comprise the step of classifying said object as malware in the case of deviation those permitted by the mask. As a result, efficient and effective method for monitoring the behavior of the good as classified or considered the primary object is provided. In the case where the reason for that the behavior of this object is malware can reclassify the object as quickly malware.

[0025]

According to a second aspect of the [0025] present invention relates to a computer object for one of the computer object to a device for classifying as malware, from each of the plurality of remote computers to store the objects or similar plurality of objects comprise one of a base computer constructed and arranged to receive the data, said base computer, said data about the computer object received from said plurality of computers are configured and arranged to compare, the base computer It is constructed and arranged to be classified equipment to classify the computer object as malware on the basis of the comparison is provided.

[0026]

According to a third aspect of the [0026] present invention, on one of the base computer the data relating to one of the computer object from a remote computer, compared with similar data received from other of the plurality of remote computers in the base computer a method of providing to allow, comprising the step of providing data related to one of the computer object that is stored in the remote computer from a remote computer to one of the base computer, said data are included in said object or a plurality of executable instructions constructed by the objects, the size of the object, the current name of the object, and the physical and folder location on the disk of said object, and original name of the object, creating a creation and modification time of the object, skilled stored in the object, product, version, and other information, the header held by the object header or the remote computer, and the object, constitution, or comprise one or more of the events, including by or said object initiated by the object when running on each of the remote computer, the data isThe provided method is transmitted in the form of the acquired key by object hashing processes run on on the remote computer is provided.

Sophos Ex. 1002
Page 531 of 683

[0027]

[0027] According to this method, which is performed by a so-called agent software running on the remote computer, enables efficient data transmission to the base computer, request for data transmission and storage is minimized, and in the base computer it is possible to perform a quick analysis.

[0028]

[0028] The key preferably has at least one of the elements representing the executable instructions configured by or said objects included in the object.

[0029]

[0029] The key preferably has at least one of the elements representing the data related to the object. The data relating to the object, and the current name of the object, and the physical and folder position on the disk of the object, and the original name of the object, and create and modify date and time of the object, to the object stored skilled in the product, version, and other information, the header held by the object header or the remote computer, and executing the object on each of the remote computer, upon which or created configuration and events, including that have been or said object initiated by the object may include at least one of.

[0030]

[0030] The key preferably has at least one of the elements representing the physical size of the object.

[0031]

According to a fourth aspect of the [0031] present invention, there is provided a method of determining a protection from malware included in the one remote computer, operating in time

Sophos Ex. 1002
Page 532 of 683

in one of the base computer is on the remote computer Yes comprising: receiving details of all or selected products of the security products, comprising: receiving similar information from other of the plurality of remote computers connected to the base computer, the security product specific combination a step of identifying any malware processes that were not identified by said other plurality of remote computers, determining method comprising is provided that.

[0032]

[0032] In this way, the base computer, for example, by a particular unique combination between the set and the operating system and a variety of security products that includes the signature file exists at a certain point in time, to a specific malware objects that there is a specific computer to obtain a susceptible or vulnerable information regarding a state having these products and settings can be used. The user can appropriately advice received, for example, proposals are subjected to improve this situation.

[0033]

[0033] Accordingly, the one remote computer may comprise the step of providing the information that malware process has sensitive possibility of attack by based on the identified user of said one remote computer.

[0034]

[0034] The details of all or selected security products, the name of the security products, and version, it is preferred to include a signature file that is loaded.

[0035]

According to a fifth aspect of the [0035] present invention, there is provided an apparatus for determining the protection from malware included in the one remote computer, all of the security products operating at a on the remote computer or comprise one of a base computer constructed and arranged to receive details of the selected product, the base computer to receive similar information from other of the plurality of remote computers connected to the base

Sophos Ex. 1002
Page 533 of 683

computer is configured and arranged to, said base computer, certain combinations any determination device that is configured and arranged to identify malware processes that were not identified by security products said other plurality of remote computers having a There is provided.

[0036]

According to a sixth aspect of the [0036] present invention, the one of the computer object is or a related object or is a descendant of the first computer object, there is provided a method of classifying as malware or safety, the first computer a step of classifying the object as malware or safety, whether or presence inherited in the key of the first of a one of the elements that uniquely identifies the computer object of the first computer object descendants or other associated computer object the one element that includes the steps of identifying the key associated with the first computer object, based on the unique identifier elements present in the key of said computer object, the computer object as malware or safety optionally classification method and a step of classification is provided.

[0037]

[0037] This aspect can be with a sign (ie, mark or marking) the object by using the concept of genealogy as malware. For example, a particular process may generate a child process, thus being related. Check the key associated with the first object, the elements present in the key of the first object are inherited and a uniquely identifying element or the first object progeny or other related objects , it may be identified.

[0038]

[0038] The method includes the steps of monitoring the activities of said first computer object, when the first computer object is determined to be subsequently malware is first classified as a safety, the first computer comprising a step of reclassifying the object as malware, and further, any computer object with a key to the unique identifier element is present, may comprise a step of automatically classifying as malware.

[0039]

Sophos Ex. 1002
Page 534 of 683

According to a seventh aspect of the [0039] present invention, the one of the computer object is or a related object or is a descendant of the first computer object, an apparatus for classifying as malware or safety, the first computer They comprise one of a computer that is configured and arranged to classify the object as malware or safety, the computer, the first offspring of the computer objects merely an element that uniquely identifies the first computer object or other of the said one element that either or exist inherited in the key of the associated computer object, the constructed and arranged to identify in the relevant key to the first computer object, the computer, the key of the computer object based on the unique identifier element present, the computer object, if classification device is constructed and arranged to classify as malware or safety by, is provided.

[0040]

According to an eighth aspect of the [0040] present invention, there is provided a method of installing software on one computer, during a software installation start of the one of the computer to see if the user has authenticated the installation the computer-generated prompt on the computer, the steps of providing to said user, receiving a step to stop the installation when the user authentication is not received, in addition, in the computer, the user authentication to proceed with the installation a step of a step of advancing the said installation, a step of acquiring data about the plurality of computers objects created or used during the installation, the installation method includes the step, the storing the data to the local computer It is provided.

[0041]

[0041] This user has not installed the new software, for example to provide a safety when not connected to a base computer having the above-mentioned type of community database. In this case, the method to be executed by agent software running on the local computer, the user data (e.g., process, new files, etc.) related to objects created during the installation of the installation while collecting simultaneously You can proceed to become.

[0042]

Sophos Ex. 1002
Page 535 of 683

[0042] The data that is locally stored, the referenced during installation to ensure that all objects created or used during the installation are part of the installation process, during the installation If all objects created or used is not part of the installation process, the step (i) to abort the installation, and (ii) providing appropriately said user computer-generated prompt on the computer of which preferably comprises at least one. As a result, it allows the creation or use only objects that installation has been requested, thus (malware, under conditions that often create an object that is not expected to be a part of the normal installation of the new software) unconsciously it is ensured in this way that the order not to install malware.

[0043]

[0043] In a preferred embodiment, the step of connecting the computer to a community database that is connectable to multiple computers, the stored data, for comparison with similar data provided by other computers and a step to be uploaded to the community database.

[0044]

[0044] This method comprises the step of downloading the data relating to a plurality of reliable installer to the computer, the data is related to a plurality of reliable installer, it was created by the related to the reliable installer or the reliable installer as proceed automatically authenticate any object, it may be referred to during the installation. Consequently, a priori installation of reliable and known software is easy.

[0045]

[0045] said data relating to a plurality of reliable installer, said may be referred to only a predetermined period of time following the receipt of user authentication to proceed with the installation in the computer.

[0046]

[0046] The present invention also includes a computer program comprising program instructions for executing any one of the above methods on a computer.

Sophos Ex. 1002
Page 536 of 683

[0047]

Examples of the present invention described with reference to the [0047] drawings, a computer process to be executed in a computer device, including a computer device itself, the present invention extends to a computer program. In particular, a computer pro ram in on or carrier carrier suitable for practicing the present invention. The program source code, object code, a code intermediate source, and may be object code in the form of partial compilation type. Alternatively, it may be suitable for other forms in the practice of the process according to the present invention. The carrier may be any entity or device capable of transmitting programs. For example, the carrier may, for example, CD-ROM or a semiconductor ROM or the like of the ROM, or for example may comprise a storage medium such as a magnetic recording medium such as a floppy disk or a hard disk. Further carriers via electrical or optical cable, or wireless, such as communications or other electrical or optical signal transmitted by the means may be a transmittable carrier.

[0048]

[0048] with reference to the accompanying drawings, an embodiment of the present invention as an example.

[0049]

Referring to [0049] FIG. 1, a computer network is generally indicated as being based on a kind of a distributed network such as the Internet 1. However, the present invention uses other types of network such as a LAN, or may be performed in the entire region. A plurality of local or "remote" computer 2 is connected via the Internet 1 to the "central" or "base" computer 3. Computer 2, respectively variously, computer, any type of server, PDA, mobile phone, may be an interactive television, or other device that takes in operating a computer object. Object in this sense, computer files, part or sub-program of the file, macro, or a web page or other code is operated by or on a computer a computer, or other run, emulate, simulation, or was interpreted it may be an event. The object 4 is schematically shown, for example, may be downloaded to the remote computer 2 via the Internet 1 as shown by line 5, or may be directly applied as indicated by line 6.

Sophos Ex. 1002
Page 537 of 683

[0050]

[0050] In one preferred embodiment, the base computer 3 maintains a database 7. When the remote computer 2 to determine whether to perform object 4 object 4 is safe, remote computer 2 acts as the database 7. Community database 7, the information associated with each object that is executed on all the remote computers 2 connected, Yuku padded with time. As further described below, representative data of each object 4 preferably takes the form of an object, and so-called signature associated with the effect (signature) or key (key). As described further below, the database 7 may further include a mask for the object 4 to set the parameters of performance and behavior of the object.

[0051]

[0051] Referring now to FIG. 2, at the start point 21, to run the computer object 4, such as the one process in the remote computer 2. In step 22, the operation of the local "agent" software running on the remote computer 2, the process operation is hooked, by searching a locus database agent software is stored on the remote computer 2, certain of the process, can find the signature or key representative of the associated objects, and / or events. If, when the local signature is present, it indicates that the considered and the process is either indicate that are considered safe, or unsafe. The dangerous process, It might be a process was discovered to be a malware, that resulted from the execution, might be dangerous or malicious results process was discovered that did not know that or predicted. If the signature is the case shown and the process is safe, the process or the event is permitted by the local agent software on the remote computer 2 to be executed in step 23. If signature, indicating its process is not safe, the process or event is stopped in step 24.

[0052]

[0052] Of course, may be present more than two states of the "safe" or "unsafe", selection may be provided to the user. For example, if one object is considered not to be locally safe, it may be given an option the user can perform related processes nevertheless. It may be given a plurality of different states for each remote computer 2. This condition, position of the time frame or remote computer, consider state, or ownership, by the central system, can be changed.

Sophos Ex. 1002
Page 538 of 683

[0053]

[0053] If the object is not known locally, details of the object, through the Internet 1 or other network, for storing in the community database 7, and preferably a further at the base computer 3 analyzing It is sent to the base computer 3 to perform. In this case, then the community database 7, at step 25, is searched for the signature of the object in the community database 7 is already stored. The community database 7, the signature representing the object, such as a program or process is executed by the remote computer 2 which are respectively monitored is supplied. In a typical practice in the field, the remote computer 2 of the connection or connections can be thousands or even millions based computer 3 may be present. Therefore, the newly exposed to the Internet 1, or otherwise any objects found in any of these remote computer 2, it is found soon. Further signatures are created, it will be transmitted to the base computer 3 by the remote computer 2 of each.

[0054]

[0054] community database 7, when it is searched for the signature of the object that was not known in advance at the remote computer 2 is involved, referred to as the signature is found, and signature object is safe case, the signature copy of, or at least the object is a message that is safe, is sent to the local database of the remote computer 2 that are involved in step 26, is stored in the local database. In this way, the remote computer 2, this information, Giving immediately to the next opportunity to meet the object 4. Another messages, in order to execute the object in the current instance is returned to the remote computer 2.

[0055]

[0055] is if discovered signatures in the community database 7, if this is shown with some reason the object is not safe, the signature is returned to the local database is copied again, as "unsafe" in step 27, with mark (In other words, mark or marking) to be. And / or, a message is sent to the remote computer 2, (can not be or run) execution of the object is canceled. And about whether or not to execute the object to / or user, choices of consent did on (informed choice) is given.

[0056]

Sophos Ex. 1002
Page 539 of 683

[0056] If, in the case where after searching the entire community database 7 is also the object is not yet known, this object is, that in this field is a completely new object that has never been seen until now is assumed. Thus, the signature in step 28, is created to represent the object. Alternatively, the signature transmitted by the remote computer 2 is used for this purpose, the signature is bad in step 29, or the community database 7 as unsafe, first, subjected indicia. Its signature is copied to the local database of the remote computer 2 that performed the first object in step 30. Then, a message is sent to the remote computer 2, it may be commanded to not perform the object to remote computers 2. Alternatively, the informed consent about whether or not the object is feasible, may be provided to the user. In addition, in step 31, it may be requested by the community database 7 a copy of the object itself from the remote computer 2.

[0057]

[0057] If a user at the remote computer 2, because they are too new to run the process, which is considered to be unsafe, and if you choose, the process may be monitored by the remote computer 2 and / or the community database 7. Also, for example, in the case that is not also also does not occur or indicated what adverse effects in the after n days, may be considered to be safe. Alternatively, the community database 7 may retain a respective instance of the process that is determined by a number of remote computers 2 that forms part of a network log (record). Instances of a particular number is recorded, to after the other specific number of instances or process is allowed to run safely executed, the signature in the community database 7 is marked indicia to be rather safe rather than unsafe good. Many other modifications in the monitoring of safety may be made within the scope of this concept.

[0058]

[0058] The details of the object 4 to be sent to the base computer 3, preferably in the form of an object 4 that uniquely identifies a signature or a "key". This is to limit the amount of primary data storage and transmission requirements. This key may be formed by a hashing function acting on an object at the remote computer 2.

[0059]

[0059] Key in the preferred embodiment is specifically arranged so as to have at least three separable elements. The first element represents executable instructions constituted by or objects

Sophos Ex. 1002
Page 540 of 683

contained within the object. The second element represents data about the object. The third element represents the physical size of the object. The data about the object in the second element, and the file name, and the physical and folder location on the disk, that the original file name, and the creation and modification date and time, skilled in the art, product and version, as well as in the object other and any information that is stored, and the file header or header is held about it by a remote computer 2, also create an object, structure, or have been or the start by an object to be executed on each of the remote computer event or the like including an object may be any or all of the other identification form. In general, the information provided in the key may include any two or more components in one or any combination of these, of the at least of these elements.

[0060]

[0060] In one preferred embodiment, for all of the executable file of the type PE (Microsoft (have been Portable Executable files defined by Microsoft)) .exe and .dll files, and the like (but is not limited thereto), check to create a Sam. Three kinds of checksum is generated, according to the nature of the files. In other words, Type 1: checksum five different sections in the file. These include import table, start in the coding section section and the end section, as well as the start section and end section of all files. This type is applied to the majority of the files to be analyzed.

[0061]

[0061] Type 2: against the old DOS or 16-bit executable file, checksum all files.

[0062]

[0062] Type 3: for files above a certain predetermined size, by sampling the file for each large chunks, and then checksum. For small files than a certain predetermined size, and checksum all files.

[0063]

To [0063] checksum process, in principle it is possible to any technology. MD5 (Message Digest

Sophos Ex. 1002
Page 541 of 683

Algorithm 5) is a cryptographic hash function which is widely used for this purpose.

[0064]

[0064] Thus, with reference to the only executable element of the checksum, by comparing the two executable elements that share a common executable code, it may generate a core checksum.

[0065]

[0065] with respect to the type 1 checksum, may be used are three of the signature process. The first signature defines all the files, change along with the changes to the contents of any file almost. Second signature, achieve only provision change of processing instructions of less process. Third of the signature, and by using the file size, this by the possibility that objects of different sizes collide is greatly reduced. By tracking or detect the occurrence of all of the signature appearing on the individual with a different counterparts, but have been created from modified or common point, edited to run a malicious functionality in some cases a new, it is possible to identify the process.

[0066]

[0066] The "metadata" is present and the newly derived heuristics to (heuristics) can be performed on the data in the community database 7.

[0067]

[0067] Data stored in the community database 7, inevitably creating one of an object, place, implementation, behavior (behavior) (behavior), identification, and, or acts on it a plurality of other objects thereby it will provide a relationship to said other plurality of objects to be working.

[0068]

Sophos Ex. 1002
Page 542 of 683

[0068] Suitable central heuristics, one of the objects is safe, or unsafe, or questionable whether in order to clarify, using a five-specific process.

[0069]

[0069] The first process of these, one or more of the name was acquired or correlation from all of the remote computer 2, which is looking at the object, position, skilled in the art, the product, using the version information. By consideration of these pieces of information for a single object, it can determine the scores is used as the degree of credibility and / or reliability of the object. Most secure objects tend not to use a large number of identity or location. The type and position of the object, may establish rules in consideration of the information. For example, temporary files, frequently using a plurality of system-generated file name which may differ on each remote computer for the same object. Object when there are only a few, as compared with the known behavior of other objects with the identification information previously (or behavior or behavioral), providing a reference point for considering its behavior. For example, a new object to the effect that version of notepad.exe, compared with the behavior of one or more other objects, also known as notepad.exe, can have its behavior. This comparison can be made to a single other objects or other objects using the same or similar identifying information. In this way, the behavior of a new pattern is identified for the new object. Thereby also, the preferred embodiment can identify a new behavior pattern as policing the behavior of an object over time, thereby to reconsider the state of the object that was considered safe first. Alternatively, a score based on the identification, may be considered in conjunction with the written score by other processes on the object to be considered another object scores, or in multiple combinations.

[0070]

[0070] The second process, one of the objects, or the object acting on the object is used relationship to a plurality of other objects that act. For example, any object created this object, what a number of objects created this object, which a plurality of objects you have created one of the registry key to run or configure this object, what a number of objects or is provided with a plurality of or the plurality of registry key is constituted by a registry key that is created by this object can be analyzed for the like. In this regard, an object by the object relative to other objects, or other objects is considered to have a relationship based on events performed on the object. This chain of simple one-to-one relationship, give a correlation complex series of points. As a result, inherited the relationship, can be considered for any of the object, its predecessor by an

Sophos Ex. 1002
Page 543 of 683

event, or its progeny by the event (ie, child and sub-child process). Thus, the known, unknown, it is known as safe, or poor with known object, or expand describing scores relationship and association with combinations thereof. Specific relationship to one or other type, the object having a number of relationships, or mixed committed relationship may be determined whether the safety or not. Alternatively, in order to reach a determination of safety or not, a score based on the relationship may be considered in conjunction with other scores. This data can directly or other objects objects associated through, and also be used to estimate the number of factors regarding their behavior (or behavior or behavior). For example, the behavior of one object, can be estimated for how they are affected or changed by the association or connection with other objects. For example, consider the notepad. Exe that Windows series operating system is supplied by Microsoft. This is, it does not have only a function of the limited range, therefore, to send data to another computer, and perform a wide range of events of such or run other programs is not expected. However, notepad. Exe of behavior can be altered by the introduction of such as a dynamic link library introduction (DLL introduced), It a new code.

In this case, notepad. Exe will have a new performance obtained by ties to the code introduced, or other objects. By using the data defining the relationships between objects, the new behavior of the program can be estimated to be due to the relationship with other objects. If, when the new behavior is malicious, any or all of the processes can be unsafe when with indicia as necessary.

[0071]

[0071] Combinations of acquired behavior, provide a basis for determining whether the object is safe. Typically, malware, show a certain behavior and features. For example malware, often there is a need for self-survival. This, if it is necessary to automatically restart the restart of an event or system become apparent. It is a typical feature of malware to create an object that causes the automatic restart or perform singular positions. Replacement of the core object of the Windows system environment is another example of the typical characteristics of malware. By providing a pattern of behavior, you can automate the determination of whether safety or the object is unsafe. Centralization of the community data in the community database 7, results in the ability to incorporate the behavior of the object rapidly, to allow rapid identification and determination of malware. Object, an event that can be considered in guiding the score may be automatically executed.

[0072]

Sophos Ex. 1002
Page 544 of 683

[0072] A third process involves time and volume. Relevant data, someday the object was seen for the first time, sometime was last seen, either was seen many times, or was seen many times in a given time interval, an increase or decrease in the acceleration in the object including whether observed. This information is very closely related to determine the spread of one object in the community of more remote computers. Score may be used to determine whether one of the objects is safe or unsafe, or whether it can not be executed or propagated without very thorough investigation too prevalent, and these metrics (metrics) is developed on the basis of. In this case, the object may be its behavior or temporarily refrain from executing additional information unresolved relationship, or blocking. This score may be used in combination with scores from other processes. Also with respect to time, in combination with other information that is not limited to but including the behavior and identity, there is a very meaningful. For example, if the named object polymorphism or random, time is a powerful qualifier. (Polymorphic viruses, so changes the encryption key to the encryption algorithm and corresponding to the time the duplication from one computer to another computer, it is difficult to detect by conventional methods.) One of the program to create a plurality of other programs, based on the activity over time, are considered as often is normal or abnormal.

[0073]

[0073] The fourth process takes into account the behavior of one object. Thus, score, based on the type of event execution execution event, or against the object by the object itself or other objects according to one of the objects can be developed. Centralized system of community database 7, can be the kind of event to infinity, it can be considered an object or both, with a place event object to run the event, or against it. Kind of some of the events, associated with the program to change external information other than the object, for example by running the event to connect to the Internet Relay Chat site program, or a non-executable file, such as a Windows host file. Action event in one of the objects, of any of the events "actors (actor)" (ie, the object is do something for the other objects) or "victim (victim)" (ie, the object of the other as to) something by the object, in combination, sequentially, a large amount, presence or absence, or the like in any combination thereof, obtained considered in various ways. Behavior events in the preferred embodiment, the remote computer 2, or may be supplied from other external sources. This process can be considered in combination or to isolate them. Furthermore, the state in combination with behavioral events of other objects that act on or object object action is considered a feature of the preferred embodiment. For example, the creation of the program, whether the program of creating safe either new or, if not known, or depending on whether the suspect, may have a different score. Similarly, the programs created by the known defective program may have a different score resulting from its creation event in accordance with the state of the object to create it.

Sophos Ex. 1002
Page 545 of 683

[0074]

[0074] The fifth of the process, to take into account the behavior of the web page or script. In this regard, the combination of web pages and the URL is as if characteristic is given that behaves as if it is an object, such as other executable is tracked or detection. In this example, web page, usually the web browser (e.g., IExplore.exe or Firefox.exe) may perform an event seen as an event to be executed by. The preferred embodiment details and signature of the identification of the web browser, used in place of the "pseudo" object identification associated with a web page that it has or running are displayed in the browser. In this regard, if safety conditions of the relevant web pages and / or web site, or unsafe, or not known, whether the suspect may be determined similarly to other objects. The "pseudo" object identification of the web page, the preferred embodiment, potentially to prevent some or all of the non-safe behavior, or web site to give the credentials to the remote user, web page or their so as to guide about the safety of the contents, it is also the web page or prevents the function of the web site, interference (interject) or limit it.

[0075]

[0075] Among the other types, the type of acquired metadata may be as follows. In other words, "Event": these define the activities of objects that act on other objects or other entity (entity) (actions), or behavior or behavior the (behaviors). Event, has three main elements. In other words, the key of the object to perform the act ("doer"), executed the act ("event type"), as well as, identification or object of the key of other realities in which activities are performed ("the victim") it is. While simple, this structure, it is possible to define the infinite series of actions and relationships. Examples of three elements in one of the event may be as follows.

[0076]

[0076]

[0077]

[0077] "Identification": these define the attributes of one object. These are file names, their

Sophos Ex. 1002
Page 546 of 683

physical location on disk or in memory, the logical position on the disk in a file system (path), one day the file was created, last accessed for eventually, end information was changed sometime, stored as skilled in the art, the product is a file and part and the version number of its contents, its original file name, as well, such as file header information, including file size, and the like, a variety of items including.

[0078]

[0078] "Origin actors (genesisactor)": is not a direct actors of events, the key of one of the objects is the ultimate parent of events being performed. For example, in the case of the installation of the software, this is first executed by a user or system, and software installation process, would be key to the object that initiated, for example, Setup.exe.

[0079]

[0079] "auxiliary data (ancillary data)": a number of events, the auxiliary data, for example may request an event of an event such as that used to record the creation of registry run key. In this context, the "event" is, actors object for which you want to create a registry run key, the event type itself (for example, "Reguranki (regrunkey)"), as well as the victim or target of the registry run key, identify. Auxiliary data in this case, to define the execution key entry itself. In other words, the hive, key of the name, is a value.

[0080]

[0080] "Event checksum": event data, a single event, actors, since the information for the identification for the victims and any auxiliary data can reach about be very large in a few hundred bytes, the system this the data itself can be summarized by the event checksum. Two events checksum is used by utilizing various algorithms, such as CRC and Adler. The checksum is the one of the core data of the event. Thus, the remote computer 2, already central computer 3 that may have data relating to the checksum these storage can transmit checksum data. In this case, it does not require additional information to a remote computer 2. The central computer 3, only if there is no reception of the checksum even once, and requests the relevant data to a remote computer 2. Thus, both the performance of the remote computer 2 and the central computer 3 is significantly improved, thereby enabling more effective scaling.

Sophos Ex. 1002
Page 547 of 683

[0081]

[0081] Thus, in the community database 7 may use the metadata acquired from the remote computer 2, to define the behavior of the process in the community throughout (or action or behavior). As described above, at least one element of the data above plurality of elements (file size, position, etc.), or two, three, four, five, or six components, or seven of all elements (or here, many of the elements) may include a more did not specifically mentioned. It is appropriate, the modeling of new automated rules for use by the community database 7, a test, and may be used for performing generation, are added to those which are utilized are further held in a local database of the remote computer 2 used as a rule, it may be carried out the identification and determination of the response of the remote computer 2 with respect to the process and the process activity of new or road.

[0082]

[0082] In addition, you can monitor the process with any of the sub-process as a homogeneous entity, able to compare the activities of the top-level process over the whole community. Further, reliable and potentially malicious execution is only occur if one or more specific sub-process is loaded. This, needless to say today user from a major source Internet of malicious code to get, by any of the code can be downloaded, such as Internet Explorer or other browsers that you can easily change the functionality, effective program Do monitoring (without blocking unnecessary) is possible.

[0083]

[0083] Frequently potentially significant portion of the plurality of users utilizing indicates a high probability of at least one of them is infected with new malware. The propagation speed is detected and recorded, it is possible to detect the malware propagation. Malware, file size, location, and in combination with other factors and, optionally as described above, such as name, on the basis of the propagation speed, can be specified as malicious or faulty. It is also possible to use a simple volume of infection as a trigger. In a further embodiment, coupled with the progress of the first attempt to execute the code in the community, due to the difference of the name in part of the same code except in name, it is expressed as vicious a portion of the code to be signed in the same way other than it pattern matching is possible.

Sophos Ex. 1002
Page 548 of 683

[0084]

[0084] This feature, in some embodiments, "in our community, there is nothing to propagate faster than X without being locked" so state to allow a period any process or event is given If you want to more quickly propagate beyond, it is subjected marked as malicious. This is the case for instance where one object is sufficiently fast propagation, given that it may possibly be infected with computer before performing the analysis to determine whether malware, safety it is for.

[0085]

[0085] This process propagates skilled in the community (i.e., propagation type source) by the identification of the time stamp stored in the community database data and marking a portion of the code having these attributes as malicious (with sign) It can be automated. By comparison, all other anti-malware provider relies on known simply as malicious model, therefore, believed to be mainly dependent on the malware that is actually reported has occurred at the end portion ing.

[0086]

[0086] Thus, early diagnosis by using a community database 7, or simply preventive measures can be taken, therefore, potentially worms and other malware to quickly propagate at a very early stage of their life cycle it is possible to stop. Infection can worm all computers connected to the Internet within a few minutes is to be generated, this feature is highly desirable.

[0087]

[0087] The data defining the propagation speed of the new software, by combining with the metadata supplied to the community database 7 collected from the remote computer 2 by the agent software, may be made even faster decisions. This includes monitoring of the process to try to hide themselves from the user by changing the random name and / or location on the remote computer 2. It also includes an attempt of the process of creating an identical copy of the complete identity (i.e., comprises the same code contents) on a computer but is different names. This is the traditional nature of the worm.

Sophos Ex. 1002
Page 549 of 683

[0088]

[0088] The signature of one of the objects may be made using the object, and may be associated with, or the mask comprises a mask that indicates the particular type of behavior expected from the object. If one of the object can be executed on the remote computer 2, even if the initial signature search 22 shows an object is safe, the operation of the object may be monitored in the mask parameter. Mask, for example, a behavior expected of the object and be open to allow communication including been of any port or interface details request was legally is created on the remote computer 2 by the object , or any external requests the creation is requested, or the Internet connection, local is expected to query is made from the object, or the network beyond the local area network, wide area network, or the Internet, etc., optionally and database may indicate the like. Thus, the mask can provide an overall picture of the envisioned "normal" behavior of that object.

[0089]

[0089] Thus, in practice, in one embodiment, the behavior of the object are continuously monitored by the remote computer 2 of one (or more), also information related to the object is exchanged with the community database 7, it is running in the mask in which the object is the assumption is determined. Any behavior departing from the mask are identified, whether the object is still safe, can be used to continually evaluated. Thus, for example, regularly (for example, every month or every year) objects to update to open a new port, or if you want to get a regular data, a flag is set to this information. If, performs object this to other remote computer, if you do the adverse effects also did not receive, or if this behavior has been informed that it is safe from other objects, as this behavior is safe behavior regarded as well, and the mask is modified to allow this. If, if that were known in advance when the new action actually leads to unsafe or malicious result, the object, even if previously been regarded as safe, and unsafe Shirushitzuke It is. Similarly, if the object is, it tries to connect to the web site and database that was known to be unsafe, or in general to try to wake the action that has been known to be an action to be performed only by the program that is not safe, again, object it may be regarded as unsafe.

[0090]

[0090] This is shown schematically in FIG. Figure 3, any of the object is, for example, show major software company, the authority of the collation, also reliable concept can be permitted in

Sophos Ex. 1002
Page 550 of 683

advance by the other party, such as a government agency. The prior permission, the supplier of a new object has not been previously released to get the pre-authorization of that object and the supplier of the mask detailing supposed to have and behavior that is allowed for the object optionally including the supply by.

[0091]

[0091] Referring to FIG. 3, for example, when one of the processes is executed, the local and / or community database is searched in step 31 previously. If this process is not the one that has been pre-authorized, a plurality of steps in FIG. 2 are performed, the process, at step 32, are not, or are allowed to run. If you are pre-authorized so that this process is determined by step 33. In step 34, it is a ready-to-run. As a result, the operation of this method may end. However, in a preferred variation, the process is monitored during execution, or is monitored each time for future execution in step 35 the monitoring state, in the range of the mask 36 in which the action is the pre-authorized It is determined. If this action is within the range of the mask 36 which is pre-authorized, continue process execution is permitted. If this action is, by pre-authorized it to further incite process or connection is not like, if you want to deviate from the mask 36 which is pre-authorized, this action is flagging in the warning step 37. Various actions may be taken at this stage. The process may be one that simply running is not allowed. Alternatively, the action early can be a pre-authorization and the contact to a trusted authority may be taken that can be confirmed whether or not acceptable. If acceptable, the mask may be modified as desired. If you can not acceptable, subjected mark if the process is not safe. Many other actions may be performed when notifying of such warning conditions.

[0092]

[0092] If the process, if it is allowed to perform but found not to have been pre-authorized at step 33, the process is monitored at step 38 to generate a mask 39 representing the normal behavior of the process It is. Data representative of this mask, the other computer may be sent to the community database 7 to scan in performing this process. By monitoring the process continues each time to run the process or during the process, it is possible to know the different arbitrary behavior to the previous behavior of the process, can change the mask. Alternatively Using this behavior, the process that was considered to be a time safe current may be determined to be regarded as unsafe.

[0093]

Sophos Ex. 1002
Page 551 of 683

[0093] In another embodiment, a computer 2, to provide information in response to periodically or requested to the community database 7, which is all or a selection of loaded or available software products on the computer 2 representative of the product may be provided with an installed agent software. In particular, this is locally loaded security products (anti-virus software, anti-spyware, such as anti-malware system that includes an anti-adware, etc.), firewall product, or of the specific setting and detail what the signature file is currently loaded , there the information about the particular version and of the information on the software setting, etc., one or more items at a time, or any version of the operating system and other software details, as well as what files are operating it may be. (It should be understood that, by audit and inspection whether they match against more items, an increase in the possibility that the computer is placed very similar to, therefore, search omission during the match search and the proportion of false positives is reduced.) Information about these software products, etc. may be provided separately to the community database. However, for reasons of storage capacity and transmission of data again, the information, the information (e.g., the hash or compression function in computer 2) it is preferably provided as a representative signature or key. 4, local security product, version, signature files, using how all of the details, such as firewall settings, whether to create a key 41 shown schematically. The key is sent to the community database 7. Community database 7, a large number, because it is supplied with such information from hundreds of thousands of users computer 2 optionally, the corresponding information, the other having a security products, etc. of the same or similar configuration It would be held in order of the computer 2. Therefore, the community database 7, can be searched at step 42 in search of other computer 2 having a security product of the same or similar combination including the same settings and loaded signature files, and the like.

[0094]

[0094] community database 7 in this embodiment, the agent software may be supplied with details of a plurality of processes executed by all the computer 2, thereby, whether one process is detected by the computer 2 I will know.

[0095]

[0095] In this manner, the community database 7, for example, including the setting and signature files existing at a certain point in time, by a specific combination with the operating system and various security products, particular where there is a particular computer 2 of can be

Sophos Ex. 1002
Page 552 of 683

used to obtain information about whether a state having a susceptible or vulnerable these products and set to malware object.

[0096]

[0096] In a simple example, for example database, the computer in the past, have an anti-virus product B version A with a download signature latest version of C, a firewall D with specific configuration E, also signature latest Although know that having anti-spyware software F having a plate C, if a particular malware process P, did not know that was not detected by the combination of program at that time, this information, the security products / setting combination can provide it to the computer 2 that has been known to have a of, and using this, the computer 2, short-term that weak in against attack by that particular malware process it is possible to show a. This information, or not to display the window 43 to the screen display computer 2, or to the user, can be presented to the user by guiding a particular web site that describes the position in more detail. For example, specific combinations such as these security products are exposed to the risk of infection of the Sobig virus the computer, the virus may be known to the user that it is undetectable by the computer. The user, specific advice (for example, to update the specific anti-virus program with a specific signature file), or software to download and install may be asked to remove this risk.

[0097]

[0097] Thus, the community database 7 is information about all security products, etc. on a specific computer in a specific time when it is supplied, in and locally generated on a computer with a particular combination of security products It is searched for events of attached mark and was not detected "malicious or bad" process. And this information is, to the user of that particular computer, by guiding the web site, for example, directly or the user, can be fed back. This information can be supplied to the fact on the real-time, thus a new user or a new computer it is possible to very quickly improve the effective safety of the computer.

[0098]

[0098] In addition to detect whether suitable methods which objects mutually related to each other, can be attached mark the object as malware using the concept of genealogy. For example, any particular process may generate a child process, hence they are associated. Check the key

Sophos Ex. 1002
Page 553 of 683

associated with the first object, the elements present in the key of the first object or is inherited and a uniquely identifies elements of the first object progeny or other related objects, it may identify. This element is referred to herein as "gene (gene)". This general technique, may be used in a number of ways.

[0099]

[0099] a) a known reliable parent process are given the ability to create a child process to run on the local computer is automatically assigned a sign that it is safe. This "inherited was" properties may be transmitted to the grandchild process or the like. This safe state is transmitted to the parent of the child process, in some cases (referred to as the "descendants (issue)" in this case) a further child process through the child process, the signature of this offspring is all automatically It can be recorded as good in the local database. As a result, even unavailable connection to the community database 7, descendants process can quickly and with good mark.

[0100]

By [0100] b) to monitor the activities of the parent process, if the parent process has been found after that the malware, it is possible to automatically record a defective or malicious in the local database all descendants process.

[0101]

[0101] c) Similarly, by monitoring the activities of this descendant process, if in the case where one of the descendants of the process has been found after to be a malware, all of one or more of the parent process and other descendants process (in other words, all) of the related processes in this context it is possible to automatically record a defective or malicious in the local database.

[0102]

[0102] d) has been performed by the parent, to create a signature for one or more child, including the capacity for one or more children, depending on the behavior and decision of the parent, can be automatically attached mark whether good or bad . In some embodiments, the

Sophos Ex. 1002
Page 554 of 683

product is the birth of the child can be "observed" or monitor, can be automatically create a signature on arrival. This results in the ability to monitor the creation of one bad program by other bad programs. Therefore, it is possible to monitor the families of one program, for example, when the grandfather creates a one program (father), which in turn creates a one defective Program (son) automatically father It can be determined to be defective program.

[0103]

[0103] e) because the child has generated already bad offspring as a parent, the ability to have inherited a child that trigger the automatic creation of signatures for further birth, may include a feature to automatically loss . As a rule, if in case the file is having one of the bad offspring, it is preferable that the ability of the inherited can be automatically deleted.

[0104]

[0104] f) clones or identical twins of an object (e.g., to observe the same process) running on other systems in the community, compares the pattern of their progeny, malware a specific process ability to make a decision regarding whether or not treated as.

[0105]

[0105] using one or more of f) from these characteristics a), it can often be used effectively without necessarily be 100% dependent on the permanent connection to a non-practical Internet, to produce the security product it is possible to provide a solution to the problem. This example is Windows Update and other processes are increasingly used by producers who wish to automatically allow expand the product latest version in the World Wide Web.

[0106]

[0106] The compared to traditional software, benefits to be considered in characteristics of these types are as follows. Antivirus software tends to have a cache of known bad signature. A is the problem, is that you always up-to-date state this. Someone Let me give you a quick example to purchase a new computer. The computer comes with a pre-loaded anti-virus product with

Sophos Ex. 1002
Page 555 of 683

signature cache. PC is built, shipped to over-the-counter, while being purchased by the user, will after a few days or a few weeks. The user starts the PC, exposed to any new virus or malware generated after the PC has been constructed. For complete protection, users connected to the Internet, is possible to download the latest version is required. This can not guarantee that precedes other activities by the user on the Internet (guarantee be physically is almost impossible). Along with a local cache of known good process, similarly to the embodiment of the present invention, in advance (without drawbacks (clean)) All good loaded a preloaded cache of previously generated signature to the software by a computer manufacturer You can ship the computer / terminal. In this case, the user, knowing that any new or updated program is detected and matched immediately, can connect to the Internet. Also, software that is any automatic updates, the signature is forced, the children and even distantly related offspring (ie, grandchildren, great-grandchildren, etc.) can function to be automatically built for.

[0107]

[0107] Here, according to the "Virus Bulletin Conference October 2005" of the Microsoft company, which was announced in Adrian Stepan: the "Defeating Polymorphism Beyond Emulation", referring to the US 60/789156, filed on Apr. 5, 2006 . The entire contents of which are incorporated by reference. In its articles and patent applications, analyzes the file to be able to determine whether the file is indeed a malware, the method of decoding the file is disclosed. US 60/789156 particular, to a method of thawing / decoding an executable computer file using a host computer, a step of dividing the executable computer file into plural basic code blocks, among the basic code block a step of translating at least some of the translational basic code blocks can be executed by the host computer, a step of linking at least some of the basic code blocks in the memory of the host computer, wherein on the host computer at least some of the basic code block, and a step in which the executable computer file to be executed to allow decompression or decoding, by analyzing the decompression or decrypted executable computer file, the executable computer file There is disclosed a decompression / decoding method that can determine whether it should be or are classified as malware. Further, US 60/789156 provides a method of thawing / decoding an executable computer file, a step of dividing the executable computer file into plural basic code blocks, at least some of said plurality of basic blocks for, create at least one read page of cache memory for storing read and the reading corresponding to the cached virtual memory address and the cached realistic address of each basic block and one of said plurality of basic blocks and the step of creating at least one write page of cache memory for storing at least for some, the writing and writing and cached realistic address corresponding to the cache virtual memory address of each basic block, the basic code block said executable by at least some of the executable computer file to be executed to allow decompression or decoding and a step of emulating, by analyzing the decompression or decrypted executable computer file of the executable computer file can be determined whether it should be or are classified as

Sophos Ex. 1002
Page 556 of 683

malware, during the execution of one basic block,At least one of the read page and writing a page of the cache memory, tested for cached realistic address corresponding to the virtual address to access the basic block, discloses a decompression / decoding method.

[0108]

[0108] The techniques disclosed in these documents can be used in this context in the analysis of detailed files is desired. However, more generally, using these disclosed techniques in the literature, improved technique disclosed in particular US 60/789156, can provide information on the activities of the files when executed on a computer. This is because the execution of the file by the techniques disclosed in these documents are emulated, thereby interpret the file activity.

[0109]

[0109] when the user wants to install software at the time of off-line, further situation arises. In a preferred embodiment, when the user tries to install a new software offline, agent software running on the user of the computer 2, the installation process as execution itself of installation is "authenticated" by the user in order to proceed, prompting the authentication to the user. This user by authentication is treated as "origin (Genesis)" event. Hereinafter, referred to that way. However, during the installation of the software to interact with other existing programs on the installation device, there is a process that is used in common. For example, a MSIEXEC Microsoft.

[0110]

[0110] origin approach, as a result of the user authentication of the user of the computer 2, comprises a process of generating a signature. These signatures are stored in a local database of the user of the computer 2. In one embodiment, these locally stored signature, so as to proceed with the installation, is referenced by the agent software during the installation process if necessary. Alternatively, it is possible to OFF security checks made by the agent software during the installation process. The OFF is performed only in a limited period of time, for example, most of the software for several minutes or the like is sufficient to install, this OFF time can be changed at will by the user's setting.

Sophos Ex. 1002
Page 557 of 683

[0111]

[0111] In any case, once the installation is complete, the user of the computer 2 is connected to the community database 7, the agent software on the user's computer 2, the community a signature associated with the installation from a local database of user It can be uploaded to the database 7. Then, along with the corresponding data from the computer 2 of the other user, using a community database 7, the installation of this particular software may make a quick determination that an amphoteric.

[0112]

[0112] As a modification of this embodiment, if it is online at the time that there is a user of the computer 2, the agent software on the user of the computer 2, to download the signature of the so-called "trusted installer" or "license installer" it may be. As a result, the "License Installer" and any of the child process of the license installer, between origin event is "current", during the few minutes after example of authentication from the user, can operate the way to obtain permission of execution . The signature of the license installer when and applied as it is applied to the community database 7, always is preferably downloaded to the remote computer 2 online.

[0113]

[0113] For this method, so as to prevent executing the license installer when the change of media took place during the origin event, there may be a further improvement. However, any unknown processes that might be malware, may be further detected and blocked. By providing a small number of licenses installer, since the minimum data is needed, especially when compared with the download of the virus signature file, it becomes easy to download. As another example, for example, adopted an installer that is very reliable, such as "Windows Update", all of the new process created by its very trusted installer, even if characterized as a quick safety good.

[0114]

[0114] For installations which occurs when connecting the remote computer 2 to the community database 7, as another option, if the software is trying to install is not known to the community

Sophos Ex. 1002
Page 558 of 683

database 7, the system blocks the installation or it is raised to alert the user. For example, you are trying to install "software. This software is not known to the "community". Do you want to proceed? The degree of message ", may be displayed to the user of the computer 2.

[0115]

Examples of [0115] The present invention has been described with reference to the examples specifically described. It should be understood, however, that the above example may be modified and changed within the scope of the present invention.

[0116]

[0116] is a diagram schematically showing an apparatus embodiment is performed of the present invention. An example of operation in a method according to an embodiment of the present invention is a flow chart illustrating schematically. Other examples of operation in a method according to an embodiment of the present invention is a flow chart illustrating schematically. The information acquisition step is a flowchart illustrating schematically.

Description of the code

[0117] 1 Internet 2 remote computer 3-based computer 4 objects 5 line 6 line 7 Community database

Sophos Ex. 1002
Page 559 of 683

Patent Translate
Powered by EPO and Google

Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

CLAIMS JP4936294

1.

1. There is provided a method of classifying one of the computer object as malware. In the base computer, comprising: receiving data about a computer object from a plurality of each of the remote computer for storing the object or similar plurality of objects, The data about the computer object received from said plurality of computers, the steps of comparing in the base computer, A step of classifying the computer object as malware on the basis of the comparison Equipped with, First a step of classifying an object as a non-malware, generating a mask for said object that defines the acceptable behavior for the object, the step of monitoring the operation of said object on at least one of said remote computer and, if you want to deviate from the ones in which the behavior was actually monitoring has been granted by the mask, classification method and further comprising said Rukoto and the step of re-classifying the object as malware.

2.

2. The transmitted from a plurality of remote computers to the base computer was and used in the comparison, the data relating to the computer object, a plurality of executable instructions constructed by or said object contained within said object, said object and size of the current name of the object, and the physical and folder location on the disk of said object, and original name of the object, and the creation and modification time of said object, stored in said object

Sophos Ex. 1002
Page 560 of 683

starting skill, product, version, and other information, the header held by the object header or the remote computer, executing the object on each of the remote computer, upon which or created configuration, by said object method according to claim 1, characterized in that it comprises a has been or events, including the object, one or more of.

3.

3. By the comparison method according to claim 1 or 2, relationship between the object and several other objects characterized in that it is identified.

4.

4. At least one other object, when it is classified as malware, the method according to claim 3, characterized by classifying said object as malware which said object is associated.

5.

Five. Said other of the plurality of objects, the method according to claim 3 or 4, characterized in that it comprises the object or similar plurality of objects stored in at least some of said plurality of remote computers.

6.

6. Said other of the plurality of objects, parent or child object, or a process-related object with respect to said object, according to any one of claims 3 to 5, characterized in that it comprises a plurality of other objects Method.

7.

7. The data A method according to any one of claims 1 to 6, characterized in that it is transmitted in the form of a key that is acquired by the hashing process wherein is executed for a plurality of

Sophos Ex. 1002
Page 561 of 683

objects on the respective remote computers .

8.

8. The key The method of claim 7, characterized in that at least one of the elements representing the executable instructions configured by or said objects included in the object.

9.

9. The key The method of claim 7 or 8, characterized in that at least one of the elements representing the data related to the object.

10.

10. The data relating to the object, and the current name of the object, and the physical and folder position on the disk of the object, and the original name of the object, and create and modify date and time of the object, to the object stored skilled in the art, the product, version, and other information and, the object at the time said the header, which is held by the object header or the remote computer, you run the object on each of the remote computer, to be or create configuration a method according to claim 9, characterized in that it comprises an event containing initiated or said object, at least one of the.

11.

11. The key method according to claim 7, in any one of 10, characterized in that at least one of the elements representing the physical size of the object.

12.

12. There is provided an apparatus for classifying one of the computer object as malware, They comprise one of a base computer constructed and arranged to receive data about a computer

Sophos Ex. 1002
Page 562 of 683

object from each of the objects or more remote computers that stores a similar plurality of objects, The base computer, said data about the computer object received from said plurality of computers are configured and arranged to compare, The base computer is constructed and arranged to classify said computer object as malware on the basis of said comparison, The base computer is first allowed constructed and arranged to generate a mask defining the behavior is for one of the objects classified as non-malware and said base computer, said on at least one of said remote computer monitors the operation of the object, actually monitored when the behavior deviates from the ones allowed by the mask, the classification apparatus according to claim Rukoto constructed and arranged to reclassify the object as malware .

13.

13. The base computer are a plurality of executable instructions constructed by or said object contained within said object, and the size of the object, the current name of the object, physical and folders on the disc of said object position, the original name of the object, and the creation and modification time of the object, skilled stored in the object, product, version, and other information, held by the object header or the remote computer and header, executing the object on each of the remote computer, and events, including that have been or the object initiated by the object when you or create the configuration, the data that includes one or more of the, to compare the apparatus of claim 12, characterized in that it is configured and arranged to.

14.

14. The base computer, by the comparison An apparatus according to claim 12 or 13 relationship between the object and several other objects characterized in that it is constructed and arranged to be identified.

15.

15. The base computer, at least one other object said object is associated with is, if it is classified as malware, according to claim 14, characterized in that it is constructed and arranged to classify the object as malware device.

16.

Sophos Ex. 1002
Page 563 of 683

16. The base computer, said plurality of other objects, characterized in that it is constructed and arranged so as to include the object or similar plurality of objects stored in at least some of said plurality of remote computers the apparatus of claim 14 or 15.

17.

17. The base computer, said plurality of other objects, claims 14, wherein the configuration and arrangement that to include a parent or child object several other objects are process-related object or to the object, 16 apparatus according to any one of.

18.

18. The base computer claims characterized in that it is constructed and arranged to handle data transmitted in the form of key that is obtained through a plurality of executed hashing process for objects on the respective remote computers device according to any one of claims 12-17.

19.

19. The key device of claim 18, characterized in that at least one of the elements representing the executable instructions configured by or said objects included in the object.

20.

20. The key device of claim 18 or 19, characterized in that at least one of the elements representing the data related to the object.

21.

twenty one. The data relating to the object, and the current name of the object, and the physical

Sophos Ex. 1002
Page 564 of 683

and folder position on the disk of the object, and the original name of the object, and create and modify date and time of the object, to the object stored skilled in the art, the product, version, and other information and, the object at the time said the header, which is held by the object header or the remote computer, you run the object on each of the remote computer, to be or create configuration the apparatus of claim 20 and events including initiated or the object, which is characterized in that it comprises at least one of the through.

twenty two. The key device of any one of claims 18 21, characterized in that at least one of the elements representing the physical size of the object.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－44677

(43)公開日　平成８年(1996)２月16日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　15/16	３８０　Ｚ			

審査請求　未請求　請求項の数３　ＯＬ　（全　６　頁）

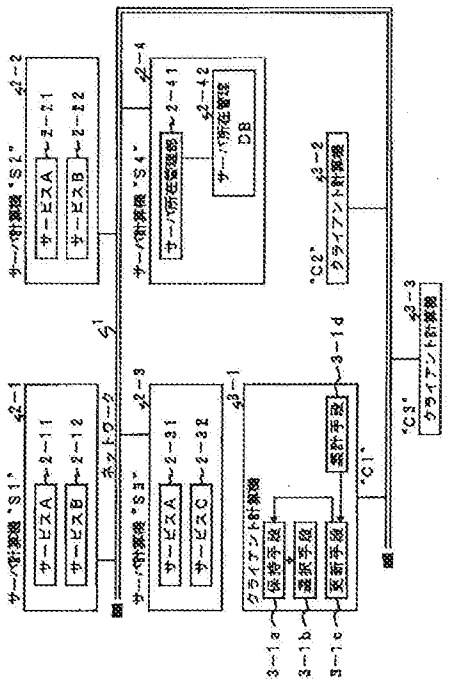
(21)出願番号　特願平6－178760

(22)出願日　平成６年(1994)７月29日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　小林　恵
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
(74)代理人　弁理士　鈴江　武彦

(54)【発明の名称】　分散処理システム

(57)【要約】
【目的】複数の計算機をネットワークで接続した計算機クラスタでサービスを提供するサーバ計算機に対する柔軟性のある負荷分散を可能にする。
【構成】所望するサービスを一意に示すサービス識別子をもとに、サービス識別子が示すサービスを提供するサーバ計算機の所在、同サーバ計算機の処理能力、及び負荷状態を求めることができる所在管理部２－４１と、所在管理部２－４１から求められた少なくとも１つのサーバ計算機の処理能力・負荷状態の情報をクライアント計算機側で保持し、保持された処理能力・負荷状態の情報をもとに、クライアント計算機側で所望するサービスを要求すべきサーバ計算機を選択し、同一のサービスを提供する複数のサーバ計算機に対して、クライアント計算機側によって負荷分散を行なう。



Sophos Ex. 1002
Page 566 of 683

【特許請求の範囲】
【請求項１】　複数の計算機をネットワークで接続したクライアント／サーバ型の分散処理システムにおいて、
所望するサービスを一意に示すサービス識別子をもとに、前記サービス識別子が示すサービスを提供するサーバ計算機の所在、同サーバ計算機の処理能力、及び負荷状態を求めることができる所在管理手段と、
前記所在管理手段から求められた少なくとも１つのサーバ計算機の処理能力・負荷状態の情報をクライアント計算機側で保持する保持手段と、
前記保持手段によって保持された処理能力・負荷状態の情報をもとに、クライアント計算機側で所望するサービスを要求すべきサーバ計算機を選択する選択手段と、
を具備し、
同一のサービスを提供する複数のサーバ計算機に対して、クライアント計算機側の前記選択手段によって負荷分散を行なうことを特徴とする分散処理システム。
【請求項２】　前記サーバ計算機の処理能力・負荷状態の変化に対応して、前記クライアント計算機が前記保持によって保持された前記サーバ計算機の処理能力及び負荷状態の情報を更新する更新手段をさらに具備し、
サーバ計算機側の状況の変化に応じて前記情報を逐次更新しながら負荷分散を行なうことを特徴とする請求項１記載の分散処理システム。
【請求項３】　前記クライアント計算機が前記選択手段によって選択した前記サーバ計算機の応答時間を前記クライアント計算機側で統計的に集計する集計手段と、
前記集計手段によって求めた応答時間の統計情報をもとに前記保持手段によって保持されたサーバ計算機の処理能力及び負荷状態の情報を更新する更新手段と、
をさらに具備し、
サーバ計算機側の状況の変化に応じて前記情報を逐次更新しながら負荷分散を行なうことを特徴とする請求項１記載の分散処理システム。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、複数の計算機がネットワークで接続された計算機クラスタ上で、クライアント／サーバ型の処理を行なう場合のサーバ計算機の負荷分散機構に関する。
【０００２】
【従来の技術】従来、複数の計算機がネットワークで接続された計算機クラスタにおいて、複数の計算機に処理を分散させる場合は、サービスを提供するサーバ計算機を固定し、予め負荷分散を決定しておくというのが一般的であった。
【０００３】
【発明が解決しようとする課題】このように従来の分散処理システムでは、各サーバ計算機に対して予め負荷分散を決定していた。しかしながら、予め固定的に負荷分散を決定しておくと、負荷状態の変化や計算機の障害といった要因を負荷分散の制御に逐次反映することが困難となってしまう。
【０００４】また、予め固定的に負荷分散を決定しておくためには、業務内容に対する十分な事前解析が必要であり、業務内容の変更や計算機構成の変更に柔軟に対応できるものではなかった。本発明はこのような点に鑑みてなされたもので、柔軟性のある負荷分散が可能な分散処理システムを提供することを目的とする。
【０００５】
【課題を解決するための手段】本発明は、複数の計算機をネットワークで接続したクライアント／サーバ型の分散処理システムにおいて、所望するサービスを一意に示すサービス識別子をもとに、前記サービス識別子が示すサービスを提供するサーバ計算機の所在、同サーバ計算機の処理能力、及び負荷状態を求めることができる所在管理手段と、前記所在管理手段から求められた少なくとも１つのサーバ計算機の処理能力・負荷状態の情報をクライアント計算機側で保持する保持手段と、前記保持手段によって保持された処理能力・負荷状態の情報をもとに、クライアント計算機側で所望するサービスを要求すべきサーバ計算機を選択する選択手段とを具備し、同一のサービスを提供する複数のサーバ計算機に対して、クライアント計算機側の前記選択手段によって負荷分散を行なうことを特徴とする。
【０００６】また、前記サーバ計算機の処理能力・負荷状態の変化に対応して、前記クライアント計算機が前記保持によって保持された前記サーバ計算機の処理能力及び負荷状態の情報を更新する更新手段をさらに具備し、サーバ計算機側の状況の変化に応じて前記情報を逐次更新しながら負荷分散を行なうことを特徴とする。
【０００７】また、前記クライアント計算機が前記選択手段によって選択した前記サーバ計算機の応答時間を前記クライアント計算機側で統計的に集計する集計手段と、前記集計手段によって求めた応答時間の統計情報をもとに前記保持手段によって保持されたサーバ計算機の処理能力及び負荷状態の情報を更新する更新手段とをさらに具備し、サーバ計算機側の状況の変化に応じて前記情報を逐次更新しながら負荷分散を行なうことを特徴とする。
【０００８】
【作用】一般に、複数の計算機をネットワークで接続した計算機クラスタ上でクライアント／サーバ型の分散処理を実現する場合は、計算機クラスタ内でグローバルに識別可能な識別子が付与される。クライアント計算機があるサービスを要求すると、そのサービスに対応する識別子からそのサービスを提供するサーバ計算機の所在を得るために所在管理に問い合わせ要求が発行される。所在管理は、通常、計算機クラスタ内に１つ存在し、サービスの識別子とそのサービスを提供するサーバ計算機の

Sophos Ex. 1002
Page 567 of 683

所在を記録したデータベースを所持している。クライアント計算機からの所在問い合わせの要求に対してデータベースを検索し、サーバ計算機の所在を返却する。

【0009】本発明は複数の計算機をネットワークで接続した計算機クラスタ上でのクライアント／サーバ型の分散処理において、サービスを提供するサーバ計算機に対する負荷分散を実現するためのものである。

【0010】所在管理手段は、サービスを提供するサーバ計算機の所在に加えて、そのサーバ計算機の処理能力及び負荷状態を管理する。クライアント計算機からの所在問い合わせの要求に対して、所在管理手段は、そのサービスを提供可能な全てのサーバ計算機の所在と処理能力・負荷状態をクライアント計算機に対して返却する。

【0011】この応答を受信したクライアント計算機は、処理能力・負荷状態の情報を保持する。処理能力・負荷状態の情報をもとに複数のサーバ計算機から1つのサーバ計算機を選択する。例えば、各サーバ計算機へのアクセス頻度を（処理能力÷負荷状態）の値をもとに比例配分する。

【0012】この方式により、あるサービスの利用開始時点での負荷状態を加味したサーバ計算機の負荷分散を、所在管理手段への所在の問い合わせと同時に実現することができる。これは、負荷分散のための付加的なトラヒックが発生しないことを意味する。

【0013】さらに本発明では、負荷状態が時間帯や計算機の故障などにより変化する場合を考慮して、クライアント計算機に配布されたサーバ計算機の処理能力・負荷状態の情報を更新するために2種類の手段を提供している。

【0014】第1は、クライアント計算機側からの要求に対する応答を返却する時点のサーバ計算機の処理能力・負荷状態を応答に設定して返却する。応答を受信したクライアント計算機は、保持していたサーバ計算機の処理能力・負荷状態を返却された値で逐次更新する。

【0015】第2は、クライアント計算機側でサーバ計算機からの応答時間の統計を取り、所在管理から受け取った処理能力・負荷状態の情報から決定した各サーバ計算機へのアクセス頻度を更新する。どちらの方法も負荷分散のためのトラヒックを発生させることなく、最新の負荷状態の反映が可能となる。

【0016】

【実施例】以下、本発明の一実施例を図面を参照して説明する。図1は、本発明の一実施例に係わる複数の計算機をネットワークで接続した計算機クラスタの全体構成を示すブロック図である。

【0017】図1において、1はネットワークである。ネットワーク1には、例えば、サーバ計算機2－1，2－2，2－3，2－4、及びクライアント計算機3－1，3－2，3－3が接続されている。

【0018】サーバ計算機2－1，2－2，2－3，2－4には、それぞれを識別するためのサーバ名（サーバ計算機名）が、"S1"，"S2"，"S3"，"S4"と設定されているものとする。

【0019】サーバ名"S1"のサーバ計算機2－1では、サービスA及びサービスBを提供するサーバプログラム2－11，2－12が動作している。また、サーバ名"S2"のサーバ計算機2－2では、サービスA及びサービスBを提供するサーバプログラム2－21，2－22が動作している。サーバ名"S3"のサーバ計算機2－3では、サービスA及びサービスCを提供するサーバプログラム2－31，2－32が動作している。サーバ名"S4"のサーバ計算機2－4には、サーバ所在管理部2－41とサーバ所在管理DB（データベース）2－42が存在する。

【0020】サーバ所在管理部2－41は、サーバ所在管理DB2－42に登録された情報を参照して、他のサーバ計算機からの問い合わせに応じたサーバ所在管理処理を行なう。

【0021】サーバ所在管理DB2－42は、各サーバ計算機上で動作するサービスを示すサービス識別子と、各サービス識別子が示すサービスが動作するサーバ計算機の所在を示す情報を格納している。図2には、サーバ所在管理DB2－42に登録された情報の一例を示している。

【0022】サーバ所在管理DB2－42には、図1に示す各サーバ計算機が提供するサービスに対応して、処理能力と負荷状態が設定されている。例えば、サービス識別子Aによって示されるサービスAは、サーバ名"S1"，"S2"，"S3"のサーバ計算機2－1，2－2，2－3上で提供されることを示している。また、サーバ名"S1"のサーバ計算機2－1の処理能力は、「100」であり、現在の負荷状態は「20」であることを表している。なお、図2に示す処理能力、負荷状態の値は、実装に依存するためこれらの値は、一例である。

【0023】次に、本実施例の動作について説明する。ここでは、クライアント名"C1"のクライアント計算機3－1が、サービス識別子Bで識別されるサービスBを要求した場合を例にして動作を説明する。なお、クライアント計算機3－1には、サーバ計算機2－4からサーバ計算機の所在を示す情報を保持するための保持手段3－1a、保持手段3－1aによって保持された情報をもとにサービスを要求すべきサーバ計算機を選択する選択手段3－1bが設けられている。

【0024】図3にクライアント計算機3－1とサーバ計算機2－4の通信シーケンスの例を示す。現在、サーバ名"S4"のサーバ計算機2－4上で所在管理部2－41が動作しているため、クライアント計算機3－1は、サーバ計算機2－4に対して、サービス識別子Bを指定して、サービス識別子Bで識別されるサービスを提

Sophos Ex. 1002
Page 568 of 683

供するサーバ計算機の所在の問い合わせ要求を発行する。

【００２５】所在管理部２－４１は、所在問い合わせ要求を受けると、指定されたサービス識別子Ｂをもとにサーバ所在管理ＤＢ２－４２を検索する。所在管理部２－４１は、サービス識別子Ｂで識別されるサービスを提供するサーバ計算機に関する情報を所在問い合わせ応答として、クライアント計算機３－１へ返却する。

【００２６】クライアント計算機３－１は、サーバ計算機２－４からの所在問い合わせ応答（サーバ計算機の所在に関する情報）を保持する。この場合、サービスＢが提供されるサーバ計算機２－１（サーバ名“Ｓ１”）とサーバ計算機２－２（サーバ名“Ｓ２”）のそれぞれの処理能力・負荷状態が保持される。

【００２７】サーバ計算機の所在に関する情報を取得したクライアント計算機３－１は、サーバの候補であるサーバ名“Ｓ１”，“Ｓ２”のサーバ計算機２－１，２－２の処理能力と負荷状態から処理を依頼するサーバ計算機を選択する。

【００２８】この例では、サーバ名“Ｓ１”のサーバ計算機２－１の処理能力がサーバ名“Ｓ２”のサーバ計算機２－２の２倍である。またサーバ名“Ｓ１”のサーバ計算機２－１の負荷状態がサーバ名“Ｓ２”のサーバ計算機２－２の１／２である。

【００２９】クライアント計算機３－１は、これらの情報をもとに、サービス識別子Ｂで識別されるサービスを要求された場合、例えば、８０％の確率でサーバ名“Ｓ１”のサーバ計算機２－１へ振り分け、２０％の確率でサーバ名“Ｓ２”のサーバ計算機へ振り分けるようにして負荷分散を行なう。

【００３０】なお、処理能力と負荷状態を示す値をもとに、どのようにサーバ計算機を振り分けるかは、要求される負荷分散のレベルの範囲内であれば、任意に設定しておくことができる。例えば、各サーバ計算機へのアクセス頻度を（処理能力÷負荷状態）の値をもとに比例配分するように設定しておくこともできる。

【００３１】クライアント計算機３－１は、前述のようにして取得したサーバ計算機の所在に関する情報を使って、サービス要求の振り分けを行なうが、時間が経過すると各サーバ計算機の負荷状態や処理能力が変化していく可能性がある。

【００３２】これに対して、サーバ計算機の負荷状態や処理能力の変化を負荷分散の制御に反映させるため、クライアント計算機３－１からのサービス要求に対する応答（サービス応答）に、その時点でのサーバ計算機の処理能力と負荷状態を設定して通知する。

【００３３】図４にクライアント計算機３－１とサーバ計算機４－１，４－２との間のサービス要求と応答の通信シーケンスの例を示す。なお、クライアント計算機３－１にはサーバ計算機からの通知に基づいて、保持手段３－１ａに保持された情報を更新する更新手段３－１ｃが設けられている。

【００３４】クライアント計算機３－１は、図４（ａ）（ｃ）において、それぞれサーバ計算機２－１，２－２にサービス要求（要求パラメータ）を送出する。各サービス要求に応じて、サーバ計算機２－１，２－２は、それぞれ図４（ｂ）（ｄ）において、サービス識別子、サーバ名、処理能力、及び負荷状態を示す情報を含むサービス応答（応答パラメータ）を、クライアント計算機３－１に返送する。

【００３５】クライアント計算機３－１は、サーバ計算機２－１，２－２から返送されたサービス応答（応答パラメータ）に含まれる前述した各情報を保持する。また、サーバ計算機２－１，２－２は、サービス識別子，サーバ名、さらには時間の経過に伴って変化した後の負荷状態や処理能力を示す値を、サービス要求に対する応答としてクライアント計算機３－１に返す。

【００３６】クライアント計算機３－１は、このサービス応答で取得した情報で、先に保持していた情報を置き換えることにより、新しい状況を反映した負荷分散が可能となる。クライアント計算機３－１は、置き換えた後の情報に基づいて、サービス要求の負荷分散を行なう。

【００３７】次に、サービス応答として、その時点でのサーバ計算機の処理能力・負荷状態を返却する機能がサーバ計算機側にない場合には、次のようにして保持された情報の更新を行なう。なお、クライアント計算機３－１は、サーバ計算機に対するサービス要求の応答時間を統計的に集計する集計手段３－１ｄを有し、更新手段３－１ｃは、集計手段３－１ｄによる集計結果に応じて保持手段３－１ａに保持された情報を更新する。

【００３８】クライアント計算機３－１は、サーバ計算機に関する情報（処理能力・負荷状態の情報）を保持し、この情報に基づいて各サーバ計算機へのアクセス頻度を決定している。

【００３９】一方で、クライアント計算機３－１は、自分が要求した各サーバ計算機に対するサービス要求の応答時間を統計的に集計する。そして、クライアント計算機３－１は、応答時間に対する集計結果をもとに、各サーバ計算機への振り分けの頻度（確率）を更新する。

【００４０】このようにして、クライアント計算機は、要求されたサービスの所在問い合わせと同時に、負荷分散のための情報を取得し、自律的に負荷分散を実現することができる。本発明では、負荷分散のために新たにクライアント／サーバ間の通信トラヒックが発生することはない。

【００４１】さらに、本発明では、サービス要求に対するサービス応答に、その時点でのサーバ計算機の処理能力・負荷状態を設定することにより、負荷分散のための最新の情報をクライアント計算機が保持することが可能となる。

Sophos Ex. 1002
Page 569 of 683

【００４２】また、クライアント計算機側でサービス要求に対するサービス応答の応答時間を統計的に集計することにより、負荷分散のための最新の情報をクライアント計算機が保持することができる。

【００４３】これらの機能は、クライアント／サーバ型のリモートプロシジャコールを実現するための基本的な機能として実装することが可能であるため、利用者は、サーバ計算機の所在や負荷分散を意識する必要はなく、負担が軽減される。

【００４４】

【発明の効果】以上説明したように本発明によれば、柔軟性のある負荷分散が可能となるものである。すなわち、クライアント計算機が要求するサービスを提供するサーバ計算機の所在を所在管理手段に問い合わせると、全てのサーバ計算機の候補の所在とその処理能力・負荷状態に関する情報が返却され、この情報に基づいてサービスを要求すべきサーバ計算機を決定することにより負荷分散を実現する。さらにサーバ計算機の処理能力や負荷状態の変化に対応して、クライアント計算機からの情報を更新することによって、負荷分散も柔軟に対応させることができる。

【図面の簡単な説明】

【図１】本発明の一実施例に係わる複数の計算機をネットワークで接続した計算機クラスタの全体構成を示すブロック図。

【図２】図１中のサーバ計算機２－４のサーバ所在管理ＤＢ２－４２が保持する情報の一例を示す図。

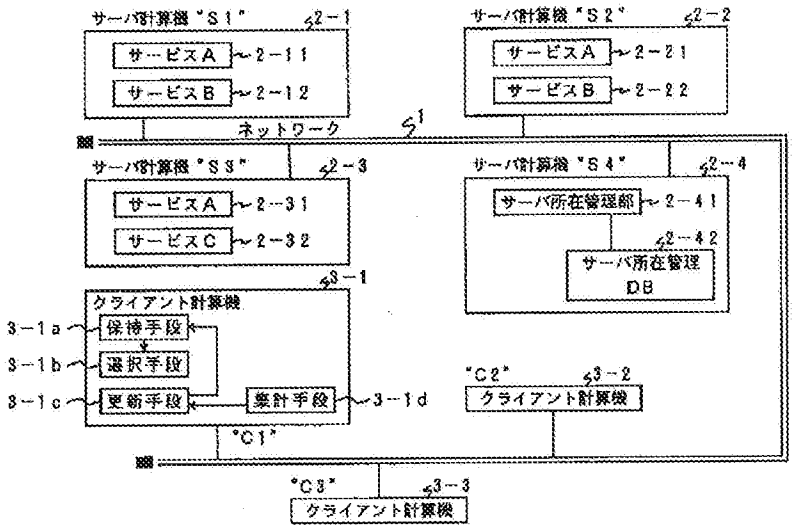
【図３】本実施例においてクライアント計算機３－１がサーバ計算機２－４のサーバ所在管理部２－４１に対して、所在問い合わせ要求を発行して、所在問い合わせ応答が返却されるまでの通信シーケンスの一例を示す図。

【図４】本実施例においてクライアント計算機３－１がサーバ計算機２－１，２－２に対して、サービス要求を発行し、サービス応答と同時にサーバ計算機の処理能力・負荷状態の情報を取得する通信シーケンスの一例を示す図。

【符号の説明】

１…ネットワーク，２－１，２－２，２－３，２－４…サーバ計算機、２－４１…サーバ所在管理部、２－４２…サーバ所在管理データベース、３－１，３－２，３－３…クライアント計算機。

【図１】



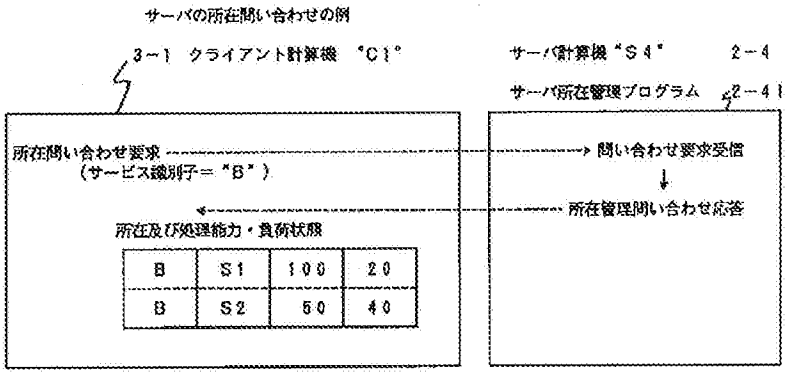
Sophos Ex. 1002
Page 570 of 683

【図2】

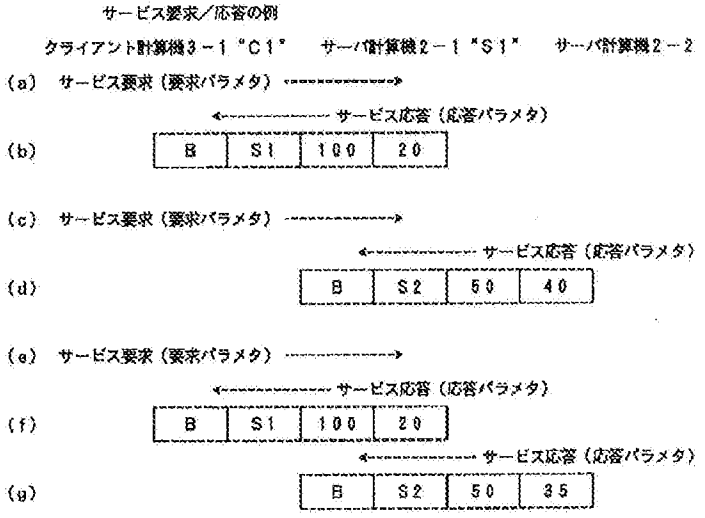
2－42　サーバ所在管理データベース

サービス識別子	サーバ名	処理能力	負荷状態
A	"S1"	100	20
A	"S2"	50	40
A	"S3"	80	20
B	"S1"	100	20
B	"S2"	50	40
C	"S3"	80	20

【図3】



【図4】



Sophos Ex. 1002
Page 571 of 683

Patent Translate
Powered by EPO and Google

Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

DESCRIPTION JPH0844677

[0001]

The present invention relates to, on more than one computer is a computer cluster, which is connected to the network, on the load-balancing mechanism of the server computer in the case of performing the processing of client / server type.

[0002]

Conventionally, in a computer cluster in which a plurality of computers connected by a network, that If you want to distribute the processing to a plurality of computers, to secure the server computer which provides the service, leave to determine the pre-load balancing the were common.

[0003]

[Invention Problems to be Solved] In this way, in the conventional distributed processing system, was to determine the pre-load distribution for each server computer. However, previously the fixedly previously determined load distribution, it can be successively reflect factors such as

Sophos Ex. 1002
Page 572 of 683

failure of the load conditions change and a computer for controlling the load distribution becomes difficult.

[0004]

Further, in order to keep determined beforehand fixedly load balancing requires sufficient pre-analysis for the business content, were not flexible response to changes in the business content change or computer configuration. The present invention has been made in view of the above problems, and an object thereof is to provide a distributed processing system capable of flexible load distribution.

[0005]

In order to achieve the object of the present invention is, in a distributed processing system of the client / server you connect more than one computer to the network, based on the service identifier that uniquely a desired service, indicated by the service identifier location of the server computer for providing services, processing capacity of the server computer, and a location management unit capable of determining the load status, the information processing capacity and load state of at least one server computer obtained from the location management device holding means for holding client computer side, based on the information of the processing capacity and load state of being held by the holding means, and selection means for selecting a server computer should require service desired by the client computer side comprising, for a plurality of server computers that provide the same service, and performs load balancing by the selection means of the client computer side.

[0006]

Also, the response to changes in the processing capacity and load state of the server computer, further comprising updating means for said client computer updates the information of the processing capacity and load state of the server computer which is held by said holding server and performing successively updated while load balancing said information in response to a change in the computer side situation.

[0007]

Sophos Ex. 1002
Page 573 of 683

In addition, the holding to the original and counting means, the statistics of the response time which is determined by the counting means in which the client computer is statistically aggregate the response time of the server computer, which were selected by the selection means in the client computer side It means further comprising updating means for updating the information on the processing power and the load state of the server computer which is held by, characterized by performing successively updated while load balancing said information in response to a change in status of the server computer side to.

[0008]

[Action] In general, if you want to implement the distributed processing of client / server type on a computer cluster connected plurality of computers at the network, globally identifiable identifier in the computer cluster is given. When you request a certain client computer services, the inquiry request is issued to the location management in order to obtain the location of the server computer that provides the service from the identifier corresponding to the service. Location management is, usually, one exists in the computer cluster, which you have the database that records the location of the server computer which provides the identifier and the service of the service. It searches the database to request the location of the inquiry from the client computer, to return the location of the server computer.

[0009]

The present invention in distributed processing in a client / server on computer cluster connecting a plurality of computers in the network, is used to achieve load balancing for a server computer for providing services.

[0010]

Location management means, in addition to the location of the server computer for providing services, to manage the throughput and load status of the server computer. To request the location of the inquiry from the client computer, location management means, to return the location and processing power, load state of all of the server computer that can provide the service to the client computer.

Sophos Ex. 1002
Page 574 of 683

[0011]

The client computer which has received this reply, holds the information processing capacity and load conditions. The information of the processing capacity and load conditions to select one of the server computer from multiple server computer to the original. For example, based on the proportional allocation of the value of the frequency of access to each server computer (processing capacity ÷ load state).

[0012]

By this method, the load distribution of the server computer which takes into account the load state of the usage start time of a service can be implemented simultaneously with the location of the inquiry to the location management device. This means that additional traffic for load balancing does not occur.

[0013]

Further, in the present invention, in consideration of a case where the load state is changed as a result of a malfunction of hours or computer, two kinds of means to update the information of the processing capacity and load state of the server computer which is distributed to the client computer It has to offer.

[0014]

The first is to return the processing capacity and load state of the server computer at the time you plan to return the response to the request from the client computer side is set in the response. The client computer which has received the response is sequentially updated with the return processing capacity and load state of the server computer that held value.

[0015]

Sophos Ex. 1002
Page 575 of 683

Secondly, take the response time statistics from the server computer on the client computer side, and updates the frequency of access to each server computer determined from the processing capacity of-load state information received from the location management. Without both methods generate the traffic for load balancing, it is possible to reflect the latest load conditions.

[0016]

Example will be described below with reference to the accompanying drawings an embodiment of the present invention. Figure 1 is a block diagram showing an overall configuration of a computer cluster connected a plurality of computers on a network according to an embodiment of the present invention.

[0017]

In Figure 1, 1 denotes a network. To network 1, for example, the server computer 2-1, 2-2, 2-3, 2-4, and the client computer 3-1, 3-2, and 3-3 are connected.

[0018]

The server computer 2-1, 2-2, 2-3, 2-4, server name to identify each (server computer name), "S1", "S2", "S3", "S4" It assumed to be set with the.

[0019]

In the server computer 2-1 server name "S1", server program 2-11,2-12 to provide a service A and service B is running. In addition, the server computer 2-2 of the server name "S2", the server program 2-21,2-22 to provide a service A and service B is running. In the server computer 2-3 of the server name "S3", the server program 2-31,2-32 to provide services A and C service is running. The server computer 2-4 of the server name "S4", server location management section 2-41 and the server location management DB (database) 2-42 is present.

Sophos Ex. 1002
Page 576 of 683

[0020]

Server location management unit 2-41 refers to the information registered in the server location management DB2-42, performs server location management processing according to an inquiry from another server computer.

[0021]

Server location management DB2-42 stores a service identifier indicating a service that runs on each server computer machine, information indicating the location of a server computer service indicated by the service identifier to operate. Figure 2 shows an example of the information that has been registered in the server location management DB2-42.

[0022]

The server location management DB2-42, in correspondence with the services that the server computer shown in FIG. 1 is provided, processing power and the load state is set. For example, the service A shown by a service identifier A shows that provided on the server computer 2-1, 2-2 and 2-3 of the server name "S1", "S2", "S3". Further, the processing capacity of the server computer 2-1 server name "S1" is "100", the current load status indicates that it is "20". The processing capability shown in FIG. 2, the value of the load condition, these values because it depends on the implementation, is one example.

[0023]

Next, the operation of the present embodiment. Here, the client computer 3-1 client name "C1", will be described the operation as an example when requesting a service B identified by the service identifier B. Note that the client computer 3-1, the holding means 3-1a for holding information indicating the location of the server computer from the server computer 2-4, based on the service information which is held by the holding means 3-1a selection means 3-1b is provided to select a server computer to be requested.

[0024]

Sophos Ex. 1002
Page 577 of 683

Figure 3 shows an example of a communication sequence of the client computer 3-1 and the server computer 2-4. Currently, since the location management unit 2-41 on the server computer 2-4 of the server name "S4" is running, the client computer 3-1, to the server computer 2-4, specify the service identifier B on, and issues a inquiry request to the location of the server computer which provides a service identified by the service identifier B.

[0025]

Location management section 2-41, when receiving the location query request, to find the server location management DB2-42 on the basis of the specified service identifier B. Location management section 2-41, the information about the server computer which provides the services that are identified by the service identifier B as the location query response, to return to the client computer 3-1.

[0026]

Client computer 3-1, to retain the location inquiry response from the server computer 2-4 (information about the location of the server computer). In this case, each of the processing capacity and load state of the server computer 2-1 service B is provided (server name "S1") and server computer 2-2 (server name "S2") is held.

[0027]

Client computer 3-1 to obtain information about the location of the server computer, the server name is the server of the candidate "S1", "S2" request the processing load from the state and processing power of the server computer 2-1, 2-2 to select a server computer for.

[0028]

In this example, the processing power of the server computer 2-1 server name "S1" is twice the server computer 2-2 of the server name "S2". Also load state of the server computer 2-1 server

Sophos Ex. 1002
Page 578 of 683

name "S1" is 1/2 of the server computer 2-2 of the server name "S2".

[0029]

The client computer 3-1, based on these information, when it is requested a service identified by the service identifier B, for example, assignment to the server computer 2-1 server name "S1" with 80% probability, with a probability of 20% so as to distribute to the server computer of the server name "S2" to perform load balancing.

[0030]

Incidentally, based on the value indicating the load condition and capacity, it is how distributing the server computer, if it is within the scope of the required load balancing level can be set arbitrarily. For example, it is also possible to set so that the original in proportioning the value of the access frequency to each server computer (throughput ÷ load condition).

[0031]

The client computer 3-1 uses the information about the whereabouts of the acquired server computer as described above, performs the allocation of the service request, load conditions and the processing capability of each server computer after a lapse of time will change there is a possibility.

[0032]

In contrast, to reflect the change in the load status and the processing capacity of the server computer to control the load distribution, the response to the service request from the client computer 3-1 (service reply), the processing of the server computer at that time to inform and set the capacity and load state.

[0033]

Sophos Ex. 1002
Page 579 of 683

Figure 4 shows an example of a service request with the communication sequence of response between the client computer 3-1 and the server computer 4-1, 4-2. Incidentally, the client computer 3-1 based on the notification from the server computer, updating means 3-1c for updating the information held in the holding unit 3-1a are provided.

[0034]

Client computer 3-1, in Figure 4 (a) (c), and sends each service request to the server computer 2-1 and 2-2 the (request parameter). Depending on the respective service request, the server computer 2-1 and 2-2 in FIGS 4 (b) (d), service identifier, the server name, processing power, and service response including information indicating the load state (Response parameters), and returns it to the client computer 3-1.

[0035]

The client computer 3-1, to hold each information described above is included in the service response sent back from the server computer 2-1 and 2-2 (response parameters). Further, server computer 2-1 and 2-2, service identifier, the server name, and further a value indicating the load state and processing capability after change over time, the client computer as a response to a service request 3- return to 1.

[0036]

The client computer 3-1, in the information obtained in the service response, by replacing the information held previously, the load distribution that reflects the new situation is possible. The client computer 3-1, based on the information after replacing performs load balancing service requests.

[0037]

Then, as the service response, if the ability to return the processing capacity and load state of the server computer at that time is not in the server computer side, it updates the information held in

Sophos Ex. 1002
Page 580 of 683

the following manner. In addition, the client computer 3-1 has an aggregate means 3-1d to statistically aggregate the response time of the service request to the server computer, updating means 3-1c, depending on the counting result of the counting means 3-1d to update the information that is held by the holding means 3-1a.

[0038]

The client computer 3-1, holds information (processing capability and information on load status) about the server computer, and determines the frequency of access to each server computer on the basis of this information.

[0039]

On the other hand, the client computer 3-1, to statistically aggregate the response time of the service request for each server computer that you have requested. Then, the client computer 3-1, based on the aggregate results for the response time, to update the frequency (probability) of the distribution to each server computer.

[0040]

In this way, the client computer, at the same time as the requested service of the location query to obtain information for load balancing, it is possible to realize an autonomous load balancing. In the present invention, communication traffic between the new client / server for load balancing does not occur.

[0041]

Furthermore, in the present invention, the service response to the service request, by setting the processing capacity and load state of the server computer at that time, the latest information for load balancing client computer can be held .

[0042]

Sophos Ex. 1002
Page 581 of 683

Further, by statistically aggregated response time of the service response to the service request on the client computer side, the latest information for the load distribution can be client computer has.

[0043]

These functions, since it can be implemented as a basic function for implementing remote procedure call client / server type, the user need not be aware of the location and load balancing of the server computer, the burden is reduced.

According to the present invention, as described above, according to the present invention, in which a flexible load balancing is possible. In other words, when the inquiry to the location management means the location of the server computer that provides a service to the client computer requests, information about the whereabouts and its processing capacity and load state of the candidate of all of the server computer is returned, on the basis of this information service to achieve load balancing by determining the server computer should require. Further in response to changes in throughput or load state of the server computer by updating the information from the client computer, it is possible to load distribution also flexibly correspond.

Sophos Ex. 1002
Page 582 of 683

Patent Translate
Powered by EPO and Google

Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

CLAIMS JPH0844677

In a plurality of computers to client / server distributed processing system that was connected by a network, based on the service identifier that uniquely a desired service, the location of the server computer that provides a service in which the service identifier is shown, the same server computer processing power, and a location management unit capable of determining the load state, and a holding means for holding the information processing capacity and load state of at least one server computer obtained from the location management device in a client computer side, the holding based on the information processing capacity and load state of being held by means, selection means for selecting a server computer should require service desired by the client computer side, to a plurality of server computers that provide the same service , distributed processing system and performs load balancing by the selection means of the client computer side. The in response to changes in processing capacity and load state of the server computer, said client computer further comprises an updating means for updating the information on the processing power and the load state of the server computer which is held by the holding, the server computer side distributed processing system of claim 1, wherein the performing successively updated while the load balancing the information according to the circumstances change. And counting means that the client computer is statistically aggregate the response time of the server computer, which were selected by the selection means in the client computer side, by the holding means on the basis of the response time of the statistical information obtained by the counting means and updating means for updating the information of the processing capacity and load conditions of the retained server computer, further comprising, and characterized by performing successively updated while load balancing said information in response to a change in status of the server computer side distributed processing system according to claim 1.

Sophos Ex. 1002
Page 583 of 683

Patent Translate
Powered by EPO and Google

Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

DESCRIPTION JPH0844677

[0001]

The present invention relates to, on more than one computer is a computer cluster, which is connected to the network, on the load-balancing mechanism of the server computer in the case of performing the processing of client / server type.

[0002]

Conventionally, in a computer cluster in which a plurality of computers connected by a network, that If you want to distribute the processing to a plurality of computers, to secure the server computer which provides the service, leave to determine the pre-load balancing the were common.

[0003]

[Invention Problems to be Solved] In this way, in the conventional distributed processing system, was to determine the pre-load distribution for each server computer. However, previously the fixedly previously determined load distribution, it can be successively reflect factors such as

Sophos Ex. 1002
Page 584 of 683

failure of the load conditions change and a computer for controlling the load distribution becomes difficult.

[0004]

Further, in order to keep determined beforehand fixedly load balancing requires sufficient pre-analysis for the business content, were not flexible response to changes in the business content change or computer configuration. The present invention has been made in view of the above problems, and an object thereof is to provide a distributed processing system capable of flexible load distribution.

[0005]

In order to achieve the object of the present invention is, in a distributed processing system of the client / server you connect more than one computer to the network, based on the service identifier that uniquely a desired service, indicated by the service identifier location of the server computer for providing services, processing capacity of the server computer, and a location management unit capable of determining the load status, the information processing capacity and load state of at least one server computer obtained from the location management device holding means for holding client computer side, based on the information of the processing capacity and load state of being held by the holding means, and selection means for selecting a server computer should require service desired by the client computer side comprising, for a plurality of server computers that provide the same service, and performs load balancing by the selection means of the client computer side.

[0006]

Also, the response to changes in the processing capacity and load state of the server computer, further comprising updating means for said client computer updates the information of the processing capacity and load state of the server computer which is held by said holding server and performing successively updated while load balancing said information in response to a change in the computer side situation.

[0007]

Sophos Ex. 1002
Page 585 of 683

In addition, the holding to the original and counting means, the statistics of the response time which is determined by the counting means in which the client computer is statistically aggregate the response time of the server computer, which were selected by the selection means in the client computer side It means further comprising updating means for updating the information on the processing power and the load state of the server computer which is held by, characterized by performing successively updated while load balancing said information in response to a change in status of the server computer side to.

[0008]

[Action] In general, if you want to implement the distributed processing of client / server type on a computer cluster connected plurality of computers at the network, globally identifiable identifier in the computer cluster is given. When you request a certain client computer services, the inquiry request is issued to the location management in order to obtain the location of the server computer that provides the service from the identifier corresponding to the service. Location management is, usually, one exists in the computer cluster, which you have the database that records the location of the server computer which provides the identifier and the service of the service. It searches the database to request the location of the inquiry from the client computer, to return the location of the server computer.

[0009]

The present invention in distributed processing in a client / server on computer cluster connecting a plurality of computers in the network, is used to achieve load balancing for a server computer for providing services.

[0010]

Location management means, in addition to the location of the server computer for providing services, to manage the throughput and load status of the server computer. To request the location of the inquiry from the client computer, location management means, to return the location and processing power, load state of all of the server computer that can provide the service to the client computer.

Sophos Ex. 1002
Page 586 of 683

[0011]

The client computer which has received this reply, holds the information processing capacity and load conditions. The information of the processing capacity and load conditions to select one of the server computer from multiple server computer to the original. For example, based on the proportional allocation of the value of the frequency of access to each server computer (processing capacity ÷ load state).

[0012]

By this method, the load distribution of the server computer which takes into account the load state of the usage start time of a service can be implemented simultaneously with the location of the inquiry to the location management device. This means that additional traffic for load balancing does not occur.

[0013]

Further, in the present invention, in consideration of a case where the load state is changed as a result of a malfunction of hours or computer, two kinds of means to update the information of the processing capacity and load state of the server computer which is distributed to the client computer It has to offer.

[0014]

The first is to return the processing capacity and load state of the server computer at the time you plan to return the response to the request from the client computer side is set in the response. The client computer which has received the response is sequentially updated with the return processing capacity and load state of the server computer that held value.

[0015]

Sophos Ex. 1002
Page 587 of 683

Secondly, take the response time statistics from the server computer on the client computer side, and updates the frequency of access to each server computer determined from the processing capacity of-load state information received from the location management. Without both methods generate the traffic for load balancing, it is possible to reflect the latest load conditions.

[0016]

Example will be described below with reference to the accompanying drawings an embodiment of the present invention. Figure 1 is a block diagram showing an overall configuration of a computer cluster connected a plurality of computers on a network according to an embodiment of the present invention.

[0017]

In Figure 1, 1 denotes a network. To network 1, for example, the server computer 2-1, 2-2, 2-3, 2-4, and the client computer 3-1, 3-2, and 3-3 are connected.

[0018]

The server computer 2-1, 2-2, 2-3, 2-4, server name to identify each (server computer name), "S1", "S2", "S3", "S4" It assumed to be set with the.

[0019]

In the server computer 2-1 server name "S1", server program 2-11,2-12 to provide a service A and service B is running. In addition, the server computer 2-2 of the server name "S2", the server program 2-21,2-22 to provide a service A and service B is running. In the server computer 2-3 of the server name "S3", the server program 2-31,2-32 to provide services A and C service is running. The server computer 2-4 of the server name "S4", server location management section 2-41 and the server location management DB (database) 2-42 is present.

Sophos Ex. 1002
Page 588 of 683

[0020]

Server location management unit 2-41 refers to the information registered in the server location management DB2-42, performs server location management processing according to an inquiry from another server computer.

[0021]

Server location management DB2-42 stores a service identifier indicating a service that runs on each server computer machine, information indicating the location of a server computer service indicated by the service identifier to operate. Figure 2 shows an example of the information that has been registered in the server location management DB2-42.

[0022]

The server location management DB2-42, in correspondence with the services that the server computer shown in FIG 1 is provided, processing power and the load state is set. For example, the service A shown by a service identifier A shows that provided on the server computer 2-1, 2-2 and 2-3 of the server name "S1", "S2", "S3". Further, the processing capacity of the server computer 2-1 server name "S1" is "100", the current load status indicates that it is "20". The processing capability shown in FIG. 2, the value of the load condition, these values because it depends on the implementation, is one example.

[0023]

Next, the operation of the present embodiment. Here, the client computer 3-1 client name "C1", will be described the operation as an example when requesting a service B identified by the service identifier B. Note that the client computer 3-1, the holding means 3-1a for holding information indicating the location of the server computer from the server computer 2-4, based on the service information which is held by the holding means 3-1a selection means 3-1b is provided to select a server computer to be requested.

[0024]

Sophos Ex. 1002
Page 589 of 683

Figure 3 shows an example of a communication sequence of the client computer 3-1 and the server computer 2-4. Currently, since the location management unit 2-41 on the server computer 2-4 of the server name "S4" is running, the client computer 3-1, to the server computer 2-4, specify the service identifier B on, and issues a inquiry request to the location of the server computer which provides a service identified by the service identifier B.

[0025]

Location management section 2-41, when receiving the location query request, to find the server location management DB2-42 on the basis of the specified service identifier B. Location management section 2-41, the information about the server computer which provides the services that are identified by the service identifier B as the location query response, to return to the client computer 3-1.

[0026]

Client computer 3-1, to retain the location inquiry response from the server computer 2-4 (information about the location of the server computer). In this case, each of the processing capacity and load state of the server computer 2-1 service B is provided (server name "S1") and server computer 2-2 (server name "S2") is held.

[0027]

Client computer 3-1 to obtain information about the location of the server computer, the server name is the server of the candidate "S1", "S2" request the processing load from the state and processing power of the server computer 2-1, 2-2 to select a server computer for.

[0028]

In this example, the processing power of the server computer 2-1 server name "S1" is twice the server computer 2-2 of the server name "S2". Also load state of the server computer 2-1 server

Sophos Ex. 1002
Page 590 of 683

name "S1" is 1/2 of the server computer 2-2 of the server name "S2".

[0029]

The client computer 3-1, based on these information, when it is requested a service identified by the service identifier B, for example, assignment to the server computer 2-1 server name "S1" with 80% probability, with a probability of 20% so as to distribute to the server computer of the server name "S2" to perform load balancing.

[0030]

Incidentally, based on the value indicating the load condition and capacity, it is how distributing the server computer, if it is within the scope of the required load balancing level can be set arbitrarily. For example, it is also possible to set so that the original in proportioning the value of the access frequency to each server computer (throughput ÷ load condition).

[0031]

The client computer 3-1 uses the information about the whereabouts of the acquired server computer as described above, performs the allocation of the service request, load conditions and the processing capability of each server computer after a lapse of time will change there is a possibility.

[0032]

In contrast, to reflect the change in the load status and the processing capacity of the server computer to control the load distribution, the response to the service request from the client computer 3-1 (service reply), the processing of the server computer at that time to inform and set the capacity and load state.

[0033]

Sophos Ex. 1002
Page 591 of 683

Figure 4 shows an example of a service request with the communication sequence of response between the client computer 3-1 and the server computer 4-1, 4-2. Incidentally, the client computer 3-1 based on the notification from the server computer, updating means 3-1c for updating the information held in the holding unit 3-1a are provided.

[0034]

Client computer 3-1, in Figure 4 (a) (c), and sends each service request to the server computer 2-1 and 2-2 the (request parameter). Depending on the respective service request, the server computer 2-1 and 2-2 in FIGS 4 (b) (d), service identifier, the server name, processing power, and service response including information indicating the load state (Response parameters), and returns it to the client computer 3-1.

[0035]

The client computer 3-1, to hold each information described above is included in the service response sent back from the server computer 2-1 and 2-2 (response parameters). Further, server computer 2-1 and 2-2, service identifier, the server name, and further a value indicating the load state and processing capability after change over time, the client computer as a response to a service request 3- return to 1.

[0036]

The client computer 3-1, in the information obtained in the service response, by replacing the information held previously, the load distribution that reflects the new situation is possible. The client computer 3-1, based on the information after replacing performs load balancing service requests.

[0037]

Then, as the service response, if the ability to return the processing capacity and load state of the server computer at that time is not in the server computer side, it updates the information held in

Sophos Ex. 1002
Page 592 of 683

the following manner. In addition, the client computer 3-1 has an aggregate means 3-1d to statistically aggregate the response time of the service request to the server computer, updating means 3-1c, depending on the counting result of the counting means 3-1d to update the information that is held by the holding means 3-1a.

[0038]

The client computer 3-1, holds information (processing capability and information on load status) about the server computer, and determines the frequency of access to each server computer on the basis of this information.

[0039]

On the other hand, the client computer 3-1, to statistically aggregate the response time of the service request for each server computer that you have requested. Then, the client computer 3-1, based on the aggregate results for the response time, to update the frequency (probability) of the distribution to each server computer.

[0040]

In this way, the client computer, at the same time as the requested service of the location query to obtain information for load balancing, it is possible to realize an autonomous load balancing. In the present invention, communication traffic between the new client / server for load balancing does not occur.

[0041]

Furthermore, in the present invention, the service response to the service request, by setting the processing capacity and load state of the server computer at that time, the latest information for load balancing client computer can be held .

[0042]

Sophos Ex. 1002
Page 593 of 683

Further, by statistically aggregated response time of the service response to the service request on the client computer side, the latest information for the load distribution can be client computer has.

[0043]

These functions, since it can be implemented as a basic function for implementing remote procedure call client / server type, the user need not be aware of the location and load balancing of the server computer, the burden is reduced.

According to the present invention, as described above, according to the present invention, in which a flexible load balancing is possible. In other words, when the inquiry to the location management means the location of the server computer that provides a service to the client computer requests, information about the whereabouts and its processing capacity and load state of the candidate of all of the server computer is returned, on the basis of this information service to achieve load balancing by determining the server computer should require. Further in response to changes in throughput or load state of the server computer by updating the information from the client computer, it is possible to load distribution also flexibly correspond.

Sophos Ex. 1002
Page 594 of 683

Patent Translate
Powered by EPO and Google

Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

CLAIMS JPH0844677

In a plurality of computers to client / server distributed processing system that was connected by a network, based on the service identifier that uniquely a desired service, the location of the server computer that provides a service in which the service identifier is shown, the same server computer processing power, and a location management unit capable of determining the load state, and a holding means for holding the information processing capacity and load state of at least one server computer obtained from the location management device in a client computer side, the holding based on the information processing capacity and load state of being held by means, selection means for selecting a server computer should require service desired by the client computer side, to a plurality of server computers that provide the same service , distributed processing system and performs load balancing by the selection means of the client computer side. The in response to changes in processing capacity and load state of the server computer, said client computer further comprises an updating means for updating the information on the processing power and the load state of the server computer which is held by the holding, the server computer side distributed processing system of claim 1, wherein the performing successively updated while the load balancing the information according to the circumstances change. And counting means that the client computer is statistically aggregate the response time of the server computer, which were selected by the selection means in the client computer side, by the holding means on the basis of the response time of the statistical information obtained by the counting means and updating means for updating the information of the processing capacity and load conditions of the retained server computer, further comprising, and characterized by performing successively updated while load balancing said information in response to a change in status of the server computer side distributed processing system according to claim 1.

Sophos Ex. 1002
Page 595 of 683

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

23552 7590 04/04/2016

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER
CHIANG, JASON

ART UNIT	PAPER NUMBER
2431	

DATE MAILED: 04/04/2016

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/372,375	02/13/2012	Melvyn Morris	04584.0012USU1	2918

TITLE OF INVENTION: METHODS AND APPARATUS FOR DEALING WITH MALWARE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	07/05/2016

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

23552 7590 04/04/2016
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/372,375	02/13/2012	Melvyn Morris	04584.0012USU1	2918

TITLE OF INVENTION: METHODS AND APPARATUS FOR DEALING WITH MALWARE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	07/05/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
CHIANG, JASON	2431	726-023000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ Applicant certifying micro entity status. See 37 CFR 1.29
  NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ❑ Applicant asserting small entity status. See 37 CFR 1.27
  NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ❑ Applicant changing to regular undiscounted fee status.
  NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

Sophos Ex. 1002
Page 597 of 683

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/372,375	02/13/2012	Melvyn Morris	04584.0012USU1	2918

23552 7590 04/04/2016

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
CHIANG, JASON	

ART UNIT	PAPER NUMBER
2431	

DATE MAILED: 04/04/2016

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 13/372,375	Applicant(s) MORRIS ET AL.	
	Examiner JASON C. CHIANG	Art Unit 2431	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *02/24/2016*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1-7,9-15 and 25*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 02/24/2016
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☐ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/JASON C CHIANG/ Examiner, Art Unit 2431	/CORDELIA ZECHER/ Supervisory Patent Examiner, Art Unit 2431

1. The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 02/24/2016 has been entered.

Information Disclosure Statement

3. The Information Disclosure Statement filed on February 24, 2016 has been entered and considered, it does not change the reasons for allowance.

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JASON C. CHIANG whose telephone number is (571)270-3393. The examiner can normally be reached on 9AM to 6PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, CORDELIA P. ZECHER can be reached on (571)272-7771. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/J. C. C./
Examiner, Art Unit 2431

/CORDELIA ZECHER/
Supervisory Patent Examiner, Art Unit 2431

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13372375	MORRIS ET AL.
	Examiner	Art Unit
	JASON C CHIANG	2431

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	23	06/04/2013	JC

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor search in East	06/04/2013	JC
Text search in East of USPGPUB, USPAT, USOCR, FPRS, EPO, JPO, DERWENT, IBM_TDB	06/05/2013	JC
Inventor search in East	12/14/2013	JC
Text search in East of USPGPUB, USPAT, USOCR, FPRS, EPO, JPO, DERWENT, IBM_TDB	12/14/2013	JC
Inventor search in East	12/11/2014	JC
Text search in East of USPGPUB, USPAT, USOCR, FPRS, EPO, JPO, DERWENT, IBM_TDB	12/11/2014	JC
Inventor search in East	7/30/2015	JC
Text search in East of USPGPUB, USPAT, USOCR, FPRS, EPO, JPO, DERWENT, IBM_TDB	7/30/2015	JC
Search in East of USPGPUB, USPAT, USOCR, FPRS, EPO, JPO, DERWENT, IBM_TDB	11/13/2015	JC
Inventor search in East	3/28/2016	JC
Search in East of USPGPUB, USPAT, USOCR, FPRS, EPO, JPO, DERWENT, IBM_TDB	3/28/2016	JC

/JASON C CHIANG/ Examiner.Art Unit 2431	

INTERFERENCE SEARCH			
US Class/ CPC Symbol	**US Subclass / CPC Group**	**Date**	**Examiner**
H04L	63/14	7/30/2015	JC
G06F	21/56	7/30/2015	JC
H04L	63/14	11/13/2015	JC
G06F	21/56	11/13/2015	JC
H04L	63/14	3/28/2016	JC
G06F	21/56	3/28/2016	JC

/JASON C CHIANG/ Examiner.Art Unit 2431	

Sophos Ex. 1002
Page 604 of 683

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13372375
Filing Date	2012-02-13
First Named Inventor	Melvyn Morris
Art Unit	2431
Examiner Name	CHIANG, JASON
Attorney Docket Number	04584.0012USU1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/J.C./	1	7761912		2010-07-20	Yee et al.	
/J.C./	2	8407790		2013-03-26	Mony	
/J.C./	3	8499283		2013-07-30	Mony	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/J.C./	1	20050172338		2005-08-04	Sandu et al.	
/J.C./	2	20060161856		2006-07-20	Heir	
/J.C./	3	20080229422		2008-09-18	Hudis et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13372375
	Filing Date	2012-02-13
	First Named Inventor	Melvyn Morris
	Art Unit	2431
	Examiner Name	CHIANG, JASON
	Attorney Docket Number	04584.0012USU1

/J.C./	4	20110047594		2011-02-24	Mahaffey et al.			

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
/J.C./	1	JP 2009-500706	JP		2009-01-08			
/J.C./	2	JP H08-44677	JP		1996-02-16			

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
/J.C./	1	Chinese Patent Application No. 201280018306.9, First Office Action mailed June 2, 2015, 26 pages. (No English translation available)	
/J.C./	2	U.S. Patent Application No. 12/703,074, Amendment and Response dated November 6, 2012, 8 pages.	
/J.C./	3	U.S. Patent Application No. 12/703,074, Amendment after Allowance dated December 7, 2012, 7 pages.	
/J.C./	4	U.S. Patent Application No. 13/372,433, Amendment and Response dated January 6, 2014, 13 pages.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13372375
	Filing Date	2012-02-13
	First Named Inventor	Melvyn Morris
	Art Unit	2431
	Examiner Name	CHIANG, JASON
	Attorney Docket Number	04584.0012USU1

/J.C./	5	U.S. Patent Application No. 13/372,433, Final Rejection mailed May 9, 2014, 22 pages.	
/J.C./	6	U.S. Patent Application No. 13/372,433, Amendment and Response dated October 9, 2014, 14 pages.	
/J.C./	7	U.S. Patent Application No. 13/372,433, Non-Final Rejection mailed September 10, 2015, 16 pages.	
/J.C./	8	U.S. Patent Application No. 13/372,439, Amendment and Response dated November 4, 2013, 12 pages.	
/J.C./	9	U.S. Patent Application No. 13/372,439, Final Rejection mailed February 24, 2014, 15 pages.	
/J.C./	10	U.S. Patent Application No. 13/372,433, Amendment and Response filed February 10, 2016, 18 pages.	
/J.C./	11	Japanese Patent Application No. 2013-553909, Office Action mailed January 26, 2016, 6 pages (English Translation).	
/J.C./	12	Chinese Patent Application No. 201280018306.9, Second Office Action mailed January 11, 2016, 11 pages (English Translation).	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Jason Chiang/	Date Considered	03/28/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13372375
Filing Date	2012-02-13
First Named Inventor	Melvyn Morris
Art Unit	2431
Examiner Name	CHIANG, JASON
Attorney Docket Number	04584.0012USU1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Andrew T. Pouzeshi/	Date (YYYY-MM-DD)	2016-02-24
Name/Print	Andrew T. Pouzeshi	Registration Number	67672

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	41	(Melvyn near Morris).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/03/28 13:18
L2	20	(Joseph near Jaroch).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/03/28 13:18
L3	18	("20050172338" | "20060161856" | "20080229422" | "20110047594" | "7761912" | "8407790" | "8499283").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/03/28 13:19
S1	9	(Melvyn near Morris).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 11:48
S2	3	(Joseph near Jaroch).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 16:51
S3	108	(Webroot).as.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 16:54
S5	0	S3 and cloud and database and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 16:58
S6	2980	(726/23).CCLS.	US-PGPUB;	OR	OFF	2013/06/04

			USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			17:04
S7	72	S6 and cloud and database and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 17:05
S8	54	("20100043072" | "20110197272" | "20090300764" | "20100064368" | "20120017200" | "20060101334" | "20090292791" | "20100306851" | "20110138361" | "8042184" | "20060069912" | "20120260304" | "7707634" | "7343626" | "20070016953" | "20110197177" | "20120266208" | "20060117055" | "20100313183" | "20110083183" | "8146135" | "8307435").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/05 11:39
S9	21	("2006/0069912").URPN.	USPAT	OR	ON	2013/06/05 11:59
S10	17	threat adj server	USPAT	OR	ON	2013/06/05 12:20
S11	2362	cloud and signature	USPAT	OR	ON	2013/06/05 13:23
S12	1181	cloud and signature and layer	USPAT	OR	ON	2013/06/05 13:23
S13	249	cloud and (signature with database)	USPAT	OR	ON	2013/06/05 13:25
S14	78	cloud and (signature with database) and (malware virus)	USPAT	OR	ON	2013/06/05 13:26
S15	143	cloud and (updat$4 near3 (signature database)) and (malware virus)	USPAT	OR	ON	2013/06/05 16:30
S16	65	(updat$4 near3 (signature database) near3 (interval certain period periodic)) and (malware virus)	USPAT	OR	ON	2013/06/05 20:09
S17	1	(09/740294).APP.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/06/05 20:37
S18	0	("(masteradjdatabase)and(virusmalwaresignature)").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/06/07 18:03
S19	1003	(master adj database) and (virus malware signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:04
S20	160	(master adj database) and (virus malware) and	US-PGPUB;	OR	ON	2013/06/07

		signature	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			18:05
S21	971	(database) and (virus near signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:33
S22	639	((stor$4 sav$4 receiv$5) with database) and (virus near signature) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:51
S23	594	((stor$4 sav$4 receiv$5) near5 database) and (virus near signature) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:51
S24	64	((stor$4 sav$4 receiv$5) near5 database) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 10:51
S25	0	((stor$4 sav$4 receiv$5) near3 content near3 database near3 storage) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:02
S26	0	((stor$4 sav$4 receiv$5) near3 database near3 storage) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:03
S27	2	((stor$4 sav$4 receiv$5) near3 content near3 database near3 storage) with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:03
S28	0	((backup) near3 database) with timestamp and (virus malware)and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2013/06/08 11:05

			IBM_TDB			
S29	0	((backup) near3 database) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:06
S30	27	((backup) near3 database) with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:06
S31	1139	((copy stor$4) near3 database) with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:20
S32	18	((copy stor$4) near3 database) with central with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:21
S33	359	((purg$4 clear$4 remov$4) near3 database near3 (period$6 every)) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:29
S34	0	(master adj database) near2 (virus malware) near2 signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S35	0	(master adj database) near3 (virus malware) near3 signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S36	0	(master adj database) with (virus malware) with signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S37	0	(master adj database) same (virus malware) same signature	US-PGPUB; USPAT; USOCR; FPRS;	OR	ON	2013/06/08 15:44

			EPO; JPO; DERWENT; IBM_TDB			
S38	19	(master adj database) same (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:45
S39	15	((primary secondary) adj database) same (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:54
S40	30	((primary secondary) adj database) with (signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:57
S41	98	(master adj database) same (signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:59
S42	10	(master adj database) same (signature) and (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:59
S43	315	(master adj database) and (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 16:03
S44	18	(virus malware) with definition with (file database) with (cloud community share$2)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 16:21
S45	271	(update refresh recover rebuild) near3 (database) with timestamp	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 20:22
S46	4	(update refresh recover rebuild) near3 (database) with timestamp same (offline off-line (off adj line)	US-PGPUB; USPAT;	OR	ON	2013/06/08 20:24

		disconnect reconnect)	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S47	1	((roll$3 adj back) near6 time) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:11
S48	7	((roll$3 adj back)) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:12
S49	11	((roll$3 adj back) rollback) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:14
S50	48	((roll$3 adj back) rollback) and ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:18
S51	21	(((roll$3 adj back) rollback) with time) and ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:23
S52	0	((restor$4) near6 time) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 11:40
S53	3	((restor$4) near6 time) and ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 11:41
S54	0	(send provid$3 transmit$4 updat$3) near3 (count near3 (threat incident)) near3 (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:01

S55	22	(send provid$3 transmit$4 updat$3) with ((count number) near3 (threat incident)) with (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:02
S56	122	(send provid$3 transmit$4 updat$3 record$4) with ((count number times) with (threat)) with (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:05
S57	635	(send provid$3 transmit$4 updat$3 record$4) with ((count number times) near5 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:08
S58	199	(send provid$3 transmit$4 updat$3 record$4) with ((count number) near5 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:09
S59	11	(send provid$3 transmit$4 updat$3 record$4) with ((count) near5 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:11
S60	43	((count) near2 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:15
S61	9	((count) near2 (threat)) and (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:15
S62	1126	(send provid$3 transmit$4 updat$3) near3 (count) near3 (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:18
S63	15	(send provid$3 transmit$4 updat$3) near3 ((increas$4 add$3) near (count)) near3 (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2013/06/09 15:20

			DERWENT; IBM_TDB			
S64	1816	((increas$4 add$3) near (count)) and (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:22
S65	27	((increas$4 add$3) near (count)) and (malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:23
S66	9	(Melvyn near Morris).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:29
S67	3	(Joseph near Jaroch).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:30
S68	813	((increas$4 add$3 generat$4) near (count)) and (malware threat)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:31
S69	742	((increas$4 add$3 generat$4) near (count)) and (malware threat) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:32
S70	0	(((seen identified) near (before previous)) with (increas$4 add$3 generat$4) near (count)) and (malware threat) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:33
S71	0	(((seen identified) near (before previous)) same ((increas$4 add$3 generat$4) near (count))) and (malware threat) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:33
S72	48	(((seen identified)) same ((increas$4 add$3 generat$4) near (count))) and (malware threat) and @ad<"20120213"	US-PGPUB; USPAT; USOCR;	OR	ON	2013/12/14 16:33

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S73	347	(master central primary global) near2 (server database) same (signature) and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/11 22:30
S74	609	(provid$4 send$4 transmit$4) near2 (master central primary global) near2 (server database) and (virus malware spyware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/11 22:35
S75	586	(provid$4 send$4 transmit$4 submit$4 post$4 report$4) adj2 (master central primary global) adj2 (server database) and (virus malware spyware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/11 22:36
S76	39	(Melvyn near Morris).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/11 23:33
S77	10	S76 and (malware).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/11 23:34
S78	190	("20100043072" | "20100332593" | "8453244" | "7051365" | "20110197272" | "20090300764" | "20100064368" | "20120017200" | "8301904" | "8347386" | "8352484" | "20060080637" | "20090172774" | "20060101334" | "20090292791" | "20100306851" | "20110138361" | "8042184" | "7231440" | "8321944" | "20090089040" | "20060272020" | "20060069912" | "20120260304" | "7707634" | "20110191299" | "20110191341" | "7814056" | "7921063" | "8116732" | "20070220043" | "20080115190" | "7343626" | "20030093429" | "20090070304" | "7188173" | "8234709" | "8296178" | "8321540" | "8332946" | "8448243" | "20070174429" | "6175869" | "20080148381" | "20070016953" | "20110197177" | "20120266208" | "8336100" | "8347375" | "20060080637" | "20060117055" | "20100313183" | "20110083183" | "8146135" | "8307435" | "8195938" | "8443447" | "20060272020" | "8225218" | "8276202" | "20030188194" | "20050187740" | "20080115190" | "20080148381" | "6219786" | "20070220043").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/13 20:26
S79	6016	(726/23).CCLS.	US-PGPUB; USPAT;	OR	OFF	2014/12/13 20:27

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S80	173	S78 NOT S79	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/13 20:27
S81	70	("20100043072" | "20110197272" | "20090300764" | "20100064368" | "20120017200" | "20060101334" | "20090292791" | "20100306851" | "20110138361" | "8042184" | "20060069912" | "20120260304" | "7707634" | "7343626" | "20070016953" | "20110197177" | "20120266208" | "20060117055" | "20100313183" | "20110083183" | "8146135" | "8307435").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/13 20:27
S82	120	S78 NOT S81	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/13 20:27
S83	544	(virus malware) and signature same behavior same (identifier ID IP computer) and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 19:55
S84	134	(virus malware) and signature same behavior same (identifier ID) and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 19:56
S85	64	(virus malware) and signature same behavior same (identifier) and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 19:57
S86	130	(virus malware) and signature same behavior same (infected) and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 20:27
S87	47	(virus malware) and (stor$4 receiv$4 send$4 provid$4) same signature same behavior same (infected) and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	OR	ON	2015/07/30 20:28

			IBM_TDB			
S88	58	(virus malware) and (stor$4 receiv$4 send$4 provid$4) same signature same behavior same (list) and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 20:32
S89	41	(Melvyn near Morris).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 20:53
S90	20	(Joseph near Jaroch).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 20:54
S93	18	("20040103315" | "20050131959" | "6842878" | "7555476" | "7921459" | "8347375" | "8543694").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/11/13 11:19

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L4	3262	(H04L63/14 G06F21/56).CPC.	US-PGPUB; USPAT	OR	ON	2016/03/28 13:22
L5	19	L4 and (signature).clm. and (behavior).clm. and (database).clm.	US-PGPUB; USPAT	OR	ON	2016/03/28 13:23
S91	2722	(H04L63/14 G06F21/56).CPC.	US-PGPUB; USPAT	OR	ON	2015/07/30 20:11
S92	20	S91 and (signature).clm. and (behavior).clm. and (database).clm.	US-PGPUB; USPAT	OR	ON	2015/07/30 20:13
S94	2997	(H04L63/14 G06F21/56).CPC.	US-PGPUB; USPAT	OR	ON	2015/11/13 13:45
S95	20	S94 and (signature).clm. and (behavior).clm. and (database).clm.	US-PGPUB; USPAT	OR	ON	2015/11/13 13:45

3/28/2016 1:41:37 PM
C:\Users\jchiang1\Documents\EAST\Workspaces\13372375-Malware.wsp

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13372375	MORRIS ET AL.
	Examiner	**Art Unit**
	JASON C CHIANG	2431

CPC								
Symbol							**Type**	**Version**
H04L		63	/	0263			F	2013-01-01
H04L		63	/	14			I	2013-01-01
G06F		21	/	56			I	2013-01-01
G06F		21	/	566			I	2013-01-01
H04L		63	/	145			I	2013-01-01
			/					
			/					
			/					
			/					
			/					
			/					
			/					
			/					
			/					
			/					

CPC Combination Sets								
Symbol							**Type**	**Set**	**Ranking**	**Version**
			/							
			/							

/JASON C CHIANG/ Examiner.Art Unit 2431	03/28/2016	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	15	
/DEDE ZECHER/ Supervisory Patent Examiner.Art Unit 2431	03/28/2016	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13372375	MORRIS ET AL.
	Examiner	**Art Unit**
	JASON C CHIANG	2431

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION									
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED				
726	23	H	0	4	L	29 / 06 (2006.0)	H	0	4	L	29 / 06 (2006.0)
CROSS REFERENCE(S)		G	0	6	F	21 / 56 (2013.0)	G	0	6	F	21 / 56 (2013.0)
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)										

/JASON C CHIANG/ Examiner.Art Unit 2431	03/28/2016	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	15	
/DEDE ZECHER/ Supervisory Patent Examiner.Art Unit 2431	03/28/2016	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13372375	MORRIS ET AL.
	Examiner	**Art Unit**
	JASON C CHIANG	2431

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1		17												
2	2		18												
3	3		19												
4	4		20												
5	5		21												
6	6		22												
7	7		23												
	8		24												
9	9	8	25												
10	10														
11	11														
12	12														
13	13														
14	14														
15	15														
	16														

/JASON C CHIANG/ Examiner.Art Unit 2431	03/28/2016	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	15	
/DEDE ZECHER/ Supervisory Patent Examiner.Art Unit 2431	03/28/2016	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13372375	MORRIS ET AL.
	Examiner	**Art Unit**
	JASON C CHIANG	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/09/2013	12/14/2013	12/13/2014	07/30/2015	11/13/2015	03/28/2016			
1	1	✓	✓	✓	=	=	=			
2	2	✓	✓	✓	=	=	=			
3	3	✓	✓	✓	=	=	=			
4	4	✓	✓	✓	=	=	=			
5	5	✓	✓	✓	=	=	=			
6	6	✓	✓	✓	=	=	=			
7	7	✓	✓	✓	=	=	=			
	8	✓	-	-	-	-	-			
9	9	✓	✓	✓	=	=	=			
10	10	✓	✓	✓	=	=	=			
11	11	✓	✓	✓	=	=	=			
12	12	✓	✓	✓	=	=	=			
13	13	✓	✓	✓	=	=	=			
14	14	✓	✓	✓	=	=	=			
15	15	✓	✓	✓	=	=	=			
	16	✓	-	-	-	-	-			
	17	N	N	N	N	N	N			
	18	N	N	N	N	N	N			
	19	N	N	N	N	N	N			
	20	N	N	N	N	N	N			
	21	N	N	N	N	N	N			
	22	N	N	N	N	N	N			
	23	N	N	N	N	N	N			
	24	N	N	N	N	N	N			
8	25			✓	=	=	=			

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13372375
Filing Date	2012-02-13
First Named Inventor	Melvyn Morris
Art Unit	2431
Examiner Name	CHIANG, JASON
Attorney Docket Number	04584.0012USU1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20060090073		2006-04-04	Steinberg et al.	
	2	20080109473		2008-05-08	Dixon et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13372375
Filing Date	2012-02-13
First Named Inventor	Melvyn Morris
Art Unit	2431
Examiner Name	CHIANG, JASON
Attorney Docket Number	04584.0012USU1

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	U.S. Patent Application No. 13/372,433, Final Rejection mailed June 1, 2016, 17 pages.	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13372375
Filing Date	2012-02-13
First Named Inventor	Melvyn Morris
Art Unit	2431
Examiner Name	CHIANG, JASON
Attorney Docket Number	04584.0012USU1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Andrew T. Pouzeshi/	Date (YYYY-MM-DD)	2016-07-01
Name/Print	Andrew T. Pouzeshi	Registration Number	67672

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	13372375
Filing Date:	13-Feb-2012
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate
Attorney Docket Number:	04584.0012USU1

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt

EFS ID:	26244732
Application Number:	13372375
International Application Number:	
Confirmation Number:	2918
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Customer Number:	23552
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate
Filer Authorized By:	Andrew T. Pouzeshi
Attorney Docket Number:	04584.0012USU1
Receipt Date:	01-JUL-2016
Filing Date:	13-FEB-2012
Time Stamp:	17:11:58
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$180
RAM confirmation Number	4428
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	2016-07-01-6thSIDS-04584-0012USU1.PDF	612018 076cd0b41069e8ae962620dcc4c348335c88cc61	no	4
Warnings:					
Information:					
2	Non Patent Literature	13372433_FOA_060116_17pgs.PDF	549215 e398d245bea80ea66dc1671c941d5183632793cd	no	17
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30805 90878d965af21dba863ff3741c2d66918e91c062	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1192038		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

23552 7590 04/04/2016
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/372,375	02/13/2012	Melvyn Morris	04584.0012USU1	2918

TITLE OF INVENTION: METHODS AND APPARATUS FOR DEALING WITH MALWARE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	07/05/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
CHIANG, JASON	2431	726-023000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 Merchant & Gould P.C.
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: WEBROOT INC.
(B) RESIDENCE: (CITY and STATE OR COUNTRY): Broomfield, Colorado

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☑ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
☑ Issue Fee
☐ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
☐ A check is enclosed.
☑ Payment by credit card. Form ~~PTO-2038 is attached~~.
☑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 132725 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
☐ Applicant certifying micro entity status. See 37 CFR 1.29
NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
☐ Applicant asserting small entity status. See 37 CFR 1.27
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
☐ Applicant changing to regular undiscounted fee status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Andrew T. Pouzeshi/ Date July 1, 2016
Typed or printed name Andrew T. Pouzeshi Registration No. 67672

Sophos Ex. 1002
Page 633 of 683

Electronic Patent Application Fee Transmittal

Application Number:	13372375
Filing Date:	13-Feb-2012
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate
Attorney Docket Number:	04584.0012USU1

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	1501	1	960	960

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**1140**

Electronic Acknowledgement Receipt

EFS ID:	26244863
Application Number:	13372375
International Application Number:	
Confirmation Number:	2918
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Customer Number:	23552
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate
Filer Authorized By:	Andrew T. Pouzeshi
Attorney Docket Number:	04584.0012USU1
Receipt Date:	01-JUL-2016
Filing Date:	13-FEB-2012
Time Stamp:	17:18:44
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	2016-07-01-7thSIDS-04584-0012USU1.PDF	612025 bf08934cf7ac6e92fb23d3a4dd5becabb5813526	no	4

Warnings:

Information:					
A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
2	Non Patent Literature	AU_1stExamReport_2012217181_041116_4pgs.PDF	224118 8d9b25f014810c38b9277686d68e9df553871189	no	4
Warnings:					
Information:					
3	Non Patent Literature	JP_NOA_2013_553909_052416_3pgs.PDF	411478 4a52d29a3ac6964ea627e9930501811b742b9402	no	3
Warnings:					
Information:					
4	Post Allowance Communication - Incoming	2016-07-01-CommentsForAllow-04584-0012USU1.PDF	69879 902757c25939ec78b2e9f346910d91d2ff0275c4	no	2
Warnings:					
Information:					
5	Issue Fee Payment (PTO-85B)	2016-07-01-IssueFeeTrans-04584-0012USU1.PDF	94147 0e4b7f650df6e3ec370bcea98552a9d9a672238b	no	1
Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	32551 d4ea54fd707837a293d6c8e0abdb9f4fb2f6c75c	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1444198		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13372375
Filing Date	2012-02-13
First Named Inventor	Melvyn Morris
Art Unit	2431
Examiner Name	CHIANG, JASON
Attorney Docket Number	04584.0012USU1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13372375
	Filing Date	2012-02-13
	First Named Inventor	Melvyn Morris
	Art Unit	2431
	Examiner Name	CHIANG, JASON
	Attorney Docket Number	04584.0012USU1

	1	Australian Patent Application No. 2012217181, First Examination Report mailed April 11, 2016, 4 pages.
	2	Japanese Patent Application No. 2013-553909, Notice of Allowance mailed May 24, 2016, 3 pages (No English translation available).

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13372375
	Filing Date	2012-02-13
	First Named Inventor	Melvyn Morris
	Art Unit	2431
	Examiner Name	CHIANG, JASON
	Attorney Docket Number	04584.0012USU1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Andrew T. Pouzeshi/	Date (YYYY-MM-DD)	2016-07-01
Name/Print	Andrew T. Pouzeshi	Registration Number	67672

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PATENT
Conf. No. 2918

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Morris, et al.	Examiner:	Chiang, Jason
Serial No.:	13/372,375	Group Art Unit:	2431
Filed:	February 13, 2012	Docket No.:	04584.0012USU1
Title:	METHODS AND APPARATUS FOR DEALING WITH MALWARE		

COMMENTS ON EXAMINER STATEMENT

Mail Stop – ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Washington, D.C. 20231

Dear Madam:

Applicant acknowledges the allowance of claims 1-7, 9-15, and 25 in the subject application by the Examiner with appreciation. Although the Examiner did not issue a Statement of Reasons for Allowance, Applicant agrees with statements made by the Examiner during the prosecution of the present application to the extent that the claims of the present invention are patentable over the references in the record. However, Applicant does not necessarily acquiesce or agree in any manner as to comments made by the Examiner regarding what the prior art does or does not teach. In addition, Applicant respectfully traverses statements made by the Examiner to the extent that any comment is intended or has the effect of limiting a claim scope, explicitly or implicitly, by not reciting verbatim the respective claim language, or is intended or has the effect of limiting a claim scope by stating or implying that all the reasons for patentability are in any way fully enumerated.

Further reasons for allowance are described and set forth in the Applicant's Specification. As the Examiner's statements are not exhaustive, such statements do not establish an estoppel against Applicant seeking and obtaining allowance of additional, broader claims in a continuation application, which Applicant reserves the right to file.

It is believed that no further fees are due with this Response. However, the Commissioner is hereby authorized to charge any deficiencies or credit any overpayment with respect to this patent application to deposit account number 13-2725.

Respectfully submitted,

Date: July 1, 2016

/Andrew T. Pouzeshi/

Andrew T. Pouzeshi, Reg. No. 67,672
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1639

23552
PATENT TRADEMARK OFFICE

Sophos Ex. 1002
Page 644 of 683

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

23552 7590 04/04/2016
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/372,375	02/13/2012	Melvyn Morris	04584.0012USU1	2918

TITLE OF INVENTION: METHODS AND APPARATUS FOR DEALING WITH MALWARE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	07/05/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
CHIANG, JASON	2431	726-023000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 Merchant & Gould P.C.
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: WEBROOT INC.
(B) RESIDENCE: (CITY and STATE OR COUNTRY): Broomfield, Colorado

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☑ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
☑ Issue Fee
☐ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
☐ A check is enclosed.
☑ Payment by credit card. Form ~~PTO-2038 is attached~~.
☑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 132725 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
☐ Applicant certifying micro entity status. See 37 CFR 1.29
NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
☐ Applicant asserting small entity status. See 37 CFR 1.27
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
☐ Applicant changing to regular undiscounted fee status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Andrew T. Pouzeshi/ Date July 1, 2016
Typed or printed name Andrew T. Pouzeshi Registration No. 67672

Sophos Ex. 1002
Page 645 of 683
PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Electronic Patent Application Fee Transmittal

Application Number:	13372375
Filing Date:	13-Feb-2012
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate
Attorney Docket Number:	04584.0012USU1

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	1501	1	960	960

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**960**

Electronic Acknowledgement Receipt

EFS ID:	26244921
Application Number:	13372375
International Application Number:	
Confirmation Number:	2918
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Customer Number:	23552
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate
Filer Authorized By:	Andrew T. Pouzeshi
Attorney Docket Number:	04584.0012USU1
Receipt Date:	01-JUL-2016
Filing Date:	13-FEB-2012
Time Stamp:	17:22:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$960
RAM confirmation Number	4571
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	2016-07-01-IssueFeeTrans-04584-0012USU1.PDF	94147 0e4b7f650df6e3ec370bcea98552a9d9a672238b	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30945 80ab9550595db4eccc67611f3d1c97206f0278a5	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	125092		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/372,375	02/13/2012	Melvyn Morris	04584.0012USU1	2918

23552 7590 07/12/2016

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER
CHIANG, JASON

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
07/12/2016	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPTO23552@merchantgould.com

Notice of Allowability	Application No. 13/372,375	Applicant(s) MORRIS ET AL.	
	Examiner JASON C. CHIANG	Art Unit 2431	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *IDS field on 07/01/2016*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1-7, 9-15 and 25*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 07/01/2016
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☐ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/JASON C CHIANG/ Examiner, Art Unit 2431	/CORDELIA ZECHER/ Supervisory Patent Examiner, Art Unit 2431

1. The present application is being examined under the pre-AIA first to invent provisions.

Corrected Notice of Allowability

2. This communication is in response to the two IDS filed after allowance on July 1, 2016.

Information Disclosure Statement

3. Two Information Disclosure Statements filed on July 1, 2016 have been entered and considered, they do not change the reasons for allowance.

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JASON C. CHIANG whose telephone number is (571)270-3393. The examiner can normally be reached on 9AM to 6PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, CORDELIA P. ZECHER can be reached on (571)272-7771. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/J. C. C./
Examiner, Art Unit 2431

/CORDELIA ZECHER/
Supervisory Patent Examiner, Art Unit 2431

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13372375
Filing Date	2012-02-13
First Named Inventor	Melvyn Morris
Art Unit	2431
Examiner Name	CHIANG, JASON
Attorney Docket Number	04584.0012USU1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13372375
	Filing Date	2012-02-13
	First Named Inventor	Melvyn Morris
	Art Unit	2431
	Examiner Name	CHIANG, JASON
	Attorney Docket Number	04584.0012USU1

/J.C./	1	Australian Patent Application No. 2012217181, First Examination Report mailed April 11, 2016, 4 pages.
/J.C./	2	Japanese Patent Application No. 2013-553909, Notice of Allowance mailed May 24, 2016, 3 pages (No English translation available).

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Jason Chiang/	Date Considered	07/07/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13372375
Filing Date	2012-02-13
First Named Inventor	Melvyn Morris
Art Unit	2431
Examiner Name	CHIANG, JASON
Attorney Docket Number	04584.0012USU1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Andrew T. Pouzeshi/	Date (YYYY-MM-DD)	2016-07-01
Name/Print	Andrew T. Pouzeshi	Registration Number	67672

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13372375
Filing Date	2012-02-13
First Named Inventor	Melvyn Morris
Art Unit	2431
Examiner Name	CHIANG, JASON
Attorney Docket Number	04584.0012USU1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/J.C./	1	20060090073		2006-04-04	Steinberg et al.	
/J.C./	2	20080109473		2008-05-08	Dixon et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13372375
Filing Date	2012-02-13
First Named Inventor	Melvyn Morris
Art Unit	2431
Examiner Name	CHIANG, JASON
Attorney Docket Number	04584.0012USU1

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
/J.C./	1	U.S. Patent Application No. 13/372,433, Final Rejection mailed June 1, 2016, 17 pages.	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Jason Chiang/	Date Considered	07/07/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13372375
Filing Date	2012-02-13
First Named Inventor	Melvyn Morris
Art Unit	2431
Examiner Name	CHIANG, JASON
Attorney Docket Number	04584.0012USU1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Andrew T. Pouzeshi/	Date (YYYY-MM-DD)	2016-07-01
Name/Print	Andrew T. Pouzeshi	Registration Number	67672

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	6	("20060090073" | "20080109473").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/07/07 11:23
S1	9	(Melvyn near Morris).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 11:48
S2	3	(Joseph near Jaroch).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 16:51
S3	108	(Webroot).as.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 16:54
S5	0	S3 and cloud and database and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 16:58
S6	2980	(726/23).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/06/04 17:04
S7	72	S6 and cloud and database and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/04 17:05
S8	54	("20100043072" | "20110197272" | "20090300764" |	US-PGPUB;	OR	ON	2013/06/05

		"20100064368" | "20120017200" | "20060101334" | "20090292791" | "20100306851" | "20110138361" | "8042184" | "20060069912" | "20120260304" | "7707634" | "7343626" | "20070016953" | "20110197177" | "20120266208" | "20060117055" | "20100313183" | "20110083183" | "8146135" | "8307435").PN.	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			11:39
S9	21	("2006/0069912").URPN.	USPAT	OR	ON	2013/06/05 11:59
S10	17	threat adj server	USPAT	OR	ON	2013/06/05 12:20
S11	2362	cloud and signature	USPAT	OR	ON	2013/06/05 13:23
S12	1181	cloud and signature and layer	USPAT	OR	ON	2013/06/05 13:23
S13	249	cloud and (signature with database)	USPAT	OR	ON	2013/06/05 13:25
S14	78	cloud and (signature with database) and (malware virus)	USPAT	OR	ON	2013/06/05 13:26
S15	143	cloud and (updat$4 near3 (signature database)) and (malware virus)	USPAT	OR	ON	2013/06/05 16:30
S16	65	(updat$4 near3 (signature database) near3 (interval certain period periodic)) and (malware virus)	USPAT	OR	ON	2013/06/05 20:09
S17	1	(09/740294).APP.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/06/05 20:37
S18	0	(" (masteradjdatabase)and(virusmalwaresignature)").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/06/07 18:03
S19	1003	(master adj database) and (virus malware signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:04
S20	160	(master adj database) and (virus malware) and signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:05
S21	971	(database) and (virus near signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:33
S22	639	((stor$4 sav$4 receiv$5) with database) and (virus	US-PGPUB;	OR	ON	2013/06/07

		near signature) and @ad<"20120213"	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			18:51
S23	594	((stor$4 sav$4 receiv$5) near5 database) and (virus near signature) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/07 18:51
S24	64	((stor$4 sav$4 receiv$5) near5 database) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 10:51
S25	0	((stor$4 sav$4 receiv$5) near3 content near3 database near3 storage) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:02
S26	0	((stor$4 sav$4 receiv$5) near3 database near3 storage) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:03
S27	2	((stor$4 sav$4 receiv$5) near3 content near3 database near3 storage) with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:03
S28	0	((backup) near3 database) with timestamp and (virus malware)and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:05
S29	0	((backup) near3 database) with timestamp and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:06
S30	27	((backup) near3 database) with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2013/06/08 11:06

			IBM_TDB			
S31	1139	((copy stor$4) near3 database) with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:20
S32	18	((copy stor$4) near3 database) with central with timestamp and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:21
S33	359	((purg$4 clear$4 remov$4) near3 database near3 (period$6 every)) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 11:29
S34	0	(master adj database) near2 (virus malware) near2 signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S35	0	(master adj database) near3 (virus malware) near3 signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S36	0	(master adj database) with (virus malware) with signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S37	0	(master adj database) same (virus malware) same signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:44
S38	19	(master adj database) same (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:45
S39	15	((primary secondary) adj database) same (virus malware)	US-PGPUB; USPAT; USOCR; FPRS;	OR	ON	2013/06/08 15:54

			EPO; JPO; DERWENT; IBM_TDB			
S40	30	((primary secondary) adj database) with (signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:57
S41	98	(master adj database) same (signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:59
S42	10	(master adj database) same (signature) and (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 15:59
S43	315	(master adj database) and (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 16:03
S44	18	(virus malware) with definition with (file database) with (cloud community share$2)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 16:21
S45	271	(update refresh recover rebuild) near3 (database) with timestamp	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 20:22
S46	4	(update refresh recover rebuild) near3 (database) with timestamp same (offline off-line (off adj line) disconnect reconnect)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/08 20:24
S47	1	((roll$3 adj back) near6 time) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:11
S48	7	((roll$3 adj back)) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT;	OR	ON	2013/06/09 10:12

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S49	11	((roll$3 adj back) rollback) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:14
S50	48	((roll$3 adj back) rollback) and ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:18
S51	21	(((roll$3 adj back) rollback) with time) and ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 10:23
S52	0	((restor$4) near6 time) same ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 11:40
S53	3	((restor$4) near6 time) and ((update) near3 (database) with timestamp)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 11:41
S54	0	(send provid$3 transmit$4 updat$3) near3 (count near3 (threat incident)) near3 (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:01
S55	22	(send provid$3 transmit$4 updat$3) with ((count number) near3 (threat incident)) with (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:02
S56	122	(send provid$3 transmit$4 updat$3 record$4) with ((count number times) with (threat)) with (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:05

S57	635	(send provid$3 transmit$4 updat$3 record$4) with ((count number times) near5 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:08
S58	199	(send provid$3 transmit$4 updat$3 record$4) with ((count number) near5 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:09
S59	11	(send provid$3 transmit$4 updat$3 record$4) with ((count) near5 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:11
S60	43	((count) near2 (threat))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:15
S61	9	((count) near2 (threat)) and (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:15
S62	1126	(send provid$3 transmit$4 updat$3) near3 (count) near3 (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:18
S63	15	(send provid$3 transmit$4 updat$3) near3 ((increas$4 add$3) near (count)) near3 (server database)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:20
S64	1816	((increas$4 add$3) near (count)) and (virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/06/09 15:22
S65	27	((increas$4 add$3) near (count)) and (malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2013/06/09 15:23

			DERWENT; IBM_TDB			
S66	9	(Melvyn near Morris).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:29
S67	3	(Joseph near Jaroch).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:30
S68	813	((increas$4 add$3 generat$4) near (count)) and (malware threat)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:31
S69	742	((increas$4 add$3 generat$4) near (count)) and (malware threat) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:32
S70	0	(((seen identified) near (before previous)) with (increas$4 add$3 generat$4) near (count)) and (malware threat) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:33
S71	0	(((seen identified) near (before previous)) same ((increas$4 add$3 generat$4) near (count))) and (malware threat) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:33
S72	48	(((seen identified)) same ((increas$4 add$3 generat$4) near (count))) and (malware threat) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 16:33
S73	347	(master central primary global) near2 (server database) same (signature) and (virus malware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/11 22:30
S74	609	(provid$4 send$4 transmit$4) near2 (master central primary global) near2 (server database) and (virus malware spyware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR;	OR	ON	2014/12/11 22:35

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S75	586	(provid$4 send$4 transmit$4 submit$4 post$4 report$4) adj2 (master central primary global) adj2 (server database) and (virus malware spyware) and @ad<"20120213"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/11 22:36
S76	39	(Melvyn near Morris).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/11 23:33
S77	10	S76 and (malware).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/11 23:34
S78	190	("20100043072" | "20100332593" | "8453244" | "7051365" | "20110197272" | "20090300764" | "20100064368" | "20120017200" | "8301904" | "8347386" | "8352484" | "20060080637" | "20090172774" | "20060101334" | "20090292791" | "20100306851" | "20110138361" | "8042184" | "7231440" | "8321944" | "20090089040" | "20060272020" | "20060069912" | "20120260304" | "7707634" | "20110191299" | "20110191341" | "7814056" | "7921063" | "8116732" | "20070220043" | "20080115190" | "7343626" | "20030093429" | "20090070304" | "7188173" | "8234709" | "8296178" | "8321540" | "8332946" | "8448243" | "20070174429" | "6175869" | "20080148381" | "20070016953" | "20110197177" | "20120266208" | "8336100" | "8347375" | "20060080637" | "20060117055" | "20100313183" | "20110083183" | "8146135" | "8307435" | "8195938" | "8443447" | "20060272020" | "8225218" | "8276202" | "20030188194" | "20050187740" | "20080115190" | "20080148381" | "6219786" | "20070220043").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/13 20:26
S79	6016	(726/23).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/12/13 20:27
S80	173	S78 NOT S79	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/13 20:27
S81	70	("20100043072" | "20110197272" | "20090300764" | "20100064368" | "20120017200" | "20060101334" |	US-PGPUB; USPAT;	OR	ON	2014/12/13 20:27

		"20090292791" | "20100306851" | "20110138361" | "8042184" | "20060069912" | "20120260304" | "7707634" | "7343626" | "20070016953" | "20110197177" | "20120266208" | "20060117055" | "20100313183" | "20110083183" | "8146135" | "8307435").PN.	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S82	120	S78 NOT S81	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/12/13 20:27
S83	544	(virus malware) and signature same behavior same (identifier ID IP computer) and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 19:55
S84	134	(virus malware) and signature same behavior same (identifier ID) and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 19:56
S85	64	(virus malware) and signature same behavior same (identifier) and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 19:57
S86	130	(virus malware) and signature same behavior same (infected) and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 20:27
S87	47	(virus malware) and (stor$4 receiv$4 send$4 provid$4) same signature same behavior same (infected) and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 20:28
S88	58	(virus malware) and (stor$4 receiv$4 send$4 provid$4) same signature same behavior same (list) and @ad<"20110215"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 20:32
S89	41	(Melvyn near Morris).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2015/07/30 20:53

			IBM_TDB			
S90	20	(Joseph near Jaroch).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/07/30 20:54
S93	18	("20040103315" | "20050131959" | "6842878" | "7555476" | "7921459" | "8347375" | "8543694").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/11/13 11:19
S96	41	(Melvyn near Morris).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/03/28 13:18
S97	20	(Joseph near Jaroch).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/03/28 13:18
S98	18	("20050172338" | "20060161856" | "20080229422" | "20110047594" | "7761912" | "8407790" | "8499283").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/03/28 13:19

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S91	2722	(H04L63/14 G06F21/56).CPC.	US-PGPUB; USPAT	OR	ON	2015/07/30 20:11
S92	20	S91 and (signature).clm. and (behavior).clm. and (database).clm.	US-PGPUB; USPAT	OR	ON	2015/07/30 20:13
S94	2997	(H04L63/14 G06F21/56).CPC.	US-PGPUB; USPAT	OR	ON	2015/11/13 13:45
S95	20	S94 and (signature).clm. and (behavior).clm. and (database).clm.	US-PGPUB; USPAT	OR	ON	2015/11/13 13:45
S99	3262	(H04L63/14 G06F21/56).CPC.	US-PGPUB; USPAT	OR	ON	2016/03/28 13:22
S100	19	S99 and (signature).clm. and (behavior).clm. and (database).clm.	US-PGPUB; USPAT	OR	ON	2016/03/28 13:23

7/7/2016 11:26:17 AM
C:\Users\jchiang1\Documents\EAST\Workspaces\13372375-Malware.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/372,375	08/09/2016	9413721	04584.0012USU1	2918

23552 7590 07/20/2016

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Melvyn Morris, Belper, UNITED KINGDOM;
Joseph Jaroch, Elk Grove Village, IL;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

Power of Attorney to Transact Business with the United States Patent and Trademark Office

I hereby revoke all previous Powers of Attorney given in the application(s) identified in the attached Transmittal for Power of Attorney to One or More Registered Practitioners ("Transmittal Form").

I hereby appoint practitioners associated with the following Customer Number associated with Sprinkle IP Law Group, PC :

109422

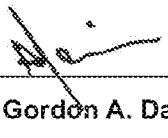
as my/our attorney(s) or agent(s) and to transact all business before the United States Patent and Trademark Office (USPTO) in connection with any and all patents and patent applications that are assigned to **Webroot Inc.** (the "assignee's patents/patent applications") in which they shall appear, any and all assignee's patents/patent applications associated with the above-referenced customer number, and any and all patents and patent applications referenced in the attached Transmittal Form.

Please recognize or change the correspondence address for the patents and patent applications referenced in the attached Transmittal Form to the address associated with the above-referenced customer number.

The undersigned is:

- ☐ Inventor or Joint Inventor
- ☒ Assignee or Person to Whom the Inventor is Under an Obligation to Assign
  *the undersigned has authority to act on behalf of the Assignee or Person to Whom the Inventor is Under an Obligation to Assign.
- ☐ Legal Representative of a Deceased or Legally Incapacitated Inventor
- ☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is currently being filed in this document)

The Transmittal Form may be completed and executed by one of the practitioners associated with the above-referenced customer number.

SIGNATURE OF APPLICANT			
Signature:		**Date:**	January 29, 2020
Name:	**Gordon A. Davies**		
Title:	Director		
Company:	**Webroot Inc.**		
I am authorized to act on behalf of the assignee.			

Electronic Acknowledgement Receipt

EFS ID:	39155196
Application Number:	13372375
International Application Number:	
Confirmation Number:	2918
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Customer Number:	23552
Filer:	John L. Adair/keunah cheun
Filer Authorized By:	John L. Adair
Attorney Docket Number:	04584.0012USU1
Receipt Date:	14-APR-2020
Filing Date:	13-FEB-2012
Time Stamp:	15:18:43
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	WEBROOT_POA_012820.pdf	42303 460c019d47e52952aad549f0d335131a49b6cfef	no	1

Warnings:

Information:	
Total Files Size (in bytes):	42303

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/372,375	02/13/2012	Melvyn Morris	04584.0012USU1

CONFIRMATION NO. 2918

109422
Sprinkle IP Law Group/OPEN
1301 W. 25th Street, Suite 408
Austin, TX 78705

POA ACCEPTANCE LETTER

OC000000116336624

Date Mailed: 04/20/2020

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 04/14/2020.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/tmwilliams/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/372,375	02/13/2012	Melvyn Morris	04584.0012USU1

CONFIRMATION NO. 2918

POWER OF ATTORNEY NOTICE

23552
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

OC000000116336569

Date Mailed: 04/20/2020

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 04/14/2020.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/tmwilliams/

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court WESTERN DISTRICT OF TEXAS on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:22-cv-00240	3/4/2022	WESTERN DISTRICT OF TEXAS

PLAINTIFF	DEFENDANT
WEBROOT, INC. and OPEN TEXT, INC.	SOPHOS LTD.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,418,250	4/9/2013	Webroot, Inc.
2	8,726,389	5/13/2014	Webroot, Inc.
3	9,578,045	2/21/2017	Webroot, Inc.
4	10,257,224	4/9/2019	Webroot, Inc.
5	10,284,591	5/7/2019	Webroot, Inc.

In the above---entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading		
	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	10,499,844	12/10/2019	Webroot, Inc.
2	9,413,721	8/9/2016	Webroot, Inc.
3			
4			
5			

In the above---entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1---Upon initiation of action, mail this copy to Director Copy 3---Upon termination of action, mail this copy to Director
Copy 2---Upon filing document adding patent(s), mail this copy to Director Copy 4---Case file copy

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court WESTERN DISTRICT OF TEXAS on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:22-cv-00342	3/31/2022	WESTERN DISTRICT OF TEXAS

PLAINTIFF	DEFENDANT
WEBROOT, INC. and OPEN TEXT, INC.	FORCEPOINT LLC

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,726,389	5/13/2014	Webroot, Inc.
2	8,438,386	5/7/2013	Webroot, Inc.
3	10,599,844	3/24/2020	Webroot, Inc.
4	9,413,721	8/9/2016	Webroot, Inc.
5	10,025,928	7/17/2018	Webroot, Inc.

In the above---entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above---entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1---Upon initiation of action, mail this copy to Director Copy 3---Upon termination of action, mail this copy to Director
Copy 2---Upon filing document adding patent(s), mail this copy to Director Copy 4---Case file copy

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Western District of Texas, Wacon Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:22-cv-00342-ADA	3/31/2022	Western District of Texas, Wacon Division

PLAINTIFF	DEFENDANT
WEBROOT, INC. and OPEN TEXT, INC.	FORCEPOINT LLC

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,726,389	5/13/2014	Webroot, Inc.
2	8,438,386	5/7/2013	Webroot, Inc.
3	10,599,844	3/24/2020	Webroot, Inc.
4	9,413,721	8/9/2016	Webroot, Inc.
5	10,025,928	7/17/2018	Webroot, Inc.

In the above---entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY
7/14/2022	☐ Amendment ☑ Answer ☐ Cross Bill ☐ Other Pleading

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	7,194,464	3/20/2007	Forcepoint LLC
2	8,938,773	1/20/2015	Forcepoint LLC
3	8,978,140	3/10/2015	Forcepoint LLC
4	9,609,001	3/28/2017	Forcepoint LLC
5	9,654,495	5/16/2017	Forcepoint LLC

In the above---entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1---Upon initiation of action, mail this copy to Director Copy 3---Upon termination of action, mail this copy to Director
Copy 2---Upon filing document adding patent(s), mail this copy to Director Copy 4---Case file copy

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court WESTERN DISTRICT OF TEXAS on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:22-cv-00240	10/27/2022	WESTERN DISTRICT OF TEXAS

PLAINTIFF	DEFENDANT
WEBROOT, INC. and OPEN TEXT, INC.	SOPHOS LTD.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,418,250	4/9/2013	Webroot, Inc.
2	8,726,389	5/13/2014	Webroot, Inc.
3	9,578,045	2/21/2017	Webroot, Inc.
4	10,257,224	4/9/2019	Webroot, Inc.
5	10,284,591	5/7/2019	Webroot, Inc.

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading		
	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	10,499,844	12/10/2019	Webroot, Inc.
2	9,413,721	8/9/2016	Webroot, Inc.
3	11,409,869	8/9/2022	Webroot, Inc.
4			
5			

In the above —entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2 Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy