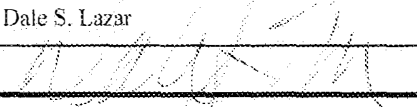


UTILITY PATENT APPLICATION TRANSMITTAL (Only for new nonprovisional applications under 37 CFR 1.53(b))		Attorney Docket No.		339000-000014
		First Inventor or Application Identifier		Melvyn Morris
		Title	METHODS AND APPARATUS FOR DEALING WITH MALWARE	

APPLICATION ELEMENTS <i>See MPEP chapter 600 concerning utility patent application contents.</i>		Commissioner for Patents Box Patent Application PO Box 1450 Alexandria, VA 22313-1450	
1. ☒ Fee Transmittal Form (e.g. PTO/SB/17) (Submit an original and a duplicate for fee processing) ☐ Applicant claims small entity status. 2. ☒ Specification Total Pages <u>55</u> 3. ☒ Drawing(s) (35 U.S.C. 113) Total Sheets <u>3</u> 4. ☒ Oath or Declaration Total Pages <u>4</u> a. ☐ Newly executed (original or copy) b. ☒ Copy from a prior application (37 C.F.R. §1.63(d)) (for continuation/divisional with box 16 completed) 5. ☒ Incorporation By Reference (usable if box 4B is checked) The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4B, is considered to be part of the disclosure of the accompanying application and is hereby incorporated by reference therein.		ACCOMPANYING DOCUMENTS 6. ☐ Assignment Papers (cover sheet & documents(s)) 7. ☐ 37 C.F.R. §3.73(b) Statement ☐ Power of (when there is an assignee) Attorney 8. ☐ English Translation Document (if applicable) 9. ☐ Information Disclosure ☐ Copies of IDS Statement (IDS)/PTO-1449 Citations 10. ☐ Preliminary Amendment 11. ☐ White Advance Serial No. Postcard 12. ☐ Certified Copy of Priority Document(s) (if foreign priority is claimed) 13. ☐ Request for Priority 14. ☒ Application Data Sheet 15. ☐ Other:	
16. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below: ☒ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application no.: 11/477,807 Prior application information: Examiner: Cordelia P. K. Zecher Group Art Unit: 2432			
17. ☒ This application is a ☒ Continuation ☐ Division ☐ Continuation-in-part (CIP) of application Serial No. 11/477,807 Filed on 6/30/2006 ☒ This application claims priority of UNITED STATES Patent Application Serial No. 11/477,807, Filed 6/30/2006			
18. CORRESPONDENCE ADDRESS 47604			

Name	Dale S. Lazar	Registration No.		28,872
Signature		Date	July 6, 2012	Telephone 703.773.4000

APPLICATION DATA SHEET

Application Information

Application Number::
Filing Date::
Application Type:: REGULAR
Subject Matter:: UTILITY
Suggested Classification::
Suggested Group Art Unit::
CD-ROM or CD-R:: NONE
Number of Disks::
Number of copies of CDs::
Sequence Submission::
Computer Readable Form (CRF):: NO
Number of Copies of CRF::
Title:: METHODS AND APPARATUS FOR
DEALING WITH MALWARE

Attorney Docket Number:: 339000-000014
Request for Early Publication:: NO
Request for Non-Publication:: NO
Suggested Drawing Figure::
Total Drawing Sheets:: 3
Small Entity:: NO
Latin Name::
Variety Denomination Name::
Petition Included:: NO
Petition Type::
Licensed US Govt. Agency::
Contract of Grant Numbers::
Secrecy Order in Parent Appln.: NO

INITIAL
7/6/2012

-1-

EASTM41503320.1

APPLICANT INFORMATION

Applicant Authority Type:: INVENTOR
Primary Citizenship Country:: UNITED KINGDOM
Status:: FULL CAPACITY
Given Name:: MELVYN
Middle Name::
Family Name:: MORRIS
Name Suffix::
City of Residence:: TURNDITCH
State or Province of
Residence:: DERBYSHIRE
Country of Residence:: UNITED KINGDOM
Street of mailing address:: REDMIRE GAP
INTAKE LANE
City of mailing address:: TURNDITCH
State or Province of mailing
address:: DERBYSHIRE
Country of mailing address:: UNITED KINGDOM
Postal or Zip Code of mailing
address:: DE58 2LU

Applicant Authority Type:: INVENTOR
Primary Citizenship Country:: UNITED KINGDOM
Status:: FULL CAPACITY
Given Name:: PAUL
Middle Name::
Family Name:: STUBBS
Name Suffix::
City of Residence:: WYBOSTON

INITIAL
7/6/2012

State or Province of BEDFORDSHIRE
Residence::
Country of Residence:: UNITED KINGDOM
Street of mailing address:: 7 ROOKERY ROAD

City of mailing address:: WYBOSTON
State or Province of mailing address:: BEDFORDSHIRE
Country of mailing address:: UNITED KINGDOM
Postal or Zip Code of mailing address:: MK44 3AX

Applicant Authority Type:: INVENTOR
Primary Citizenship Country:: UNITED KINGDOM
Status:: FULL CAPACITY
Given Name:: MARKUS
Middle Name::
Family Name:: HARTWIG
Name Suffix::

City of Residence:: MILTON KEYNES
State or Province of Residence:: BUCKINGHAMSHIRE
Country of Residence:: UNITED KINGDOM
Street of mailing address:: EXCHANGE HOUSE
494 MIDSUMMER BLVD.
City of mailing address:: MILTON KEYNES
State or Province of mailing address:: BUCKINGHAMSHIRE
Country of mailing address:: UNITED KINGDOM

INITIAL
7/6/2012

Postal or Zip Code of mailing address::	MK9 2EA
Applicant Authority Type::	INVENTOR
Primary Citizenship Country::	UNITED KINGDOM
Status::	FULL CAPACITY
Given Name::	DARREN
Middle Name::	
Family Name::	HARTER
Name Suffix::	
City of Residence::	HUCCLECOTE
State or Province of Residence::	GLOUCESTERSHIRE
Country of Residence::	UNITED KINGDOM
Street of mailing address::	178 BARDWOOD ROAD
City of mailing address::	HUCCLECOTE
State or Province of mailing address::	GLOUCESTERSHIRE
Country of mailing address::	UNITED KINGDOM
Postal or Zip Code of mailing address::	GL4 3JZ

CORRESPONDENCE INFORMATION

CORRESPONDENCE NUMBER::	47604
PHONE NUMBER::	703-773-4149
FAX NUMBER::	703-773-5200
E-MAIL ADDRESS::	DALE.LAZAR@DLAPIPER.COM

INITIAL
7/6/2012

REPRESENTATIVE INFORMATION

Representative Customer 47604
Number::

DOMESTIC PRIORITY INFORMATION

Application::	Continuity Type::	Parent Application::	Parent Filing Date::
This Application	Continuation of	11/477,807	6/30/06

FOREIGN PRIORITY INFORMATION

Country::	Application Number::	Filing Date::	Priority Claimed
GB	0513375.6	6/30/05	YES

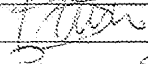
ASSIGNEE INFORMATION

Assignee Name:: PREVX LTD.
Street mailing address:: 3 NEW PARK PLACE

City mailing address:: PARK PRIDE
State or Province of mailing address:: DERBY
Country of mailing address:: UNITED KINGDOM
Postal or Zip Code of mailing address:: DE24 8DZ

INITIAL
7/6/2012

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 and CORRESPONDENCE ADDRESS INDICATION FORM	Application Number	11/477,807		
	Filing Date	June 30, 2006		
	First Named Inventor	Melvyn MORRIS et al.		
	Art Unit	Unknown		
	Examiner Name	Unknown		
	Attorney Docket Number	339000-P0003		
I hereby revoke all previous powers of attorney given in the above-identified application.				
I hereby appoint:				
☒ Practitioners associated with the Customer Number: 47604 OR ☐ Practitioner(s) name below:				
Name		Registration Number		
as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith.				
Please recognize or change the correspondence address for the above-identified application to:				
☒ The address associated with the above-mentioned Customer Number: 47604 OR ☐ The address associated with Customer Number:				
OR				
☐ Firm or individual name				
Address				
City		State	Zip	
Country				
Telephone		Email		
I am the:				
☐ Applicant/Inventor. ☒ Assignee of record of the entire interest. See 37 CFR 3.71. <i>Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)</i>				
SIGNATURE of Applicant or Assignee of Record				
Signature			Date	26/3/17
Name	Paul Scrubbs		Telephone	
Title and Company	DIRECTOR, PREVX LTD			
NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*				
☒ *Total of 1 forms are submitted.				

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.

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: Prevx Limited

Application No./Patent No./Control No.: 11/477,807 Filed/Issue Date: June 30, 2006

Entitled: METHODS AND APPARATUS FOR DEALING WITH MALWARE

Prevx Limited,
(Name of Assignee)

a Corporation
(Type of Assignee: corporation, partnership, university, government agency, etc.)

States that it is:

1. ☒ the assignee of the entire right, title, and interest; or
2. ☐ an assignee of less than the entire right, title and interest
(The extent (by percentage) of its ownership interest is _____%)

In the patent application/ patent identified above by virtue of either:

- 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 018348, Frame 0840, or a true copy of the original assignment is attached.

OR

- B. ☐ A chain of title from the inventor(s), of the present 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.
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.

- ☐ Additional documents in the chain of title are listed on a supplemental sheet.

As required by 37 CFR 3.73(b)(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 assignees.

[Signature]
Signature

26/3/7
Date

Paul Sturbs
Printed or Typed Name

Telephone Number

Director
Title

FOR UTILITY
ORIGINAL
DECLARATION

RULE 63 (37 C.F.R. 1.63)
DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATION
IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

As a below named inventor, I hereby declare that my residence, post office address and citizenship are as stated below next to my name, and I believe I am an original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the INVENTION ENTITLED Methods and Apparatus for Dealing with Malware, the specification of which was filed on 30th June 2006 as U.S. Application No. 11/477807.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above. I acknowledge the duty to disclose all information known to me to be material to patentability as defined in 37 C.F.R. 1.56. Except as noted below, I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT International Application which designated at least one other country than the United States, listed below and have also identified below any foreign application for patent or inventor's certificate, or PCT International Application, filed by me or my assignee disclosing the subject matter claimed in this application and having a filing date (1) before that of the application on which priority is claimed, or (2) if no priority claimed, before the filing date of this application:

PRIOR FOREIGN APPLICATION(S)

Number	Country	Filed	Date First Laid Open Or Published	Date Patented or Granted	Priority Claimed
0513375.6	GB	30th June 2005			Yes

Except as noted below, I hereby claim domestic priority benefit under 35 U.S.C. 115(e) or 120 and/or 365(c) of the indicated United States applications listed below and PCT International applications listed above or below and, if this is a continuation-in-part (CIP) application, insofar as the subject matter disclosed and claimed in this application is in addition to that disclosed in such prior applications. I acknowledge the duty to disclose all information known to me to be material to patentability as defined in 37 C.F.R. 1.56 which became available between the filing date of each such prior application and the national or PCT International filing date of this application.

PRIOR U.S. PROVISIONAL, NONPROVISIONAL AND/OR PCT APPLICATION(S)

Application Number	Filed	Status	Priority Claimed
		pending, abandoned, patented	

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that wilful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such wilful false statements may jeopardize the validity of the application or any patent issued thereon.

And I hereby appoint Pillsbury Winthrop Shaw Pittman LLP, Intellectual Property Group, (to whom all communications are to be directed), and persons of that firm who are associated with USPTO Customer No. 00909 individually and collectively my attorneys to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith and with the resulting patent, and I hereby authorize them to delete from that Customer No. names of persons no longer with their firm, to add new persons of their firm to that Customer No., and to act and rely on instructions from and communicate directly with the person/assignee/attorney/firm/organization who/which first sends/sent this case to them and by whom/which I hereby declare that I have consented after full disclosure to be represented unless/until I instruct the above firm and/or an attorney of that firm in writing to the contrary.

Power of Attorney to Customer Number

00909

INVENTOR'S SIGNATURE:

Date:

Name	Melvyn	MORRIS	
	First	Middle Initial	Family Name
Residence	Turnditch	United Kingdom	GB
	City	State/Foreign Country	Country of Citizenship
Mailing Address	Redmire Gap, Intake Lane, Turnditch, Derbyshire DE58 2LU, United Kingdom		

INVENTOR'S SIGNATURE:

Date:

Name	Paul	Stubbs	
	First	Middle Initial	Family Name
Residence	Wyboston	United Kingdom	GB
	City	State/Foreign Country	Country of Citizenship
Mailing Address	7 Rookery Road, Wyboston, Bedfordshire MK44 3AX, United Kingdom		

INVENTOR'S SIGNATURE: *M. Hartwig* Date:

Name	Markus		HARTWIG
	First	Middle Initial	Family Name
Residence	Milton Keynes	United Kingdom	DE
	City	State/Foreign Country	Country of Citizenship
Mailing Address	Exchange House, 494 Midsummer Boulevard, Milton Keynes, Buckinghamshire MK9 2EA, United Kingdom		

INVENTOR'S SIGNATURE: *D. Harter* Date:

Name	Darren		Harter
	First	Middle Initial	Family Name
Residence	Hucclecote	United Kingdom	GB
	City	State/Foreign Country	Country of Citizenship
Mailing Address	176 Barnwood Road, Hucclecote, Gloucester Gloucestershire GL4 3JZ, United Kingdom		

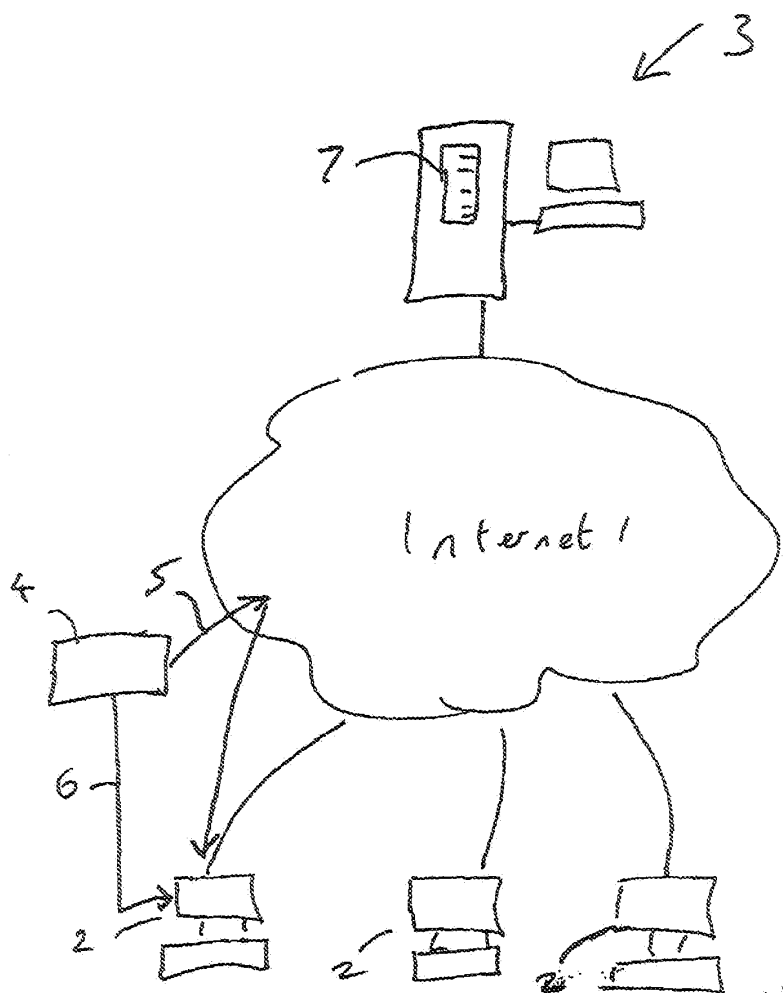
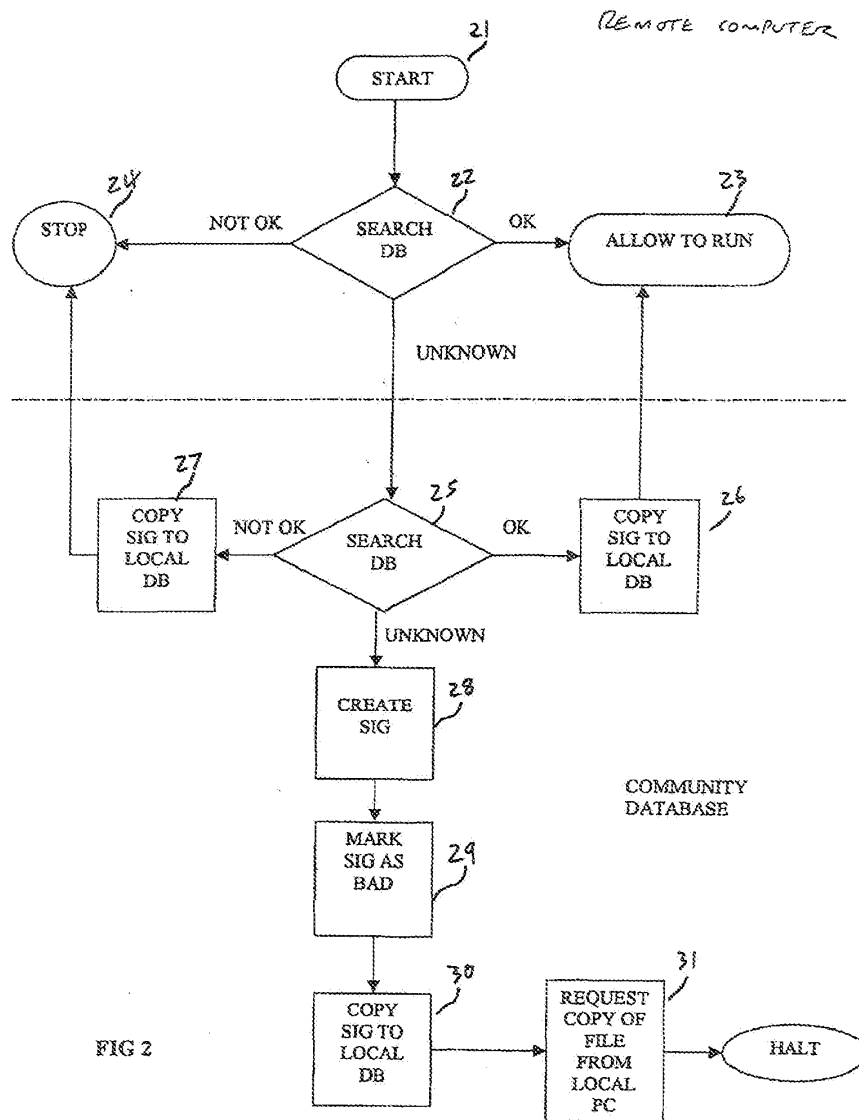


FIG. 1



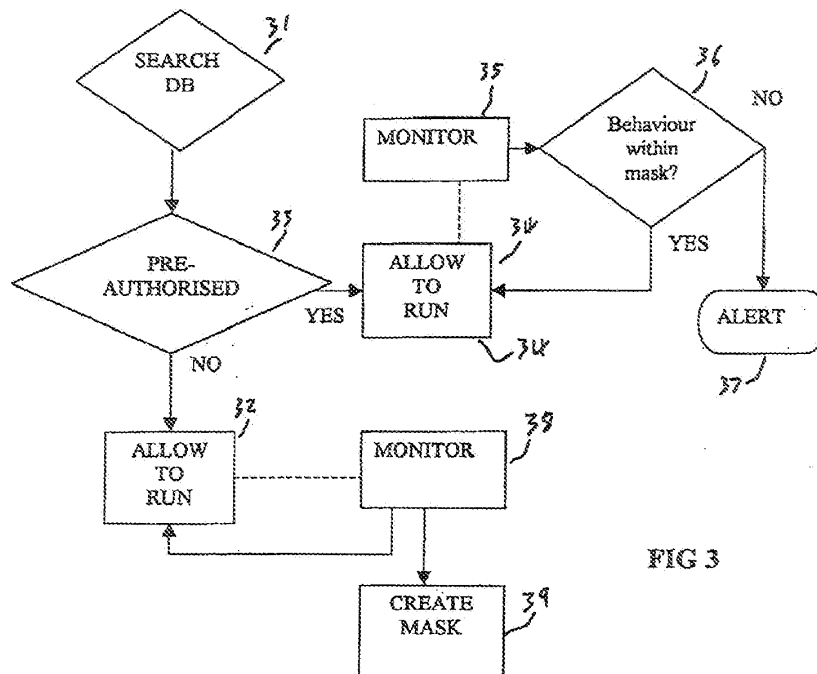


FIG 3

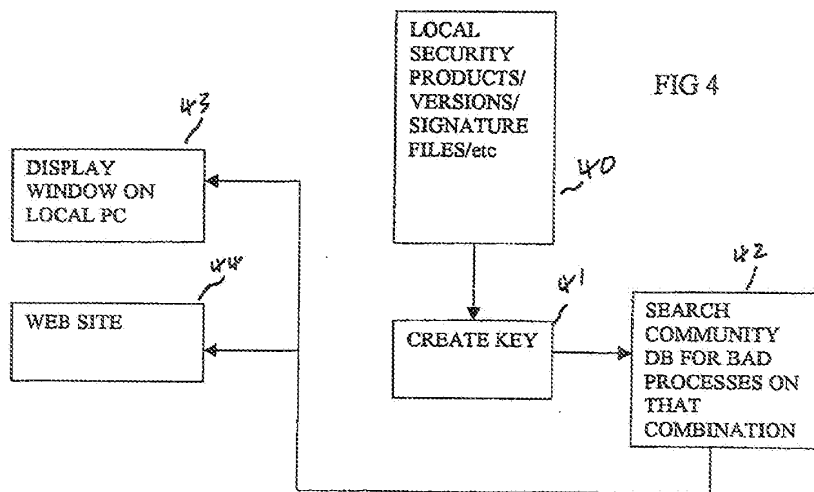


FIG 4

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 M Morris		
Filer:		Dale S. Lazar/Ava M. Dixon		
Attorney Docket Number:		339000-000014		
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	9	60	540
Miscellaneous-Filing:				
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				1790

Electronic Acknowledgement Receipt	
EFS ID:	13197626
Application Number:	13543866
International Application Number:	
Confirmation Number:	7855
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn M Morris
Customer Number:	47604
Filer:	Dale S. Lazar/Ava M. Dixon
Filer Authorized By:	Dale S. Lazar
Attorney Docket Number:	339000-000014
Receipt Date:	08-JUL-2012
Filing Date:	
Time Stamp:	17:57:21
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$ 1790
RAM confirmation Number	7301
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	----------------------------------	------------------	------------------

1		ContinuationApplication.pdf	22532318 fab6ed76e21649afa5bba0686755bc454a0bb06a	yes	68
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal of New Application		1	1	
	Application Data Sheet		2	6	
	Oath or Declaration filed		7	10	
	Specification		11	57	
	Claims		58	64	
	Abstract		65	65	
	Drawings-only black and white line drawings		66	68	
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	36670 c7af8d596457aa1bde33e67a0deeffa0a0b4ecc17	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			22568988		
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. <u>New Applications Under 35 U.S.C. 111</u> 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. <u>National Stage of an International Application under 35 U.S.C. 371</u> 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. <u>New International Application Filed with the USPTO as a Receiving Office</u> 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.					

METHODS AND APPARATUS
FOR DEALING WITH MALWARE

This application is a continuation of U.S. Application
5 No. 11/477,807 filed June 30, 2006, which claims priority
to United Kingdom Application No. 0513375.6, filed June 30,
2005. The entirety of all of the above-listed Applications
are incorporated herein by reference.

The present invention relates generally to methods and
10 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
15 computer has from malware. In another aspect, the present
invention relates to a method and apparatus for classifying
a computer object as malware or as safe. In another
aspect, the present invention relates to a method of
installing software on a computer.

20

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
25 the like.

A typical anti-malware product, such as anti-virus
scanning software, scans objects or the results of an
algorithm applied to the object or part thereof to look for
30 signatures in the object that are known to be indicative of
the presence of a virus. Generally, the method of dealing
with malware is that when new types of malware are

EAST\48798496.1

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
5 signatures are then released as updates to their anti-malware programs. Heuristic methods have also been employed.

These systems work well for protecting against known
10 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 combating that malware being generated or updated and supplied to users.
15 Thus, users are at risk from new malware for a certain period of time which might be up to a week or even more. Moreover, in order to try to defeat anti-virus products, the malware writers use obfuscation techniques in order to attempt to hide the signature or signature base data of the
20 virus code from detection. Typically, the obfuscation involves encrypting or packing the viral code.

WO-A-2004/097602 describes a system that analyses computer files received or generated by a local computer
25 and compares these with a database of known files to determine whether a particular file is known and if so whether it has been known about long enough that it can be regarded as "safe". However, in practice, on its own this is not likely to provide for adequate protection because,
30 for example, the active payload of a virus or Trojan may only be programmed to activate at a particular date, or upon receiving a message or instruction from a local or

EAST\48798496.1

remote system or process, or on the occurrence of a particular event that may be many months or even years after the process has been first run or is released. Thus, just looking at the age of a file is an unsatisfactory way
5 of determining whether it is properly safe and will remain so.

In the system of US-A-2004/0083408, a worm in a file is detected by examining connection attempts made by the
10 specific file running on a computer.

US-A-6944772, US-A-6772346, EP-A-1549012 and EP-A-1280040 all disclose "community-based" anti-malware systems in which a plurality of "local" computers all
15 connect via a network (which may be a LAN or the Internet, for example) to a central computer. On encountering a file that is not already known to them, the local computers send a request to the central computer for authorisation to run the file. If the file is recognised at the central
20 computer, then the central computer can send permission for the local computer to run the file if the file is known to be safe or send a "deny" command if the file is known to be malicious. However, in each of these prior art proposals, if the file is not known at the central computer, then the
25 whole file is sent to the central computer where it can be analysed to determine whether it should be regarded as safe or malware. Such analysis is typically carried out manually or "semi-manually" by subjecting the file to detailed analysis, for example by emulation or
30 interpretation, which can still take days given the human involvement that is typically required. There is therefore still a considerable period of time before a new file is

EAST\48798496.1

classified as safe or as malware. In the case of these prior art systems, the request for authorisation to run the file that is sent by a local computer to the central computer may comprise sending a checksum or "signature" or
5 "key" that uniquely represents the file.

A similar community-based anti-malware system is disclosed in WO-A-02/33525. In this system, in the case that a local computer is seeking clearance to run a file
10 that is not known by the central computer to be safe or malware, some limited audit information about the prevalence of the file on other local computers can be sent to a human system administrator associated with the local computer that is seeking permission to run the file. The
15 human system administrator can therefore make a better informed though still "manual" decision as to whether or not the file is safe to run.

In the system of US-A-2004/0073810, a metafile
20 containing data about an attachment or other transmitted file is sent to a central computer. The data about that file is analysed to determine a likelihood of the transmitted file being malware. A specific example given is that if the transmitted file has been transmitted via at
25 least a certain number of servers, then it should be treated as malware.

In the systems disclosed in US-A-2005/0021994 and US-A-2004/0153644, pre-approved files, which may be
30 certified as safe by for example the software vendor associated with the files, may be permitted always to run without further checking. In one embodiment of the system

EAST\48798496.1

of US-A-2004/0153644, monitoring is carried out to decide that a file is malicious if an abnormally high number of requests by that file is received at a central authority from plural local computers in a time period or if an
5 abnormally high number of requests by that file on a single computer is received from the single local computer in a time period.

In the system of US-A-2004/0006704, a comparison is
10 made between installed versions of software on a computer with a database of software versions and their known vulnerabilities. A user of the computer can therefore be informed of specific risks and how to minimise those risks by updating existing or installing new software.

15

In the system of WO-A-03/021402, a central database holds a virtual image of all files stored on each of plural local computers. If a threat in one local computer is identified, other local computers with a similar
20 configuration can be notified of the risk.

Thus, the prior art systems either rely on deep analysis of a new object in order to determine whether or not the object is malicious, which introduces delay and
25 therefore risk to users during the period that the file is analysed and new anti-malware signatures distributed, or limited analysis of the operation of the particular object or its method of transmission to a computer is carried out to decide a likelihood of the object being malicious.

30

EAST\48798496.1

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

at a base computer, receiving data about a computer
5 object from each of plural remote computers on which the
object or similar objects are stored;
comparing in the base computer the data about the
computer object received from the plural computers; and,
classifying the computer object as malware on the
10 basis of said comparison.

Compared to the prior art that relies solely on
signature matching, this aspect allows a comparison to be
made between the objects and/or their effects on the
15 different remote computers to determine whether or not a
particular object should be classed as good or as malware.
Sophisticated pattern analysis can be carried out. This
allows a rapid determination of the nature of the object to
be made, without requiring detailed analysis of the object
20 itself as such to determine whether it malware and also
avoids the need to generate new signatures to be used for
signature matching as in the conventional prior art anti-
virus software.

25 In a preferred embodiment, the data about the computer
object that is sent from the plural remote computers to the
base computer and that is used in the comparison includes
one or more of: executable instructions contained within
or constituted by the object; the size of the object; the
30 current name of the object; the physical and folder
location of the object on disk; the original name of the
object; the creation and modification dates of the object;

EAST\48798496.1

vendor, product and version and any other information
stored within the object; the object header or header held
by the remote computer; and, events initiated by or
involving the object when the object is created, configured
5 or runs on the respective remote computers.

Preferably, the comparing identifies relationships
between the object and other objects. In an example, this
can be used immediately and automatically to mark a child
10 object as bad (or good) if the or a parent or other related
object is bad (or good). Thus, if at least one other
object to which said object is related is classed as
malware, then the method may comprise classifying said
object as malware. Said other objects include the object
15 or similar objects stored on at least some of the remote
computers. Said other objects may include other objects
that are parent objects or child objects or otherwise
process-related objects to said object.

20 In a most preferred embodiment, the data is sent in
the form of key that is obtained by a hashing process
carried out in respect of the objects on the respective
remote computers. A major advantage of using such a key is
that it keeps down the volume of data that needs to be
25 transmitted to the base computer. Given that there may be
thousands or even millions of connected remote computers
and further given that each may send details about very
many objects, this can be an important advantage.

30 The key preferably has at least one component that
represents executable instructions contained within or
constituted by the object. This important preferred

EAST\48798496.1

feature allows a comparison to be made at the base computer of only the executable instructions of the object. This means for example that differently named objects that basically have the same executable instructions, which is often an indicator that the objects are malware, can nevertheless be regarded as the "same" object for this purpose. As another example, a new version of a program may be released which has minor changes compared to a previous version already known to the base computer and which in substance, at least in respect of the executable instructions, can be regarded as being the same as the previous version. In that case, the minor differences can be ignored and the objects regarded as being the same. Not only is this useful in distinguishing between malware and for example revised versions of previous software, it also keeps down the data transmission and storage requirements because the base computer can inform the remote computers that an apparently new object is for this purpose the same as a previously known object, thus avoiding having the remote computers send full details about the object or the object itself to the base computer.

The key preferably has at least one component that represents data about said object. Said data about said object may include at least one of: the current name of the object; the physical and folder location of the object on disk; the original name of the object; the creation and modification dates of the object; vendor, product and version and any other information stored within the object; the object header or header held by the remote computer; and, events initiated by or involving the object when the

EAST\48798496.1

object is created, configured or runs on the respective remote computers.

The key preferably has at least one component that
5 represents the physical size of the object.

Where more than one of these components are present in the key, the plural components are preferably severable.

10 The method may comprise initially classifying an object as not malware, generating a mask for said object that defines acceptable behaviour for the object, and comprising monitoring operation of the object on at least one of the remote computers and reclassifying the object as
15 malware if the actual monitored behaviour extends beyond that permitted by the mask. This provides an efficient and effective way of monitoring the behaviour of an object that has been classified or regarded as good and allows the object to be reclassified quickly as malware if the
20 behaviour of the object warrants it.

According to a second aspect of the present invention, there is provided apparatus for classifying a computer object as malware, the apparatus comprising:

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

the base computer being constructed and arranged to
30 compare the data about the computer object received from said plural computers; and,

EAST\48798496.1

the base computer being constructed and arranged to classify the computer object as malware on the basis of said comparison.

5 According to a third aspect of the present invention, there is provided a method of providing data about a computer object from a remote computer to a base computer so that a comparison can be made at the base computer with similar data received from other remote computers, the
10 method comprising:

 providing from a remote computer to a base computer data about a computer object that is stored on the remote computer;

 the data including one or more of: executable
15 instructions contained within or constituted by the object; the size of the object; the current name of the object; the physical and folder location of the object on disk; the original name of the object; the creation and modification dates of the object; vendor, product and version and any
20 other information stored within the object; the object header or header held by the remote computer; and, events initiated by or involving the object when the object is created, configured or runs on the respective remote computers;

25 the data being sent in the form of key that is obtained by a hashing process carried out in respect of the object on the remote computer.

 This method, which may be carried out by so-called
30 agent software running on the remote computer, allows for efficient sending of data to the base computer, which minimises data transmission and storage requirements and

EAST\48798496.1

also permits rapid analysis to be made at the base computer.

The key preferably has at least one component that
5 represents executable instructions contained within or constituted by the object.

The key preferably has at least one component that represents data about said object. Said data about said
10 object may include at least one of: the current name of the object; the physical and folder location of the object on disk; the original name of the object; the creation and modification dates of the object; vendor, product and version and any other information stored within the object;
15 the object header or header held by the remote computer; and, events initiated by or involving the object when the object is created, configured or runs on the respective remote computers.

20 The key preferably has at least one component that represents the physical size of the object.

According to a fourth aspect of the present invention, there is provided a method of determining the protection
25 that a remote computer has from malware, the method comprising:

receiving at a base computer details of all or selected security products operating at a point in time on said remote computer;

30 receiving similar information from other remote computers connected to the base computer; and,

EAST\48798496.1

identifying any malware processes that were not identified by said other remote computers having that particular combination of security products.

5 In this way, the base computer can be used to obtain information as to whether for example a particular, specific combination of operating system and various security products, including settings and signature files existing at a point in time, renders a particular computer
10 having those products and settings susceptible or vulnerable to any particular malware object. The user can be advised accordingly and for example provided with recommendations for remedying the situation.

15 The method may therefore comprise providing information to the user of said remote computer that said remote computer may be susceptible to attack by said malware processes on the basis of said identifying.

20 The details of all or selected security products preferably includes the name of the security products, versions, and loaded signature files.

According to a fifth aspect of the present invention,
25 there is provided apparatus for determining the protection that a remote computer has from malware, the apparatus comprising:

 a base computer constructed and arranged to receive computer details of all or selected security products
30 operating at a point in time on said remote computer;

the base computer being constructed and arranged to receive similar information from other remote computers connected to the base computer; and,

the base computer being constructed and arranged to
5 identify any malware processes that were not identified by said other remote computers having that particular combination of security products.

According to a sixth aspect of the present invention,
10 there is provided a method of classifying a computer object as malware or as safe, wherein said computer object is a descendant or otherwise related object of a first computer object, the method comprising:

classifying a first computer object as malware or as
15 safe;

identifying in a key relating to said first computer object a component that uniquely identifies the first computer object and that is inherited or otherwise present in the key of a descendant or other related computer object
20 of the first computer object; and,

classifying said computer object as malware or as safe as the case may be on the basis of the unique identifier component being present in the key of said computer object.

25 This aspect uses the concept of ancestry to enable objects to be marked as malware. For example, any particular process may spawn child processes which are therefore related. The key relating to the first object may be inspected to identify a component that uniquely
30 identifies the first object and that is inherited or otherwise present in the key of a descendant or other related object of the first object.

EAST\48798496.1

The method may comprise monitoring activities of said first computer object and reclassifying the first computer object as malware in the case that it was initially
5 classified as safe and subsequently determined to be malware, the method further comprising automatically classifying as malware any computer object that has a key in which said unique identifier component is present.

10 According to a seventh aspect of the present invention, there is provided apparatus for classifying a computer object as malware or as safe, wherein said computer object is a descendant or otherwise related object of a first computer object, the apparatus comprising:

15 a computer constructed and arranged to classify a first computer object as malware or as safe;

the computer being constructed and arranged to identify in a key relating to said first computer object a component that uniquely identifies the first computer
20 object and that is inherited or otherwise present in the key of a descendant or other related computer object of the first computer object; and,

the computer being constructed and arranged to classify said computer object as malware or as safe as the
25 case may be on the basis of the unique identifier component being present in the key of said computer object.

According to an eighth aspect of the present invention, there is provided a method of installing
30 software on a computer, the method comprising:

on initiation of installation of software on a computer, providing a computer-generated prompt on the

EAST\48798496.1

computer to a user to ascertain whether the user authorises the installation; and,

ceasing the installation if a user authorisation is not received, else:

- 5 receiving at the computer the user's authorisation to proceed with the installation;
- proceeding with the installation;
- obtaining data about computer objects that are created or used during the installation;
- 10 storing said data at the local computer.

This provides for security when a user is installing new software and is not for example connected to a base computer having a community database of the type mentioned
15 above. In that case, the method, which may be implemented in agent software running on the local computer, allows the user to permit the installation to proceed whilst at the same time gathering data about the objects (such as processes, new files, etc.) that are created during the
20 installation.

Preferably, the locally stored data is referred to during the installation to ensure that all objects created or used during the installation are part of the
25 installation process, and, if it is found that objects created or used during the installation are not part of the installation process, either or both of: (i) ceasing the installation and (ii) providing a computer-generated prompt on the computer to the user accordingly. This allows the
30 method to ensure that only those objects that are required for the installation are permitted to be created or used and thus avoids unwittingly allowing malware to install

EAST\48798496.1

(given that malware often creates objects that are not expected as part of a normal installation of new software).

In a preferred embodiment, the method comprises
5 connecting the computer to a community database that is connectable to a plurality of computers, and uploading the stored data to the community database for comparison with similar data provided by other computers.

10 The method may comprise downloading data about trusted installers to the computer, said data about trusted installers being referred to during the installation such that any objects relating to or created by the trusted installer are automatically authorised to proceed. This
15 facilitates installation of software that is known a priori to be trustworthy.

Said data about trusted installers may be referred to only for a predetermined time period following receipt at
20 the computer of the user's authorisation to proceed with the installation.

The present invention also includes computer programs comprising program instructions for causing a computer to
25 perform any of the methods described above.

Although the embodiments of the invention described with reference to the drawings comprise computer processes performed in computer apparatus and computer apparatus
30 itself, the invention also extends to computer programs, particularly computer programs on or in a carrier, adapted for putting the invention into practice. The program may

EAST\48798496.1

be in the form of source code, object code, a code intermediate source and object code such as in partially compiled form, or in any other form suitable for use in the implementation of the processes according to the invention.

- 5 The carrier be any entity or device capable of carrying the program. For example, the carrier may comprise a storage medium, such as a ROM, for example a CD ROM or a semiconductor ROM, or a magnetic recording medium, for example a floppy disk or hard disk. Further, the carrier
10 may be a transmissible carrier such as an electrical or optical signal which may be conveyed via electrical or optical cable or by radio or other means.

Embodiments of the present invention will now be
15 described by way of example with reference to the accompanying drawings, in which:

Figure 1 shows schematically apparatus in which an embodiment of the present invention may be implemented;
20

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

25 Figure 3 is a flowchart showing schematically the operation of another example of a method according to an embodiment of the present invention; and,

Figure 4 is a flowchart showing schematically an
30 information obtaining stage.

EAST\48798496.1

Referring to Figure 1, a computer network is generally shown as being based around a distributed network such as the Internet 1. The present invention may however be implemented across or use other types of network, such as a
5 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
10 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
15 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.

In one preferred embodiment, the base computer 3 holds
20 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
25 computers 2. As will be discussed further below, data representative of each object 4 preferably takes the form of a so-called signature or key relating to the object and its effects. As will also be discussed further below, the database 7 may further include a mask for the object 4 that
30 sets out the parameters of the object's performance and operation.

EAST\48798496.1

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 local "agent" software running on the remote computer 2, the operation of the process is hooked so that the agent software 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 software 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.

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 central system to take account of the location, status or ownership of the remote computer or timeframe.

If the object is unknown 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

EAST\48798496.1

and preferably 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.

15

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.

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

FAST\48798496.1

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:

5 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
10 sent by the remote computer 2 is used for this purpose, and this signature is initially marked as bad or unsafe 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
15 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
20 remote computer 2.

 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
25 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
30 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

EAST\48798496.1

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.

5

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

The key in the preferred embodiment is specially arranged to have at least three severable components, a first of said components representing executable instructions contained within or constituted by the object, a second of said components representing data about said object, and a third of said 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, 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.

EAST\48798496.1

In one preferred embodiment, a check sum 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
5 checksums are generated depending on the nature of the file:

Type 1: five different sections of the file are check summed. These include the import table, a section at the
10 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;

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

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

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

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

EAST\48798496.1

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. 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.

15 This "meta data" enables current and newly devised heuristics to be run on the data in the community database 7.

20 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 that either act upon it or are acted upon by it.

25 The preferred central heuristics use five distinct processes to establish if an object is safe, unsafe or suspicious.

30 The first of the said processes utilises the singularity or plurality of names, locations, vendor, product and version information captured and correlated from all of the remote computers 2 that have seen the

EAST\48798496.1

object. By considering the plurality of this information for a single object, a score can be determined which can be used as a measure of the authenticity and/or credibility of the object. Most safe objects tend not to use a large
5 plurality of identifying information or locations. Rules can be established to consider this information in respect of the type of object and its location. For example, temporary files often utilise a plurality of system generated file names which may differ on each remote
10 computer for the same object. Where an object has little plurality, then it provides a reference point to consider its behaviour in comparison to the known behaviours of other objects that have previously used that identifying information. For example, a new object that purports to be
15 a version of notepad.exe can have its behaviour compared with the behaviour of one or more other objects that are also known as notepad.exe. This comparison may be against a single other object or multiple other objects that use the same or even similar identifying information. In this
20 way, new patterns of behaviour can be identified for the new object. Also it allows the preferred embodiment to police an object's behaviour over time to identify new behavioural patterns that may cause an object that was previously considered safe to have its status reconsidered.
25 Alternatively, the score based on identities may be considered along with scores for other objects or scores created by other processes on this object to be considered in combinations.

30 The second of the said processes utilises an object's relationship to other objects that act upon it or upon which it acts. For example, analysis can be made of which

EAST\48798496.1

object created this object, which objects this object created, which objects created a registry key to run or configure this object, which objects were configured by or had registry keys created by this object, etc. In this
5 regard an object is considered to have a relationship based on the event performed by it upon another object, or upon it by another object. This simple 1-to-1 relationship chain provides a complex series of correlation points, allowing ancestral relationships to be considered for any
10 object and its predecessors by event or its issue (i.e. child and sub-child processes) by event. This allows a score to be developed that describes its relationships and associations with known, unknown, known safe or known bad objects or a combination thereof. Objects that have
15 specific relationships, volumes of relationships or mixes of relationships to one type or another may be judged safe or unsafe accordingly. Alternatively, the relationship-based score may be considered along with other scores to arrive at a determination of safe or unsafe. This data can
20 also be used to deduce a number of factors about objects related directly or via other objects and their behaviours. For example it is possible to deduce how one object's behaviour can be influenced or changed by its association or linkage to another. Consider for example notepad.exe as
25 supplied by Microsoft with the Windows series of operating systems. It has a limited range of functionality and would not be expected therefore to perform a wide variety of events, such as transmitting data to another computer or running other programs etc. However, the behaviour of
30 notepad.exe could be modified by injecting new code into it, such as via dynamic link library injection (DLL injection). In this case notepad.exe would now have new

EAST\48798496.1

capabilities derived by the code injection or linkage to another object. Using the data that defines the relationships between objects it is possible to deduce that the new behaviours of a program can be attributed to the association with another object. If that new behaviour is malevolent, then it is possible to mark either or all processes as unsafe as appropriate.

The combination of behaviours captured provide a basis to determine if the object is safe or unsafe. Malware typically exhibit certain behaviour and characteristics. For example, malware frequently has a need to self-persist. This manifests itself in the need to automatically restart on system restarts or upon certain events. Creating objects in specific locations to auto restart or trigger execution is a typical characteristic of malware. Replacing core objects of the Windows system environment are another example of typical characteristics of malware. By providing a pattern of behaviour, the determination of objects to be unsafe or safe can be automated. The centralisation of the community data in the community database 7 provides the ability to rapidly assimilate object behaviours, allowing for the rapid identification and determination of malware. Objects may also perform events upon themselves which can be considered in deriving a score.

The third said process involves time and volumes. Relevant data includes when the object was first seen, when it was last seen, how many times it has been seen, how many times it has been seen in a given interval of time, and the increase or decrease of acceleration in it being seen.

EAST\48798496.1

This information is highly relevant in determining the prevalence of an object in the community of remote computers. A score is developed based on these metrics which can be used to determine if an object is safe, unsafe
5 or too prevalent to allow it to execute or propagate without very thorough examination. In this case, the object can be temporarily held or blocked from executing pending further information about its behaviour or relationships. This score may also be used in combination
10 with scores from other processes. Time is also highly relevant in combination with other information, including but not limited to behaviours and identities. For example in the case of polymorphic or randomly named objects, time is a powerful qualifier. (A polymorphic virus changes its
15 encryption algorithm and the corresponding encryption keys each time it replicates from one computer to another and so can be difficult to detect by conventional measures.) A program that creates other programs can often be considered normal or abnormal based on its activity over time.

20

The fourth said process considers the behaviour of an object. This allows a score to be developed based on the types of events performed by an object or events performed on it by itself or other objects. The centralised system
25 of the community database 7 allows for an unlimited number of event types and can consider the object performing the event or the object having the event performed upon it, or both. Some event types also relate to external information other than objects, for example a program performing an
30 event to connect with an Internet Chat Relay site, or a program modifying a non-executable file such as the Windows hosts file. The behavioural events of an object, be they

EAST\48798496.1

as "actor" (i.e. the object doing something to another object) or as "victim" (i.e. the object has something done to it by another object) of any event can be considered in many ways, such as in combination, in sequence, in volume, 5 in presence or absence, or in any combination thereof. The behavioural events in the preferred embodiment may have been provided by a remote computer 2 or from other external sources. The process can consider these in isolation or in combination. Furthermore it is a feature of the preferred 10 embodiment that the behavioural events can be considered in combination with the status of other objects upon which the object acts or that act upon the object. For example, creating a program may have a different score if the program being created is safe, unsafe, new, unknown or 15 suspicious. Similarly, a program that is created by a known bad program will likely have a different score attributed to its creation event depending on the status of the object creating it.

20 The fifth process considers the behaviour of a web page or script. In this respect, the web page and url combination is assigned a unique identity which allows its behaviour to be tracked as if it were an object like any other executable file. In this example, the web page may 25 perform events that would normally be seen as events performed by the web browser (e.g. IExplore.exe or Firefox.exe). The preferred embodiment substitutes the identifying details and signatures of the web browser for the "pseudo" object identity associated with the web page 30 being displayed or executing within the browser. In this respect, the status of the web page and/or web site to which it relates may be determined as safe, unsafe, unknown

EAST\48798496.1

or suspicious in the same way as any other object. The web page's "pseudo" object identity also allows the preferred embodiment to block, interject or limit the functionality of that web page or web site to prevent some or all of its potentially unsafe behaviour or to provide the remote user with qualifying information to guide them about the safety of the web site, web page or their content.

Amongst other types, the types of meta data captured might be:

"Events": these define the actions or behaviours of an object acting upon another object or some other entity. The event has 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 an other entity upon which the act is being performed (the "Victim"). 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:

<u>Actor</u>	<u>Event Type</u>	<u>Victim</u>
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	Object4

"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

EAST\48798496.1

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
5 it is part of and the version number of the file and its contents, its original file name, and its file size.

"Genesisactor" - the key of an object that is not the direct Actor of an event but which is the ultimate parent
10 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.

15 "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"),
20 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.

"Event Checksums": because the event data can be
25 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
30 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

EAST\48798496.1

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
5 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.

10 Thus, the meta data 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
15 or five or six or all seven (or more elements not specifically mentioned here). This may be used accordingly to model, test and create new automated rules 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
20 computers 2 to identify and determine the response of the remote computers 2 to new or unknown processes and process activity.

Moreover, it is possible to monitor a process along
25 with any optional sub-processes as an 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
30 effective monitoring (without unnecessary blocking) of programs, such as Internet Explorer or other browsers, whose functionality may be easily altered by downloadable

EAST\48798496.1

optional code that users acquire from the Internet, which is of course the principal source of malevolent code today.

The potentially high volume of active users gives a
5 high probability of at least one of them being infected by
new malware. The speed of propagation can be detected and
recorded so that the propagation of malware can be detected
and malware designated as bad on the basis of the speed of
propagation, optionally in combination with the other
10 factors discussed above, such as file size, location and
name. The simple volume of infection can also be used as a
trigger. In a further embodiment, difference of naming of
an otherwise identical piece of code combined with
acceleration of first attempts to execute the code within
15 the community allows pattern matching that will show up an
otherwise identically signed piece of code as bad.

This feature allows the statement in some embodiments
that "nothing will propagate in our community faster than X
20 without being locked down", so that if any process or event
propagates more quickly over a given duration, it is marked
as bad. This is for reasons of safety given that if for
example an object is propagating quickly enough, then it
might infect computers before it can be analysed to
25 determine whether or not it is malware.

This process can be automated by the identification of
the vector of propagation in the community (i.e. the source
of type of propagation), from timestamp data held in the
30 community database and the marking of a piece of code that
has these attributes as bad. By comparison, it is believed
that all other anti-malware providers rely on a simplistic

EAST\48798496.1

known bad model and therefore are reliant primarily on malware infection actually occurring on terminals and being reported.

5 Thus, the community database 7 can be used to make early diagnosis, or simply to take precautionary measures, and thus stop potentially fast propagating worms and other malware very, very early in their life cycle. Given that it is possible to create a worm that can infect every
10 computer connected to the Internet within a matter of a few minutes, this feature is highly desirable.

Even faster determination may be made by combining data defining the speed of propagation of a new piece of
15 software with metadata collected by the agent software from the remote computers 2 and fed to the community database 7. This includes monitoring processes that attempt to conceal themselves from the user by randomly changing name and/or location on the remote computers 2. It also includes a
20 process's attempt to create an identical copy (i.e. with identical code contents) on the computer but with a different name. This is a classic attribute of a worm.

The signature of an object may comprise or be
25 associated with a mask which can be built up with use of that object and which indicates the particular types of behaviour to be expected from the object. 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
30 operation of that object may be monitored within the parameters of the mask. The mask might indicate for example, the expected behaviour of the object; any external

EAST\48798496.1

requests or Internet connections that that object might
legitimately have to make or call upon the remote computer
2 to make, including details of any ports or interfaces
that might be required to be opened to allow such
5 communication; any databases, either local or over a local
area network or wide area network or Internet, that may be
expected to be interrogated by that object; and so on.
Thus, the mask can give an overall picture of the expected
"normal" behaviour of that object.

10

In practice, therefore, in one embodiment the
behaviour of the object is continually monitored at the
remote computer(s) 2 and information relating to that
object continually sent to and from the community database
15 7 to determine whether the object is running within its
expected mask. Any behaviour that extends beyond the mask
is identified and can be used to continually assess whether
the object continues to be safe or not. Thus, if for
example the object, on a regular basis (say monthly or
20 yearly) opens a new port to update itself or to obtain
regular data, then this information is flagged. If it is
found that the object has done this on other remote
computers and has had no ill effects, or this behaviour is
known from other objects and known to be safe, then this
25 behaviour might be considered as safe behaviour and the
mask is then modified to allow for this. If it has been
found previously that this new behaviour in fact causes
unsafe or malevolent results, then the object can then be
marked as unsafe even if previously it was considered safe.
30 Similarly, if the object attempts to connect to a known
unsafe website, database or to take action that is known as

EAST\48798496.1

generally being action only taken by unsafe programs, then again the object may be considered to be unsafe.

This is shown schematically in Figure 3. Figure 3
5 also shows the concept that any object can be pre-
authorised by, for example a trusted partner, such as a
major software company, a verification authority, a
Government department, and so on. Pre-authorisation
enables a supplier of a new object, which has not been
10 released before, to get pre-authorisation for that object,
and optionally includes the provision by that supplier of a
mask detailing the expected and allowable behaviour of that
object.

15 Referring to Figure 3 for example, when a process is
run, the local and/or community databases are searched as
before at step 31. If the process is not a pre-authorised
one, then the steps of Figure 2 may be taken and the
process might be allowed to run or not at step 32. If the
20 process is pre-authorised, as determined at step 33, then
it is immediately allowed to run, step 34. This may
terminate the operation of the method. However, in a
preferred variation, the process is then monitored whilst
running, and is monitored each time it is run in the future
25 in a monitoring state step 35 to determine whether its
behaviour falls within its pre-authorised mask 36. If the
behaviour falls within the pre-authorised behaviour, then
the process is allowed to continue to run. If the
behaviour extends beyond the allowed mask, such as by
30 trying to instigate further processes or connections that
have not been pre-authorised, then this behaviour is
flagged at an alert step 37. Various actions could be

EAST\48798496.1

taken at this stage. The process might simply not be allowed to run. Alternatively, the trusted authority that initially enabled pre-authorisation might be contacted, who may be able to confirm that this behaviour is acceptable or
5 not. If it is acceptable, then the mask could be modified accordingly. If not acceptable, then the process might be marked as unsafe. Many other actions may be taken upon the noting of such an alert state.

10 If the process has been found not to be pre-authorised at step 33 but is nevertheless allowed to run, then the process is monitored at step 38 in order to generate a mask
39 representative of the normal behaviour of that process. Data representative of this mask might be sent to the
15 community database 7 for scanning when other computers run that process. By continually monitoring a process each time it is run or during running of the process, any behaviour that differs from previous behaviour of the process can be noted and the mask can be modified, or this
20 behaviour might be used to determine that a process that was once considered safe should now be considered to be unsafe.

In another embodiment, a computer 2 may have agent
25 software installed that periodically or on-demand provides information to the community database 7 that is representative of all or selected ones of the software products loaded on or available the computer 2. In particular, this may be information on one or more of: all
30 the locally-loaded security products (such as anti-malware systems including anti-virus software, anti-spyware, anti-adware and so on), firewall products, specific settings and

EAST\48798496.1

details of which signature files are currently loaded,
version details for the operating system and other
software, and also information such as which files are
operating and the particular version and software settings
5 at any time. (It will be understood from the following
that auditing and testing for a match for more of these
criteria increases the likelihood of computers being very
similarly arranged and thus reduces the rate of false
negatives and positives during the match search.)

10

The information relating to these software products,
etc. may be provided individually to the community
database. Preferably however, again for reasons of data
quantity for storage and transmission, the information is
15 provided as a signature or key representative of the
information (e.g. by a hashing or compression function at
the computer 2). Figure 4 shows schematically how the
details of all local security products, versions, signature
files, firewall settings, etc. 40 are used to create a key
20 41. The key is transmitted to the community database 7.
Since the community database 7 is provided with such
information from many, possibly millions, of users'
computers 2, it is likely to hold corresponding information
for other computers 2 that have the same or a similar
25 configuration of security products, etc. Thus, the
community database 7 can be searched at step 42 for other
computers 2 having the same or a similar combination of
security products including the same setting, signature
files loaded and so on.

30

The community database 7 in this embodiment is also
provided by the agent software with details of processes

EAST\48798496.1

run by every computer 2 and thus knows whether or not a process has been detected by each computer 2.

In this way, the community database 7 can be used to
5 obtain information as to whether for example a particular, specific combination of operating system and various security products, including settings and signature files existing at a point in time, renders a particular computer 2 having those products and settings susceptible or
10 vulnerable to any particular malware object.

In a simple example, if for example the database knows that a computer in the past has version A of anti-virus product B with downloaded signature update C, and also has
15 a firewall D with particular settings E, and perhaps anti-spyware software F with signature updates G, but that a particular malware process P was not detected by this combination of programs at that point in time, then this information can be provided to a computer 2 that is known
20 as having that combination of security programs/settings, and can be used to indicate that that computer 2 is vulnerable in the short term to attack by that particular malware process. This information can be presented to the user either by displaying a window 43 on the screen display
25 of the computer 2 or by directing the user to a particular website which explains the position in more detail. The user might be informed for example that their particular combination of security products, etc., exposes their computer to a risk of being infected by the Sobig virus as
30 that virus is not detectable by their computer. The user might be offered specific advice (e.g. to update a particular anti-virus program with a particular signature

EAST\48798496.1

file) or software to download and install to remove the risk.

Thus, the community database 7, when provided with
5 information relating to all the security products, etc. on
a particular computer at a particular time, is searched for
events for processes marked as "bad" that occurred on
computers with that particular mix of security products and
that were not locally detected. This information can then
10 be fed back to the user of the particular computer, for
example directly or by directing the user to a website.
This information can be provided virtually in real-time,
allowing a new user or a user of a new computer to be able
to increase the computer's effective security very quickly.

15

The preferred method also tracks which objects are
related to each other and uses the concept of ancestry to
enable objects to be marked as malware. For example, any
particular process may spawn child processes which are
20 therefore related. The key relating to the first object
may be inspected to identify a component that uniquely
identifies the first object and that is inherited or
otherwise present in the key of a descendant or other
related object of the first object. This component is
25 referred to herein as a "gene". This general technique may
be used in a number of ways:

a) A known and trusted parent process is afforded
the ability to create child processes which may be
30 automatically marked as safe to run on the local computer.
It is also possible that this "inherited" property may be
passed down to grand children processes and so on. This

EAST\48798496.1

safe status is passed to the parent's child processes and possibly, through them, further child processes (referred to here as "issue"), such signatures for the issue can all automatically be recorded in the local database as good.

5 This allows the issue processes to be quickly marked as good, even if a connection to the community database 7 is not available.

b) By monitoring activity of the parent process, if
10 it is later found that the parent process is malware, then all of the issue processes can all automatically be recorded in the local database as bad.

c) Similarly, by monitoring activity of the issue
15 processes, if it is later found that one of the issue processes is malware, then one or more of the parent process and all of the other issue processes (i.e. all of the related processes in this context) can all automatically be recorded in the local database as bad.

20

d) Parental creation of a signature for a child or children including the ability for these to be automatically marked as either good or bad depending on the parent's behaviour and determination. Note that in some
25 embodiments the product can "watch" or monitor the birth of a child process and automatically create the signature upon arrival. This provides the ability to monitor the creation of a bad program by another bad program. It is possible therefore to monitor the ancestry of a program so if for
30 example the grandfather creates a program (the father) and this in turn creates a bad program (the son), it is

EAST\48798496.1

possible automatically to determine the father as a bad program.

e) A feature may be included that allows for
5 automatic forfeiture of a child's inherited ability to
trigger the automatic creation of signatures on any further
births because the child, as parent, has already produced
bad offspring. Preferably, a rule is that if a file has
one bad offspring then the inherited ability can be
10 automatically removed.

f) An ability to watch clones or identical twins of
objects (e.g. the same process running on other systems in
the community) to compare the pattern of their issue and to
15 make decisions as to whether or not to treat any particular
process as malware.

One or more of these features a) to f) can be used to
provide a solution to the problem of producing a security
20 product that can be used effectively without 100% reliance
on being permanently connected to the Internet, which is
often impractical. Examples of this are Windows Update and
other processes used more and more by vendors who wish to
be able to roll out product updates automatically across
25 the worldwide web.

Possible benefits of these types of features above
conventional software are as follows. Antivirus software
tends to have a cache of known bad signatures. The problem
30 is keeping this up to date. Take the simple example of
someone buying a new computer. The computer comes with an
antivirus product preloaded with a signature cache.

EAST\48798496.1

Between the time when the PC was built, shipped to the store and bought by the user several days or weeks will have passed. The user starts the PC and is exposed to any new virus or malware which was created after the PC was
5 built. Full protection requires the user to connect to the internet and download updates. This cannot be guaranteed to occur ahead of other activities by the user on the internet (almost physically impossible to guarantee). With a local cache of known good processes, as in the
10 embodiments of the present invention, it is possible to ship the computer/terminal preloaded with a pre-generated cache of signatures for all of the good (clean) software preloaded by the computer manufacturer. In this case the user can connect to the internet knowing that any new or
15 updated programs will be immediately detected and verified. Also any auto-updating software can function forcing signatures to be automatically built for its children and more remote off-spring (i.e. grandchildren, great-grandchildren, etc).

20

Reference is now made to "Defeating Polymorphism: Beyond Emulation" by Adrian Stepan of Microsoft Corporation published in "Virus Bulletin Conference, October 2005" and also to US 60/789156 filed on 5th April 2006, the entire
25 content of which are hereby incorporated by reference. In that paper and patent application, there are disclosed methods of decrypting files to allow the files to be analysed to determine whether or not the file actually is malware. In US 60/789156 in particular, there is disclosed
30 a method of unpacking/decrypting an executable computer file using a host computer, the method comprising: partitioning the executable computer file into plural basic

EAST\48798496.1

blocks of code; translating at least some of the basic
blocks of code into translated basic blocks of code that
can be executed by the host computer; linking at least some
of the translated basic blocks of code in memory of the
5 host computer; and, executing at least some of the
translated basic blocks of code on the host computer so as
to enable the executable computer file to be unpacked or
decrypted, whereupon the unpacked or decrypted executable
computer file can be analyzed to determine whether the
10 executable computer file is or should be classed as
malware. There is also disclosed in US 60/789156 a method
of unpacking/decrypting an executable computer file, the
method comprising: partitioning the executable computer
file into plural basic blocks of code; creating at least a
15 read page of cache memory for at least some of the basic
blocks, the read page of cache memory storing a read cached
real address corresponding to a read cached virtual memory
address for the respective basic block, and creating at
least a write page of cache memory for at least some of the
20 basic blocks, the write page of cache memory storing a
write cached real address corresponding to a write cached
virtual memory address for the respective basic block; and,
emulating the executable file by executing at least some of
the basic blocks of code so as to enable the executable
25 computer file to be unpacked or decrypted, whereupon the
unpacked or decrypted executable computer file can be
analyzed to determine whether the executable computer file
is or should be classed as malware; wherein during the
execution of a basic block, at least one of the read page
30 and the write page of cache memory is checked for a cached
real address corresponding to the virtual address that is
being accessed for said basic block.

EAST\48798496.1

The techniques disclosed in these documents can be used in the present context when it is desired to analyse a file in detail. More generally however, the techniques
5 disclosed in these papers, and particularly the enhanced techniques disclosed in US 60/789156, can be used to provide information about the activity of a file when it is run on a computer because the techniques disclosed in these papers emulate the running of the file and therefore allow
10 the file's activity to be interpreted.

A further situation arises when users wish to install software while offline. In a preferred embodiment, when a user attempts to install new software while offline, agent
15 software running on the user's computer 2 prompts the user for authorisation to allow the installation process to proceed such that the execution of the installation can itself be "authorised" by the user. This authorisation by the user is treated as a "Genesis" event and will be so
20 termed hereinafter. However there are some processes commonly used in installation of software that communicate with other existing programs on the installation machine, e.g. Microsoft's MSIEXEC.

25 The Genesis approach involves a process that generates signatures as a result of the user's authorisation on the user's computer 2. Those signatures are stored in the local database on the user's computer 2. In one embodiment, those locally stored signatures are referred to
30 as necessary by the agent software during the installation process so that the installation can proceed. Alternatively, the security checks made by the agent

EAST\48798496.1

software can be switched off during the installation process. The switching off may only be for a limited duration, such as a few minutes which should be sufficient to allow most software to be installed, the off time
5 optionally being user-configurable.

In any event, once the installation has been completed and the user's computer 2 connected to the community database 7, the agent software on the user's computer 2 can
10 upload the signatures relating to the installation from the user's local database to the community database 7. With corresponding data from other users' computers 2, the community database 7 can then be used to make a rapid determination that the installation of this particular
15 software is benign.

As a variant to this embodiment, when a user's computer 2 is at some point in time on-line, the agent software on the user's computer 2 may download signatures
20 of a so-called "trusted installer" or "licensed installer". This allows the operation of a method such that a "licensed installer" and any child processes of the licensed installer are permitted to execute while a Genesis event is "current", e.g. within a period of minutes after an
25 authorisation from the user. Preferably signatures of licensed installers are always downloaded, as and when added to the community database 7, to a remote computer 2 while online.

30 There may be further refinements to this method, such as to prevent licensed installers executing if a media change has occurred during the currency of a Genesis event.

EAST\48798496.1

However, any unknown processes, which may be malware, may still be detected and blocked. Having a small number of licensed installers facilitates download, as minimal data is required, especially compared to downloading virus signature files. As another example, super-trusted installers, such as for example "Windows Update", may be employed whereby all new processes created by the super-trusted installer are marked immediately as safe.

10 In the case of an installation occurring when the remote computer 2 is connected to the community database 7, another option is that if the software that is about to be installed is not known to the community database 7, then the system will block the installation or alert the user.

15 For example, a message may be displayed at the user's computer 2 to the effect that "You are about to install some software. This software is not known to [the community]. Are you sure you wish to proceed?".

20 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.

CLAIMS

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

5 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, wherein said data includes information about events initiated or involving the object when the object is created, configured or runs
10 on the respective remote computers, said information including at least the identify of the object initiating the event, the event type, and the identity of the object or other entity on which the event is being performed;
 storing at the base computer said data received from
15 plural remote computers;
 comparing in the base computer the data about the computer object received from the plural computers to identify relationships between the object and other objects or entities; and,
20 classifying the computer object as malware on the basis of said comparison.

2. A method according to claim 1, wherein the relationship is between objects related directly, or
25 between objects related via other objects.

3. A method according to claim 1, wherein where an object and other objects are found to have a relationship, monitoring those related objects as a homogenous entity.
30

4. A method according to claim 1, comprising deducing an object to be malware based on the behaviour of a related

EAST\48798496.1

object.

5. A method according to claim 1, wherein if at least one other object to which said object is related is classed
5 as malware, then classifying said object as malware.

6. A method according to claim 1, wherein said other objects include the object or similar objects stored on at least some of the remote computers.

10

7. A method according to claim 1, wherein said other objects include other objects that are parent objects or child objects or otherwise process-related objects to said object.

15

8. A method according to claim 1, wherein the data about the computer object that is sent from the plural remote computers to the base computer and that is used in the comparison includes one or more of: executable
20 instructions contained within or constituted by the object;
the size of the object; the current name of the object;
the physical and folder location of the object on disk;
25 the original name of the object;
the creation and modification dates of the object;
vendor, product and version and any other information stored within the object; and,
the object header or header held by the remote
30 computer.

9. A method according to claim 1, wherein the data is

EAST\48798496.1

sent in the form of key that is obtained by a hashing process carried out in respect of the objects on the respective remote computers.

5 10. A method according to claim 9, wherein the key has at least one component that represents executable instructions contained within or constituted by the object.

11. A method according to claim 9, wherein the key has
10 at least one component that represents data about said object.

12. A method according to claim 11, wherein said data about said object includes at least one of:
15 the current name of the object;
 the physical and folder location of the object on disk;
 the original name of the object;
 the creation and modification dates of the object;
20 vendor, product and version and any other information stored within the object;
 the object header or header held by the remote computer; and,
 events initiated by or involving the object when the
25 object is created, configured or runs on the respective remote computers.

13. A method according to claim 9, wherein the key has at least one component that represents the physical size of
30 the object.

14. A method according to claim 1, comprising

EAST\48798496.1

initially classifying an object as not malware, generating a mask for said object that defines acceptable behaviour for the object, and comprising monitoring operation of the object on at least one of the remote computers and

- 5 reclassifying the object as malware if the actual monitored behaviour extends beyond that permitted by the mask.

15. Apparatus for classifying a computer object as malware, the apparatus comprising:

- 10 a base computer constructed and arranged to receive data about a computer object from each of plural remote computers on which the object or similar objects are stored, wherein said data includes information about events initiated or involving the object when the object is
- 15 created, configured or runs on the respective remote computers, said information including at least the identify of the object initiating the event, the event type, and the identity of the object or other entity on which the event is being performed;

- 20 the base computer being constructed and arranged to compare the data about the computer object received from said plural computers to identify relationships between the object and other objects or entities; and,

- the base computer being constructed and arranged to
- 25 classify the computer object as malware on the basis of said comparison.

16. Apparatus according to claim 15, wherein the base computer is constructed and arranged so as to identify the
- 30 relationship between objects related directly, or between objects related via other objects.

EAST\48798496.1

17. Apparatus according to claim 15, wherein the base computer is constructed and arranged so as, where an object and other objects are found to have a relationship, to monitoring those related objects as a homogenous entity.

5

18. Apparatus according to claim 15, wherein the base computer is constructed and arranged so as to deduce an object to be malware based on the behaviour of a related object.

10

19. Apparatus according to claim 15, wherein the base computer is constructed and arranged so that if at least one other object to which said object is related is classed as malware, then said object is classified as malware.

15

20. Apparatus according to claim 15, wherein the base computer is constructed and arranged so that said other objects include the object or similar objects stored on at least some of said remote computers.

20

21. Apparatus according to claim 15, wherein the base computer is constructed and arranged so that said other objects include other objects that are parent objects or child objects or otherwise process-related objects to said object.

25

22. Apparatus according to claim 15, wherein the base computer is constructed and arranged so as to compare the data where the data includes one or more of:

30

executable instructions contained within or constituted by the object;

the size of the object; the current name of the

EAST\48798496.1

object;

the physical and folder location of the object on
disk;

the original name of the object;

5 the creation and modification dates of the object;
vendor, product and version and any other information
stored within the object; and,
the object header or header held by the remote
computer.

10

23. Apparatus according to claim 15, wherein the base
computer is constructed and arranged so as to be able to
process data that is sent in the form of key that is
obtained by a hashing process carried out in respect of the
15 objects on said respective remote computers.

24. Apparatus according to claim 23, wherein the key
has at least one component that represents executable
instructions contained within or constituted by the object.

20

25. Apparatus according to claim 23, wherein the key
has at least one component that represents data about said
object.

25 26. Apparatus according to claim 25, wherein said data
about said object includes at least one of: the current
name of the object;

the physical and folder location of the object on
disk;

30 the original name of the object;
the creation and modification dates of the object;
vendor, product and version and any other information

EAST\48798496.1

stored within the object;

the object header or header held by the remote
computer; and,

events initiated by or involving the object when the
5 object is created, configured or runs on the respective
remote computers.

27. Apparatus according to claim 23, wherein the key
has at least one component that represents the physical
10 size of the object.

28. Apparatus according to claim 15, wherein the base
computer is constructed and arranged to generate a mask for
an object that is initially classed not as malware, said
15 mask defining acceptable behaviour for the object, and the
base computer is constructed and arranged to monitor
operation of the object on at least one of the remote
computers and to reclassify the object as malware if the
actual monitored behaviour extends beyond that permitted by
20 the mask.

29. A computer program recorded on non-transitory
computer readable medium comprising program instructions
for causing a computer to perform the method of claim 1.

METHODS AND APPARATUS
FOR DEALING WITH MALWARE

ABSTRACT

5

In one aspect, a method of classifying a computer object as malware includes receiving at a base computer data about a computer object from each of plural remote computers on which the object or similar objects are
10 stored. The data about the computer object received from the plural computers is compared in the base computer. The computer object is classified as malware on the basis of said comparison. In one embodiment, the data about the computer object includes one or more of: executable
15 instructions contained within or constituted by the object; the size of the object; the name of the object; the logical storage location or path of the object on the respective remote computers; the vendor of the object; the software product and version associated with the object; and, events
20 initiated by or involving the object when the object is created, configured or runs on the respective remote computers.

EAST\48798496.1



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
13/543,866	07/08/2012	2431	1790	339000-000014	29	2

CONFIRMATION NO. 7855

FILING RECEIPT



OC000000055461283

47604
DLA PIPER LLP US
P. O. BOX 2758
RESTON, VA 20195

Date Mailed: 07/23/2012

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, Turnditch, UNITED KINGDOM;
Paul Stubbs, Wyboston, UNITED KINGDOM;
Markus Hartwig, Milton Keynes, UNITED KINGDOM;
Darren Harter, Hucclecote, UNITED KINGDOM;

Assignment For Published Patent Application

PREVX LTD., PARK PRIDE, UNITED KINGDOM

Power of Attorney: The patent practitioners associated with Customer Number 47604

Domestic Priority data as claimed by applicant

This application is a CON of 11/477,807 06/30/2006

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.)

UNITED KINGDOM 0513375.6 06/30/2005

Request to Retrieve - This application either claims priority to one or more applications filed in an intellectual property Office that participates in the Priority Document Exchange (PDX) program or contains a proper **Request to Retrieve Electronic Priority Application(s)** (PTO/SB/38 or its equivalent). Consequently, the USPTO will attempt to electronically retrieve these priority documents.

If Required, Foreign Filing License Granted: 07/18/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/543,866**

Projected Publication Date: 11/01/2012

page 1 of 3

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 Assets Control, 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](https://www.selectusa.gov).

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 13/543,866			
APPLICATION AS FILED - PART I									
(Column 1)		(Column 2)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY			
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	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), (l), 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))	29	minus 20 = *	9			x 60 =	540		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2	minus 3 = *				x 250 =	0.00		
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	1790		
APPLICATION AS AMENDED - PART II									
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY	
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)	
	Total (37 CFR 1.16(i))	*	Minus **	=	x	=	x	=	
	Independent (37 CFR 1.16(h))	*	Minus ***	=	x	=	x	=	
	Application Size Fee (37 CFR 1.16(s))								
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
				TOTAL ADD'L FEE		TOTAL ADD'L FEE			
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY	
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)	
	Total (37 CFR 1.16(i))	*	Minus **	=	x	=	x	=	
	Independent (37 CFR 1.16(h))	*	Minus ***	=	x	=	x	=	
	Application Size Fee (37 CFR 1.16(s))								
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
				TOTAL ADD'L FEE		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	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/543,866	07/08/2012	Melvyn Morris	339000-000014

47604
DLA PIPER LLP US
P. O. BOX 2758
RESTON, VA 20195

CONFIRMATION NO. 7855
POA ACCEPTANCE LETTER



OC000000055461725

Date Mailed: 07/23/2012

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 07/08/2012.

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.

/ttruong/

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
13/543,866	07/08/2012	Melvyn Morris	339000-000014

CONFIRMATION NO. 7855

PUBLICATION NOTICE



OC000000057387491

47604
DLA PIPER LLP US
P. O. BOX 2758
RESTON, VA 20195

Title:METHODS AND APPARATUS FOR DEALING WITH MALWARE

Publication No.US-2012-0278895-A1

Publication Date:11/01/2012

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

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: Prevx Limited
 3 New Park Place, Pride Park
 Derby, United Kingdom DE24 8DZ

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		Date	October 26, 2012
Name	David Huberman, Esq.	Telephone	720-842-3627
Title	Director		

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 1456, Alexandria, VA 22313-1456.

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

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: Prevx Limited
Application No./Patent No.: 13/543,866 Filed/Issue Date: 2012-07-08
Titled: METHODS AND APPARATUS FOR DEALING WITH MALWARE
Prevx Limited, 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 018348, Frame 0840, 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.

[Page 1 of 2]

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.

/Bradley M. Knepper/

Signature

Bradley M. Knepper

Printed or Typed Name

2012-11-30

Date

44,189

Title or Registration Number

[Page 2 of 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 Acknowledgement Receipt	
EFS ID:	14351755
Application Number:	13543866
International Application Number:	
Confirmation Number:	7855
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Customer Number:	47604
Filer:	Bradley M. Knepper/Leslie Roberts
Filer Authorized By:	Bradley M. Knepper
Attorney Docket Number:	339000-000014
Receipt Date:	30-NOV-2012
Filing Date:	08-JUL-2012
Time Stamp:	13:55:03
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	POA_Executed_Prevx_AIA.pdf	912728 db9c376ddb33b6c00063bc3d63fb2b6deb bbc85	no	1
Warnings:					
Information:					

2	Assignee showing of ownership per 37 CFR 3.73.	STATEMENT.pdf	120051 ec649be4e3d1127239b80f29342a28df239d921b	no	3
Warnings:					
Information:					
Total Files Size (in bytes):			1032779		
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. <u>New Applications Under 35 U.S.C. 111</u> 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. <u>National Stage of an International Application under 35 U.S.C. 371</u> 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. <u>New International Application Filed with the USPTO as a Receiving Office</u> 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
13/543,866	07/08/2012	Melvyn Morris	339000-000014

47604
DLA PIPER LLP US
P. O. BOX 2758
RESTON, VA 20195

CONFIRMATION NO. 7855
POWER OF ATTORNEY NOTICE



OC000000058042106

Date Mailed: 12/12/2012

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 11/30/2012.

- 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).

/zabaha/

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
13/543,866	07/08/2012	Melvyn Morris	339000-000014

CONFIRMATION NO. 7855

POA ACCEPTANCE LETTER



OC000000058042135

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

Date Mailed: 12/12/2012

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 11/30/2012.

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.

/zabaha/

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

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/543,866
				Filing Date	July 8, 2012
				First Named Inventor	Melvyn Morris
				Art Unit	2431
				Examiner Name	
Sheet	1	of	4	Attorney Docket Number	6890-93-CON

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	6338141	01/08/2002	Wells	
	2	6772346	08/03/2004	Chess	
	3	6944772	09/13/2005	Dozortsev	
	4	7013483	03/14/2006	Cohen et al.	
	5	7093239	08/15/2006	van der Made	
	6	2001/0052014	12/13/2001	Sheymov et al.	
	7	2002/0099952	07/25/2002	Lambert et al.	
	8	2003/0023857	01/30/2003	Hinchliffe	
	9	2003/0084323	05/01/2003	Gales	
	10	2003/0101381	05/29/2003	Mateev	
	11	2003/0135791	07/17/2003	Natvig	
	12	2004/0006704	01/08/2004	Dahlstrom	
	13	2004/0039921	02/26/2004	Chuang	
	14	2004/0068618	04/08/2004	Hooker	
	15	2004/0073810	04/15/2004	Racine	
	16	2004/0083408	04/29/2004	Spiegel	
	17	2004/0153644	08/05/2004	McCorkendale	
	18	2004/0255165	12/16/2004	Szor	
	19	2005/0021994	01/27/2005	Barton	
	20	2005/0027686	02/03/2005	Shipp	
	21	2005/0086500	04/21/2005	Albomoz	
	22	2005/0022014	06/27/2005	Shipman	
	23	2005/0210035	09/22/2005	Kester et al.	
	24	2007/0016953	01/18/2007	Morris et al.	
	25	2008/0209562	08/28/2008	Szor	
	26	2008/0320595	12/25/2008	van der Made	
	27	2009/0271867	10/29/2009	Zhang	
	28	2012/0278891	11/01/2012	Morris et al.	

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. Applicant's unique citation designation number (optional). See Kipds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.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. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/543,866
				Filing Date	July 8, 2012
				First Named Inventor	Melvyn Morris
				Art Unit	2431
				Examiner Name	
Sheet	2	of	4	Attorney Docket Number	6890-93-CON

UNPUBLISHED U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number Number-kind Code ² (if known)	Filing Date MM-DD-YYYY	Name of Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	29	60/789156	04/05/2006	Chiriac	

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
	30	EP 1315066	05/28/2003	BRITISH TELECOMM		
	31	EP 1280040	03/24/2004	ORKS ASSOC TECH INC		
	32	EP 1536341	06/01/2005	MICROSOFT CORPORATION		
	33	EP 1549012	06/29/2005	DATACT TECHNOLOGIES N V		
	34	EP 1549012	06/29/2005	DATACENTER TECHNOLOGIES		
	35	JP 3-233629	10/17/1991	NEC CORP		(English abstract also cited)
	36	JP 6-110718	04/22/1994	TOSHIBA CORP		(English abstract also cited)
	37	JP 9-504395	04/28/1997			
	38	JP 2003-196112	07/11/2003	HEWLETT PACKARD CO		(English abstract also cited)
	39	WO 95/12162	05/04/1995	SOPHOS PLC		
	40	WO 96/30829	10/03/1996	APPLE COMPUTER INC.		
	41	WO 99/15966	04/01/1999	SYMANTEC CORPORATION		
	42	WO 02/33525	04/25/2002	CHUANG SHYNE SONG		

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. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.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. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/543,866
				Filing Date	July 8, 2012
				First Named Inventor	Melvyn Morris
				Art Unit	2431
				Examiner Name	
Sheet	3	of	4	Attorney Docket Number	6890-93-CON

	43	WO 03/021402	03/13/2003	CRYPTIC SOFTWARE LTD		
	44	WO 2004/097602	11/11/2004	MESSAGELABS LTD		

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.
	45	English Language Abstract of JP 3-233629 published October 17, 1991
	46	English Language Abstract and Translation of JP 6-110718 published April 22, 1994
	47	English Language Abstract of JP 2003-196112 published July 11, 2003
	48	Image File Wrapper of related U.S. Application No. 11/694,261 electronically captured from PAIR on June 21, 2012
	49	ZENKIN "Fighting Against the invisible Enemy - Methods for detecting an unknown virus," Computers & Security, Elsevier Science Publishers, Amsterdam, NL, Vol. 20, No. 4, Jul. 31, 2001, pages 316-321, XP004254268
	50	International Search Report issued in PCT/GB2006/002439 issued January 15, 2007
	51	English Translation of Official Action for China Patent Application No. 201110036121.8, dated Sep. 24, 2012, 8 pages
	52	Official Action with English translation for China Patent Application No. 201110036121.8, dated Oct. 10, 2011, 14 pages
	53	Japanese Office Action issued in JP 2008-518975 on September 13, 2011
	54	English Language Translation of Japanese Office Action issued in JP 2008-518975 on September 13, 2011
	55	EXAMINER KANE, Official Action for U.S. Patent Application No. 11/477,807, mailed Jan. 13, 2010, 8 pages (Attorney's Ref. No. 6890-93)
	56	EXAMINER ZECHER, Official Action for U.S. Patent Application No. 11/477,807, mailed May 04, 2010, 13 pages (6890-93)
	57	EXAMINER ZECHER, Official Action for U.S. Patent Application No. 11/477,807, mailed Sep. 28, 2010, 11 pages (Attorney's Ref. No. 6890-93)
	58	EXAMINER ZECHER, Official Action for U.S. Patent Application No. 11/477,807, mailed Feb. 15, 2011, 13 pages (Attorney's Ref. No. 6890-93)
	59	EXAMINER ZECHER, Official Action for U.S. Patent Application No. 11/477,807, mailed Jul. 25, 2011, 13 pages (Attorney's Ref. No. 6890-93)

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. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.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. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. 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 <i>(Use as many sheets as necessary)</i>				Application Number	13/543,866
				Filing Date	July 8, 2012
				First Named Inventor	Melvyn Morris
				Art Unit	2431
				Examiner Name	
Sheet	4	of	4	Attorney Docket Number	6890-93-CON

	60	EXAMINER ZECHER, Notice of Allowance for U.S. Patent Application No. 11/477,807, mailed Mar. 21, 2012, 9 pages (Attorney's Ref. No. 6890-93)
	61	EXAMINER ZECHER, Notice of Allowance for U.S. Patent Application No. 11/477,807, mailed Dec. 13, 2012, 7 pages (Attorney's Ref. No. 6890-93)

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. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.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. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. * Applicant is to place a check mark here if English language Translation is attached.

Electronic Acknowledgement Receipt	
EFS ID:	14793548
Application Number:	13543866
International Application Number:	
Confirmation Number:	7855
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Customer Number:	22442
Filer:	Bradley M. Knepper/Robert Roe-Pachirat
Filer Authorized By:	Bradley M. Knepper
Attorney Docket Number:	6890-93-CON
Receipt Date:	25-JAN-2013
Filing Date:	08-JUL-2012
Time Stamp:	14:24:40
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		IDS_01.pdf	738938 f70a9f11b05df56794b7d504fd1dc35296462b35	yes	7

	Multipart Description/PDF files in .zip description		
	Document Description	Start	End
	Transmittal Letter	1	3
	Information Disclosure Statement (IDS) Form (SB08)	4	7
Warnings:			
Information:			
Total Files Size (in bytes):		738938	
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. <u>New Applications Under 35 U.S.C. 111</u> 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. <u>National Stage of an International Application under 35 U.S.C. 371</u> 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. <u>New International Application Filed with the USPTO as a Receiving Office</u> 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.: 7855
Serial No.: 13/543,866	)	Examiner:
Filed: July 8, 2012	)	
Atty. File No.: 6890-93-CON	)	<u>INFORMATION DISCLOSURE</u>
Entitled: "Methods and Apparatus for Dealing	)	<u>STATEMENT</u>
With Malware"	)	<i>Electronically Submitted</i>
	)	

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/unpublished patent applications/patent application publications are not enclosed in accordance with 37 C.F.R. § 1.98(a).
- ☒ Copies of the cited references 30 – 61 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. 11/477,807 filed 06/30/06, 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. 11/477,807 filed 06/30/06 (Attorney's Ref. No. 6890-93)
 - Serial No. 13/543,865 filed 07/08/12 (Attorney's Ref. No. 6890-93-DIV)
- ☐ 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.

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: _____


Bradley M. Knepper
Registration No. 44189
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: January 24, 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.
13/543,866	07/08/2012	INV001Melvyn Morris	6890-93-CON	7855
22442	7590	03/22/2013		
Sheridan Ross PC 1560 Broadway Suite 1200 Denver, CO 80202			EXAMINER ZECHER, CORDELIA P K	
			ART UNIT 2432	PAPER NUMBER
			NOTIFICATION DATE 03/22/2013	DELIVERY MODE 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. 13/543,866	Applicant(s) MORRIS ET AL.	
	Examiner CORDELIA ZECHER	Art Unit 2432	

-- 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 08 July 2012.

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) 1-29 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) 1-29 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 08 July 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).

a) ☒ All b) ☐ Some * c) ☐ None of:

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

2. ☒ Certified copies of the priority documents have been received in Application No. 11/477,807.

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/08)
 Paper No(s)/Mail Date _____.

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

4) ☐ Other: _____.

DETAILED ACTION

This action is responsive to the non-provisional application filed on July 8, 2012.

Claims 1 – 29 are pending. Claims 1 and 15 are independent.

Drawings

The drawings are objected to because Figure 1 is an informal drawing and difficult to read. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as “amended.” If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either “Replacement Sheet” or “New Sheet” pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

- (a) TITLE OF THE INVENTION.
- (b) CROSS-REFERENCE TO RELATED APPLICATIONS.
- (c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
- (d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT.
- (e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC.
- (f) BACKGROUND OF THE INVENTION.
 - (1) Field of the Invention.
 - (2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
- (g) BRIEF SUMMARY OF THE INVENTION.
- (h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
- (i) DETAILED DESCRIPTION OF THE INVENTION.
- (j) CLAIM OR CLAIMS (commencing on a separate sheet).
- (k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
- (l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

The disclosure is objected to because of the following informalities: The specification fails to be separated into the appropriate sections listed above.

The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is

requested in correcting any errors of which applicant may become aware in the specification.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of 35 U.S.C. 112(b):

(B) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1 and 15 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

Claims 1 and 15 refer to "the information including at least the identify of the object". It is unclear if the information includes the identity of the object, how to identify the object, or what information. For the purposes of examination it is assumed the information includes that actual identity of the object.

Claim Rejections - 35 USC § 103

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:

Art Unit: 2432

(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 negated by the manner in which the invention was made.

The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148

USPQ 459 (1966), that are applied for establishing a background for determining

obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1 – 12, 15 – 26, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Omote US Publication 2006/0085857 A1, and further in view of Dozortsev US Publication 2003/0177394 A1.

Referring to claims 1, 15 and 29, Omote teaches:

Receiving data about a computer object, wherein said data includes information about events initiated or involving the object when the object is created, configured or runs on the respective remote computers, said information including at least the identity of the object initiating the event, the event type, and the identity of the object or other entity on which the event is being performed (paragraphs 39-42).

Storing at the base computer said data received (paragraph 42-43, and 51).

Comparing in the base computer the data about the computer object to identify relationships between the object and other objects or entities (paragraphs 41-42).

Classifying the computer object as malware on the basis of said comparison (paragraphs 63-64).

Omote does not explicitly disclose that the received information is for a plurality of remote computer. However, Dozortsev discloses suspect signatures are forwarded on to the central computer (paragraphs 22 and 45). Omote and Dozortsev are analogous art because they are from the same field of endeavor, virus detection. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Omote and Dozortsev before him or her, to modify the network virus activity detection system of Omote to include the central computer of Dozortsev. The suggestion/motivation for doing so would have been so that the central computer in this way communicates to the client computer the experience of other client computers connected to the central computer (paragraph 52).

Referring to claims 2 and 16, Omote discloses the relationship is between objects related directly, or between objects related via other objects (paragraph 41).

Referring to claims 3 and 17, Omote discloses an object and other objects are found to have a relationship, monitoring those related objects as a homogenous entity (paragraph 63).

Referring to claims 4 and 18, Omote discloses deducing an object to be malware based on the behavior of a related object (paragraph 63).

Referring to claims 5 and 19, Omote discloses if at least one other object to which said object is related is classed as malware, then classifying said object as malware (paragraphs 78 and 79). In addition, Dozortsev teaches if the object is related to a malicious executable code then disabling the executable code (paragraph 25).

Referring to claims 6 and 20, Omote discloses said other objects include the object or similar objects stored on the computer (paragraph 42). Omote does not explicitly disclose that the received information is for a plurality of remote computer. However, Dozortsev discloses suspect signatures are forwarded on to the central computer (paragraphs 22 and 45). Omote and Dozortsev are analogous art because they are from the same field of endeavor, virus detection. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Omote and Dozortsev before him or her, to modify the network virus activity detection system of Omote to include the central computer of Dozortsev. The suggestion/motivation for doing so would have been so that the central computer in this way communicates to the client computer the experience of other client computers connected to the central computer (paragraph 52).

Referring to claims 7 and 21, Omote discloses said other objects include other objects that are parent objects or child objects or otherwise process-related objects to said object (paragraph 41 and 63).

Referring to claims 8 and 22, Omote teaches the data about the computer object that is used in the comparison includes the current name of the object (paragraph 40). Omote does not explicitly disclose that the received information is for a plurality of

remote computer. However, Dozortsev discloses suspect signatures are forwarded on to the central computer (paragraphs 22 and 45). Omote and Dozortsev are analogous art because they are from the same field of endeavor, virus detection. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Omote and Dozortsev before him or her, to modify the network virus activity detection system of Omote to include the central computer of Dozortsev. The suggestion/motivation for doing so would have been so that the central computer in this way communicates to the client computer the experience of other client computers connected to the central computer (paragraph 52).

Referring to claims 9 and 23, Dozortsev discloses the data is sent in the form of key that is obtained by a hashing process carried out in respect of the objects on the respective remote computers (paragraph 21). Omote and Dozortsev are analogous art because they are from the same field of endeavor, virus detection. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Omote and Dozortsev before him or her, to modify the network virus activity detection system of Omote to include the unique signature of Dozortsev. The suggestion/motivation for doing so would have been to have a unique signature of the executable code for comparison (paragraph 21).

Referring to claims 10 and 24, Dozortsev discloses the key has at least one component that represents executable instructions contained within or constituted by the object (paragraph 21). Omote and Dozortsev are analogous art because they are from the same field of endeavor, virus detection. At the time of the invention, it would

have been obvious to one of ordinary skill in the art, having the teachings of Omote and Dozortsev before him or her, to modify the network virus activity detection system of Omote to include the unique signature of Dozortsev. The suggestion/motivation for doing so would have been to have a unique signature of the executable code for comparison (paragraph 21).

Referring to claims 11 and 25, Dozortsev discloses the key has at least one component that represents data about said object (paragraph 21). Omote and Dozortsev are analogous art because they are from the same field of endeavor, virus detection. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Omote and Dozortsev before him or her, to modify the network virus activity detection system of Omote to include the unique signature of Dozortsev. The suggestion/motivation for doing so would have been to have a unique signature of the executable code for comparison (paragraph 21).

Referring to claims 12 and 26, Omote discloses said data about said object includes the current name of the object (paragraph 40).

Claims 13, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Omote in view of Dozortsev as applied above, and further in view of Barton et al's US Publication 2005/0021994 A1.

Omote in view of Dozortsev discloses all the limitations of the parent claims. Omote in view of Dozortsev does not explicitly disclose the data about the object including the size of the object. However, Barton discloses indicating for the object the

file name, size and location (pages 2-3, paragraph 39). Omote in view of Dozortsev and Barton are analogous art because they are from the same field of endeavor, malware detection. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Omote in view of Dozortsev and Barton before him or her, to modify the rules of Omote in view of Dozortsev to include the data size of Barton. The suggestion/motivation for doing so would have been the characteristics are strongly indicative of a particular file being one of the candidates (page 1, paragraph 14).

Claims 14 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Omote in view of Dozortsev, as applied above, and further in view of Kester et al US Publication 2005/0210035 A1.

Omote in view of Dozortsev teaches all the limitations of the parent claim, and initially classifying an object as not malware, and changing the status of the object after an investigation (Dozortsev, paragraphs 37-41). Omote in view of Dozortsev does not explicitly disclose generating a mask for said object that defines acceptable behaviour for the object, and monitoring operation of the object on at least one of the remote computers and reclassifying the object as malware if the actual monitored behaviour extends beyond that permitted by the mask. However, Kester discloses determining access privileges for an application based on the expected network behavior of an application (paragraph 43), and then monitoring the behavior of an application based on access privileges(paragraphs 41, 55 and 56).

Omote in view of Dozortsev and Kester are from the same field of endeavor, malware. At the time of invention, it would have been obvious to one of ordinary skill in the art to modify the investigation of Omote in view of Dozortsev to include the privileges based on behavior of Kester. The suggestion for doing so would have been for the system to be able to keep or change a previous access privilege based on the subsequent activity of an application (paragraph 41).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CORDELIA ZECHER whose telephone number is (571)272-7771. The examiner can normally be reached on Monday - Thursday 8:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. 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.

/CORDELIA ZECHER/
Primary Examiner, Art Unit 2432

Notice of References Cited	Application/Control No. 13/543,866	Applicant(s)/Patent Under Reexamination MORRIS ET AL.	
	Examiner CORDELIA ZECHER	Art Unit 2432	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2003/0177394 A1	09-2003	Dozortsev, Dmitri	713/201
*	B	US-2005/0021994 A1	01-2005	Barton et al.	713/200
*	C	US-2005/0210035 A1	09-2005	Kester et al.	707/010
*	D	US-2006/0085857 A1	04-2006	Omote et al.	726/024
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

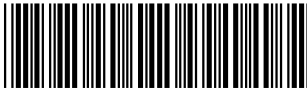
FOREIGN PATENT DOCUMENTS

*		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. 13543866	Applicant(s)/Patent Under Reexamination MORRIS ET AL.
	Examiner CORDELIA ZECHER	Art Unit 2432

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	24 (text)	3/14/13	CZ

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor Search	3/14/13	CZ
Searched EAST (see attached)	3/14/13	CZ

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

--	--

Receipt date: 01/25/2013

13543866 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/543,866
				Filing Date	July 8, 2012
				First Named Inventor	Melvyn Morris
				Art Unit	2431
				Examiner Name	
Sheet	1	of	4	Attorney Docket Number	6890-93-CON

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	6338141	01/08/2002	Wells	
	2	6772346	08/03/2004	Chess	
	3	6944772	09/13/2005	Dozortsev	
	4	7013483	03/14/2006	Cohen et al.	
	5	7093239	08/15/2006	van der Made	
	6	2001/0052014	12/13/2001	Sheymov et al.	
	7	2002/0099952	07/25/2002	Lambert et al.	
	8	2003/0023857	01/30/2003	Hinchliffe	
	9	2003/0084323	05/01/2003	Gales	
	10	2003/0101381	05/29/2003	Mateev	
	11	2003/0135791	07/17/2003	Natvig	
	12	2004/0006704	01/08/2004	Dahlstrom	
	13	2004/0039921	02/26/2004	Chuang	
	14	2004/0068618	04/08/2004	Hooker	
	15	2004/0073810	04/15/2004	Racine	
	16	2004/0083408	04/29/2004	Spiegel	
	17	2004/0153644	08/05/2004	McCorkendale	
	18	2004/0255165	12/16/2004	Szor	
	19	2005/0021994	01/27/2005	Barton	
	20	2005/0027686	02/03/2005	Shipp	
	21	2005/0086500	04/21/2005	Albomoz	
	22	2005/0022014	06/27/2005	Shipman	
	23	2005/0210035	09/22/2005	Kester et al.	
	24	2007/0016953	01/18/2007	Morris et al.	
	25	2008/0209562	08/28/2008	Szor	
	26	2008/0320595	12/25/2008	van der Made	
	27	2009/0271867	10/29/2009	Zhang	
	28	2012/0278891	11/01/2012	Morris et al.	

Examiner Signature	/Cordelia Zecher/	Date Considered	03/14/2013
--------------------	-------------------	-----------------	------------

*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. Applicant's unique citation designation number (optional). See Kipds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.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. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.Z./

Receipt date: 01/25/2013

13543866 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/543,866
				Filing Date	July 8, 2012
				First Named Inventor	Melvyn Morris
				Art Unit	2431
				Examiner Name	
Sheet	2	of	4	Attorney Docket Number	6890-93-CON

UNPUBLISHED U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number Number-kind Code ² (if known)	Filing Date MM-DD-YYYY	Name of Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	29	60/789156	04/05/2006	Chiriac	

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
/C.Z./	30	EP 1315066	05/28/2003	BRITISH TELECOMM		
/C.Z./	31	EP 1280040	03/24/2004	ORKS ASSOC TECH INC		
/C.Z./	32	EP 1536341	06/01/2005	MICROSOFT CORPORATION		
/C.Z./	33	EP 1549012	06/29/2005	DATACT TECHNOLOGIES N V		
/C.Z./	34	EP 1549012	06/29/2005	DATACENTER TECHNOLOGIES		
/C.Z./	35	JP 3-233629	10/17/1991	NEC CORP		(English abstract also cited)
/C.Z./	36	JP 6-110718	04/22/1994	TOSHIBA CORP		(English abstract also cited)
/C.Z./	37	JP 9-504395	04/28/1997			
/C.Z./	38	JP 2003-196112	07/11/2003	HEWLETT PACKARD CO		(English abstract also cited)
/C.Z./	39	WO 95/12162	05/04/1995	SOPHOS PLC		
/C.Z./	40	WO 96/30829	10/03/1996	APPLE COMPUTER INC.		
/C.Z./	41	WO 99/15966	04/01/1999	SYMANTEC CORPORATION		
/C.Z./	42	WO 02/33525	04/25/2002	CHUANG SHYNE SONG		

Examiner Signature	/Cordelia Zecher/	Date Considered	03/14/2013
-----------------------	-------------------	--------------------	------------

*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. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.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. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.Z./

Receipt date: 01/25/2013

13543866 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/543,866
				Filing Date	July 8, 2012
				First Named Inventor	Melvyn Morris
				Art Unit	2431
				Examiner Name	
Sheet	3	of	4	Attorney Docket Number	6890-93-CON

/C.Z./	43	WO 03/021402	03/13/2003	CRYPTIC SOFTWARE LTD		
/C.Z./	44	WO 2004/097602	11/11/2004	MESSAGELABS LTD		

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.
/C.Z./	45	English Language Abstract of JP 3-233629 published October 17, 1991
/C.Z./	46	English Language Abstract and Translation of JP 6-110718 published April 22, 1994
/C.Z./	47	English Language Abstract of JP 2003-196112 published July 11, 2003
/C.Z./	48	Image File Wrapper of related U.S. Application No. 11/694,261 electronically captured from PAIR on June 21, 2012
/C.Z./	49	ZENKIN "Fighting Against the invisible Enemy - Methods for detecting an unknown virus," Computers & Security, Elsevier Science Publishers, Amsterdam, NL, Vol. 20, No. 4, Jul. 31, 2001, pages 316-321, XP004254268
/C.Z./	50	International Search Report issued in PCT/GB2006/002439 issued January 15, 2007
/C.Z./	51	English Translation of Official Action for China Patent Application No. 201110036121.8, dated Sep. 24, 2012, 8 pages
/C.Z./	52	Official Action with English translation for China Patent Application No. 201110036121.8, dated Oct. 10, 2011, 14 pages
/C.Z./	53	Japanese Office Action issued in JP 2008-518975 on September 13, 2011
/C.Z./	54	English Language Translation of Japanese Office Action issued in JP 2008-518975 on September 13, 2011
	55	EXAMINER KANE, Official Action for U.S. Patent Application No. 11/477,807, mailed Jan. 13, 2010, 8 pages (Attorney's Ref. No. 6890-93)
	56	EXAMINER ZECHER, Official Action for U.S. Patent Application No. 11/477,807, mailed May 04, 2010, 13 pages (6890-93)
	57	EXAMINER ZECHER, Official Action for U.S. Patent Application No. 11/477,807, mailed Sep. 28, 2010, 11 pages (Attorney's Ref. No. 6890-93)
	58	EXAMINER ZECHER, Official Action for U.S. Patent Application No. 11/477,807, mailed Feb. 15, 2011, 13 pages (Attorney's Ref. No. 6890-93)
	59	EXAMINER ZECHER, Official Action for U.S. Patent Application No. 11/477,807, mailed Jul. 25, 2011, 13 pages (Attorney's Ref. No. 6890-93)

Examiner Signature	/Cordelia Zecher/	Date Considered	03/14/2013
--------------------	-------------------	-----------------	------------

*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. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.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. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.Z./

Receipt date: 01/25/2013

13543866 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/543,866
				Filing Date	July 8, 2012
				First Named Inventor	Melvyn Morris
				Art Unit	2431
				Examiner Name	
Sheet	4	of	4	Attorney Docket Number	6890-93-CON

60	EXAMINER ZECHER, Notice of Allowance for U.S. Patent Application No. 11/477,807, mailed Mar. 21, 2012, 9 pages (Attorney's Ref. No. 6890-93)
61	EXAMINER ZECHER, Notice of Allowance for U.S. Patent Application No. 11/477,807, mailed Dec. 13, 2012, 7 pages (Attorney's Ref. No. 6890-93)

Examiner Signature	/Cordelia Zecher/	Date Considered	03/14/2013
-----------------------	-------------------	--------------------	------------

*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. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.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. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. * Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.Z./



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. 7855

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.		
13/543,866	07/08/2012	726	2432	6890-93-CON		
APPLICANTS Melvyn Morris, Turnditch, UNITED KINGDOM; Paul Stubbs, Wyboston, UNITED KINGDOM; Markus Hartwig, Milton Keynes, UNITED KINGDOM; Darren Harter, Hucclecote, UNITED KINGDOM; ** CONTINUING DATA ***** This application is a CON of 11/477,807 06/30/2006 ** FOREIGN APPLICATIONS ***** UNITED KINGDOM 0513375.6 06/30/2005 ** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** 07/18/2012						
Foreign Priority claimed ☒ Yes ☐ No 35 USC 119(a-d) conditions met ☒ Yes ☐ No Verified and <u>/CORDELIA P K</u> <u>ZECHER/</u> Acknowledged <u>Examiner's Signature</u>		☐ Met after Allowance <u>Initials</u>	STATE OR COUNTRY UNITED KINGDOM	SHEETS DRAWINGS 3	TOTAL CLAIMS 29	INDEPENDENT CLAIMS 2
ADDRESS Sheridan Ross PC 1560 Broadway Suite 1200 Denver, CO 80202 UNITED STATES						
TITLE METHODS AND APPARATUS FOR DEALING WITH MALWARE						
FILING FEE RECEIVED 1790	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		

EAST Search History**EAST Search History (Prior Art)**

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	"20070016953"	US-PGPUB; USPAT	OR	ON	2010/01/07 08:58
S2	1	("20060026684").PN.	US-PGPUB; USPAT	OR	OFF	2010/04/28 08:32
S3	1	S2 and malware	US-PGPUB; USPAT	OR	ON	2010/04/28 08:33
S4	1164	726/24.ccls.	US-PGPUB; USPAT	OR	ON	2010/04/28 08:33
S5	2821	726/23-25.ccls.	US-PGPUB; USPAT	OR	ON	2010/04/28 08:34
S6	6	((("6772346") or ("6944772") or ("20040006704") or ("20040073810") or ("20050021994") or ("20040153644"))).PN.	US-PGPUB; USPAT	OR	OFF	2010/04/28 09:18
S7	1	("20030177394").PN.	US-PGPUB; USPAT	OR	OFF	2010/04/28 10:48
S8	0	central near database with each with network	US-PGPUB; USPAT	OR	ON	2010/04/28 12:51
S9	0	database with each with network	US-PGPUB; USPAT	OR	ON	2010/04/28 12:51
S10	115859	database with network	US-PGPUB; USPAT	OR	ON	2010/04/28 12:52
S11	2632	central near database with network	US-PGPUB; USPAT	OR	ON	2010/04/28 12:52
S12	30	central near database with network with separate	US-PGPUB; USPAT	OR	ON	2010/04/28 12:53
S13	17	central near database with distribute with network	US-PGPUB; USPAT	OR	ON	2010/04/28 12:53
S14	199	central near database with distribut\$3 with network	US-PGPUB; USPAT	OR	ON	2010/04/28 12:54
S15	0	central near database with distribute with network with known	US-PGPUB; USPAT	OR	ON	2010/04/28 12:54
S16	4	central near database with distribut\$3 with network with known	US-PGPUB;	OR	ON	2010/04/28 12:55

			USPAT			
S17	240	database with distribut\$3 with network with known	US-PGPUB; USPAT	OR	ON	2010/04/28 12:55
S18	24	database with distribut\$3 with network with known and (virus or malware)	US-PGPUB; USPAT	OR	ON	2010/04/28 12:56
S19	4	("20030023857" "20050027686" "6338141" "7013483").PN.	US-PGPUB; USPAT	OR	ON	2011/02/09 08:21
S20	3433	726/23-25.ccls.	US-PGPUB; USPAT	OR	ON	2011/02/09 08:35
S21	282	S20 and mask\$3	US-PGPUB; USPAT	OR	ON	2011/02/09 08:35
S22	35	S20 and mask\$3 and malware	US-PGPUB; USPAT	OR	ON	2011/02/09 08:35
S23	328	S20 and control\$3 with environment	US-PGPUB; USPAT	OR	ON	2011/02/09 08:43
S24	65	S20 and control\$3 with environment and malware	US-PGPUB; USPAT	OR	ON	2011/02/09 08:43
S25	18	S20 and defin\$3 with boundary and malware	US-PGPUB; USPAT	OR	ON	2011/02/09 08:45
S26	5	S20 and access\$3 with rights with object and malware	US-PGPUB; USPAT	OR	ON	2011/02/09 08:46
S27	2	"20020099952"	US-PGPUB; USPAT	OR	ON	2011/02/09 09:11
S28	24	(updat\$3 or modif\$4) with token and S20	US-PGPUB; USPAT	OR	ON	2011/02/09 10:54
S29	37	("20010049793" "20030225698" "20040068721" "20050203819" "20060031686" "4713753" "4805222" "4926476" "5367624" "5481700" "5819091" "5915025" "5958051" "5978484" "5983349" "5991519" "6295605" "6378069" "6405202" "6775779" "6931540" "6981281" "7028180" "7051366" "7076557").PN. OR ("7350204").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2011/02/09 11:23
S30	32	S29 and (modif\$4 or updat\$3)	US-PGPUB; USPAT; USOCR	OR	ON	2011/02/09 11:23
S31	6232	automatic\$4 with (updat\$3 or chang\$3 or modif\$4) with access	US-PGPUB; USPAT; USOCR	OR	ON	2011/02/09 11:35
S32	29	S20 and S31	US-PGPUB; USPAT;	OR	ON	2011/02/09 11:35

			USOCR			
S33	18	"7350204"	US-PGPUB; USPAT	OR	ON	2011/07/21 09:19
S34	1	"7350204".pn.	US-PGPUB; USPAT	OR	ON	2011/07/21 09:19
S35	42	("20010049793" "20030225698" "20040068721" "20050203819" "20060031686" "4713753" "4805222" "4926476" "5367624" "5481700" "5819091" "5915025" "5958051" "5978484" "5983349" "5991519" "6295605" "6378069" "6405202" "6775779" "6931540" "6981281" "7028180" "7051366" "7076557").PN. OR ("7350204").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2011/07/21 09:21
S36	106	("2002/0099952").URPN.	USPAT	OR	ON	2011/07/21 09:46
S37	16	("20020026578" "20020099952" "20020124170" "20030033535" "20040064708" "20040078604" "20040117615" "20050138388" "5941947" "6151590" "6397261" "6571335" "6810525" "7010600" "7194664").PN. OR ("7509497").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2011/07/21 09:49
S38	1	(S35 or S36 or S37) and behaviour	US-PGPUB; USPAT; USOCR	OR	ON	2011/07/21 09:50
S39	1	"7698713".pn.	US-PGPUB; USPAT; USOCR	OR	ON	2011/07/21 09:51
S40	2	"20030131152"	US-PGPUB; USPAT; USOCR	OR	ON	2011/07/21 09:52
S41	57	(S35 or S36 or S37) and behavior	US-PGPUB; USPAT; USOCR	OR	ON	2011/07/21 09:52
S42	2	"20050210035"	US-PGPUB; USPAT; USOCR	OR	ON	2011/07/21 10:01
S43	2	S42 and behav\$5	US-PGPUB; USPAT; USOCR	OR	ON	2011/07/21 10:04
S44	20	("20040153644" "6338141" "20030084323" "20050027686" "6772346" "20050210035" "6944772" "20050021994" "20030023857" "20040083408" "20050022014" "20040006704" "20010052014" "20030101381" "7013483" "20020099952" "20040039921" "20050086500" "20040073810" "20050021994" "20030177394").PN.	US-PGPUB; USPAT	OR	ON	2012/02/17 13:30

S45	5	("20040083408" "20050022014" "20030101381" "20040039921" "20050086500").PN.	US-PGPUB; USPAT	OR	ON	2012/02/17 13:34
S46	3172	generat\$3 with profile with automatic\$4	US-PGPUB; USPAT	OR	ON	2012/02/17 14:56
S47	4255	726/23-25.ccls.	US-PGPUB; USPAT	OR	ON	2012/02/17 14:56
S48	25	generat\$3 with profile with automatic\$4 and S47	US-PGPUB; USPAT	OR	ON	2012/02/17 14:56
S55	7	("20030135791" "20040068618" "20040255165" "20080209562" "20080320595" "20090271867" "7093239").PN.	US-PGPUB; USPAT	OR	ON	2012/12/11 08:38
S59	1	"20120278895"	US-PGPUB; USPAT	OR	ON	2013/03/14 08:28
S60	5	((("20120260340") or ("20070016953") or ("20120266208") or ("20120260304") or ("20120278891"))).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/03/14 08:36
S61	2355	726/24.ccls.	US-PGPUB; USPAT	OR	ON	2013/03/14 08:50
S62	28	("20010052014" "20020099952" "20030023857" "20030084323" "20030103810" "20030135791" "20040006704" "20040039921" "20040068618" "20040073810" "20040083408" "20040153644" "20040255165" "20050021994" "20050022014" "20050027686" "20050086500" "20050210035" "20070016953" "20080209562" "20080320595" "20090271867" "20120278891" "6338141" "6772346" "6944772" "7013483" "7093239").PN.	US-PGPUB; USPAT	OR	ON	2013/03/14 09:03
S63	8	S62 and (parent or child)	US-PGPUB; USPAT	OR	ON	2013/03/14 09:14
S64	439	S61 and (parent or child)	US-PGPUB; USPAT	OR	ON	2013/03/14 09:21
S65	17	S61 and (parent or child) with relationship	US-PGPUB; USPAT	OR	ON	2013/03/14 09:28
S66	21	("20020069370" "20020099952" "20020116627" "20020162015" "20030172109" "20040078591" "20040148524" "20040255163" "20050182958" "20070107052" "5822517" "5867647" "6338141" "6405318" "6499109" "6560323" "6973577" "7024694" "7174569" "7216225").PN. OR ("7752668").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2013/03/14 10:20
S67	3	("2006/0085857").URPN.	USPAT	OR	ON	2013/03/14 10:20

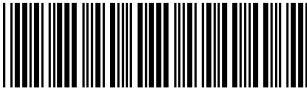
EAST Search History

S68	8	(S66 or S67) and (parent or child)	USPAT	OR	ON	2013/03/14 10:20
S69	1	"20040078591"	US- PGPUB; USPAT	OR	ON	2013/03/14 10:24

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S49	1022	726/24.ccls.	USPAT	OR	ON	2012/02/17 14:59
S50	0	(behavior and malware and classify\$3 and automatic\$4 and generat\$3 and monitor\$3 and allow\$3).clm.	USPAT	OR	ON	2012/02/17 15:06
S51	1036	726/24.ccls.	USPAT	OR	ON	2012/03/12 11:36
S52	0	(class\$6 and object and malware and automatic\$4 and generat\$3 and mask\$3 and monitor\$3).clm.	USPAT	OR	ON	2012/03/12 11:37
S53	0	(class\$6 and object and malware and automatic\$4 and generat\$3 and monitor\$3).clm.	USPAT	OR	ON	2012/03/12 11:37
S54	0	S53 and S51	USPAT	OR	ON	2012/03/12 11:37
S56	1319	726/24.ccls.	USPAT	OR	ON	2012/12/11 08:43
S57	0	(class\$6 and object and malware and automatic\$4 and generat\$3 and monitor\$3).clm.	USPAT	OR	ON	2012/12/11 08:43
S58	0	S57 and S56	USPAT	OR	ON	2012/12/11 08:43

3/ 18/ 2013 8:50:52 AM**C:\ Users\ czecher\ Documents\ EAST\ Workspaces\ 13543866.wsp**

<i>Index of Claims</i> 	Application/Control No. 13543866	Applicant(s)/Patent Under Reexamination MORRIS ET AL.
	Examiner CORDELIA ZECHER	Art Unit 2432

✓	Rejected
=	Allowed

-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

☐ Claims renumbered in the same order as presented by applicant			☐ CPA			☐ T.D.			☐ R.1.47		
CLAIM		DATE									
Final	Original	03/14/2013									
	1	✓									
	2	✓									
	3	✓									
	4	✓									
	5	✓									
	6	✓									
	7	✓									
	8	✓									
	9	✓									
	10	✓									
	11	✓									
	12	✓									
	13	✓									
	14	✓									
	15	✓									
	16	✓									
	17	✓									
	18	✓									
	19	✓									
	20	✓									
	21	✓									
	22	✓									
	23	✓									
	24	✓									
	25	✓									
	26	✓									
	27	✓									
	28	✓									
	29	✓									



PRIORITY DOCUMENT EXCHANGE

FAILURE STATUS REPORT

An attempt by the Office to electronically retrieve, under the Priority Document Exchange programs (PDX and DAS), 0513375.6 to which priority is claimed has FAILED on 06/10/2013.

For further questions or assistance, please contact our EBC Customer Support Center at

1-866-217-9197 (toll-free)

571-272-4100 (local)

M-F 6AM - Midnight (Eastern Time)

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Application Number	13/543,866
				Filing Date	July 8, 2012
				First Named Inventor	Melvyn Morris
				Art Unit	2432
				Examiner Name	Cordelia P.K. Zecher
Sheet	1	of	1	Attorney Docket Number	6890-93-CON

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	7793338	09/07/2010	Beddoe 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.
	2	Official Action for China Patent Application No. 201110036124.1, dated Apr. 17, 2013, 7 pages
	3	EXAMINER ZECHER, Official Action for U.S. Patent Application No. 13/543,865, mailed Apr. 15, 2013, 9 pages (Attorney's Ref. No. 6890-93-DIV)

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. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.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. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

Electronic Patent Application Fee Transmittal				
Application Number:		13543866		
Filing Date:		08-Jul-2012		
Title of Invention:		METHODS AND APPARATUS FOR DEALING WITH MALWARE		
First Named Inventor/Applicant Name:		Melvyn Morris		
Filer:		Brent Robert Lindon/Robert Roe-Pachirat		
Attorney Docket Number:		6890-93-CON		
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:	16095994
Application Number:	13543866
International Application Number:	
Confirmation Number:	7855
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Customer Number:	22442
Filer:	Brent Robert Lindon/Robert Roe-Pachirat
Filer Authorized By:	Brent Robert Lindon
Attorney Docket Number:	6890-93-CON
Receipt Date:	20-JUN-2013
Filing Date:	08-JUL-2012
Time Stamp:	13:48:00
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	5
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 1.17 (Patent application and reexamination processing fees)	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	CN2011100361241_OA_04-17-2013.pdf	445813	no	7
			cde3cbe1ba5ef83ef7c5dea97890518411ce976e		
Warnings:					
Information:					
2	Non Patent Literature	6890-93-DIV_OA_04-15-2013.pdf	321027	no	9
			da384ccee5e4ca96e1eb2ca465c75e12d49e837b		
Warnings:					
Information:					
3		6890-93-CON_IDS_02.pdf	150459	yes	4
			086f4a4d440d17d263885806f366564832c5eeaa		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal Letter		1	3	
	Information Disclosure Statement (IDS) Form (SB08)		4	4	
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	30536	no	2
			130abd9a383b015e56f1f9f06dd9debb418d329f		
Warnings:					
Information:					
Total Files Size (in bytes):			947835		

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: 2432
Melvyn Morris	)	Confirmation No.: 7855
Serial No.: 13/543,866	)	Examiner: Cordelia P.K. Zecher
Filed: July 8, 2012	)	
Atty. File No.: 6890-93-CON	)	<u>SUPPLEMENTAL</u>
Entitled: "Methods and Apparatus for Dealing	)	<u>INFORMATION DISCLOSURE</u>
With Malware"	)	<u>STATEMENT</u>
	)	<i>Electronically Submitted</i>

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

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.

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/
Brent R. Lindon
Registration No. 67424
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: June 20, 2013

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of: Melvyn Morris

Application No.: 13/543,866

Filed: July 08, 2012

Atty. File No.: 6890-93-CON

For: Methods and Apparatus for Dealing with
Malware

) Group Art Unit: 2432

) Examiner: Zecher, Cordelia PK

) Confirmation No.: 7855

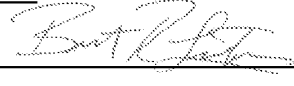
CERTIFICATE OF TRANSMISSION

I HEREBY CERTIFY THAT THIS CORRESPONDENCE
IS BEING TRANSMITTED VIA THE U.S. PATENT AND
TRADEMARK OFFICE ELECTRONIC FILING SYSTEM
(EFS-WEB) ON

JUNE 24, 2013

SHERIDAN ROSS P.C.

BY: BRENT R. LINDON

SIGNATURE: _____


AMENDMENT AND RESPONSE

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 March 22, 2013. Although Applicant believes that no additional fees are due in connection with filing this Amendment and Response, please credit any overpayment or charge any underpayment 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.

Amendments to the Drawings being on page 8 of this paper.

Remarks begin on page 9 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, wherein said data includes information about events initiated or involving the object when the object is created, configured or runs on the respective remote computers, said information including at least the ~~identify~~ identity of the object initiating the event, the event type, and the identity of the object or other entity on which the event is being performed;

storing at the base computer said data received from plural remote computers;

comparing in the base computer the data about the computer object received from the plural computers to identify relationships between the object and other objects or entities; and, classifying the computer object as malware on the basis of said comparison.

2. (Previously Presented) A method according to claim 1, wherein the relationship is between objects related directly, or between objects related via other objects.

3. (Previously Presented) A method according to claim 1, wherein where an object and other objects are found to have a relationship, monitoring those related objects as a homogenous entity.

4. (Previously Presented) A method according to claim 1, comprising deducing an object to be malware based on the behaviour of a related object.

5. (Previously Presented) A method according to claim 1, wherein if at least one other object to which said object is related is classed as malware, then classifying said object as malware.

6. (Previously Presented) A method according to claim 1, wherein said other objects include the object or similar objects stored on at least some of the remote computers.

7. (Previously Presented) A method according to claim 1, wherein said other objects include other objects that are parent objects or child objects or otherwise process-related objects to said object.

8. (Previously Presented) A method according to claim 1, wherein the data about the computer object that is sent from the plural remote computers to the base computer and that is used in the comparison includes one or more of: executable instructions contained within or constituted by the object;

the size of the object; the current name of the object;

the physical and folder location of the object on disk;

the original name of the object;

the creation and modification dates of the object;

vendor, product and version and any other information stored within the object; and,

the object header or header held by the remote computer.

9. (Previously Presented) A method according to claim 1, wherein the data is sent in the form of key that is obtained by a hashing process carried out in respect of the objects on the respective remote computers.

10. (Previously Presented) A method according to claim 9, wherein the key has at least one component that represents executable instructions contained within or constituted by the object.

11. (Previously Presented) A method according to claim 9, wherein the key has at least one component that represents data about said object.

12. (Previously Presented) A method according to claim 11, wherein said data about said object includes at least one of:

- the current name of the object;
- the physical and folder location of the object on disk;
- the original name of the object;
- the creation and modification dates of the object;
- vendor, product and version and any other information stored within the object;
- the object header or header held by the remote computer; and,
- events initiated by or involving the object when the object is created, configured or runs on the respective remote computers.

13. (Previously Presented) A method according to claim 9, wherein the key has at least one component that represents the physical size of the object.

14. (Previously Presented) A method according to claim 1, comprising initially classifying an object as not malware, generating a mask for said object that defines acceptable behaviour for the object, and comprising monitoring operation of the object on at least one of the remote computers and reclassifying the object as malware if the actual monitored behaviour extends beyond that permitted by the mask.

15. (Currently Amended) Apparatus for classifying a computer object as malware, the apparatus comprising:

- a base computer constructed and arranged to receive data about a computer object from each of plural remote computers on which the object or similar objects are stored, wherein said data includes information about events initiated or involving the object when the object is created, configured or runs on the respective remote computers, said information including at least the ~~identify~~-identity of the object initiating the event, the event type, and the identity of the object or other entity on which the event is being performed;

the base computer being constructed and arranged to compare the data about the computer object received from said plural computers to identify relationships between the object and other objects or entities; and;

the base computer being constructed and arranged to classify the computer object as malware on the basis of said comparison.

16. (Previously Presented) Apparatus according to claim 15, wherein the base computer is constructed and arranged so as to identify the relationship between objects related directly, or between objects related via other objects.

17. (Previously Presented) Apparatus according to claim 15, wherein the base computer is constructed and arranged so as, where an object and other objects are found to have a relationship, to monitoring those related objects as a homogenous entity.

18. (Previously Presented) Apparatus according to claim 15, wherein the base computer is constructed and arranged so as to deduce an object to be malware based on the behaviour of a related object.

19. (Previously Presented) Apparatus according to claim 15, wherein the base computer is constructed and arranged so that if at least one other object to which said object is related is classed as malware, then said object is classified as malware.

20. (Previously Presented) Apparatus according to claim 15, wherein the base computer is constructed and arranged so that said other objects include the object or similar objects stored on at least some of said remote computers.

21. (Previously Presented) Apparatus according to claim 15, wherein the base computer is constructed and arranged so that said other objects include other objects that are parent objects or child objects or otherwise process-related objects to said object.

22. (Previously Presented) Apparatus according to claim 15, wherein the base computer is constructed and arranged so as to compare the data where the data includes one or more of:

- executable instructions contained within or constituted by the object;
- the size of the object; the current name of the object;
- the physical and folder location of the object on disk;
- the original name of the object;
- the creation and modification dates of the object;
- vendor, product and version and any other information stored within the object; and,
- the object header or header held by the remote computer.

23. (Previously Presented) Apparatus according to claim 15, wherein the base computer is constructed and arranged so as to be able to process data that is sent in the form of key that is obtained by a hashing process carried out in respect of the objects on said respective remote computers.

24. (Previously Presented) Apparatus according to claim 23, wherein the key has at least one component that represents executable instructions contained within or constituted by the object.

25. (Previously Presented) Apparatus according to claim 23, wherein the key has at least one component that represents data about said object.

26. (Previously Presented) Apparatus according to claim 25, wherein said data about said object includes at least one of: the current name of the object;

- the physical and folder location of the object on disk;
- the original name of the object;
- the creation and modification dates of the object;
- vendor, product and version and any other information stored within the object;
- the object header or header held by the remote computer; and,

events initiated by or involving the object when the object is created, configured or runs on the respective remote computers.

27. (Previously Presented) Apparatus according to claim 23, wherein the key has at least one component that represents the physical size of the object.

28. (Previously Presented) Apparatus according to claim 15, wherein the base computer is constructed and arranged to generate a mask for an object that is initially classed not as malware, said mask defining acceptable behaviour for the object, and the base computer is constructed and arranged to monitor operation of the object on at least one of the remote computers and to reclassify the object as malware if the actual monitored behaviour extends beyond that permitted by the mask.

29. (Previously Presented) A computer program recorded on non-transitory computer readable medium comprising program instructions for causing a computer to perform the method of claim 1.

AMENDMENTS TO THE DRAWINGS

In response to the Office Action dated March 22, 2013, in connection with the above-identified patent application, enclosed for filing with said application are three sheets of formal drawings illustrating Figs. 1-4 of the application. Figs. 1-4 constitute all of the drawings in the application.

REMARKS

Applicant respectfully requests reconsideration of this application as amended. Claims 1 and 15 have been amended, without intending to abandon or to dedicate to the public any patentable subject matter. Accordingly, claims 1-29 are currently pending.

Drawings

In response to the Office Action dated March 22, 2013, in connection with the above-identified patent application, enclosed for filing with said application are three sheets of formal drawings illustrating Figs. 1-4 of the application. Figs. 1-4 constitute all of the drawings in the application.

Specification

In response to the Office Action dated March 22, 2013, the Office Action correctly characterizes the arrangement specified in 37 C.F.R. 1.77(b) as “guidelines” of a “preferred” layout that is “suggested” for the Applicant’s use. Thus, the Office Action itself acknowledges that the arrangement is discretionary on the part of the Applicant. In this case, Applicant declines the suggestion in the Office Action.

Claim Rejections Under 35 U.S.C. § 112

Claims 1 and 15 were rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention. Claims 1 and 15 have been amended and therefore, are believed to overcome this rejection. Accordingly, Applicant respectfully requests reconsideration and withdrawal of the rejection of the claims 1 and 15 be withdrawn.

Claim Rejections Under 35 U.S.C. § 103

Claims 1-12, 15-26, and 29 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Publication No. 2006/0085857 A1 to Omote et al. (hereinafter “Omote”) and further in view of U.S. Publication No. 2003/0177394 A1 to Dozortsev (hereinafter “Dozortsev”). Claims 13 and 27 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Omote in view of Dozortsev and further in view of U.S. Patent Publication

No. 2005/0021994 A1 to Barton et al. (hereinafter “Barton”). Claims 14 and 28 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Omote in view of Dozortsev and further in view of U.S. Patent Publication No. 2005/0210035 A1 to Kester et al. (hereinafter “Kester”). When determining whether a claim is obvious under 35 U.S.C. § 103, an examiner must make “a searching comparison of the claimed invention – including all its limitations – with the teaching of the prior art.” In re Ochiai, 71 F.3d 1565, 1572 (Fed. Cir. 1995) (emphasis added). Thus, “obviousness requires a suggestion of all limitations in a claim.” CFMT, Inc. v. Yieldup Intern. Corp., 349 F.3d 1333, 1342 (Fed. Cir. 2003) (citing In re Royka, 490 F.2d 981, 985 (CCPA 1974) (holding that to establish prima facie obviousness of a claimed invention, all the claim features must be taught or suggested by the prior art)). However, whether considered alone or in combination, the cited references do not disclose a 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, wherein said data includes information about events initiated or involving the object when the object is created, configured or runs on the respective remote computers, said information including at least the identify identity of the object initiating the event, the event type, and the identity of the object or other entity on which the event is being performed; storing at the base computer said data received from plural remote computers; comparing in the base computer the data about the computer object received from the plural computers to identify relationships between the object and other objects or entities; and classifying the computer object as malware on the basis of said comparison as claimed. In particular, the cited references do not teach, suggest or describe at least comparing in the base computer the data about the computer object received from the plural computers to identify relationships between the object and other objects or entities. Accordingly, the rejections of the claims as anticipated by or obvious in view of the cited references should be reconsidered and withdrawn.

The Claimed Invention

The claimed invention generally relates to classifying a computer object as malware which includes receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored; such data may be stored in a community database which provides an extensive corollary of an object’s creation, configuration, execution, behavior,

identities, and relationships to other objects that either act upon it or are acted upon by it. The stored data may then be compared to identify relationships between the object and other objects or entities. Based on this comparison, the computer object may be classified as malware.

The Omote Reference

The Omote reference is generally directed to generating process tree information and then using the process tree information for determining whether or not the process to be discriminated is an illegal process. *See e.g., Omote*, ¶ 0037, ¶ 0041. Specifically, “discrimination rule information based on the hierarchical relationship among processes is stored to designate common behavior to illegal processes so that it can be determined whether or not a process being operated in a computer is an illegal process by the activities of a virus.” *See e.g., Omote*, ¶ 0013. That is, Omote makes no mention of at least comparing in the base computer the data about the computer object received from the plural computers and then classifying the computer object as malware on the basis of said comparison. Indeed, the Office states that “Omote does not explicitly disclose that the received information is for a plurality of remote computer.” *See e.g., Office Action dated March 22, 2013*, page 6. Thus, the Office relies upon Dozortsev to teach this feature.

The Dozortsev Reference

The Dozortsev reference is generally directed to a central computer, including a database that is adapted to “store and analyze a plurality of executable code signatures, including signatures of malicious, legitimate, those executable codes identity of which is being investigated and those that have not been received for an investigation.” *See e.g., Dozortsev*, Abstract. Specifically, “[u]pon detection of the occurrence of a potentially dangerous event, the monitoring software pinpoints the executable code responsible for it. Once the executable code is pinpointed, the monitoring application creates a unique suspect signature (using MD5 or another algorithm) for that module or a corresponding file and then transmits the suspect signature to the central computer.” *See e.g., Dozortsev*, ¶ 0021. Additionally, paragraph [0045] of Dozortsev provides:

If the signature doesn't match an entry in the local database, it is then forwarded for comparison to the central computer 165 and subsequent events are then identical to those described above with respect to the first working session with like numerals denoting like steps of FIG. 1. The analysis of the suspect signature includes comparison of the suspect

signature with the plurality of signatures stored in the database. If signatures match an entry in the database, subsequent steps will depend on how the signature is flagged. It must be appreciated that the types and the number of flags in the current invention can be more than described here. If the signature is flagged "new, executable code is not received" 52, the system will attempt to download the actual suspect executable code from the client computer to the central server. If the signature is flagged "received, under investigation" 54, the following message is forwarded to the client computer, "The executable code is being investigated" 56. If the signature is flagged "legitimate" 58, a corresponding message is sent to the client computer and the monitoring software on the client computer is commanded to allow the executable code in question to be executed and/or an event to proceed 60. If the signature is flagged "malicious" 62, the monitoring application receives a command to terminate the event 64. Event termination can be accomplished by terminating the process, but it can also be accomplished by a variety of temporary or permanent means. The system can also be configured to allow the end user to override the system's decision, for instance to allow a "malicious" executable code to operate.

See e.g., Dozortsev, ¶ 0021. That is, nowhere does Dozortsev teach at least comparing in the base computer the data about the computer object received from the plural computers to identify relationships between the object and other objects or entities. Instead, Dozortsev appears to be teaching merely matching signatures to determine if a suspect executable code is in the database on the central computer. There is no disclosure in Omotoe and Dozortsev, taken alone, or in any combination of at least storing at the base computer said data received from plural remote computers, comparing in the base computer the data about the computer object received from the plural computers to identify relationships between the object and other objects or entities; and classifying the computer object as malware on the basis of said comparison, wherein said data includes information about events initiated or involving the object when the object is created, configured or runs on the respective remote computers, said information including at least the identity of the object initiating the event, the event type, and the identity of the object or other entity on which the event is being performed. This is simply not taught or disclosed by any of the cited references.

CONCLUSION

Accordingly, at least based on the above, the independent claim is patentably distinguishable from the cited reference. The dependent claims are further distinguishable at least based on the above and the additional feature(s) recited therein.

With all objections and rejections having been overcome, Applicants respectfully submit the application is in condition for allowance. Withdrawal of the outstanding rejection and a prompt notice of allowance are respectfully solicited.

Should the Examiner believe anything further is desirable in order to place the application in even better condition for allowance, the Examiner is encouraged to contact Applicant's undersigned representative at the telephone number listed below.

The Commissioner is hereby authorized to charge to deposit account number 19-1970 any fees under 37 CFR § 1.16 and 1.17 that may be required by this paper and to credit any overpayment to that Account. If any extension of time is required in connection with the filing of this paper and has not been separately requested, such extension is hereby Petitioned.

Respectfully submitted,

SHERIDAN ROSS P.C.

Date: June 24, 2013

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

1/3

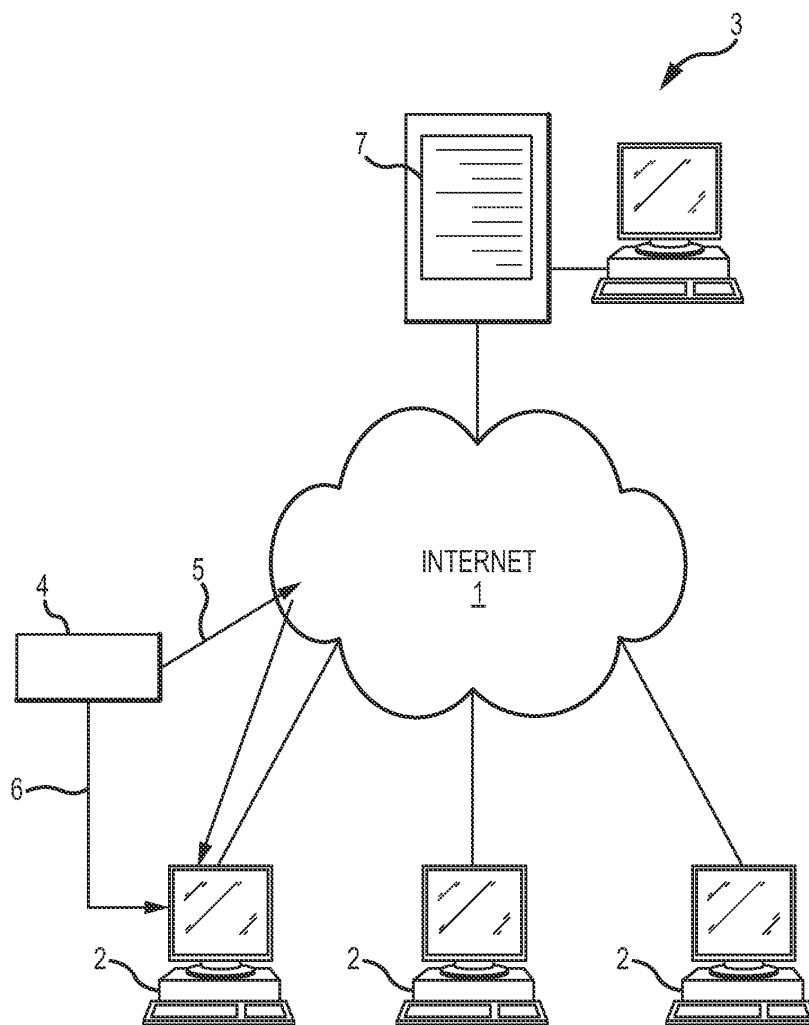


FIG.1

2/3

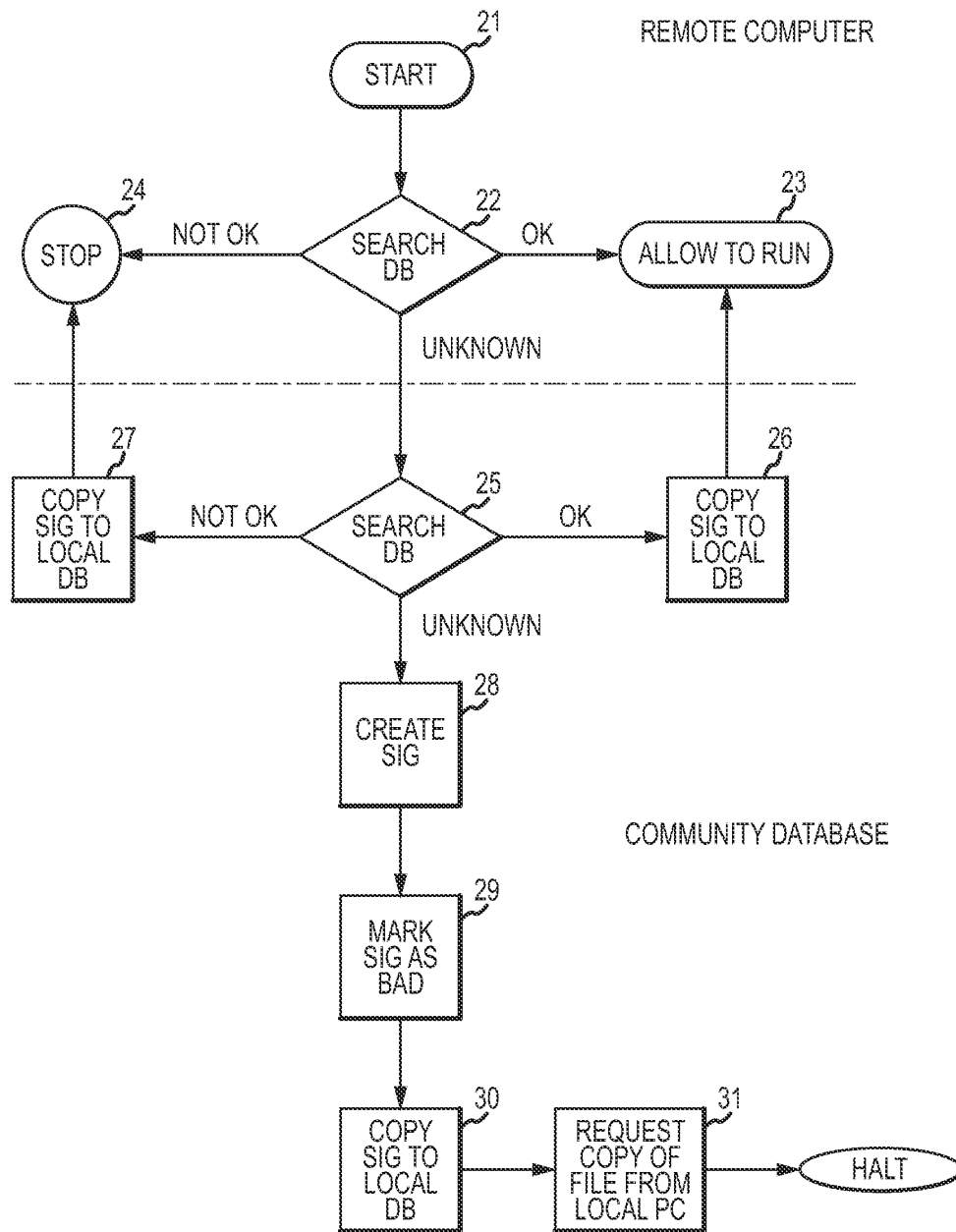


FIG.2

3/3

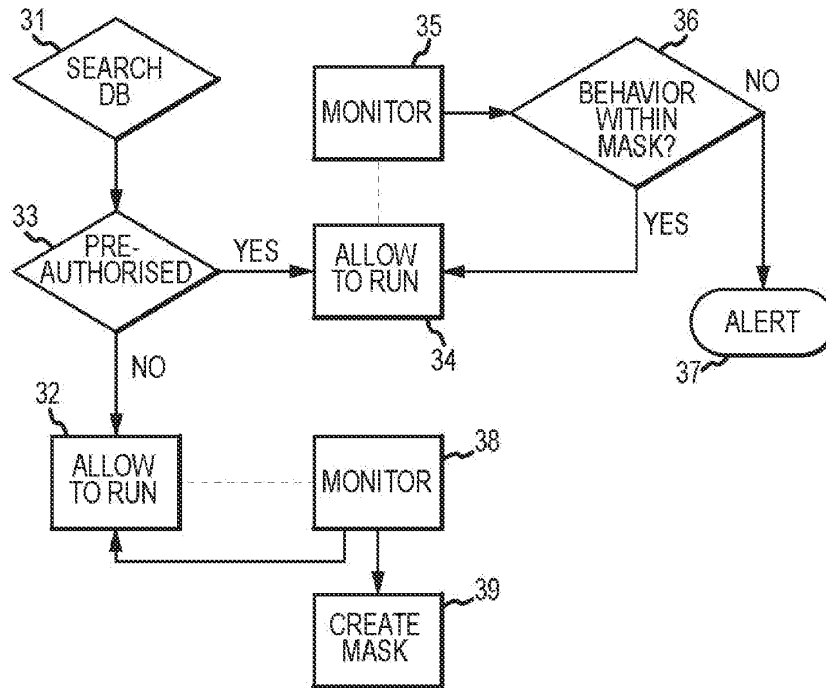


FIG.3

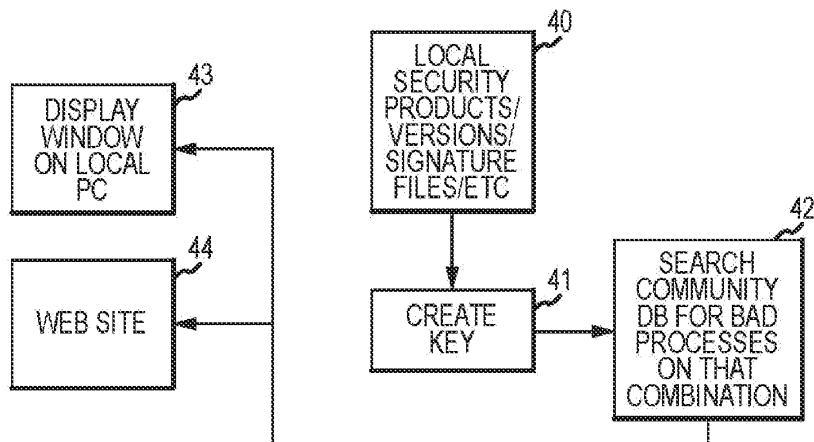


FIG.4

Electronic Acknowledgement Receipt	
EFS ID:	16140863
Application Number:	13543866
International Application Number:	
Confirmation Number:	7855
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:	6890-93-CON
Receipt Date:	25-JUN-2013
Filing Date:	08-JUL-2012
Time Stamp:	01:59:07
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		AMEND_01.pdf	159114 f283b68359166c7659941a6a107d371e493035cd	yes	13

Multipart Description/PDF files in .zip description					
Document Description			Start	End	
Amendment/Req. Reconsideration-After Non-Final Reject			1	1	
Claims			2	6	
Drawings-only black and white line drawings			7	7	
Applicant Arguments/Remarks Made in an Amendment			8	13	
Warnings:					
Information:					
2	Drawings-only black and white line drawings	FORMAL_FIGS.pdf	262130	no	3
			103d7cbe07f455f662a25ddad5a3edfcb1d7b90c		
Warnings:					
Information:					
Total Files Size (in bytes):			421244		
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. <u>New Applications Under 35 U.S.C. 111</u> 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. <u>National Stage of an International Application under 35 U.S.C. 371</u> 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. <u>New International Application Filed with the USPTO as a Receiving Office</u> 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.					

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 13/543,866		Filing Date 07/08/2012		☐ To be Mailed	
APPLICATION AS FILED – PART I										
(Column 1)			(Column 2)		SMALL ENTITY ☐ OR		OTHER THAN SMALL ENTITY			
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	OR	RATE (\$)	FEE (\$)			
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A				
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A				
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A				
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X \$ =		OR	X \$ =				
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X \$ =			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 \$250 (\$125 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.										
APPLICATION AS AMENDED – PART II										
(Column 1)			(Column 2)	(Column 3)	SMALL ENTITY OR		OTHER THAN SMALL ENTITY			
AMENDMENT	06/25/2013	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)		RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	* 26	Minus	** 29	= 0	X \$ =		OR	X \$80=	0
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X \$ =		OR	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		OR	TOTAL ADD'L FEE	0
(Column 1)			(Column 2)	(Column 3)	SMALL ENTITY OR		OTHER THAN SMALL ENTITY			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)		RATE (\$)	ADDITIONAL FEE (\$)
	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))									
						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 number found in the appropriate box in column 1.										

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.

Legal Instrument Examiner:
/POLIN ANG/



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.
13/543,866	07/08/2012	Melvyn Morris	6890-93-CON	7855
22442	7590	07/08/2013		
Sheridan Ross PC 1560 Broadway Suite 1200 Denver, CO 80202			EXAMINER ZECHER, CORDELIA P K	
			ART UNIT 2432	PAPER NUMBER
			NOTIFICATION DATE 07/08/2013	DELIVERY MODE 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

<i>Applicant-Initiated Interview Summary</i>	Application No.	
	13/543,866	
	Applicant(s)	
	Examiner	Art Unit
	CORDELIA ZECHER	2432

All participants (applicant, applicant's representative, PTO personnel):

(1) CORDELIA ZECHER. (3) ____.

(2) Brent Linden. (4) ____.

Date of Interview: 01 July 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: Omote, Dozortsev.

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...)

Possible amendments to clarify the claims were discussed. Specifically clarifying that the pieces of information received from the remote computers are associated to assist in the determining of malware. Such amendments would require further search and consideration.

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

/CORDELIA ZECHER/ Primary Examiner, Art Unit 2432	
--	--

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.



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.
13/543,866	07/08/2012	Melvyn Morris	6890-93-CON	7855
22442	7590	07/12/2013		
Sheridan Ross PC 1560 Broadway Suite 1200 Denver, CO 80202			EXAMINER ZECHER, CORDELIA P K	
			ART UNIT 2432	PAPER NUMBER
			NOTIFICATION DATE 07/12/2013	DELIVERY MODE 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. 13/543,866	Applicant(s) MORRIS ET AL.	
	Examiner CORDELIA ZECHER	Art Unit 2432	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 25 June 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) 1-29 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) 1-29 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 25 June 2013 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/08)
Paper No(s)/Mail Date _____.

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

4) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

Applicant's arguments, see Remarks, filed June 25, 2013, with respect to the specification and drawings have been fully considered and are persuasive. The objection to the specification and drawings has been withdrawn.

Applicant's arguments with respect to 112 have been fully considered and are persuasive. The 112 rejection of claims 1 – 29 has been withdrawn.

Applicant's arguments with respect to the 103 rejection have been fully considered but they are not persuasive.

Applicant argues that Dozortsev does not teach or suggest comparing in the base computer data about the computer objects received from the plural remote computers to identify relationships between the object and other objects or entities. The examiner disagrees. The examiner finds that Dozortsev teaches comparing the received signature with the stored signature to determine if there is a match (paragraph 36, Figure 1, #50). This comparison is determining a relationship between the received signature and the stored signature.

Applicant argues that there is no disclosure in Omotoe and Dozortsev, taken alone, or in any combination of at least storing at the base computer said data received from plural remote computers, comparing in the base computer the data about the computer object received from the plural computers to identify relationships between the object and other objects or entities; and classifying the computer object as malware on the basis of said comparison, wherein said data includes information about events

initiated or involving the object when the object is created, configured or runs on the respective remote computers, said information including at least the identity of the object initiating the event, the event type, and the identity of the object or other entity on which the event is being performed.

The examiner disagrees. The examiner finds, as explained above, Dozortsev teaches at a central computer receiving and storing data received from plural remote computers, and comparing the data about the object received with the stored data to determine if there is a match (paragraphs 22 and 36), and classifying the process as malicious when a match is found (paragraph 36, Figure 1, #62). Omote discloses identifying malware using data about the object to classify it, such as the identity of the object, the event type, and the identity of the object or other entity on which the event is being performed (paragraphs 62-64). Therefore the combination of Omote and Dozortsev discloses the disputed claim limitations.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on June 20, 2013 was filed after the mailing date of the Non-Final Rejection on March 22, 2013. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Drawings

The drawings were received on June 25, 2013. These drawings are acceptable.

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

Claims 1 – 12, 15 – 26, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Omote US Publication 2006/0085857 A1, and further in view of Dozortsev US Publication 2003/0177394 A1.

Referring to claims 1, 15 and 29, Omote teaches:

Receiving data about a computer object, wherein said data includes information about events initiated or involving the object when the object is created, configured or runs on the respective remote computers, said information including at least the identity of the object initiating the event, the event type, and the identity of the object or other entity on which the event is being performed (paragraphs 39-42).

Storing at the base computer said data received (paragraph 42-43, and 51).

Comparing in the base computer the data about the computer object to identify relationships between the object and other objects or entities (paragraphs 41-42).

Classifying the computer object as malware on the basis of said comparison (paragraphs 63-64).

Omote does not explicitly disclose that the received information is for a plurality of remote computer. However, Dozortsev discloses suspect signatures are forwarded on to the central computer (paragraphs 22 and 45). Omote and Dozortsev are analogous art because they are from the same field of endeavor, virus detection. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Omote and Dozortsev before him or her, to modify the network virus activity detection system of Omote to include the central computer of Dozortsev. The suggestion/motivation for doing so would have been so that the central computer in this way communicates to the client computer the experience of other client computers connected to the central computer (paragraph 52).

Referring to claims 2 and 16, Omote discloses the relationship is between objects related directly, or between objects related via other objects (paragraph 41).

Referring to claims 3 and 17, Omote discloses an object and other objects are found to have a relationship, monitoring those related objects as a homogenous entity (paragraph 63).

Referring to claims 4 and 18, Omote discloses deducing an object to be malware based on the behavior of a related object (paragraph 63).

Referring to claims 5 and 19, Omote discloses if at least one other object to which said object is related is classed as malware, then classifying said object as malware (paragraphs 78 and 79). In addition, Dozortsev teaches if the object is related to a malicious executable code then disabling the executable code (paragraph 25).

Referring to claims 6 and 20, Omote discloses said other objects include the object or similar objects stored on the computer (paragraph 42). Omote does not explicitly disclose that the received information is for a plurality of remote computer. However, Dozortsev discloses suspect signatures are forwarded on to the central computer (paragraphs 22 and 45). Omote and Dozortsev are analogous art because they are from the same field of endeavor, virus detection. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Omote and Dozortsev before him or her, to modify the network virus activity detection system of Omote to include the central computer of Dozortsev. The suggestion/motivation for doing so would have been so that the central computer in this way communicates to the client computer the experience of other client computers connected to the central computer (paragraph 52).

Referring to claims 7 and 21, Omote discloses said other objects include other objects that are parent objects or child objects or otherwise process-related objects to said object (paragraph 41 and 63).

Referring to claims 8 and 22, Omote teaches the data about the computer object that is used in the comparison includes the current name of the object (paragraph 40). Omote does not explicitly disclose that the received information is for a plurality of remote computer. However, Dozortsev discloses suspect signatures are forwarded on to the central computer (paragraphs 22 and 45). Omote and Dozortsev are analogous art because they are from the same field of endeavor, virus detection. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the

teachings of Omote and Dozortsev before him or her, to modify the network virus activity detection system of Omote to include the central computer of Dozortsev. The suggestion/motivation for doing so would have been so that the central computer in this way communicates to the client computer the experience of other client computers connected to the central computer (paragraph 52).

Referring to claims 9 and 23, Dozortsev discloses the data is sent in the form of key that is obtained by a hashing process carried out in respect of the objects on the respective remote computers (paragraph 21). Omote and Dozortsev are analogous art because they are from the same field of endeavor, virus detection. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Omote and Dozortsev before him or her, to modify the network virus activity detection system of Omote to include the unique signature of Dozortsev. The suggestion/motivation for doing so would have been to have a unique signature of the executable code for comparison (paragraph 21).

Referring to claims 10 and 24, Dozortsev discloses the key has at least one component that represents executable instructions contained within or constituted by the object (paragraph 21). Omote and Dozortsev are analogous art because they are from the same field of endeavor, virus detection. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Omote and Dozortsev before him or her, to modify the network virus activity detection system of Omote to include the unique signature of Dozortsev. The suggestion/motivation for

doing so would have been to have a unique signature of the executable code for comparison (paragraph 21).

Referring to claims 11 and 25, Dozortsev discloses the key has at least one component that represents data about said object (paragraph 21). Omote and Dozortsev are analogous art because they are from the same field of endeavor, virus detection. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Omote and Dozortsev before him or her, to modify the network virus activity detection system of Omote to include the unique signature of Dozortsev. The suggestion/motivation for doing so would have been to have a unique signature of the executable code for comparison (paragraph 21).

Referring to claims 12 and 26, Omote discloses said data about said object includes the current name of the object (paragraph 40).

Claims 13, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Omote in view of Dozortsev as applied above, and further in view of Barton et al's US Publication 2005/0021994 A1.

Omote in view of Dozortsev discloses all the limitations of the parent claims. Omote in view of Dozortsev does not explicitly disclose the data about the object including the size of the object. However, Barton discloses indicating for the object the file name, size and location (pages 2-3, paragraph 39). Omote in view of Dozortsev and Barton are analogous art because they are from the same field of endeavor, malware detection. At the time of the invention, it would have been obvious to one of ordinary

skill in the art, having the teachings of Omote in view of Dozortsev and Barton before him or her, to modify the rules of Omote in view of Dozortsev to include the data size of Barton. The suggestion/motivation for doing so would have been the characteristics are strongly indicative of a particular file being one of the candidates (page 1, paragraph 14).

Claims 14 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Omote in view of Dozortsev, as applied above, and further in view of Kester et al US Publication 2005/0210035 A1.

Omote in view of Dozortsev teaches all the limitations of the parent claim, and initially classifying an object as not malware, and changing the status of the object after an investigation (Dozortsev, paragraphs 37-41). Omote in view of Dozortsev does not explicitly disclose generating a mask for said object that defines acceptable behaviour for the object, and monitoring operation of the object on at least one of the remote computers and reclassifying the object as malware if the actual monitored behaviour extends beyond that permitted by the mask. However, Kester discloses determining access privileges for an application based on the expected network behavior of an application (paragraph 43), and then monitoring the behavior of an application based on access privileges (paragraphs 41, 55 and 56).

Omote in view of Dozortsev and Kester are from the same field of endeavor, malware. At the time of invention, it would have been obvious to one of ordinary skill in the art to modify the investigation of Omote in view of Dozortsev to include the

privileges based on behavior of Kester. The suggestion for doing so would have been for the system to be able to keep or change a previous access privilege based on the subsequent activity of an application (paragraph 41).

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

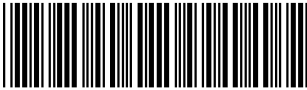
A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened 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 mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CORDELIA ZECHER whose telephone number is (571)272-7771. The examiner can normally be reached on Monday - Thursday 8:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. 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.

/CORDELIA ZECHER/
Primary Examiner, Art Unit 2432

<i>Index of Claims</i> 	Application/Control No. 13543866	Applicant(s)/Patent Under Reexamination MORRIS ET AL.
	Examiner CORDELIA ZECHER	Art Unit 2432

✓	Rejected
=	Allowed

-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

☐ Claims renumbered in the same order as presented by applicant				☐ CPA		☐ T.D.		☐ R.1.47	
CLAIM		DATE							
Final	Original	03/14/2013	07/01/2013						
	1	✓	✓						
	2	✓	✓						
	3	✓	✓						
	4	✓	✓						
	5	✓	✓						
	6	✓	✓						
	7	✓	✓						
	8	✓	✓						
	9	✓	✓						
	10	✓	✓						
	11	✓	✓						
	12	✓	✓						
	13	✓	✓						
	14	✓	✓						
	15	✓	✓						
	16	✓	✓						
	17	✓	✓						
	18	✓	✓						
	19	✓	✓						
	20	✓	✓						
	21	✓	✓						
	22	✓	✓						
	23	✓	✓						
	24	✓	✓						
	25	✓	✓						
	26	✓	✓						
	27	✓	✓						
	28	✓	✓						
	29	✓	✓						

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Application Number	13/543,866
				Filing Date	July 8, 2012
				First Named Inventor	Melvyn Morris
				Art Unit	2432
				Examiner Name	Cordelia P.K. Zecher
Sheet	1	of	1	Attorney Docket Number	6890-93-CON

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	7793338	09/07/2010	Beddoe 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.
	2	Official Action for China Patent Application No. 201110036124.1, dated Apr. 17, 2013, 7 pages
	3	EXAMINER ZECHER, Official Action for U.S. Patent Application No. 13/543,865, mailed Apr. 15, 2013, 9 pages (Attorney's Ref. No. 6890-93-DIV)

Examiner Signature	/Cordelia Zecher/	Date Considered	07/01/2013
--------------------	-------------------	-----------------	------------

*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. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.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. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.Z./

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of: Melvyn Morris	)	Group Art Unit: 2432
	)	
Application No.: 13/543,866	)	Examiner: Zecher, Cordelia PK
	)	
Filed: July 08, 2012	)	Confirmation No.: 7855
	)	
Atty. File No.: 6890-93-CON	)	
	)	
	)	
For: Methods and Apparatus for Dealing with	)	
Malware	)	
	)	

RESPONSE TO INTERVIEW SUMMARY

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

Commissioner:

Applicant would like to thank Examiner Zecher for her time during the telephonic interview on July 01, 2013. Examiner Zecher and Applicant's representative, Brent Lindon, discussed the current rejection to clarify the issues at hand, discussed possible additions to the claims, and differences between the cited art and the present claims. Specifically discussed was clarifying that the pieces of information received from the remote computers are associated to assist in the determining of malware; however, such amendments would require further search and consideration. Again, Applicant appreciates the Examiner's attention and assistance.

Respectfully submitted,

SHERIDAN ROSS P.C.

Date: August 06, 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:	16518087
Application Number:	13543866
International Application Number:	
Confirmation Number:	7855
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:	6890-93-CON
Receipt Date:	06-AUG-2013
Filing Date:	08-JUL-2012
Time Stamp:	18:46:07
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	Miscellaneous Incoming Letter	Response_to_Interview_Summ ary.pdf	65360 7ac14ff6a050dbbde81cbc99c8b5b0a2a3d638	no	1

Warnings:

Information:

Total Files Size (in bytes):	65360
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. <u>New Applications Under 35 U.S.C. 111</u> 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. <u>National Stage of an International Application under 35 U.S.C. 371</u> 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. <u>New International Application Filed with the USPTO as a Receiving Office</u> 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.	



PRIORITY DOCUMENT EXCHANGE

FAILURE STATUS REPORT

An attempt by the Office to electronically retrieve, under the Priority Document Exchange programs (PDX and DAS), 0513375.6 to which priority is claimed has FAILED on 10/04/2013.

For further questions or assistance, please contact our EBC Customer Support Center at

1-866-217-9197 (toll-free)

571-272-4100 (local)

M-F 6AM - Midnight (Eastern Time)

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL **(Submitted Only via EFS-Web)**

Application Number	13543866	Filing Date	2012-07-08	Docket Number (if applicable)	6890-93-CON	Art Unit	2432
First Named Inventor	Melvyn Morris			Examiner Name	Zecher, Cordelia PK		

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

Doc code: RCEX

Doc description: Request for Continued Examination (RCE)

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)	2012-11-12
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.

Electronic Patent Application Fee Transmittal				
Application Number:		13543866		
Filing Date:		08-Jul-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:		6890-93-CON		
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:				
Claims in excess of 20	2202	1	40	40
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 - 1 month with \$0 paid	2251	1	100	100
Miscellaneous:				
Request for Continued Examination	2801	1	600	600
Total in USD (\$)				740

Electronic Acknowledgement Receipt	
EFS ID:	17374041
Application Number:	13543866
International Application Number:	
Confirmation Number:	7855
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:	6890-93-CON
Receipt Date:	12-NOV-2013
Filing Date:	08-JUL-2012
Time Stamp:	16:11:46
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 740
RAM confirmation Number	3535
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_02.pdf	146209	yes	14
			6acc297c3141af26f0ba0dd8e17a16a6dc76655		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Amendment Submitted/Entered with Filing of CPA/RCE		1	1	
	Claims		2	8	
	Applicant Arguments/Remarks Made in an Amendment		9	14	
Warnings:					
Information:					
2	Extension of Time	sb0022_EOT_1mo.pdf	186997	no	2
			a6295d5c9ae275e9a96256f1a7846a882a313752		
Warnings:					
Information:					
3	Request for Continued Examination (RCE)	sb0030e_RCE.pdf	697541	no	3
			fea6ee4fa7f6fb18e1f8e780e8e24d33804a4970		
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	34127	no	2
			80c594afc10f36b0bba785bc8cfe79d66a7e9a0		
Warnings:					
Information:					
Total Files Size (in bytes):			1064874		

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: Melvyn Morris	)	Group Art Unit: 2432
	)	
Application No.: 13/543,866	)	Examiner: Zecher, Cordelia PK
	)	
Filed: July 08, 2012	)	Confirmation No.: 7855
	)	
Atty. File No.: 6890-93-CON	)	
	)	
	)	
For: Methods and Apparatus for Dealing with	)	
Malware	)	
	)	
	)	

AMENDMENT AND RESPONSE

Mail Stop 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 July 12, 2013. Submitted herewith is a Petition for a one month Extension of Time along with the requisite fee. Additionally, a Request for Continued Examination together with the required fees has been filed concurrently herewith. Additionally, payment in the amount for \$40.00 for one additional dependent claim has been made concurrently herewith. Although Applicant believes that no additional fees are due in connection with filing this Amendment and Response, please credit any overpayment or charge any underpayment 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 9 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 a first remote computers-computer~~ on which the object or similar objects are stored, wherein said data includes information about events initiated or involving the object when the object is created, configured or runs on the ~~respective-first remote computers-computer~~, said information including at least the identity of ~~the-an~~ object initiating the event, the event type, and ~~the-an~~ identity of the object or other entity on which the event is being performed;

at the base computer, receiving data about the computer object from a second remote computer on which the object or similar objects are stored, wherein said data includes information about events initiated or involving the object when the object is created, configured or runs on the second remote computer, said information including at least the identity of the object initiating the event, the event type, and the identity of the object or other entity on which the event is being performed;

storing at the base computer said data received from ~~plural~~ the first and second remote computers;

correlating, by the base computer, at least a portion of the data about the computer object received from the first remote computer to at least a portion of the data about the computer object received from the second remote computer;

comparing, ~~in-by~~ by the base computer, the correlated data about the computer object received from the first and second plural remote computers to ~~identify relationships between the object and other objects or entities to identify relationships between the correlated data and the other objects or entities;~~ and

classifying, by the base computer, the computer object as malware on the basis of said comparison.

2. (Original) A method according to claim 1, wherein the relationship is between objects related directly, or between objects related via other objects.

3. (Currently Amended) A method according to claim 1, wherein where an object and other objects are found to have a relationship, monitoring those related objects as a homogenous entity and identifying a common object of the homogenous entity as a malware object.

4. (Original) A method according to claim 1, comprising deducing an object to be malware based on the behaviour of a related object.

5. (Original) A method according to claim 1, wherein if at least one other object to which said object is related is classed as malware, then classifying said object as malware.

6. (Currently Amended) A method according to claim 1, wherein said other objects include the object or similar objects stored on at least ~~someone~~ one of the first and second remote computers.

7. (Original) A method according to claim 1, wherein said other objects include other objects that are parent objects or child objects or otherwise process-related objects to said object.

8. (Currently Amended) A method according to claim 1, wherein the data about the computer object that is sent from the ~~plural~~ respective remote ~~computers~~ computer to the base computer and that is used in the comparison includes one or more of:

- executable instructions contained within or constituted by the object;
- the size of the object; the current name of the object;
- the physical and folder location of the object on disk;
- the original name of the object;
- the creation and modification dates of the object;

vendor, product and version and any other information stored within the object; and,
the object header or header held by the respective remote computer.

9. (Currently Amended) A method according to claim 1, wherein the data is sent in the form of a key that is obtained by a hashing process carried out in respect of the objects on the respective remote ~~computers~~computer.

10. (Original) A method according to claim 9, wherein the key has at least one component that represents executable instructions contained within or constituted by the object.

11. (Original) A method according to claim 9, wherein the key has at least one component that represents data about said object.

12. (Currently Amended) A method according to claim 11, wherein said data about said object includes at least one of:

- the current name of the object;
- the physical and folder location of the object on disk;
- the original name of the object;
- the creation and modification dates of the object;
- vendor, product and version and any other information stored within the object;
- the object header or header held by the respective remote computer; and,
- events initiated by or involving the object when the object is created, configured or runs on the respective remote computers.

13. (Original) A method according to claim 9, wherein the key has at least one component that represents the physical size of the object.

14. (Currently Amended) A method according to claim 1, comprising initially classifying an object as not malware, generating a mask for said object that defines acceptable behaviour for the object, ~~and comprising~~ monitoring an operation of the object on at least one of

the first and second remote computers and reclassifying the object as malware if the actual monitored behaviour extends beyond that permitted by the mask.

15. (Currently Amended) Apparatus for classifying a computer object as malware, the apparatus comprising:

a base computer constructed and arranged to receive data about a computer object from ~~each of plural~~ a first remote ~~computers~~ computer on which the object or similar objects are stored, wherein said data includes information about events initiated or involving the object when the object is created, configured or runs on the ~~respective first remote computers~~ computer, said information including at least the identity of the object initiating the event, the event type, and the identity of the object or other entity on which the event is being performed;

the base computer being constructed and arranged to receive data about the computer object from a second remote computer on which the object or similar objects are stored, wherein said data includes information about events initiated or involving the object when the object is created, configured or runs on the second remote computer, said information including at least the identity of the object initiating the event, the event type, and the identity of the object or other entity on which the event is being performed;

the base computer being constructed and arranged to correlate at least a portion of the data about the computer object received from the first remote computer to at least a portion of the data about the computer object received from the second remote computer;

the base computer being constructed and arranged to compare the data about the computer object received from ~~said plural~~ the first and second remote computers to other objects or entities to identify relationships between the correlated data object and the other objects or entities; and

the base computer being constructed and arranged to classify the computer object as malware on the basis of said comparison.

16. (Original) Apparatus according to claim 15, wherein the base computer is constructed and arranged so as to identify the relationship between objects related directly, or between objects related via other objects.

17. (Currently Amended) Apparatus according to claim 15, wherein the base computer is constructed and arranged so as, where an object and other objects are found to have a relationship, to monitoring those related objects as a homogenous entity and identify a common object of the homogenous entity as a malware object.

18. (Original) Apparatus according to claim 15, wherein the base computer is constructed and arranged so as to deduce an object to be malware based on the behaviour of a related object.

19. (Original) Apparatus according to claim 15, wherein the base computer is constructed and arranged so that if at least one other object to which said object is related is classed as malware, then said object is classified as malware.

20. (Currently Amended) Apparatus according to claim 15, wherein the base computer is constructed and arranged so that said other objects include the object or similar objects stored on at least ~~some one of said~~ the first and second remote computers.

21. (Original) Apparatus according to claim 15, wherein the base computer is constructed and arranged so that said other objects include other objects that are parent objects or child objects or otherwise process-related objects to said object.

22. (Currently Amended) Apparatus according to claim 15, wherein the base computer is constructed and arranged so as to compare the data where the data includes one or more of:

- executable instructions contained within or constituted by the object;
- the size of the object; the current name of the object;
- the physical and folder location of the object on disk;
- the original name of the object;
- the creation and modification dates of the object;
- vendor, product and version and any other information stored within the object; and,
- the object header or header held by the respective remote computer.

23. (Currently Amended) Apparatus according to claim 15, wherein the base computer is constructed and arranged so as to be able to process data that is sent in the form of a key that is obtained by a hashing process carried out in respect of the objects on said respective remote ~~computers~~computer.

24. (Original) Apparatus according to claim 23, wherein the key has at least one component that represents executable instructions contained within or constituted by the object.

25. (Original) Apparatus according to claim 23, wherein the key has at least one component that represents data about said object.

26. (Currently Amended) Apparatus according to claim 25, wherein said data about said object includes at least one of:

- the current name of the object;
- the physical and folder location of the object on disk;
- the original name of the object;
- the creation and modification dates of the object;
- vendor, product and version and any other information stored within the object;
- the object header or header held by the respective remote computer; and[[,]]
- events initiated by or involving the object when the object is created, configured or runs on the respective remote computers.

27. (Original) Apparatus according to claim 23, wherein the key has at least one component that represents the physical size of the object.

28. (Currently Amended) Apparatus according to claim 15, wherein the base computer is constructed and arranged to generate a mask for an object that is initially classed not as malware, said mask defining acceptable behaviour for the object, and the base computer is constructed and arranged to monitor an operation of the object on at least one of the first and

second remote computers and to reclassify the object as malware if the actual monitored behaviour extends beyond that permitted by the mask.

29. (Original) A computer program recorded on non-transitory computer readable medium comprising program instructions for causing a computer to perform the method of claim 1.

30. (New) A method according to claim 1, wherein the data received about the computer object from the first remote computer is different than the data received about the computer object from the second remote computer.

REMARKS

The above-identified patent application has been reviewed in light of the Examiner's Action dated July 12, 2013. Claims 1, 3, 6, 8, 9, 12, 14, 15, 17, 20, 22, 23, 26, and 28 have been amended, without intending to abandon or to dedicate to the public any patentable subject matter. Claim 30 has been added. Accordingly, claims 1-30 are now pending. As set forth herein, reconsideration and withdrawal of the rejections of the claims are respectfully requested.

Claim Rejections Under 35 U.S.C. § 103

Claims 1-12, 15-26, and 29 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Publication No. 2006/0085857 A1 to Omote et al. (hereinafter "Omote") and further in view of U.S. Publication No. 2003/0177394 A1 to Dozortsev (hereinafter "Dozortsev"). Claims 13 and 27 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Omote in view of Dozortsev and further in view of U.S. Patent Publication No. 2005/0021994 A1 to Barton et al. (hereinafter "Barton"). Claims 14 and 28 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Omote in view of Dozortsev and further in view of U.S. Patent Publication No. 2005/0210035 A1 to Kester et al. (hereinafter "Kester"). 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, Latest Revision July 2008. The Applicant respectfully submits that not all features of the claimed invention are taught or suggested by the cited references.

In particular, whether considered alone or in combination, the cited references do not disclose a method comprising: at a base computer, receiving data about a computer object from a first remote computer on which the object or similar objects are stored, wherein said data includes information about events initiated or involving the object when the object is created, configured or runs on the first remote computer, said information including at least the identity of an object initiating the event, the event type, and an identity of the object or other entity on which the event is being performed, at the base computer, receiving data about the computer object from a second remote computer on which the object or similar objects are stored, wherein said data includes information about events initiated or involving the object when the object is created, configured or runs on the second remote computer, said information including at least the identity of the object initiating the event, the event type, and the identity of the object or other entity on which the event is being performed, storing at the base computer said data received from the first and second remote computers, correlating, by the base computer, at least a portion of the data about the computer object received from the first remote computer to at least a portion of the data about the computer object received from the second remote computer, comparing, by the base computer, the correlated data about the computer object received from the first and second remote computers to other objects or entities to identify relationships between the correlated data and the other objects or entities; an. In particular, the cited references do not teach, suggest or describe at least correlating, by the base computer, at least a portion of the data about the computer object received from the first remote computer to at least a portion of the data about the same computer object received from the second remote computer and then comparing the correlated data about the computer object to identify relationships between the object and other objects or entities. Accordingly, the rejections of the claims as obvious in view of the cited references should be reconsidered and withdrawn.

The Claimed Invention

The claimed invention generally relates to classifying a computer object as malware utilizing a community database which provides an extensive corollary of an object's creation, configuration, execution, behavior, identities, and relationships to other objects that either act upon it or are acted upon by it. This relationship chain provides a series of correlation points, allowing ancestral relationships to be considered for any object and its predecessors by event or

its issue. *See e.g., Applicant's specification-as-published*, ¶ 0102. The stored data may then be compared to identify relationships between the object and other objects or entities. Based on this comparison, the computer object may be classified as malware.

The Omote Reference

The Omote reference is generally directed to a network virus activity detection system implemented in the client PC which generates process tree information and then uses this process tree information to determine whether or not the process to be discriminated is an illegal process. *See e.g., Omote*, ¶ 0037, ¶ 0038, ¶ 0041. Specifically, “discrimination rule information based on the hierarchical relationship among processes is stored to designate common behavior to illegal processes so that it can be determined whether or not a process being operated in a computer is an illegal process by the activities of a virus.” *See e.g., Omote*, ¶ 0013. As Omote is generally directed to a system implemented on a PC, Omote makes no mention of at least receiving data about a computer object from a first remote computer and receiving data about the computer object from a second remote computer. Additionally, there is no suggestion in Omote where at least a portion of the data about the computer object from the first and second remote computers is correlated, the correlated data then being compared to other objects or entities to identify relationships. At least such a feature is not disclosed or taught by Omote. Dozortsev does not teach that which Omote lacks.

The Dozortsev Reference

The Dozortsev reference is generally directed to a central computer, including a database that is adapted to “store and analyze a plurality of executable code signatures, including signatures of malicious, legitimate, those executable codes identity of which is being investigated and those that have not been received for an investigation.” *See e.g., Dozortsev*, Abstract. Specifically, “[u]pon detection of the occurrence of a potentially dangerous event, the monitoring software pinpoints the executable code responsible for it. Once the executable code is pinpointed, the monitoring application creates a unique suspect signature (using MD5 or another algorithm) for that module or a corresponding file and then transmits the suspect signature to the central computer.” *See e.g., Dozortsev*, ¶ 0021. Additionally, paragraph [0045] of Dozortsev provides:

If the signature doesn't match an entry in the local database, it is then forwarded for comparison to the central computer 165 and subsequent events are then identical to those described above with respect to the first working session with like numerals denoting like steps of FIG. 1. The analysis of the suspect signature includes comparison of the suspect signature with the plurality of signatures stored in the database. If signatures match an entry in the database, subsequent steps will depend on how the signature is flagged. It must be appreciated that the types and the number of flags in the current invention can be more than described here. If the signature is flagged "new, executable code is not received" 52, the system will attempt to download the actual suspect executable code from the client computer to the central server. If the signature is flagged "received, under investigation" 54, the following message is forwarded to the client computer, "The executable code is being investigated" 56. If the signature is flagged "legitimate" 58, a corresponding message is sent to the client computer and the monitoring software on the client computer is commanded to allow the executable code in question to be executed and/or an event to proceed 60. If the signature is flagged "malicious" 62, the monitoring application receives a command to terminate the event 64. Event termination can be accomplished by terminating the process, but it can also be accomplished by a variety of temporary or permanent means. The system can also be configured to allow the end user to override the system's decision, for instance to allow a "malicious" executable code to operate.

See e.g., Dozortsev, ¶ 0021. That is, Dozortsev teaches sending signatures to a system where the signatures may or may not be matched to other signatures residing on the system. Nowhere does Dozortsev teach at least receiving data about a computer object from a first remote computer and receiving data about the computer object from a second remote computer. Additionally, there is no suggestion in Dozortsev where at least a portion of the data about the computer object from the first and second remote computers is correlated, the correlated data then being compared to other objects or entities to identify relationships. Instead, Dozortsev appears to be teaching merely matching signatures to determine if a suspect executable code is in the database on the central computer. Omote and Dozortsev, taken alone, or in any combination, do not teach or suggest at least correlating, by the base computer, at least a portion of the data about the computer object received from the first remote computer to at least a portion of the data about the computer object received from the second remote computer; and comparing, by the base computer, the correlated data about the computer object received from the first and second remote computers to other objects or entities to identify relationships between the correlated data and the other objects or entities. This is simply not taught or disclosed by any of the cited references.

Accordingly, at least based on the above, the independent claim is patentably distinguishable from the cited reference. The dependent claims are further distinguishable at least based on the above and the additional feature(s) recited therein. Therefore, Applicant respectfully submits that the rejections of claims 1-29 should be reconsidered and withdrawn.

Independently allowable dependent claims

In addition to depending from allowable independent claims, the dependent claims provide additional and independent reasons for allowance. For instance, dependent claim 30 requires that the data received about the computer object from the first remote computer is different than the data received about the computer object from the second remote computer. That is, the received data concerns the same object, however, the feature claimed requires that the received data is different. Nowhere is at least this feature taught or disclosed in the cited references.

As another example, dependent claims 3 and 17 require that where an object and other objects are found to have a relationship, monitoring those related objects as a homogenous entity and identifying a common object of the homogenous entity as a malware object. Indeed, ¶ 0065 of Omote teaches that by comparing the process designation result with the process log 19, the contents of the parent process of the process to be discriminated 2X are designated, and it is determined whether or not the process of the process to be discriminated 2X is an illegal process under the service of the parent process and the grandpa process based on the illegal rule file 18. *See e.g., Omote*, ¶ 0065. However, there is no teaching relating to identifying a common object of the homogenous entity as a malware object. Accordingly, at least the rejection of claims 3 and 17 should be reconsidered and withdrawn.

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: November 12, 2013

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

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)		Docket Number (Optional) 6890-93-CON																																		
Application Number 13/543,866	Filed 2012-07-08																																			
For METHODS AND APPARATUS FOR DEALING WITH MALWARE																																				
Art Unit 2432	Examiner ZECHER, CORDELIA PK																																			
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): <table style="width: 100%; border-collapse: collapse;"><thead><tr><th></th><th style="text-align: center;"><u>Fee</u></th><th style="text-align: center;"><u>Small Entity Fee</u></th><th style="text-align: center;"><u>Micro Entity Fee</u></th><th></th></tr></thead><tbody><tr><td>☒ One month (37 CFR 1.17(a)(1))</td><td style="text-align: center;">\$200</td><td style="text-align: center;">\$100</td><td style="text-align: center;">\$50</td><td>\$ <u>100.00</u></td></tr><tr><td>☐ Two months (37 CFR 1.17(a)(2))</td><td style="text-align: center;">\$600</td><td style="text-align: center;">\$300</td><td style="text-align: center;">\$150</td><td>\$ _____</td></tr><tr><td>☐ Three months (37 CFR 1.17(a)(3))</td><td style="text-align: center;">\$1,400</td><td style="text-align: center;">\$700</td><td style="text-align: center;">\$350</td><td>\$ _____</td></tr><tr><td>☐ Four months (37 CFR 1.17(a)(4))</td><td style="text-align: center;">\$2,200</td><td style="text-align: center;">\$1,100</td><td style="text-align: center;">\$550</td><td>\$ _____</td></tr><tr><td>☐ Five months (37 CFR 1.17(a)(5))</td><td style="text-align: center;">\$3,000</td><td style="text-align: center;">\$1,500</td><td style="text-align: center;">\$750</td><td>\$ _____</td></tr></tbody></table> ☒ 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 <u>191970</u>. ☒ 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 <u>67424</u> ☐ attorney or agent acting under 37 CFR 1.34. Registration number _____ <table style="width: 100%; border-collapse: collapse;"><tr><td style="width: 50%; padding: 5px;">/Brent R. Lindon/ _____ Signature</td><td style="width: 50%; padding: 5px;">November 12, 2013 _____ Date</td></tr><tr><td style="padding: 5px;">Brent R. Lindon _____ Typed or printed name</td><td style="padding: 5px;">303-863-9700 _____ Telephone Number</td></tr></table> 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.				<u>Fee</u>	<u>Small Entity Fee</u>	<u>Micro Entity Fee</u>		☒ One month (37 CFR 1.17(a)(1))	\$200	\$100	\$50	\$ <u>100.00</u>	☐ 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	\$ _____	/Brent R. Lindon/ _____ Signature	November 12, 2013 _____ Date	Brent R. Lindon _____ Typed or printed name	303-863-9700 _____ Telephone Number
	<u>Fee</u>	<u>Small Entity Fee</u>	<u>Micro Entity Fee</u>																																	
☒ One month (37 CFR 1.17(a)(1))	\$200	\$100	\$50	\$ <u>100.00</u>																																
☐ 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	\$ _____																																
/Brent R. Lindon/ _____ Signature	November 12, 2013 _____ Date																																			
Brent R. Lindon _____ Typed or printed name	303-863-9700 _____ Telephone Number																																			

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.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875				Application or Docket Number 13/543,866		Filing Date 07/08/2012		☐ To be Mailed	
ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO									
APPLICATION AS FILED – PART I									
(Column 1)		(Column 2)							
FOR	NUMBER FILED	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), (l), 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									
(Column 1)		(Column 2)		(Column 3)					
AMENDMENT	11/12/2013	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE (\$)	ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	* 30	Minus	** 29	= 1		x \$40 =	40	
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0		x \$210 =	0	
	☐ Application Size Fee (37 CFR 1.16(s))								
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
						TOTAL ADD'L FEE		40	
(Column 1)		(Column 2)		(Column 3)					
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	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.									

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 <i>(Use as many sheets as necessary)</i>				Application Number	13/543,866
				Filing Date	July 8, 2012
				First Named Inventor	Melvyn Morris
				Art Unit	2431
				Examiner Name	Trang T. Doan
Sheet	1	of	1	Attorney Docket Number	6890-93-CON

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	2002/0194490	12/19/2002	Halperin et al.	
	2	2003/0131256	07/10/2003	Ackroyd	
	3	2003/0195861	10/16/2003	McClure 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.
	4	Official Action for European Patent Application No. 06755686.0 dated Jul. 31, 2013, 5 pages.
	5	EXAMINER ARBUTINA, Extended European Search Report for European Patent Application No. 13167434.3 dated Aug. 1, 2013, 6 pages.
	6	EXAMINER ARBUTINA, Extended European Search Report for European Patent Application No. 13167436.8 dated Aug. 30, 2013, 5 pages.
	7	EXAMINER ZECHER, Official Action for U.S. Patent Application No. 13/543,865, mailed Aug. 6, 2013, 11 pages (Attorney's Ref. No. 6890-93-DIV)

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. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.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. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

Electronic Acknowledgement Receipt	
EFS ID:	17527672
Application Number:	13543866
International Application Number:	
Confirmation Number:	7855
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:	6890-93-CON
Receipt Date:	27-NOV-2013
Filing Date:	08-JUL-2012
Time Stamp:	17:48:56
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	EP06755686_OA_07-31-2013.pdf	113825 1c0efaf95e729649fedbd47b7598a91c717ab47a	no	5
Warnings:					
Information:					

2	Non Patent Literature	EP13167434_EESR_08-01-2013.pdf	161055 4c4040a4cf0a728e1906460c9c965c73f15e6bc8	no	6
Warnings:					
Information:					
3	Non Patent Literature	EP13167436_EESR_08-30-2013.pdf	148651 baeedf49f38a1cd156f1797ed3e1cc59de623744	no	5
Warnings:					
Information:					
4	Non Patent Literature	6890-93-DIV_OA_08-06-2013.pdf	371702 66282c60f4fa89badc4a22f80898b9e1aecf97bb	no	11
Warnings:					
Information:					
5		IDS_03.pdf	371800 91dfc1ac17a4534adf6ae1444fc2ecd35af6619a	yes	4
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal Letter		1	3	
	Information Disclosure Statement (IDS) Form (SB08)		4	4	
Warnings:					
Information:					
Total Files Size (in bytes):			1167033		
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.: 7855
Serial No.: 13/543,866	)	Examiner: Trang T. Doan
Filed: July 8, 2012	)	
Atty. File No.: 6890-93-CON	)	<u>SUPPLEMENTAL</u>
Entitled: "Methods and Apparatus for Dealing	)	<u>INFORMATION DISCLOSURE</u>
With Malware"	)	<u>STATEMENT</u>
	)	<i>Electronically Submitted</i>

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

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.

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/
Brent R. Lindon
Registration No. 67424
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: 11/27/2013



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

NOTICE OF ALLOWANCE AND FEE(S) DUE

22442 7590 12/26/2013
Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

EXAMINER

DOAN, TRANG T

ART UNIT

PAPER NUMBER

2431

DATE MAILED: 12/26/2013

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/543,866	07/08/2012	Melvyn Morris	6890-93-CON	7855

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	\$1780	\$300	\$0	\$2080	03/26/2014

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)

22442 7590 12/26/2013
Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

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.
13/543,866	07/08/2012	Melvyn Morris	6890-93-CON	7855

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	\$1780	\$300	\$0	\$2080	03/26/2014

EXAMINER	ART UNIT	CLASS-SUBCLASS
DOAN, TRANG T	2431	726-024000

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, 1 _____
 (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. 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
☐ Applicant asserting small entity status. See 37 CFR 1.27
☐ Applicant changing to regular undiscounted fee status.

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.

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.

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. _____



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.
13/543,866	07/08/2012	Melvyn Morris	6890-93-CON	7855
22442 7590 12/26/2013 Sheridan Ross PC 1560 Broadway Suite 1200 Denver, CO 80202				
EXAMINER DOAN, TRANG T				
ART UNIT PAPER NUMBER 2431				
DATE MAILED: 12/26/2013				

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 0 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 0 day(s).

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 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.

**Notices of Allowance and Fee(s) Due mailed between October 1, 2013 and
December 31, 2013**

(Addendum to PTOL-85)

If the “Notice of Allowance and Fee(s) Due” has a mailing date on or after October 1, 2013 and before January 1, 2014, the following information is applicable to this application.

If the issue fee is being timely paid on or after January 1, 2014, the amount due is the issue fee and publication fee in effect January 1, 2014. On January 1, 2014, the issue fees set forth in 37 CFR 1.18 decrease significantly and the publication fee set forth in 37 CFR 1.18(d)(1) decreases to \$0.

If an issue fee or publication fee has been previously paid in this application, applicant is not entitled to a refund of the difference between the amount paid and the amount in effect on January 1, 2014.

Notice of Allowability	Application No. 13/543,866	Applicant(s) MORRIS ET AL.	
	Examiner TRANG DOAN	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 amendment filed on 11/12/2013.
☐ 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 1-30. 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. 11/477,807.
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)	5. ☐ Examiner's Amendment/Comment
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date <u>11/27/2013</u>	6. ☒ Examiner's Statement of Reasons for Allowance
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material	7. ☐ Other _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____.	

	/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

2. This action is in response to the amendment filed on 11/12/2013.
3. Claims 1, 3, 6, 8-9, 12, 14-15, 17, 20, 22-23, 26 and 28 have been amended. Claim 30 has been added. Claims 1-30 are pending for consideration.

Continued Examination Under 37 CFR 1.114

4. 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 11/12/2013 has been entered.

Information Disclosure Statement

5. The information disclosure statement (IDS) submitted on 11/27/2013 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Response to Arguments

6. Applicant's arguments, filed on 11/12/2013, with respect to claims 1-29 have been fully considered and are persuasive. The rejection of claims 1-29 has been withdrawn.

Allowable Subject Matter

7. Claims 1-30 are allowed.
8. The following is an examiner's statement of reasons for allowance: As noted above, the Examiner agrees with the Applicant's arguments on pages 11-12 of the Remarks, specifically that the prior art, taken alone, or in any combination, does not teach or suggest the combination of claim limitations including "*at least correlating, by the base computer, at least a portion of the data about the computer object received from the first remote computer to at least a portion of the data about the computer object received from the second remote computer; comparing, by the base computer, the correlated data about the computer object received from the first and second remote computers to other objects or entities to identify relationships between the correlated data and the other objects or entities; and classifying, by the base computer, the computer object as malware on the basis of said comparison*". The Examiner was unable to find a teaching, suggestion, or motivation that would render the above limitations obvious. Claims 1-30 are, therefore, novel and not obvious.

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

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRANG DOAN whose telephone number is (571)272-0740. The examiner can normally be reached on Monday-Friday.

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.

/TRANG DOAN/
Examiner, Art Unit 2431

/CORDELIA ZECHER/
Supervisory Patent Examiner, Art Unit 2431

Notice of References Cited	Application/Control No. 13/543,866	Applicant(s)/Patent Under Reexamination MORRIS ET AL.	
	Examiner TRANG DOAN	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-2002/0087734 A1	07-2002	Marshall et al.	709/310
*	B	US-2004/0006704 A1	01-2004	Dahlstrom et al.	713/200
*	C	US-2006/0085857 A1	04-2006	Omote et al.	726/024
*	D	US-7,603,374 B2	10-2009	Cameron et al.	1/1
	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.

Web Images More...

Sign in

correlating object from one compute to another computer malware relationships

Scholar Page 2 of 27 results (0.05 sec)

My Citations

Articles

Case law

My library New!

Any time

Since 2013

Since 2012

Since 2009

Custom range:

2005

Search

Sort by relevance

Sort by date

☐ include patents

☐ include citations

Create alert

[PDF] J. UCS

R. Maurer, Q. Gubud, A. Salomaa, K. Tschernmann · 1995 · academia.edu

... funds research and development projects on innovative ICT technologies dealing with creation of intelligent digital **objects** and knowledge ... and the capability to embed those into content, supports minimal integration allowing to switch from **one** application to **another** ...

Related articles Cite Save More

[PDF] from academia.edu

[book] Enhancing network survivability using intelligent agents.

M. Shajari · 2005 · dspace.hi.unb.ca

... process. Unknown attacks go undetected; **another** shortcoming of the current systems is ... large-scale attack on the Internet affects everyone, but at the same time, no **one** owns the problem. ... of their incoming traffic policy. Ptacek explains some **other** shortcomings of network- ...

Cited by 4 Related articles All 4 versions Cite Save More

[PDF] Advanced Detection and Immunisation of Network Based Security Threats

J. Graves, F. Greig · 2004 · soc.napier.ac.uk

... A **second** aim is to investigate and develop an approach based upon a test bench network. ... any kind of monitoring or checking involved in the process of switching it from **one** end to ... specify the protocols themselves but instead how they relate to and react with the **other** layers of ...

Related articles All 2 versions Cite Save

[PDF] from utas.edu.au

Applying Expert System Technology in a Distributed Monitoring System: An Efficient Response Mechanism for Unknown Threats

RBM Cooke · 2005 · eprints.utas.edu.au

... legitimate. **Another** example of the successfulness of this technique is when an ... Typically no- **one** will challenge an appropriately dressed cleaning staff. With this inside access the ... use many **other** techniques including brute forcing passwords, stack smashing, and ...

Cited by 1 Related articles Cite Save

[PDF] Center for Internet Epidemiology and Defenses

S. Savage, G.M. Voelker, G. Vigna, N. Hansen · cseweb.ucsd.edu

... 2.2.6 Global **Correlation** and Coordination ... We intend to leverage this infrastructure to **correlate** the results of our Honeyfarm infrastructure and to seed the Honeyfarm ... They have come to serve as **one** of the primary sources and clearinghouses for Internet-related data as well as ...

Related articles All 2 versions Cite Save More

[PDF] from dlac.mil

Situational awareness analysis tools for aiding discovery of security events and patterns

V. Kumar, Y. Kim, J. Sivasubya, Z. Zhang, M. Shaveek · 2005 · DTIC Document

... Even when alerts are **correlated**, a false negative can effectively disconnect two graphs that are ... are then fed into a multi-step Level-II analysis system that **correlate** and fuse ... system consists of three major steps and modules -- anchor point identification via **correlating** and fusing ...

Cited by 1 Related articles All 2 versions Cite Save More

[PDF] VALIDUS HOLDINGS, LTD.

A No - Directors Stock Compensation Plan dated as of ... 1 - validusholdings.com

... Item 1. Business Overview ... The Company seeks to underwrite **other** specialty lines with very limited exposure **correlation** with its property, marine and energy portfolios ... to assess the adequacy of risk pricing and to monitor its overall exposure to risk in **correlated** geographic zones ...

Cite Save More

Create alert

Previous 1 2

About Google Scholar All About Google Privacy & Terms Give us feedback

EAST Search History**EAST Search History (Interference)**

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1	receiv\$3 with object with created with remote adj computer\$1 with identity with event adj type.clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2013/12/10 22:55
L2	0	second adj remote adj computer with identity with event adj type with object with performed.clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2013/12/10 22:56
L3	0	correlat\$3 with portion with data with object with remote adj computer with second adj remote adj computer.clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2013/12/10 22:57
L4	0	compar\$3 with base adj computer with correlated adj data with object with identity with relationship\$1 with object\$1.clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2013/12/10 22:58
L5	8	classify\$3 with base adj computer with computer object with malware with comparison.clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2013/12/10 22:58

12/ 10/ 2013 11:04:24 PM**C:\Users\tdoan2\Documents\EAST\Workspaces\13543866.wsp**

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Application Number	13/543,866
				Filing Date	July 8, 2012
				First Named Inventor	Melvyn Morris
				Art Unit	2431
				Examiner Name	Trang T. Doan
Sheet	1	of	1	Attorney Docket Number	6890-93-CON

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
/T.D./	1	2002/0194490	12/19/2002	Halperin et al.	
/T.D./	2	2003/0131256	07/10/2003	Ackroyd	
/T.D./	3	2003/0195861	10/16/2003	McClure 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.
/T.D./	4	Official Action for European Patent Application No. 06755686.0 dated Jul. 31, 2013, 5 pages.
/T.D./	5	EXAMINER ARBUTINA, Extended European Search Report for European Patent Application No. 13167434.3 dated Aug. 1, 2013, 6 pages.
/T.D./	6	EXAMINER ARBUTINA, Extended European Search Report for European Patent Application No. 13167436.8 dated Aug. 30, 2013, 5 pages.
/T.D./	7	EXAMINER ZECHER, Official Action for U.S. Patent Application No. 13/543,865, mailed Aug. 6, 2013, 11 pages (Attorney's Ref. No. 6890-93-DIV)

Examiner Signature	/Trang Doan/	Date Considered	12/10/2013
--------------------	--------------	-----------------	------------

*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. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.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. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

Web Images More...

Sign in

correlating object from one compute to another computer malware relationships

Scholar About 27 results (0.05 sec)

My Citations

Did you mean: correlating object from one **computer** to another computer malware relationships "classify"

Articles

Case law

My library New!

Any time

Since 2013

Since 2012

Since 2009

Custom range

2005

Search

Sort by relevance

Sort by date

include patents

include citations

Create alert

Spatial-temporal modeling of malware propagation in networks
Z Chen, C Li - *Neural Networks, IEEE Transactions on*, 2005 - [IEEE Xplore](#) [IEEE.org](#)
... Digital Object Identifier 10.1109/TNN.2005.853425 ... (15) where, and. If the status of node is independent of that of node 0. Otherwise, if the status of nodes is positively (or negatively) **correlated**, ... Fig. 7. Spatial **correlation** in 2-D-lattice with 10 000 nodes, = 0 1, and = 0 1. ...
Cited by 52 Related articles All 19 versions Cite Save

[CITATION] Reversing: secrets of reverse engineering
S Eiland - 2005 - Wiley.com
Cited by 202 Related articles All 9 versions Cite Save More

System for email processing and analysis
T Yu - US Patent App. 11/678,577, 2005 - Google Patents
... Groups of similar content items (eg, words, phrases, images, ASCII text, etc.) are **correlated** and analysis can ... is looked up in the thesaurus by a matching process and any related **item** with a ... The degree of **correlation** can be used in a calculation of the sameness of the message ...
Cited by 51 Related articles All 2 versions Cite Save

[CITATION] Cissp Certification All In One Exam Study Guide
S Harris - 2004 - Dreamtech Press
Cite Save

Application of Exploratory Multivariate Analysis for Network Security
K Labio, VR Venen - *OTHER INFORMATION SECURITY* ..., 2005 - [books.google.com](#)
... In diana, the initial clustering (at step 0) consists of **one** large cluster containing all n **objects**. ... PCA summarizes the variation in **correlated** multivariate attributes to a set of noncorrelated components, each of which is ... A data frame is an S **object** normally used to store a data matrix ...
Cited by 5 Related articles All 5 versions Cite Save

Unsupervised anomaly detection in network intrusion detection using clusters
R Leung, S Li, 2005 - ... eighth Australian conference on Computer ..., 2005 - [dl.acm.org](#)
... linearly with the number of **objects** in the data set and the number of attributes of the **objects** ...
2.2.3 Grid-based Methods Grid-based methods divide the **object** space into a finite number of cells ... node-link (a pointer to the next node in the FP tree carrying the same frequent **item**) ...
Cited by 151 Related articles All 10 versions Cite Save

[PDF] IA initiatives
M Corne, KM Goertzel, D Dywan, K Heeselefrom, ... - Newsletter, 2004 - [iwar.org.uk](#)
... DAML is **one** such knowledge representa- tion language, based on Web standards, that is capable of expressing an ontology in ... Roles are interpreted as binary **relations** between **objects**. ... Essentially, a triple is a three-element set that consists of a subject, predicate, and **object** ...
Related articles All 26 versions Cite Save More

[PDF] A categorization of computer security monitoring systems and the impact on the design of audit sources
BA Kozminski, RH Stafford - *Purdue University, West Lafayette*, ..., 2004 - [cerias.purdue.edu](#)
... for the generation of bills for system usage, measure system utilization, and **other** similar behaviors. ... This means that a monitoring system needs to be ported to handle **different** operating systems ...
One technique that is used to overcome these limitations is to monitor network traffic ...
Cited by 29 Related articles All 6 versions Cite Save

[PDF] Improving Large-Scale Network Traffic Simulation with Multi-Resolution Models
G Li, 2005 - 129.170.213.101
... Theoretical analysis, based on mathematical constructs, is **one** of the basic techniques used for this ... network traffic as continuous functions of packet rates with time, is **another** technique to ... is natural to describe network traffic in such a way that the whole **computation** expense is ...
Cited by 4 Related articles All 12 versions Cite Save More

[PDF] Ursa Major Starting to Take Shape
P S. ACADEMIA S. - *Citeseer*
... Ursa Major will be a large-scale **object** store, in the NASD and OSD style, based on ... We continue to work on the book, and several **other** schools have picked up this trend ... **One** transaction paves the cache with instructions, while close followers enjoy a nearly miss-free execution ...
All 5 versions Cite Save More

[PDF] On the Self-Protection of Firewalls and Distributed Intrusion Detection systems
H Heebom, VB Ab - 2001 - *Citeseer*
... making sure that every subject in the system receives access to the **objects** that it ... The operating system usually offers the following security mechanisms: memory protection, **object** protection, access control ... **One** may be that no software patch is availa- ble from the vendor and ...
Cited by 2 Related articles All 3 versions Cite Save More

The structure and function of complex networks
MEJ Newman - *SIAM review*, 2003 - SIAM
[\[PDF\] from arxiv.org](#)

... Digital **Object** Identifier. ... and Mathematical Organization Theory. (2013) Computational study of the US stock market evolution: a rank **correlation**-based network ... Neurocomputing 99, 178-187. (2013) Networks of noisy oscillators with **correlated** degree and frequency dispersion. ... Cited by 10286 Related articles All 136 versions Cite Save

[PDF: The Internet Motion Sensor-A Distributed Blackhole Monitoring System.](#) [PDF](#) from uod.gr
M. Eddak, E. Ciolek, F. Jahanian, J. Naeem, D. Watson - NDSS, 2005 - ead.uod.gr

... size of a light telescope, the greater the visibility into fainter, smaller, further and older **objects**. ... very significant amount of normalized local /S traffic, those blocks do not always **correlate** with the ... **One** artifact of more recent worms is that after compro- mising a system, these worms ... Cited by 231 Related articles All 15 versions Cite Save More

[PDF: CERIAS Tech Report 2004-26 A CATEGORIZATION OF COMPUTER SECURITY MONITORING SYSTEMS AND THE IMPACT ON THE DESIGN OF AUDIT](#) [PDF](#) from oberlin.edu
RA. Kuehman - 2004 - cs.oberlin.edu

... "signature" and "misuse" as if the terms were identical). While **one** could arguably ... Most of them are **objects** that are not supposed to be accessed based on the expressed pol- ... attack. • Deflection -- redirect an attack from the **item** being protected. ... Related articles All 7 versions Cite Save More

[book: Impacts and Risk Assessment of Technology for Internet Security: Enabled Information Small-medium Enterprises \(TEISMEs\).](#)

[CA Shrivastava](#) - 2016 - books.google.com

... **Correlation** between annual sales and vulnerability coefficient ... 2 Chapter I eC among consumers and the immediate progression of TEI implementation by **other** SMEs ... The fact that **one** can use the Internet search browsers to explore and view, or for receiving and transmitting ... Cited by 11 Related articles All 9 versions Cite Save More

[PDF: Survey/analysis of Levels I, II, and III attack attribution techniques](#) [PDF](#) from psu.edu

G. Cohen, K. Narayanaswamy - C&S Inc., Apr, 2004 - Citeseer

... via a tunnel to **another** router cooperating with you, but still not be willing to route **other** packets that ... **Another** problem is that the trust **relationship** described above is transitive. ... data and that data will be passed along and accepted until it reaches a link where **one** neighbor does ... Cited by 2 Related articles All 2 versions Cite Save More

[Information Assurance Cyber Ecology](#) [PDF](#) from dtic.mil

J. Jorgensen, P. Rotsignol - 2003 - DTIC Document

... 13 2.4 EVOLUTIONARY **COMPUTATION** While many **other** researchers have examined and developed specific technologies to counter cyber attack ... **One** of the most important challenges confronting us is to be able to derive ... All 2 versions Cite Save More

[Automatic detection of software security vulnerabilities in executable program files](#) [PDF](#) from auburn.edu

JAYE TEVIS - 2005 - stu.auburn.edu

... 1.1 Making Software More Secure The news of **another** virus threatening our **computers** has become a regularly expected ... be birthed through validation errors, **object** reuse, authentication errors, and boundary ... 16 **One other** area of exploitation to consider is core dumps. ... Cited by 3 Related articles All 2 versions Cite Save

[Proceedings of the International GI Workshop on Detection of Intrusions and Malware & Vulnerability Assessment](#) [TXT](#) from tu-dortmund.de

U. Piegat, M. Meier - ... of the International GI Workshop on, 2004 - eldorado.tu-dortmund.de

... It is evident that **correlating** alerts that refer to failed attacks can result in the detection ... However, the **correlation** systems mentioned above assume that real attacks trigger more than a single ... systems can focus on alert clusters and discard all alerts that have not been **correlated**. ... Related articles All 3 versions Cite Save

[De-perimeterisation: Benefits and limitations](#)

G. Palmer - Information Security Technical Report, 2005 - Elsevier

... The **object** of this document is to provide an introduction to De-P and the foremost ... and individual engineers' creativity will hardly have seamless integration for management and the **correlation** of security ... possible to conclude that the process of De-P is a real **one** and something ... Cited by 9 Related articles All 2 versions Cite Save

Create alert

Did you mean to search for: correlating object from one **computer** to another computer malware relationships "classify"

1 2 Next

[About Google Scholar](#) [All About Google](#) [Privacy & Terms](#) [Give us feedback](#)

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	49	identif\$4 with common with object\$1 with (inherit\$3 descendant\$3 relat\$3) and (malware good bad malicious virus\$2 un\$safe safe trojan worm spyware adware) with (behavior\$1 relat\$3 pattern\$1 relationship\$1)	US-PGPUB; USPAT; USOCR; EPO; DERWENT	OR	ON	2013/12/10 23:19
S2	6	726/22-26.ccls. and correlat\$3 with (data file\$1 information object\$1) with relationship\$1 and classify\$3 with (malware good bad malicious virus\$2 safe trojan worm spyware adware)	US-PGPUB; USPAT; USOCR; EPO; DERWENT	OR	ON	2013/12/10 12:51
S3	4	(morris stubbs hartwig harter).in. and correlat\$3 with (data file\$1 information object\$1) with relationship\$1 and classify\$3 with (malware good bad malicious virus\$2 safe trojan worm spyware adware)	US-PGPUB; USPAT; USOCR; EPO; DERWENT	OR	ON	2013/12/10 12:53
S4	27	("20010052014" "20020099952" "20030023857" "20030084323" "20030101381" "20030135791" "20030177394" "20040006704" "20040039921" "20040068618" "20040083408" "20040083810" "20040153644" "20040255165" "20050021994" "20050022014" "20050027686" "20050086500" "20050210035" "20080209562" "20080320595" "20090271867" "6338141" "6772346" "6944772" "7013483" "7093239").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/12/10 12:57
S5	5	("7793338" "20060085857" "20030101381" "20030195861" "20040006704").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/12/10 12:58
S6	6	726/22-26.ccls. and correlat\$3 with (data file\$1 information object\$1) with relationship\$1 and classify\$3 with (malware good bad malicious virus\$2 safe trojan worm spyware adware)	US-PGPUB; USPAT; USOCR; EPO; DERWENT	OR	OFF	2013/12/10 14:15
S7	32	correlat\$3 with (data file\$1 information object\$1 signature\$1 key\$1) with relationship\$1 and classify\$3 with (malware good bad malicious virus\$2 un\$safe safe trojan worm spyware adware)	US-PGPUB; USPAT; USOCR; EPO; DERWENT	OR	ON	2013/12/10 14:58
S8	9	correlat\$3 with (data file\$1 information object\$1 signature\$1 key\$1 relationship\$1) and classify\$3 and relationship\$1 with	US-PGPUB; USPAT;	OR	ON	2013/12/10 15:03

		scor\$3 with (malware good bad malicious virus\$2 un\$safe safe trojan worm spyware adware)	USOCR; EPO; DERWENT			
S9	16	classify\$3 with correlat\$3 with (data file\$1 information object\$1 signature\$1 key\$1 relationship\$1) and scor\$3 with (malware good bad malicious virus\$2 un\$safe safe trojan worm spyware adware)	US- PGPUB; USPAT; USOCR; EPO; DERWENT	OR	ON	2013/12/10 15:05
S10	26	(compar\$3 identif\$4) with relationship\$1 with (object\$1 key\$1 signature child parent) and classif\$5 with (malware good bad malicious virus\$2 un\$safe safe trojan worm spyware adware) with compar\$4	US- PGPUB; USPAT; USOCR; EPO; DERWENT	OR	ON	2013/12/10 15:25
S11	51	relationship\$1 with (object\$1 key\$1 signature child parent) and classif\$5 with (malware good bad malicious virus\$2 un\$safe safe trojan worm spyware adware) with compar\$4	US- PGPUB; USPAT; USOCR; EPO; DERWENT	OR	ON	2013/12/10 15:26
S12	13	relationship\$1 with (object\$1 key\$1 signature child parent) and homogenous near1 entity	US- PGPUB; USPAT; USOCR; EPO; DERWENT	OR	ON	2013/12/10 15:29
S13	0	(identif\$5 establish\$3 indicat\$3 associat\$3 link\$3) with homogenous near1 entity with (malware good bad malicious virus\$2 un\$safe safe trojan worm spyware adware)	US- PGPUB; USPAT; USOCR; EPO; DERWENT	OR	ON	2013/12/10 15:31
S14	4	deduc\$3 with (object\$1 key\$1 signature\$1) with (malware good bad malicious virus\$2 un\$safe safe trojan worm spyware adware) with (behavior\$1 relat\$3 relationship\$1)	US- PGPUB; USPAT; USOCR; EPO; DERWENT	OR	ON	2013/12/10 15:33
S15	2727	(object\$1 key\$1 signature\$1) with (child\$1 parent\$1) and (malware good bad malicious virus\$2 un\$safe safe trojan worm spyware adware) with (behavior\$1 relat\$3 relationship\$1)	US- PGPUB; USPAT; USOCR; EPO; DERWENT	OR	ON	2013/12/10 16:13
S16	146	(object\$1 key\$1 signature\$1) with (child\$1 parent\$1) and (malware good bad malicious virus\$2 un\$safe safe trojan worm spyware adware) with (behavior\$1 relat\$3 relationship\$1) and (compar\$4) with (size folder location name creation date) with (object key signature)	US- PGPUB; USPAT; USOCR; EPO; DERWENT	OR	ON	2013/12/10 16:16
S17	9	(object\$1 key\$1 signature\$1) with (child\$1 parent\$1) and (classif\$5 identif\$5 correlat\$3) with (malware good bad malicious virus\$2 un\$safe safe trojan worm spyware adware) with (behavior\$1 relat\$3 relationship\$1) and (compar\$4) with (size folder location name creation date header) with (object key signature)	US- PGPUB; USPAT; USOCR; EPO; DERWENT	OR	ON	2013/12/10 16:17

EAST Search History

S18	11	("20030159070" "20030172293" "20050091192" "20050155031" "20050182964" "20060026684" "20070028304" "20070067843" "20070234062" "7356843" "7389539").PN.	US- PGPUB; USPAT; USOCR	OR	OFF	2013/12/10 16:20
S19	0	"2006008587"	US- PGPUB; USPAT; USOCR	OR	OFF	2013/12/10 16:23
S20	2	"20060085857"	US- PGPUB; USPAT; USOCR	OR	OFF	2013/12/10 16:23
S21	684	correlat\$3 with (portion part segment chunk block) with (information object key signature data) with computer.clm.	US- PGPUB; USPAT; USOCR; EPO; DERWENT	OR	ON	2013/12/10 23:01
S22	36	correlat\$3 with (portion part segment chunk block) with (information object key signature data) with (second two more several many) near1 computer.clm.	US- PGPUB; USPAT; USOCR; EPO; DERWENT	OR	ON	2013/12/10 23:02

12/ 10/ 2013 11:20:08 PM

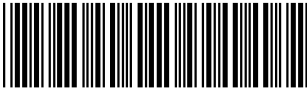
C:\Users\tdoan2\Documents\EAST\Workspaces\13543866.wsp

Issue Classification 	Application/Control No. 13543866	Applicant(s)/Patent Under Reexamination MORRIS ET AL.	
	Examiner TRANG DOAN	Art Unit 2431	

CPC						
Symbol					Type	Version

CPC Combination Sets					
Symbol				Type	Set

/TRANG DOAN/ Examiner.Art Unit 2431 (Assistant Examiner)	12/10/2013 (Date)	Total Claims Allowed: 30	
/CORDELIA ZECHER/ Supervisory Patent Examiner.Art Unit 2431 (Primary Examiner)	12/11/2013 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 4

<i>Index of Claims</i> 	Application/Control No. 13543866	Applicant(s)/Patent Under Reexamination MORRIS ET AL.
	Examiner TRANG DOAN	Art Unit 2431

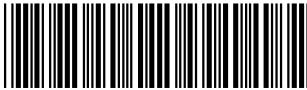
✓	Rejected
=	Allowed

-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47									
CLAIM		DATE							
Final	Original	03/14/2013	07/01/2013	12/10/2013					
	1	✓	✓	=					
	2	✓	✓	=					
	3	✓	✓	=					
	4	✓	✓	=					
	5	✓	✓	=					
	6	✓	✓	=					
	7	✓	✓	=					
	8	✓	✓	=					
	9	✓	✓	=					
	10	✓	✓	=					
	11	✓	✓	=					
	12	✓	✓	=					
	13	✓	✓	=					
	14	✓	✓	=					
	15	✓	✓	=					
	16	✓	✓	=					
	17	✓	✓	=					
	18	✓	✓	=					
	19	✓	✓	=					
	20	✓	✓	=					
	21	✓	✓	=					
	22	✓	✓	=					
	23	✓	✓	=					
	24	✓	✓	=					
	25	✓	✓	=					
	26	✓	✓	=					
	27	✓	✓	=					
	28	✓	✓	=					
	29	✓	✓	=					
	30			=					

Search Notes 	Application/Control No. 13543866	Applicant(s)/Patent Under Reexamination MORRIS ET AL.
	Examiner CORDELIA ZECHER	Art Unit 2432

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	24 (text)	3/14/13	cz

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor Search	3/14/13	cz
Searched EAST (see attached)	3/14/13	cz
Updated East: (726/22-26) with limited text search; and text search only.	12/10/2013	T.D.
Scholar Google Search: see attached search history.	12/10/2013	T.D.

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
	Claims Search Only.	12/10/2013	T.D.

--	--

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Application Number	13/543,866
				Filing Date	July 8, 2012
				First Named Inventor	Melvyn Morris
				Art Unit	2431
				Examiner Name	Trang T. Doan
Sheet	1	of	1	Attorney Docket Number	6890-93-CON

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

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.
	1	Official Action with English Translation for China Patent Application No. 20110036124.1, dated Oct. 23, 2013, 8 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. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.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. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

Electronic Patent Application Fee Transmittal				
Application Number:		13543866		
Filing Date:		08-Jul-2012		
Title of Invention:		METHODS AND APPARATUS FOR DEALING WITH MALWARE		
First Named Inventor/Applicant Name:		Melvyn Morris		
Filer:		Brent Robert Lindon/Robert Roe-Pachirat		
Attorney Docket Number:		6890-93-CON		
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:	17936294
Application Number:	13543866
International Application Number:	
Confirmation Number:	7855
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Customer Number:	22442
Filer:	Brent Robert Lindon/Robert Roe-Pachirat
Filer Authorized By:	Brent Robert Lindon
Attorney Docket Number:	6890-93-CON
Receipt Date:	16-JAN-2014
Filing Date:	08-JUL-2012
Time Stamp:	16:54:46
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	3701
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 1.17 (Patent application and reexamination processing fees)	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		6890-93-CON_IDS_04.pdf	147472 d18468d6fc0a147de53bd54fdc37b98362a ae75f	yes	4
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal Letter		1	3	
	Information Disclosure Statement (IDS) Form (SB08)		4	4	
Warnings:					
Information:					
2	Non Patent Literature	CN201110036124_OA_10-23-2013.pdf	304552 ac52ea364105070a6492a318c5be6e53e80 fc738	no	8
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30536 5f87c7bcaee7b4f3eabc1a7af25499a04ced 7609	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			482560		
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. <u>New Applications Under 35 U.S.C. 111</u> 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. <u>National Stage of an International Application under 35 U.S.C. 371</u> 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. <u>New International Application Filed with the USPTO as a Receiving Office</u> 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.: 7855
Serial No.: 13/543,866	)	Examiner: Trang T. Doan
Filed: July 8, 2012	)	
Atty. File No.: 6890-93-CON	)	<u>SUPPLEMENTAL</u>
Entitled: "Methods and Apparatus for Dealing	)	<u>INFORMATION DISCLOSURE</u>
With Malware"	)	<u>STATEMENT</u>
	)	<i>Electronically Submitted</i>

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

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.

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/

Brent R. Lindon

Registration No. 67424

1560 Broadway, Suite 1200

Denver, Colorado 80202-5141

(303) 863-9700

Date: January 16, 2014



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.
13/543,866	07/08/2012	Melvyn Morris	6890-93-CON	7855
22442	7590	03/17/2014	EXAMINER	
Sheridan Ross PC 1560 Broadway Suite 1200 Denver, CO 80202			DOAN, TRANG T	
			ART UNIT	PAPER NUMBER
			2431	
			NOTIFICATION DATE	DELIVERY MODE
			03/17/2014	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

Notice of Allowability	Application No. 13/543,866	Applicant(s) MORRIS ET AL.	
	Examiner TRANG DOAN	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 the IDS filed on 1/16/2014.
☐ 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 1-30. 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. 11/477,807.
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)	5. ☐ Examiner's Amendment/Comment
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date <u>1/16/2014</u>	6. ☐ Examiner's Statement of Reasons for Allowance
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material	7. ☐ Other _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____.	

	/CORDELIA ZECHER/ Supervisory Patent Examiner, Art Unit 2431
--	---

DETAILED ACTION

1. The present application is being examined under the pre-AIA first to invent provisions.
2. Claims 1-30 are allowed.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 1/16/2014 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRANG DOAN whose telephone number is (571)272-0740. The examiner can normally be reached on Monday-Friday.

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.

/TRANG DOAN/
Examiner, Art Unit 2431

/CORDELIA ZECHER/
Supervisory Patent Examiner, Art Unit 2431

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Application Number	13/543,866
				Filing Date	July 8, 2012
				First Named Inventor	Melvyn Morris
				Art Unit	2431
				Examiner Name	Trang T. Doan
Sheet	1	of	1	Attorney Docket Number	6890-93-CON

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

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.
/T.D./	1	Official Action with English Translation for China Patent Application No. 20110036124.1, dated Oct. 23, 2013, 8 pages

Examiner Signature	/Trang Doan/	Date Considered	03/03/2014
--------------------	--------------	-----------------	------------

*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. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.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. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

Application Serial No. 13/543,866
37 CFR § 1.312 Amendment

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of: Melvyn Morris	)	Group Art Unit: 2432
	)	
Application No.: 13/543,866	)	Examiner: Doan, Trang T
	)	
Filed: July 08, 2012	)	Confirmation No.: 7855
	)	
Atty. File No.: 6890-93-CON	)	
	)	
	)	
For: Methods and Apparatus for Dealing with	)	
Malware	)	
	)	
	)	

AMENDMENT AFTER ALLOWANCE PURSUANT TO 37 CFR § 1.312

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

Commissioner:

Applicant(s) submit this Amendment After Allowance pursuant to 37 CFR § 1.312 in response to the Notice of Allowance and Fee(s) Due having a mailing date of December 26, 2013. An amendment may be entered after the mailing of a Notice of Allowance but prior to payment of the issue fee upon the recommendation of the primary examiner. Therefore, it is respectfully requested that the above-referenced application be amended as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 9 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 a first remote computer on which the computer object or similar computer objects are stored, wherein said data includes information about events initiated or involving the computer object when the computer object is created, configured or runs on the first remote computer, said information including at least ~~the~~ an identity of an object initiating the event, the event type, and an identity of ~~the-an~~ an object or other entity on which the event is being performed;

at the base computer, receiving data about the computer object from a second remote computer on which the computer object or similar computer objects are stored, wherein said data includes information about events initiated or involving the computer object when the computer object is created, configured, or runs on the second remote computer, said information including at least ~~the-an~~ an identity of ~~the-an~~ an object initiating the event, the event type, and ~~the-an~~ an identity of ~~the-an~~ an object or other entity on which the event is being performed;

storing, at the base computer, said data received from the first and second remote computers;

correlating, by the base computer, at least a portion of the data about the computer object received from the first remote computer to at least a portion of the data about the computer object received from the second remote computer;

comparing, by the base computer, the correlated data about the computer object received from the first and second remote computers to other objects or entities to identify relationships between the correlated data and the other objects or entities; and

classifying, by the base computer, the computer object as malware on the basis of said comparison.

2. (Original) A method according to claim 1, wherein the relationship is between objects related directly, or between objects related via other objects.

3. (Previously Presented) A method according to claim 1, wherein where an object and other objects are found to have a relationship, monitoring those related objects as a homogenous entity and identifying a common object of the homogenous entity as a malware object.

4. (Original) A method according to claim 1, comprising deducing an object to be malware based on the behaviour of a related object.

5. (Currently Amended) A method according to claim 1, wherein if at least one other object to which said computer object is related is classed as malware, then classifying said computer object as malware.

6. (Previously Presented) A method according to claim 1, wherein said other objects include the object or similar objects stored on at least one of the first and second remote computers.

7. (Currently Amended) A method according to claim 1, wherein said other objects include other objects that are parent objects or child objects or otherwise process-related objects to said computer object.

8. (Currently Amended) A method according to claim 1, wherein the data about the computer object that is sent from the respective remote computer to the base computer and that is used in the comparison includes one or more of:

executable instructions contained within or constituted by the computer object;
the size of the computer object;
the current name of the computer object;
the physical and folder location of the computer object on disk;
the original name of the computer object;

the creation and modification dates of the computer object;
vendor, product and version and any other information stored within the computer object;
and[[,]]
the computer object header or header held by the respective remote computer.

9. (Previously Presented) A method according to claim 1, wherein the data is sent in the form of a key that is obtained by a hashing process carried out in respect of the objects on the respective remote computer.

10. (Currently Amended) A method according to claim 9, wherein the key has at least one component that represents executable instructions contained within or constituted by the computer object.

11. (Currently Amended) A method according to claim 9, wherein the key has at least one component that represents data about said computer object.

12. (Currently Amended) A method according to claim 11, wherein said data about said computer object includes at least one of:
the current name of the computer object;
the physical and folder location of the computer object on disk;
the original name of the computer object;
the creation and modification dates of the computer object;
vendor, product and version and any other information stored within the computer object;
the computer object header or header held by the respective remote computer; and,
events initiated by or involving the computer object when the computer object is created, configured or runs on the respective remote computers.

13. (Currently Amended) A method according to claim 9, wherein the key has at least one component that represents the physical size of the computer object.

14. (Currently Amended) A method according to claim 1, comprising initially classifying ~~an~~ a computer object as not malware, generating a mask for said computer object that defines acceptable behaviour for the computer object, monitoring an operation of the computer object on at least one of the first and second remote computers and reclassifying the computer object as malware if the actual monitored behaviour extends beyond that permitted by the mask.

15. (Currently Amended) ~~An Apparatus~~ apparatus for classifying a computer object as malware, the apparatus comprising:

a base computer constructed and arranged to receive data about a computer object from a first remote computer on which the computer object or similar computer objects are stored, wherein said data includes information about events initiated or involving the computer object when the computer object is created, configured, or runs on the first remote computer, said information including at least ~~the~~ an identity of ~~the~~ an object initiating the event, the event type, and ~~the~~ an identity of ~~the~~ an object or other entity on which the event is being performed;

the base computer being constructed and arranged to receive data about the computer object from a second remote computer on which the computer object or similar computer objects are stored, wherein said data includes information about events initiated or involving the computer object when the computer object is created, configured, or runs on the second remote computer, said information including at least ~~the~~ an identity of ~~the~~ an object initiating the event, the event type, and ~~the~~ an identity of ~~the~~ an object or other entity on which the event is being performed;

the base computer being constructed and arranged to correlate at least a portion of the data about the computer object received from the first remote computer to at least a portion of the data about the computer object received from the second remote computer;

the base computer being constructed and arranged to compare the data about the computer object received from the first and second remote computers to other objects or entities to identify relationships between the correlated data and the other objects or entities; and

the base computer being constructed and arranged to classify the computer object as malware on the basis of said comparison.

16. (Currently Amended) ~~The Apparatus~~apparatus according to claim 15, wherein the base computer is constructed and arranged so as to identify the relationship between objects related directly, or between objects related via other objects.

17. (Currently Amended) ~~The Apparatus~~apparatus according to claim 15, wherein the base computer is constructed and arranged so as, where an object and other objects are found to have a relationship, to ~~monitoring~~monitor those related objects as a homogenous entity and identify a common object of the homogenous entity as a malware object.

18. (Currently Amended) ~~The apparatus~~Apparatus according to claim 15, wherein the base computer is constructed and arranged so as to deduce an object to be malware based on the behaviour of a related object.

19. (Currently Amended) ~~The apparatus~~Apparatus according to claim 15, wherein the base computer is constructed and arranged so that if at least one other object to which said object is related is classed as malware, then said object is classified as malware.

20. (Currently Amended) ~~The apparatus~~Apparatus according to claim 15, wherein the base computer is constructed and arranged so that said other objects include the object or similar objects stored on at least one of the first and second remote computers.

21. (Currently Amended) ~~Apparatus~~The apparatus according to claim 15, wherein the base computer is constructed and arranged so that said other objects include other objects that are parent objects or child objects or otherwise process-related objects to said object.

22. (Currently Amended) ~~The apparatus~~Apparatus according to claim 15, wherein the base computer is constructed and arranged so as to compare the data where the data includes one or more of:

executable instructions contained within or constituted by the computer object;
the size of the computer object;
the current name of the computer object;

the physical and folder location of the computer object on disk;
the original name of the computer object;
the creation and modification dates of the computer object;
vendor, product, and version and any other information stored within the computer object; and
the computer object header or header held by the respective remote computer.

23. (Currently Amended) ~~The apparatus~~ Apparatus according to claim 15, wherein the base computer is constructed and arranged so as to be able to process data that is sent in the form of a key that is obtained by a hashing process carried out in respect of the objects on said respective remote computer.

24. (Currently Amended) ~~The apparatus~~ Apparatus according to claim 23, wherein the key has at least one component that represents executable instructions contained within or constituted by the computer object.

25. (Currently Amended) ~~The apparatus~~ Apparatus according to claim 23, wherein the key has at least one component that represents data about said computer object.

26. (Currently Amended) Apparatus according to claim 25, wherein said data about said object includes at least one of:

the current name of the computer object;
the physical and folder location of the computer object on disk;
the original name of the computer object;
the creation and modification dates of the computer object;
vendor, product, and version and any other information stored within the computer object;
the computer object header or header held by the respective remote computer; and
events initiated by or involving the computer object when the computer object is created, configured, or runs on the respective remote computers.

27. (Currently Amended) ~~The apparatus~~Apparatus according to claim 23, wherein the key has at least one component that represents the physical size of the computer object.

28. (Currently Amended) ~~The apparatus~~Apparatus according to claim 15, wherein the base computer is constructed and arranged to generate a mask for ~~an a computer~~ object that is initially classed not as malware, said mask defining acceptable behaviour for the computer object, and the base computer is constructed and arranged to monitor an operation of the computer object on at least one of the first and second remote computers and to reclassify the computer object as malware if the actual monitored behaviour extends beyond that permitted by the mask.

29. (Original) A computer program recorded on non-transitory computer readable medium comprising program instructions for causing a computer to perform the method of claim 1.

30. (Previously Presented) A method according to claim 1, wherein the data received about the computer object from the first remote computer is different than the data received about the computer object from the second remote computer.

REMARKS

A Notice of Allowance and Fee(s) Due was mailed on December 26, 2013. The amendments to the claims set forth above make changes to Claims 1, 5, 7, 8, and 10-28 to address typographical errors in the claims and to ensure the consistent use of terms. No claims have been canceled. Accordingly, Claims 1-30 remain present and ready for issue.

These amendments are required to correct typographical errors and to ensure the consistent use of terms, and therefore ensure proper protection of the invention. No substantial amount of additional work on the part of the Office is required. In particular, the scope of the claims is not affected by the proposed amendments. Therefore, the claims remain patentable. This amendment was not presented earlier because it was discovered only after Applicant reviewed the allowed claims.

Pursuant to 37 C.F.R. §1.312, an amendment may be entered after the mailing of a Notice of Allowance, but prior to the payment of the Issue Fee, upon the recommendation of the primary Examiner. Therefore, it is respectfully requested that the above-referenced application be amended as set forth herein.

The Examiner is invited to contact the undersigned by telephone if doing so would expedite the resolution of this case.

Respectfully submitted,

SHERIDAN ROSS P.C.

Date: March 17, 2014

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:	18496513
Application Number:	13543866
International Application Number:	
Confirmation Number:	7855
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:	6890-93-CON
Receipt Date:	17-MAR-2014
Filing Date:	08-JUL-2012
Time Stamp:	16:29:16
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		Rule_312_Amendment.pdf	124470 b72f95d5d88bbe1cf214a03eeaa1a46b1da b0559	yes	9

	Multipart Description/PDF files in .zip description		
	Document Description	Start	End
	Response After Final Action	1	1
	Claims	2	8
	Applicant Arguments/Remarks Made in an Amendment	9	9
Warnings:			
Information:			
Total Files Size (in bytes):		124470	
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. <u>New Applications Under 35 U.S.C. 111</u> 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. <u>National Stage of an International Application under 35 U.S.C. 371</u> 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. <u>New International Application Filed with the USPTO as a Receiving Office</u> 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)

22442 7590 12/26/2013
 Sheridan Ross PC
 1560 Broadway
 Suite 1200
 Denver, CO 80202

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.

Kathy Johnston	(Depositor's name)
/Kathy Johnston/	(Signature)
March 25, 2014	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/543,866	07/08/2012	Melvyn Morris	6890-93-CON	7855

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	\$1780	\$300	\$0	\$2080	03/26/2014

EXAMINER	ART UNIT	CLASS-SUBCLASS
DOAN, TRANG T	2431	726-024000

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, 1 Sheridan Ross P.C.
 (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. 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)

PREVX LIMITED

UNITED KINGDOM

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 191970 (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
☒ Applicant asserting small entity status. See 37 CFR 1.27
☐ Applicant changing to regular undiscounted fee status.

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.

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.

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 /Brent R. Lindon/

Date March 25, 2014

Typed or printed name Brent R. Lindon

Registration No. 67,424

Electronic Patent Application Fee Transmittal				
Application Number:		13543866		
Filing Date:		08-Jul-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:		6890-93-CON		
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:				
Utility Appl Issue Fee	2501	1	480	480
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				480

Electronic Acknowledgement Receipt	
EFS ID:	18576215
Application Number:	13543866
International Application Number:	
Confirmation Number:	7855
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:	6890-93-CON
Receipt Date:	25-MAR-2014
Filing Date:	08-JUL-2012
Time Stamp:	14:50:25
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 480
RAM confirmation Number	1069
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	Issue Fee Payment (PTO-85B)	Issue_Fee_.pdf	81668 2600153acf83b65b12b91e9819fccde1be305a0b	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30480 72a10d2201e330c2eb75db081854aa6e245c687	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			112148		
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. <u>New Applications Under 35 U.S.C. 111</u> 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. <u>National Stage of an International Application under 35 U.S.C. 371</u> 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. <u>New International Application Filed with the USPTO as a Receiving Office</u> 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.
13/543,866	07/08/2012	Melvyn Morris	6890-93-CON	7855
22442	7590	03/26/2014	EXAMINER	
Sheridan Ross PC 1560 Broadway Suite 1200 Denver, CO 80202			DOAN, TRANG T	
			ART UNIT	PAPER NUMBER
			2431	
			NOTIFICATION DATE	DELIVERY MODE
			03/26/2014	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

Response to Rule 312 Communication	Application No.	Applicant(s)
	13/543,866	MORRIS ET AL.
	Examiner	Art Unit
	TRANG DOAN	2431

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

1. ☒ The amendment filed on 17 March 2014 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.

/CORDELIA ZECHER/ Supervisory Patent Examiner, Art Unit 2431	/TRANG DOAN/ Examiner, Art Unit 2431
---	---

Receipt date: 01/25/2013

13543866 - GAU: 2432

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	13/543,866
				Filing Date	July 8, 2012
				First Named Inventor	Melvyn Morris
				Art Unit	2431
				Examiner Name	
Sheet	1	of	4	Attorney Docket Number	6890-93-CON

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	6338141	01/08/2002	Wells	
	2	6772346	08/03/2004	Chess	
	3	6944772	09/13/2005	Dozortsev	
	4	7013483	03/14/2006	Cohen et al.	
	5	7093239	08/15/2006	van der Made	
	6	2001/0052014	12/13/2001	Sheymov et al.	
	7	2002/0099952	07/25/2002	Lambert et al.	
	8	2003/0023857	01/30/2003	Hinchliffe	
	9	2003/0084323	05/01/2003	Gales	
	10	2003/0101381	05/29/2003	Mateev	
	11	2003/0135791	07/17/2003	Natvig	
	12	2004/0006704	01/08/2004	Dahlstrom	
	13	2004/0039921	02/26/2004	Chuang	
	14	2004/0068618	04/08/2004	Hooker	
	15	2004/0073810	04/15/2004	Racine	
	16	2004/0083408	04/29/2004	Spiegel	
	17	2004/0153644	08/05/2004	McCorkendale	
	18	2004/0255165	12/16/2004	Szor	
	19	2005/0021994	01/27/2005	Barton	
	20	2005/0027686	02/03/2005	Shipp	
	21	2005/0086500	04/21/2005	Albomoz	
	22	2005/0022014	~~06/27/2005~~	Shipman I-2005	
	23	2005/0210035	09/22/2005	Kester et al.	
	24	2007/0016953	01/18/2007	Morris et al.	
	25	2008/0209562	08/28/2008	Szor	
	26	2008/0320595	12/25/2008	van der Made	
	27	2009/0271867	10/29/2009	Zhang	
	28	2012/0278891	11/01/2012	Morris et al.	

Change(s) applied
to document,
N.D.W./
1/31/2014

Examiner Signature	/Cordelia Zecher/	Date Considered	03/14/2013
--------------------	-------------------	-----------------	------------

*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. Applicant's unique citation designation number (optional). See Kipds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.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. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.Z./



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.
13/543,866	05/13/2014	8726389	6890-93-CON	7855
22442	7590	04/23/2014		
Sheridan Ross PC 1560 Broadway Suite 1200 Denver, CO 80202				

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, Turnditch, UNITED KINGDOM;
Paul Stubbs, Wyboston, UNITED KINGDOM;
Markus Hartwig, Milton Keynes, UNITED KINGDOM;
Darren Harter, Hucclecote, UNITED KINGDOM;

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.

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/AIA/82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	13/543,866
Filing Date	07-08-2012
First Named Inventor	Melvyn Morris
Title	METHODS AND APPARATUS FOR DEALING WITH MALWARE
Art Unit	2431
Examiner Name	DOAN, TRANG T
Attorney Docket Number	04584.0116USC1

SIGNATURE of Applicant or Patent Practitioner

Signature	/Andrew T. Pouzeshi/	Date (Optional)	2017-01-11
Name	Andrew T. Pouzeshi	Registration Number	67672
Title (if Applicant is a juristic entity)	Attorney for Applicant		
Applicant Name (if Applicant is a juristic entity)	Webroot Inc.		

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 1 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.

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.

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: WEBROOT INC.

Application No./Patent No.: 8,726,389

Filed/Issue Date: 05-13-2014

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 it is:

1. ☒ the assignee of the entire right, title, and interest in;
2. ☐ an assignee of less than the entire right, title, and interest in
(The extent (by percentage) of its ownership interest is _____ %); or
3. ☐ the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

the patent application/patent identified above, by virtue of either:

- 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 _____, Frame _____, or for which a copy therefore is attached.

OR

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

1. From: Morris et al.

To: PREVX LIMITED

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

Reel 035450, Frame 0609, or for which a copy thereof is attached.

2. From: PREVX LIMITED

To: WEBROOT SOLUTIONS LTD

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

Reel 032991, Frame 0418, or for which a copy thereof is attached.

3. From: WEBROOT SOLUTIONS LTD

To: WEBROOT INC.

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

Reel 037886, Frame 0085, 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(b)(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/

2017-01-11

Signature

Date

Andrew T. Pouzeshi

Attorney for Applicant

Printed or Typed Name

Title

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.

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 Acknowledgement Receipt	
EFS ID:	28031521
Application Number:	13543866
International Application Number:	
Confirmation Number:	7855
Title of Invention:	METHODS AND APPARATUS FOR DEALING WITH MALWARE
First Named Inventor/Applicant Name:	Melvyn Morris
Customer Number:	22442
Filer:	Andrew T. Pouzeshi/Elizabeth Pallardy
Filer Authorized By:	Andrew T. Pouzeshi
Attorney Docket Number:	6890-93-CON
Receipt Date:	11-JAN-2017
Filing Date:	08-JUL-2012
Time Stamp:	12:00:49
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	Application Data Sheet	04584_0116USC1_SuppADS. PDF	984472 d089369fd8aea0b866896673505fb92a17e8939a	no	5

Warnings:

Information:					
This is not an USPTO supplied ADS fillable form					
2	Power of Attorney	04584_0116USC1_POA.PDF	359248 dc1dedf4a8bc671c25e4b2b7e0376d40798cc056	no	2
Warnings:					
Information:					
3	Assignee showing of ownership per 37 CFR 3.73	04584_0116USC1_373.PDF	429495 43e54fa2d508e4191a8dec6612e3c754644ba430	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			1773215		
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. <u>New Applications Under 35 U.S.C. 111</u> 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. <u>National Stage of an International Application under 35 U.S.C. 371</u> 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. <u>New International Application Filed with the USPTO as a Receiving Office</u> 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.					

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	339000-000014
		Application Number	<u>13/543,866</u>
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				
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	Derbyshire	Country Of Residence	UK	
Citizenship under 37 CFR 1.41(b)		GB		
Mailing Address of Applicant:				
Address 1		Redmire Gap, Intake Lane		
Address 2		Turnditch		
City	Derbyshire	State/Province		
Postal Code	DE56 2LU	Country	UK	
Applicant 2				
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
	Paul		Stubbs	
Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service				
City	Bedfordshire	Country Of Residence	UK	
Citizenship under 37 CFR 1.41(b)		GB		
Mailing Address of Applicant:				
Address 1		7 Rookery Road		
Address 2		Wyboston		
City	Bedfordshire	State/Province		
Postal Code	MK44 3AX	Country	UK	
Applicant 3				
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
	Markus		Hartwig	
Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service				
City	Buckinghamshire	Country Of Residence	UK	

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	339000-000014	
		Application Number	13/543,866	
Title of Invention	METHODS AND APPARATUS FOR DEALING WITH MALWARE			
Citizenship under 37 CFR 1.41(b)		DE		
Mailing Address of Applicant:				
Address 1	Exchange House, 494 Midsummer Boulevard			
Address 2	Milton Keynes			
City	Buckinghamshire	State/Province		
Postal Code	MK9 2EA	Country	UK	
Applicant 4				
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
	Darren		Harter	
Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service				
City	Gloucestershire	Country Of Residence	UK	
Citizenship under 37 CFR 1.41(b)		GB		
Mailing Address of Applicant:				
Address 1	178 Barnwood Road, Hucclecote			
Address 2	Gloucester			
City	Gloucestershire	State/Province		
Postal Code	GL4 3JZ	Country	UK	
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.	
Customer Number	47604 <u>23552</u>
Email Address	Add Email Remove Email

Application Information:

Title of the Invention	METHODS AND APPARATUS FOR DEALING WITH MALWARE		
Attorney Docket Number	339000-000014 <u>04584.0116USC1</u>	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)	3	Suggested Figure for Publication (if any)	1

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	339000-000014
		Application Number	<u>13/543,866</u>
Title of Invention	METHODS AND APPARATUS FOR DEALING WITH MALWARE		

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	~~47604~~ <u>23552</u>		

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	Pending	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	11477807	2006-06-30
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button.			

Foreign Priority Information:

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 [†]	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
0513375.6	GB	2005-06-30	☒ Yes ☐ No
Additional Foreign Priority Data may be generated within this form by selecting the Add button.			

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

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	339000-000014
		Application Number	<u>13/543,866</u>
Title of Invention	METHODS AND APPARATUS FOR DEALING WITH MALWARE		

If the Assignee is an Organization check here. ☒			
Organization Name	~~Prevx Limited~~ <u>Webroot Inc.</u>		
Mailing Address Information:			
Address 1	~~3 New Park Place~~ <u>385 Interlocken Crescent</u>		
Address 2	~~Pride Park~~		
City	~~Derby~~ <u>Broomfield</u>	State/Province	<u>CO</u>
Country	~~UK~~ <u>USA</u>	Postal Code	DE24 8DZ <u>80021</u>
Phone Number		Fax Number	
Email Address			
Additional Assignee Data may be generated within this form by selecting the Add button.			

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	<u>/Andrew T. Pouzeshi/</u>			Date (YYYY-MM-DD)	<u>2017-01-11</u>
First Name	<u>Andrew T.</u>	Last Name	<u>Pouzeshi</u>	Registration Number	<u>67672</u>

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.



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
13/543,866	07/08/2012	Melvyn Morris	04584.0116USC1

CONFIRMATION NO. 7855

POA ACCEPTANCE LETTER



OC000000088574873

23552
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

Date Mailed: 01/23/2017

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 01/11/2017.

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.

/ldvan/



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
13/543,866	07/08/2012	Melvyn Morris	6890-93-CON

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

CONFIRMATION NO. 7855
POWER OF ATTORNEY NOTICE



OC000000088574832

Date Mailed: 01/23/2017

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 01/11/2017.

- 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.

/ldvan/

Large Entity Declaration

PATENT
IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Number: 13/543,866

Current Date: July 25, 2017

Filing Date: July 8, 2012

Patent Number: 8,726,389

Issue Date: May 13, 2014

CHANGE OF ENTITY STATUS PURSUANT TO 37 C.F.R. §1.27 (g)(2)

Commissioner for Patents
Mail Stop M Correspondence
P.O. Box 1450
Alexandria, VA 22313-1450

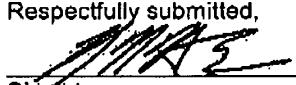
Sir:

This communication hereby notifies the United States Patent and Trademark Office
that small entity status is no longer applicable for the above-identified patent.

**COMPANY or FIRM
NAME AND ADDRESS:**

Webroot Inc.
385 Interlocken Crescent, Suite 800
Broomfield, Colorado 80021

Respectfully submitted,


Signature

Ryan Howe

Printed Name

General Counsel

Title

OR

Reg. # if US Attorney _____

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

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. 6:22-cv-00239	DATE FILED 3/4/2022	U.S. DISTRICT COURT WESTERN DISTRICT OF TEXAS
PLAINTIFF WEBROOT, INC. and OPEN TEXT, INC.		DEFENDANT TREND MICRO INC.
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		
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: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

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. 6:22-cv-00240	DATE FILED 3/4/2022	U.S. DISTRICT COURT WESTERN DISTRICT OF TEXAS
PLAINTIFF WEBROOT, INC. and OPEN TEXT, INC.		DEFENDANT 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: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

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. 6:22-cv-00241	DATE FILED 3/4/2022	U.S. DISTRICT COURT WESTERN DISTRICT OF TEXAS
PLAINTIFF WEBROOT, INC. and OPEN TEXT, INC.		DEFENDANT CROWDSTRIKE, INC. and CROWDSTRIKE HOLDINGS, INC.
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		
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: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

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. 6:22-cv-00342	DATE FILED 3/31/2022	U.S. DISTRICT COURT WESTERN DISTRICT OF TEXAS
PLAINTIFF WEBROOT, INC. and OPEN TEXT, INC.		DEFENDANT 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