AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Western District of Texas, Waco Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:22-cv-00241	3/4/2022	Western District of Texas, Waco Division

PLAINTIFF	DEFENDANT
Webroot, Inc. and OpenText Inc.	CrowdStrike, Inc. and CrowdStrike Holdings, Inc.

	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 patent(s)/ trademark(s) have been included:

DATE INCLUDED 9/7/2022

INCLUDED BY ☑ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	11,409,869	8/9/2022	Webroot, Inc.
2	8,719,932	5/6/2014	Webroot, Inc.
3	8,201,243	6/12/2012	Webroot, Inc.
4	8,181,244	5/15/2012	Webroot, Inc.
5	8,856,505	10/7/2014	Webroot, Inc.
6	8,763,123	6/24/2014	Webroot, Inc.

In the above---entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1---Upon initiation of action, mail this copy to Director Copy 3---Upon termination of action, mail this copy to Director
Copy 2---Upon filing document adding patent(s), mail this copy to Director Copy 4---Case file copy

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Western District of Texas, Waco Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:22-cv-00239	3/4/2022	Western District of Texas, Waco Division

PLAINTIFF	DEFENDANT
Webroot, Inc. and OpenText Inc.	TrendMicro, Inc.

	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 patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY
8/31/2022	☑ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	11,409,869	8/9/2022	Webroot, Inc.
2	8,719,932	5/6/2014	Webroot, Inc.
3	8,201,243	6/12/2012	Webroot, Inc.
4	8,181,244	5/15/2012	Webroot, Inc.
5	8,856,505	10/7/2014	Webroot, Inc.

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

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
11/408,145	04/20/2006	Matthew L. Boney	6890-62

CONFIRMATION NO. 8007

IMPROPER CPOA LETTER

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

OC000000116718667

Date Mailed: 05/12/2020

NOTICE REGARDING POWER OF ATTORNEY

This is in response to the power of attorney filed 04/14/2020. The power of attorney in this application is not accepted for the reason(s) listed below:

- The power of attorney is from an assignee and the statement required by 37 CFR 3.73(c) has not been received.

/trwoodson/

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

109422
Sprinkle IP Law Group/OPEN
1301 W. 25th Street, Suite 408
Austin, TX 78705
UNITED STATES

Trend Micro, Inc.
EX1002-3

Power of Attorney to Transact Business with the United States Patent and Trademark Office

I hereby revoke all previous Powers of Attorney given in the application(s) identified in the attached Transmittal for Power of Attorney to One or More Registered Practitioners ("Transmittal Form").

I hereby appoint practitioners associated with the following Customer Number associated with Sprinkle IP Law Group, PC :

109422

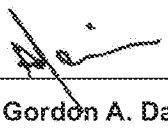
as my/our attorney(s) or agent(s) and to transact all business before the United States Patent and Trademark Office (USPTO) in connection with any and all patents and patent applications that are assigned to **Webroot Inc.** (the "assignee's patents/patent applications") in which they shall appear, any and all assignee's patents/patent applications associated with the above-referenced customer number, and any and all patents and patent applications referenced in the attached Transmittal Form.

Please recognize or change the correspondence address for the patents and patent applications referenced in the attached Transmittal Form to the address associated with the above-referenced customer number.

The undersigned is:

- ☐ Inventor or Joint Inventor
- ☒ Assignee or Person to Whom the Inventor is Under an Obligation to Assign
  *the undersigned has authority to act on behalf of the Assignee or Person to Whom the Inventor is Under an Obligation to Assign.
- ☐ Legal Representative of a Deceased or Legally Incapacitated Inventor
- ☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is currently being filed in this document)

The Transmittal Form may be completed and executed by one of the practitioners associated with the above-referenced customer number.

SIGNATURE OF APPLICANT			
Signature:		**Date:**	January 29, 2020
Name:	**Gordon A. Davies**		
Title:	Director		
Company:	**Webroot Inc.**		
I am authorized to act on behalf of the assignee.			

Electronic Acknowledgement Receipt

EFS ID:	39150548
Application Number:	11408145
International Application Number:	
Confirmation Number:	8007
Title of Invention:	BACKWARD RESEARCHING TIME STAMPED EVENTS TO FIND AN ORIGIN OF PESTWARE
First Named Inventor/Applicant Name:	Matthew L. Boney
Customer Number:	22442
Filer:	John L. Adair/keunah cheun
Filer Authorized By:	John L. Adair
Attorney Docket Number:	6890-62
Receipt Date:	14-APR-2020
Filing Date:	20-APR-2006
Time Stamp:	11:29:50
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	WEBROOT_POA_012820.pdf	42303 460c019d47e52952aad549f0d335131a49b6cfef	no	1

Warnings:

Information:	
Total Files Size (in bytes):	42303

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

Large Entity Declaration

Schedule A – Patents assigned to *Assignee*

APPLICATION NUMBER	FILING DATE	PATENT NUMBER	ISSUE DATE
~~11104201~~	~~04/12/2005~~	~~7346611~~	~~03/18/2008~~
11105978	04/14/2005	7349931	03/25/2008
12830021	07/02/2010	8140839	03/20/2012
11462943	08/07/2006	8171550	05/01/2012
11408145	04/20/2006	8181244	05/15/2012

PAGE 3/3 * RCVD AT 9/7/2016 5:34:15 AM [Eastern Daylight Time] * SVR:W-PTOFAX-003/9 * DNIS:2736500 * CSID: * DURATION (mm-ss):00-47

CPA GLOBAL®

Liberation House,
Castle Street, St Helier,
Jersey JE1 1BI,
Channel Islands

t: 44 (0) 1534 888 711
e: enquiries@cpaglobal.com
f: 44 (0) 1534 868 747
cpaglobal.com

CPA Global Limited
Registered as a Company under the Companies (Jersey) Law 1991,
number 93745. Registered office: Liberation House, Castle Street,
St Helier, Jersey JE1 1BI, Channel Islands.

FAX TO:

3 Pages

Commissioner of Patents and Trademarks
Attn. Maintenance Fee Branch
Office of Finance – Maintenance Fee Division
2051 Jamieson Ave – Suite 300
Alexandria, VA 22314

Fax no.: 001 571 273-6500

7 September 2016

RE: Entity status amends to Large

Dear Sirs,

Please find attached declaration form for **five** cases to be amended to **LARGE** Entity status.

Many thanks for your assistance.

Kind regards,

Soraia Da Silva
IP Supplier Payments

E: supplier@cpaglobal.com
T: 011 44 1534 888711
F: 011 44 1534 811347

Certificate of Facsimile Transmission

I hereby certify that this document is being facsimile transmitted to the USPTO at 001 571-273-6500 on the date shown below.

Date
7-Sep-16

Signed

PAGE 1/3 * RCVD AT 9/7/2016 5:34:15 AM [Eastern Daylight Time] * SVR:W-PTOFAX-003/9 * DNIS:2736500 * CSID: * DURATION (mm-ss):00-47

Small Entity Declaration

PATENT
IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Number: 11/408145 **Current Date:** 03 AUGUST 2015

Filing Date: 20 APRIL 2006

Patent Number: 8181244

Issue Date: 15 MAY 2012

ASSERTION OF SMALL ENTITY STATUS PURSUANT TO 37 C.F.R. §1.27 (c)(1)

Commissioner for Patents
Mail Stop M Correspondence
P.O. Box 1450
Alexandria, VA 22313-1450

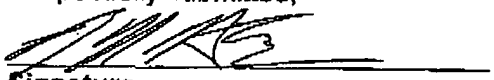
Sir:

This communication hereby asserts that the above-identified patent is entitled to small entity status.

COMPANY or FIRM NAME AND ADDRESS:

Webroot Inc.
385 Interlocken Crescent, Suite 800
Broomfield, CO 80021
USA

Respectfully submitted,



Signature
Ryan Howe
Printed Name
General Counsel
Title

OR
Reg. # if US Attorney_____

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
11/408,145	04/20/2006	Matthew L. Boney	WEBR-045/00US 303666-2050

CONFIRMATION NO. 8007

POA ACCEPTANCE LETTER

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

OC000000056953625

Date Mailed: 10/18/2012

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 10/02/2012.

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.

/mteklemichael/

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

Trend Micro, Inc.
EX1002-10

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

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

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

I hereby appoint:

■ Practitioners associated with Customer Number: 22442

OR

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

Name	Registration Number	Name	Registration Number

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

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

■ The address associated with Customer Number: 22442

OR

☐	Firm or Individual Name		
	Address		
	City	State	Zip
	Country		
	Telephone	Email	

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

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

SIGNATURE of Assignee of Record

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

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

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

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

Electronic Acknowledgement Receipt

EFS ID:	13890477
Application Number:	11408145
International Application Number:	
Confirmation Number:	8007
Title of Invention:	BACKWARD RESEARCHING TIME STAMPED EVENTS TO FIND AN ORIGIN OF PESTWARE
First Named Inventor/Applicant Name:	Matthew L. Boney
Customer Number:	22903
Filer:	Bradley M. Knepper/Erica Picard
Filer Authorized By:	Bradley M. Knepper
Attorney Docket Number:	WEBR-045/00US 303666-2050
Receipt Date:	02-OCT-2012
Filing Date:	20-APR-2006
Time Stamp:	13:52:17
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	Assignee showing of ownership per 37 CFR 3.73.	STATEMENT.pdf	119871 d5ef620dff51c2fb6a349ba240d50da4fdc2c351	no	3

Warnings:	
Information:	

2	Power of Attorney	POA.pdf	59485 68e3501600681cf461a6a1ad6257bc47dc71e26d	no	1

Warnings:	
Information:	
Total Files Size (in bytes):	179356

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office;U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of1995, no persons arerequired to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: Webroot Inc.

Application No./Patent No.: 8,181,244 Filed/Issue Date: 2012-05-15

Titled: BACKWARD RESEARCHING TIME STAMPED EVENTS TO FIND AN ORIGIN OF PESTWARE

Webroot Inc., a Corporation

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

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

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

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

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

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

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

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

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

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

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

A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, 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: Matthew L. Boney To: Webroot Software, Inc.

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

   Reel 017986, Frame 0435, or for which a copy thereof is attached.

2. From: Webroot Software, Inc. To: Webroot Inc.

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

   Reel 028953, Frame 0917, or for which a copy thereof is attached.

This collection of information is required by37 CFR3.73(b). The information is required toobtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentialityis governed by35 U.S.C. 122and 37 CFR1.11 and1.14. Thiscollection is estimated to take 12 minutes to complete, including gathering, preparing, and submittingthe completed application form to the USPTO.Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent tothe Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.**SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450**

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

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

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

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

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

4. From: _____ To: _____

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

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

5. From: _____ To: _____

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

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

6. From: _____ To: _____

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

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

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

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

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

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

/Bradley M. Knepper/	2012-10-02
Signature	Date
Bradley M. Knepper	44,189
Printed or Typed Name	Title or Registration Number

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the informationin order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an InternationalApplication filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, arecord may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from thissystem of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/83 (11-08)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

REQUEST FOR WITHDRAWAL AS ATTORNEY OR AGENT AND CHANGE OF CORRESPONDENCE ADDRESS

Application Number	SEE SCHEDULE A
Filing Date	SEE SCHEDULE A
First Named Inventor	SEE SCHEDULE A
Art Unit	SEE SCHEDULE A
Examiner Name	SEE SCHEDULE A
Attorney Docket Number	SEE SCHEDULE A

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

Please withdraw me as attorney or agent for the above identified patent application, and

☒ all the practitioners of record;

☐ the practitioners (with registration numbers) of record listed on the attached paper(s); or

☐ the practitioners of record associated with Customer Numbers: 58249 and 22903

NOTE: The immediately preceding box should only be marked when the practitioners were appointed using the listed Customer Number.

The reason(s) for this request are those described in 37 CFR :

☐ 10.40(b)(1) ☐ 10.40(b)(2) ☐ 10.40(b)(3) ☒ 10.40(b)(4)

☐ 10.40(c)(1)(i) ☐ 10.40(c)(1)(ii) ☐ 10.40(c)(1)(iii) ☐ 10.40(c)(1)(iv)

☐ 10.40(c)(1)(v) ☐ 10.40(c)(1)(vi) ☐ 10.40(c)(2) ☐ 10.40(c)(3)

☐ 10.40(c)(4) ☐ 10.40(c)(5) ☐ 10.40(c)(6). Please explain below:

Certifications

Check each box below that is factually correct. WARNING: If a box is left unchecked, the request will likely not be approved.

1. ☒ I/We have given reasonable notice to the client, prior to the expiration of the response period, that the practitioner(s) intend to withdraw from employment.

2. ☒ I/We have delivered to the client or a duly authorized representative of the client all papers and property (including funds) to which the client is entitled.

3. ☒ I/We have notified the client of any responses that may be due and the time frame within which the client must respond.

Please provide an explanation, if necessary:
SEE ATTACHED LETTER FROM WEBROOT, INC. REQUESTING TRANSFER OF FILES.

This collection of information is required by 37 CFR 1.36. 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.

American LegalNet, Inc.
www.FormsWorkflow.com
Trend Micro, Inc.
EX1002-17

PTO/SB/83 (11-08)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

REQUEST FOR WITHDRAWAL AS ATTORNEY OR AGENT AND CHANGE OF CORRESPONDENCE ADDRESS

Complete the following section only when the correspondence address will change. *Changes of address will only be accepted to an inventor or an assignee that has properly made itself of record pursuant to 37 CFR 3.71.*

Change the correspondence address and direct all future correspondence to:

A. ☐ The address of the inventor or assignee associated with Customer Number:

OR

B. ☒ Inventor or Assignee name	Webroot, Inc. c/o Sheridan Ross
Address	1560 Broadway, Suite 1200

City Denver	State CO	Zip 80202	Country US
Telephone 303-863-9700		Email rbrunelli@sheridanross.com	

I am authorized to sign on behalf of myself and all withdrawing practitioners.

Signature		
Name	Mark R. Schafer	Registration No. 65,336
Address	777 6th Street NW, Ste. 1100	

City Washington	State DC	Zip 20001	Country UA
Date 2012-09-20		Telephone No. 720 566-4044	

NOTE: ***Withdrawal is effective when approved rather than when received.***

This collection of information is required by 37 CFR 1.36. 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.

American LegalNet, Inc.
www.FormsWorkflow.com

SCHEDULE A

Application No.	Application Date	Inventor	Group Art Unit	Examiner	Cooley Docket No.	Conf. No.
11/031,615	Jan-07-2005	THOMAS	2163	LE, Uyen	WEBR-001/01US 303666-2010	3544
10/956,573	Oct-01-2004	THOMAS	2162	Alam, Shahid	WEBR-003/00US 303666-2004	7086
10/956,274	Oct-01-2004	BERTMAN	2135	Truong, Thanhnga B.	WEBR-004/00US 303666-2008	6861
10/956,574	Oct-01-2004	THOMAS	2162	BULLOCK, Joshua	WEBR-005/00US 303666-2007	7085
11/104,201	Apr-12-2005	BURTSCHER	2167	KIM, Chong	WEBR-010/00US 303666-2014	1307
11/104,202	Apr-12-2005	BURTSCHER	2436	CERVETTI, David G.	WEBR-011/00US 303666-2011	1284
11/462,827	Aug-07-2006	SCHNEIDER	2438	LANE, Gregory A.	WEBR-023/00US 303666-2024	5954
13/460,655	Apr-30-2012	SCHNEIDER	2431		WEBR-023/01US 303666-2124	9502
11/145,592	Jun-06-2005	NICHOLS	2167	UDDIN, Mohammed	WEBR-024/00US 303666-2027	4495
11/258,536	Oct-25-2005	MOOD	2432	PERUNGAVOOR, Venkatanaray	WEBR-026/00US 303666-2028	2648
11/334,318	Jan-18-2006	HORNE	4144	WATSON, Joshua C.	WEBR-033/00US 303666-2038	6611
11/334,307	Jan-18-2006	HORNE	2431	ZIA, Syed	WEBR-034/00US 303666-2039	6605
11/334,317	Jan-18-2006	HORNE	2431	Avery, Jeremiah L.	WEBR-035/00US 303666-2040	6608
11/460,032	Jul-26-2006	BURTSCHER	2439	OLION, Brian L.	WEBR-037/00US 303666-2042	1341
11/386,595	Mar-22-2006	NICHOLS	2439	LE, Canh	WEBR-038/00US 303666-2046	4954
11/386,590	Mar-22-2006	NICHOLS	2195	WAI, Eric Charles	WEBR-039/00US 303666-2045	4944
11/386,594	Mar-22-2006	NICHOLS	2189	Peikari, Behzad	WEBR-040/00US 303666-2044	4951
11/408,146	Apr-20-2006	BONEY	2438	RAHMAN, Mahfuzur	WEBR-044/00US 303666-2049	8009
13/490,294	Jun-06-2012	BONEY	2431		WEBR-044/01US 303666-2126	1064
11/408,145	Apr-20-2006	BONEY	2438	RAHMAN, Mahfuzur	WEBR-045/00US 303666-2050	8007
13/460,648	Apr-30-2012	BONEY	2431		WEBR-045/01US 303666-2125	8780
11/482,903	Jul-07-2006	SPROWLS	2438	Truong, Thanhnga B.	WEBR-057/00US 303666-2069	6773
13/184,925	Jul-18-2011	SPROWLS	2438	Truong, Thanhnga B.	WEBR-057/01US 303666-2121	1361
13/184,931	Jul-18-2011	SPROWLS	2438	Truong, Thanhnga B.	WEBR-057/02US 303666-2122	1371
11/465,680	Aug-18-2006	WANG	2115	Connolly, Mark A.	WEBR-059/00US 303666-2065	1654
12/829,749	Jul-02-2010	WANG	2115	Connolly, Mark A.	WEBR-059/01US 303666-2119	9140
12/830,021	Jul-02-2010	WANG	2115	Connolly, Mark A.	WEBR-059/02US 303666-2120	9668
13/413,391	Mar-06-2012	WANG	2115		WEBR-059/03US 303666-2123	7167
11/462,943	Aug-07-2006	BURTSCHER	2438	LANE, Gregory A.	WEBR-060/00US 303666-2067	6147
11/462,956	Aug-07-2006	BURTSCHER	2197	DAS, Chameli	WEBR-061/00US 303666-2070	6168
11/462,781	Aug-07-2006	MCCLOY	2442		WEBR-063/00US 303666-2066	5887
12/236,419	Sep-23-2008	ADAMS	2491	SHAW, Brian F	WEBR-072/00US 303666-2108	7849

Trend Micro, Inc.
EX1002-19

Webroot
385 Interlocken Crescent Boulevard
Suite 800
Broomfield, CO 80021
Toll-Free: 800.870.8102
www.webroot.com

July 17, 2012

BY EMAIL

Wayne O. Stacy, Esq.
Cooley LLP
380 Interlocken Crescent
Suite 900
Broomfield, CO 80021

RE: Engagement of Sheridan Ross P.C.

Dear Wayne:

As you and I discussed recently, Webroot Inc. has elected to consolidate its intellectual property prosecution work with Sheridan Ross P.C. Accordingly, I write to request that you arrange for the items listed below to be forwarded Sheridan Ross as soon as possible:

- Lists of all patent, trademark, and copyright matters your firm has handled – and is currently handling – for Webroot;
- A docket report for each patent, trademark, and copyright matter detailing upcoming deadlines through December 31, 2012;
- Physical files for each patent, trademark, and copyright matter;
- Electronic files for each patent, trademark, and copyright matter, if available; and
- A master list of all items forwarded to Sheridan Ross.

All items should be sent to the attention of Robert Brunelli, 1560 Broadway, Suite 1200, Denver, Colorado 80202; rbrunelli@sheridanross.com.

Webroot anticipates that the fees/costs associated with providing the foregoing materials to Sheridan Ross will be minimal, and in no event will exceed $500 per docket. If you expect fees/costs greater than that amount, please contact me immediately.

Please note that you need not notify foreign associates of Webroot's engagement of Sheridan Ross. Sheridan Ross will handle those notifications.

Thank you for your attention to this matter.

Sincerely,

David Huberman
General Counsel
Webroot Inc.

Electronic Acknowledgement Receipt

EFS ID:	13800942
Application Number:	11408145
International Application Number:	
Confirmation Number:	8007
Title of Invention:	BACKWARD RESEARCHING TIME STAMPED EVENTS TO FIND AN ORIGIN OF PESTWARE
First Named Inventor/Applicant Name:	Matthew L. Boney
Customer Number:	22903
Filer:	Mark Randolph Schafer/Sherry Bitler
Filer Authorized By:	Mark Randolph Schafer
Attorney Docket Number:	WEBR-045/00US 303666-2050
Receipt Date:	20-SEP-2012
Filing Date:	20-APR-2006
Time Stamp:	18:35:07
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	Change of Address	WEBR-Req2Withdraw.pdf	282148 8bb7d27bcb066b34eeeca860249160c928194588	no	4

Warnings:	
Information:	

Total Files Size (in bytes):	282148

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/408,145	05/15/2012	8181244	WEBR-045/00US 303666-2050	8007

22903 7590 04/25/2012

COOLEY LLP
ATTN: PATENT GROUP
Suite 1100
777 - 6th Street, NW
WASHINGTON, DC 20001

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 929 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):

Matthew L. Boney, Longmont, CO;

AMENDMENTS TO THE SPECIFICATION:

Change(s) applied to document, /A.E.G./ 2/22/2012

Please replace the paragraph nos. [0003], [0005], [0015], [0016], [0018], [0031], [0034], [0035], [0037], [0041], and [0043] with the following paragraphs. The amendments to paragraph nos. [0003], [0005], [0015], [0016], [0018], [0031], [0034], [0035], [0037], [0041], and [0043] are indicated by strikethough and underlining.

[0003] Also shown is a file storage device 118 that is coupled to the research module 108 and an activity monitor 116. In this embodiment the file storage device includes an activity log ~~120~~121, a pestware file 124 and a collection of *N* files 130. The file storage device 118 is described herein in several implementations as hard disk drive for convenience, but this is certainly not required, and one of ordinary skill in the art will recognize that other storage media may be utilized without departing from the scope of the present invention. In addition, one of ordinary skill in the art will recognize that the storage device 118, which is depicted for convenience as a single storage device, may be realized by multiple (e.g., distributed) storage devices.

[0005] In accordance with several embodiments, the research module 108 is configured to receive an indication that either known pestware is residing on the computer or activities indicative of pestware have occurred or are occurring on the protected computer. In response, the research module 108 is configured to research the activity log ~~120~~121 and/or the *N* files 130, which include information (e.g., historical logs) relating to events on the computer 100, to identify a source of the pestware 122, 124 or pestware-related activities, which may be reported by the reporting module 114 to a centralized data store for subsequent pestware management purposes.

Please type a plus sign (+) inside this box → [+]

PTO/SB/08A (08-00)

Substitute for form 1449A/PTO		*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT		Application Number	11/408,145
		Filing Date	04/20/2006
		First Named Inventor	Matthew L. Boney
		Group Art Unit	2154
(use as many sheets as necessary)		Examiner Name	Not Yet Assigned
Sheet	2 of 3	Attorney Docket Number	WEBR-045/00US

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	U.S. Patent Document Number	Kind Code[2] (*if known*)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY
		US 2004/0187023	A1	ALAGNA, MICHAEL ANTHONY, ET AL.	09/23/04
		US 2004/0225877	A1	HUANG	11/11/04
		US 2005/0038697	A1	~~JEFFREY~~ Aaron	02/2005
		US 2005/0154885		VISCOMI ET AL.	07/2005
		US 2005/0138433	A1	LINETSKY, GENE	06/23/05
		2006/0075494		BERTMAN ET AL.	04/2006
		2006/0075501		THOMAS ET AL.	04/2006
		2006/0161988		COSTEA ET AL.	07/2006
		10/956,573		STEVE THOMAS	N/A Filed: 10/01/04
		10/956,574		STEVE THOMAS	N/A Filed: 10/01/04
		10/956,818		MATTHEW BONEY	N/A Filed: 10/01/04
		11/257,609		MICHAEL BURTSCHER	N/A Filed: 10/25/05
		11/237,291		PHILIP MADDALONI	N/A Filed: 09/28/05
		11/408,215		MATTHEW BONEY	N/A Filed: 04/20/06
		11/408,146		MATTHEW BONEY	N/A Filed: 04/20/06

Change(s) applied to document
/A.J.P./
3/5/2012

Examiner Signature	/Mahfuzur Rahman/	Date Considered	12/21/2011

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

[1] Unique citation designation number.
[2] See attached Kinds of U.S. Patent Documents.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH./M.R./

Hitachi Micro, Inc.
EX1002-25

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)

22903 7590 01/23/2012

COOLEY LLP
ATTY: Patent Group
Suite 1100
777 - 6th Street, NW
WASHINGTON, DC 20001

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/408,145	04/20/2006	BONEY, Matthew L.	WEBR-045/00US 303666-2050	8007

TITLE OF INVENTION:
BACKWARD RESEARCHING TIME STAMPED EVENTS TO FIND AN ORIGIN OF PESTWARE

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1740	$300	$0	$2040	04/23/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
RAHMAN, Mahfuzur	2438	726-022000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 COOLEY LLP
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: Webroot Inc.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Broomfield CO

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 credit any overpayment, to Deposit Account Number 50-1283 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from any one other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature /Mark R. Schafer/ Date 2012-04-17

Typed or printed name Mark R. Schafer Registration No. 65,336

This collection of information 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.

Electronic Patent Application Fee Transmittal

Application Number:	11408145
Filing Date:	20-Apr-2006
Title of Invention:	BACKWARD RESEARCHING TIME STAMPED EVENTS TO FIND AN ORIGIN OF PESTWARE
First Named Inventor/Applicant Name:	Matthew L. Boney
Filer:	Mark Randolph Schafer/Sherry Bitler
Attorney Docket Number:	WEBR-045/00US 303666-2050

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:				
Utility Appl issue fee	1501	1	1740	1740
Publ. Fee- early, voluntary, or normal	1504	1	300	300

Trend Micro, Inc.
EX1002-27

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**2040**

Electronic Acknowledgement Receipt

EFS ID:	12559780
Application Number:	11408145
International Application Number:	
Confirmation Number:	8007
Title of Invention:	BACKWARD RESEARCHING TIME STAMPED EVENTS TO FIND AN ORIGIN OF PESTWARE
First Named Inventor/Applicant Name:	Matthew L. Boney
Customer Number:	22903
Filer:	Mark Randolph Schafer/Sherry Bitler
Filer Authorized By:	Mark Randolph Schafer
Attorney Docket Number:	WEBR-045/00US 303666-2050
Receipt Date:	17-APR-2012
Filing Date:	20-APR-2006
Time Stamp:	16:05:06
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$2040
RAM confirmation Number	2802
Deposit Account	501283
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	Issue Fee Payment (PTO-85B)	WEBR04500US_Part_B_Issue_Fee_Transmittal.pdf	109580 ca716bb78451ad13ae11a250a66bb5bb511f778d	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	32318 9b9e0e37a66c59c08bbaaf3167090e52396f3202	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	141898		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

22903 7590 01/23/2012

COOLEY LLP
ATTN: PATENT GROUP
Suite 1100
777 - 6th Street, NW
WASHINGTON, DC 20001

EXAMINER
RAHMAN, MAHFUZUR

ART UNIT	PAPER NUMBER
2438	

DATE MAILED: 01/23/2012

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/408,145	04/20/2006	Matthew L. Boney	WEBR-045/00US 303666-2050	8007

TITLE OF INVENTION: BACKWARD RESEARCHING TIME STAMPED EVENTS TO FIND AN ORIGIN OF PESTWARE

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1740	$300	$0	$2040	04/23/2012

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 SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

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.

Trend Micro, Inc.
EX1002-31

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)

22903 7590 01/23/2012

COOLEY LLP
ATTN: PATENT GROUP
Suite 1100
777 - 6th Street, NW
WASHINGTON, DC 20001

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.
11/408,145	04/20/2006	Matthew L. Boney	WEBR-045/00US 303666-2050	8007

TITLE OF INVENTION: BACKWARD RESEARCHING TIME STAMPED EVENTS TO FIND AN ORIGIN OF PESTWARE

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1740	$300	$0	$2040	04/23/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
RAHMAN, MAHFUZUR	2438	726-022000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:

❑ Issue Fee

❑ Publication Fee (No small entity discount permitted)

❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

❑ A check is enclosed.

❑ Payment by credit card. Form PTO-2038 is attached.

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

❑ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

❑ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information 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.

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.
11/408,145	04/20/2006	Matthew L. Boney	WEBR-045/00US 303666-2050	8007

22903 7590 01/23/2012

COOLEY LLP
ATTN: PATENT GROUP
Suite 1100
777 - 6th Street, NW
WASHINGTON, DC 20001

EXAMINER	
RAHMAN, MAHFUZUR	

ART UNIT	PAPER NUMBER
2438	

DATE MAILED: 01/23/2012

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 586 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 586 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.

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No.	Applicant(s)	
	11/408,145	BONEY, MATTHEW L.	
	Examiner	Art Unit	
	MAHFUZUR RAHMAN	2438	

-- 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 *9/28/2011*.

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 *1-4,6,8,10-16,20,22, and 23*.

4. ☐ 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 the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ 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).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 4/18/2007
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *12/20/2011* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/M. R./
Examiner, Art Unit 2438

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	11/408,145	BONEY, MATTHEW L.	
	Examiner	Art Unit	
	MAHFUZUR RAHMAN	2438	

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

(1) *MAHFUZUR RAHMAN*. (3)_____.

(2) *Mark Schafer*. (4)_____.

Date of Interview: *20 December 2011*.

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 and 12*.

Identification of prior art discussed: *N/A*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicant's representative agreed to amend independent claims to include limitations from claims 5, 19, and 21 and also, it was agreed to add proposed limitations from the specification (i.e. issuing a timestamp after receiving the time of interest to initiate the pestware research). Claims, 19, and 21 have been cancelled as discussed.

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of 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

/M. R./ Examiner, Art Unit 2438	

DETAILED ACTION

This office action is response to the proposed amendment on 12/20/2011 in which claims 1-4, 6, 8, 10-16, 20, 22-23 are presented for examination. Claims 1, 4, 12, and 20 have been amended. Claims 5, 19, and 21 have been cancelled.

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with applicant's representative Mark Schafer on December 20, 2011. The examiner-initiated interview summary (PTO 413B) is attached herein.

Amendment to the Claims

2. CLAIMS:

Please replace all the claims as follows:

1. (currently amended) A method for identifying an origin of suspected pestware activity on a computer, the method comprising:

monitoring, with a kernel-mode driver, activity on the computer;

generating an activity log on a file storage device of the computer from the kernel-mode driver;

receiving, from a user via an interface of the computer, a time of interest relating to a suspicion of pestware on the computer, wherein the time of interest includes a time interval;

issuing a timestamp after receiving the time of interest;

identifying, based upon the time of interest, indicia of pestware, wherein the identifying is initiated by the issuing the timestamp; and

accessing, using a hardware processor of the computer, at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify, based at least in part upon the identified indicia of pestware, a reference to an identity of an externally networked source that is suspected of originating pestware;

wherein the recorded history of externally networked sources is stored on [[a]]the file storage device.

4. (currently amended) The method of claim 3, wherein following the references includes following at least one reference in [[an]]the activity log from the event to a suspected pestware process.

5. (canceled)

12. (currently amended) A system for identifying a source of suspected pestware on a computer, the system comprising:

a hardware processor;

a file storage device coupled to the hardware processor;

a timestamp module configured to be executed by the hardware processor, ~~and~~ to generate a time of interest including a time interval in response to detected activity on the computer that is indicative of pestware, to issue a timestamp after generating the time of interest, and to initiate, in response to the issuance of the timestamp, identification of indicia of pestware;

a research portion configured to be executed by the hardware processor and to access at least one log on a file storage device of the computer to relate the time of interest to at least one externally networked source of potential pestware activity on the computer; ~~and~~

a kernel-mode driver configured to monitor activity on the computer and to generate an activity log that is included within the at least one log; and

a reporting portion configured to be executed by the hardware processor and to generate a report that identifies the at least one externally networked source of potential pestware activity.

19. (canceled)

20. (currently amended) The system of claim 12, wherein the timestamp module is further configured to generate the time of interest as a point in time.

21. (canceled)

Allowable Subject Matter

3. Claims 1-4, 6, 8, 10-16, 20, 22-23 are allowed.

Reasons for Allowance

4. The following is an examiner's statement of reasons for allowance:

As to independent claim 1, the prior art of records (US 2004/0024864 A1 to Porras and US 20070094725 A1 to Borders) alone or in combination fail to anticipate or render obvious the claimed feature.

Porras (primary prior art of record) is directed to a method and system that identifies a user, process, or application associated with subsequent audit records related to a user or process wherein appropriate action is taken against only those sessions and applications that are related to an attack which allows the source to be identified if an IDS determines that the session is part of an attack on the host computer (See, Porras: Paragraphs 0005 and 0015)

The invention of Borders (secondary prior art of record) provides an improved method, system for detecting security threats on a computer network wherein the

method also includes monitoring the data stream to detect a security threat based on a set of heuristics related to legitimate, outbound, application layer messages, and generating a signal if a security threat is detected (See, Borders: Paragraphs 0066-0067).

Applicant's invention is novel as the combination of prior art references fails to teach the claimed invention and falls into impermissible hindsight reconstruction of applicant's claims at the time the applicant's invention was made because of the non-obvious claimed limitations. For example, Claim 1 recites:

"monitoring, with a kernel-mode driver, activity on the computer;

generating an activity log on a file storage device of the computer from the kernel-mode driver;

receiving, from a user via an interface of the computer, a time of interest relating to a suspicion of pestware on the computer, wherein the time of interest includes a time interval;

issuing a timestamp after receiving the time of interest;

identifying, based upon the time of interest, indicia of pestware, wherein the identifying is initiated by the issuing the timestamp; and…..

identify, based at least in part upon the identified indicia of pestware, a reference to an identity of an externally networked source that is suspected of originating pestware;

wherein the recorded history of externally networked sources is stored on the file storage device..".

where applicant's invention is directed to identifying an origin of suspected pestware activity by establishing a time of interest relating to a suspicion of pestware on the computer wherein a timestamp is issued after receiving the time of interest and the

identifying of pestware is initiated by the issuing of the timestamp. Further, the system identifies indicia of pestware and a reference to identity a source that is suspected of originating pestware from an externally networked source.

None of the prior art of records, either taken by itself or in any combination, would have anticipated or made obvious at or before the time the application was filed where a timestamp is issued after receiving the time of interest and the identifying of pestware is initiated by the issuing of timestamp wherein monitoring and generating an activity log is performed from the kernel-mode driver.

Claims 2-4, 6, 8, 10 -11 are also allowed by virtue of the dependency on the base claim 1.

Independent Claims 12 recites similar features as in claim 1 and is allowed for the same reason stated above for claim 1.

Claims 13-16, 20, and 22-23 are also allowed by virtue of their dependency on base claim 12.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to MAHFUZUR RAHMAN whose telephone number is (571)270-7638. The examiner can normally be reached on Monday thru Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on (571) - 272-3787. 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.

/M. R./

Examiner, Art Unit 2438

/Taghi T. Arani/

Supervisory Patent Examiner, Art Unit 2438

Notice of References Cited	Application/Control No. 11/408,145	Applicant(s)/Patent Under Reexamination BONEY, MATTHEW L.	
	Examiner MAHFUZUR RAHMAN	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-			
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Elements of Computer Security|http://www.google.com/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=8&ved=0CEwQFjAH&url=http%3A%2F%2Fcms.vle.ase.md%2Fget%2Fpdf%2F7664&ei=_pzyTp3mMeLL0QG7-9zLAg&usg=AFQjCNEmOz7OxykRPyP1_ePiXGgJI1WGWA&sig2=XE_fLI7CTuchuObMdbGYtA|David Salomon|2010
	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.

Trend Micro, Inc.
EX1002-44

Please type a plus sign (+) inside this box → [+]

PTO/SB/08A (08-00)

Substitute for form 1449A/PTO		*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT		Application Number	11/408,145
		Filing Date	04/20/2006
		First Named Inventor	Matthew L. Boney
(use as many sheets as necessary)		Group Art Unit	2154
		Examiner Name	Not Yet Assigned
Sheet	1 of 3	Attorney Docket Number	WEBR-045/00US

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	U.S. Patent Document Number	Kind Code[2] (*if known*)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY
		5,623,600		JI, ET AL.	04/22/97
		5,920,696		BRANDT ET AL.	07/1999
		5,951,698		CHEN ET AL.	09/1999
		6,069,628		FARRY, ET AL.	05/30/00
		6,073,241		ROSENBERG, ET AL.	06/06/00
		6,092,194		TOUBOUL	07/18/00
		6,154,844		TOUBOUL	11/28/00
		6,167,520		TOUBOUL	12/26/00
		6,310,630		KULKARNI, ET AL.	10/30/01
		6,397,264		STASNICK, ET AL.	05/28/02
		6,405,316		KRISHNAN ET AL.	06/2002
		6,460,060		MADDALOZZO, JR., ET AL.	10/01/02
		6,480,962		TOUBOUL	11/12/02
		6,535,931		CELI, JR.	03/18/03
		6,611,878		DE ARMAS, ET AL.	08/26/03
		6,633,835		MORAN ET AL.	10/14/03
		6,667,751		WYNN, ET AL.	12/23/03
		6,701,441		BALASUBRAMANIAM, ET AL.	03/02/04
		6,772,345		SHETTY	08/2004
		6,785,732		BATES, ET AL.	08/31/04
		6,804,780		TOUBOUL	10/12/04
		6,813,711		DIMENSTEIN	11/02/04
		6,829,654		JUNGEK	12/07/04
		6,910,134		MAHER ET AL.	06/2005
		6,965,968		TOUBOUL	11/15/05
		7,058,822		EDERY ET AL.	06/06/06
		7,107,617		HURSEY ET AL.	09/2006
		US 2002/0162015		TANG	10/2002
		US 2002/0166063		LACHMAN ET AL.	11/2002
		US 2003/0065943		GEIS ET AL.	04/2003
		US 2003/0074581		HURSEY ET AL.	04/2003
		US 2003/0101381		MATEEV ET AL.	05/2003
		US 2003/0159070		MAYER ET AL.	08/2003
		US 2003/0217287	A1	KRUGLENKO	11/20/03
		US 2004/0030914	A1	KELLEY, ET AL.	02/12/04
		US 2004/0034794	A1	MAYER ET AL.	02/19/04
		US 2004/0064736	A1	OBRECHT, MARK ERIC, ET AL.	04/01/04
		US 2004/0080529	A1	WOJCIK, PAUL KAZIMIERZ	04/29/04
		US 2004/0143763	A1	RADATTI	07/22/04

Examiner Signature	/Mahfuzur Rahman/	Date Considered	12/21/2011

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

[1] Unique citation designation number.
[2] See attached Kinds of U.S. Patent Documents.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH./M.R./

Hulu, LLC et al. v. Webpass, Inc.
EX1002-45

Please type a plus sign (+) inside this box → [+]

PTO/SB/08A (08-00)

Substitute for form 1449A/PTO		*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT		Application Number	11/408,145
		Filing Date	04/20/2006
		First Named Inventor	Matthew L. Boney
		Group Art Unit	2154
(use as many sheets as necessary)		Examiner Name	Not Yet Assigned
Sheet	2 of 3	Attorney Docket Number	WEBR-045/00US

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	U.S. Patent Document Number	Kind Code[2] (*if known*)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY
		US 2004/0187023	A1	ALAGNA, MICHAEL ANTHONY, ET AL.	09/23/04
		US 2004/0225877	A1	HUANG	11/11/04
		US 2005/0038697	A1	JEFFREY	02/2005
		US 2005/0154885		VISCOMI ET AL.	07/2005
		US 2005/0138433	A1	LINETSKY, GENE	06/23/05
		2006/0075494		BERTMAN ET AL.	04/2006
		2006/0075501		THOMAS ET AL.	04/2006
		2006/0161988		COSTEA ET AL.	07/2006
		10/956,573		STEVE THOMAS	N/A Filed: 10/01/04
		10/956,574		STEVE THOMAS	N/A Filed: 10/01/04
		10/956,818		MATTHEW BONEY	N/A Filed: 10/01/04
		11/257,609		MICHAEL BURTSCHER	N/A Filed: 10/25/05
		11/237,291		PHILIP MADDALONI	N/A Filed: 09/28/05
		11/408,215		MATTHEW BONEY	N/A Filed: 04/20/06
		11/408,146		MATTHEW BONEY	N/A Filed: 04/20/06

Examiner Signature	/Mahfuzur Rahman/	Date Considered	12/21/2011

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

[1] Unique citation designation number.
[2] See attached Kinds of U.S. Patent Documents.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH./M.R./

Hitachi Micro, Inc.
EX1002-46

Please type a plus sign (+) inside this box → [+]

PTO/SB/08A (08-00)

Substitute for form 1449A/PTO		*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT		Application Number	11/408,145
		Filing Date	04/20/2006
		First Named Inventor	Matthew L. Boney
		Group Art Unit	2154
(use as many sheets as necessary)		Examiner Name	Not Yet Assigned
Sheet	3 of 3	Attorney Docket Number	WEBR-045/00US

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document			Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	T[4]
		Office[1]	Number[2]	Kind Code[3] (if known)			

OTHER – 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[2]
	I.	Codeguru, Three Ways to Inject Your Code Into Another Process, by Robert Kuster, August 4, 2003, 22 pgs.	
	II.	Codeguru, Managing Low-Level Keyboard Hooks With The Windows API for VB .Net, by Paul Kimmel, April 18, 2004, 10 pgs.	
	III.	Codeguru, Hooking The Keyboard, by Anoop Thomas, December 13, 2001, 6 pgs.	
	IV.	~~Illusive Security, Wolves in Sheep's Clothing: malicious DLLs Injected Into trusted Host Applications, Author Unknown,~~ http://home.arcor.de/scheinsicherheit/dll.htm 13 pgs.	/M.R./
	V.	DevX.com, Intercepting Systems API Calls, by Seung-Woo Kim, May 13, 2004, 6 pgs.	
	VI.	Microsoft.com, How To Subclass A Window in Windows 95, Article ID 125680, July 11, 2005, 2 pgs.	
	VII.	MSDN, Win32 Hooks by Kyle Marsh, July 29, 1993, 15 pgs.	
	VII.	PCT Search Report, PCT/US05/34874, 07/05/06, 7 Pages	
	VIII	Yurcik, William et al., "A Planning Framework for Implementing Virtual Private Networks, June 2001, IT Pro, IEEE, pages 41-44	

Examiner Signature	/Mahfuzur Rahman/	Date Considered	12/21/2011

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

[1] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3).
[2] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document.
[3] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible.
[4] Applicant is to place a check mark here if English language Translation is attached.

[1] Unique citation designation number.
[2] Applicant is to place a check mark here if English language Translation attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R./

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11408145	BONEY, MATTHEW L.
	Examiner	**Art Unit**
	MAHFUZUR RAHMAN	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/15/2009	02/02/2010	09/08/2010	03/23/2011	12/21/2011				
1	1	✓	✓	✓	✓	=				
2	2	✓	✓	✓	✓	=				
3	3	✓	✓	✓	✓	=				
4	4	✓	✓	✓	✓	=				
	5	✓	✓	✓	✓	-				
5	6	✓	✓	✓	✓	=				
	7	✓	-	-	-	-				
6	8	✓	✓	✓	✓	=				
	9	✓	-	-	-	-				
7	10	✓	✓	✓	✓	=				
8	11	✓	✓	✓	✓	=				
9	12	✓	✓	✓	✓	=				
10	13	✓	✓	✓	✓	=				
11	14	✓	✓	✓	✓	=				
12	15	✓	✓	✓	✓	=				
13	16	✓	✓	✓	✓	=				
	17	✓	-	-	-	-				
	18	✓	-	-	-	-				
	19	✓	✓	✓	✓	-				
14	20	✓	✓	✓	✓	=				
	21	✓	✓	✓	✓	-				
15	22	✓	✓	✓	✓	=				
16	23	✓	✓	✓	✓	=				

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11408145	BONEY, MATTHEW L.
	Examiner	Art Unit
	MAHFUZUR RAHMAN	2438

SEARCHED

Class	Subclass	Date	Examiner
726	22	12/20/2011	MR

SEARCH NOTES

Search Notes	Date	Examiner
East search, search terms used:(determin$5 or identif$4 or locat$3 or detect$3 or look$3 or find$3) with (source or origin$5 or network or outside or outsource or external$3 or remot$2 compromised or suspicious or suspected or abnormal or server or service or device or computer or outsource or resource) same (Identification or identity$3 or id or identifier or address or name)	12/21/2011	MR
Performed Inventor/Assignee name search	12/21/2011	MR
Keyword search of 726/5,22,23,24,27;709/224,713/100 1	12/21/2011	MR

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner
709	224	12/20/2011	MR
713	100	12/20/2011	MR
726	5,23,24,27	12/20/2011	MR
	((period or date or duration or rang$3 or length or day) with (initiat$3 or issu$5) near4 (Time$1stamp$3 or time adj stamp$3) and kernel with (monitor$3 or track$3)and (log or record or event)).clm.	12/21/2011	MR

/MAHFUZUR RAHMAN/ Examiner.Art Unit 2438	

Trend Micro, Inc.
EX1002-49

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S9	17	(US-20090158430-$ or US-20070250928-$ or US-20070220043-$ or US-20070168694-$ or US-20070094725-$ or US-20070016953-$ or US-20060136720-$ or US-20050268112-$ or US-20040225877-$ or US-20040064515-$ or US-20040034794-$ or US-20040024864-$ or US-20030159070-$).did. or (US-7480683-$ or US-6633835-$ or US-6460060-$).did. or (WO-9845778-$).did.	US-PGPUB; USPAT; EPO	OR	ON	2011/03/23 10:57
S10	17	S9 and (@ad<"20060420" or rlad <"20060420")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 11:01
S11	13	S9 and @ad<"20060420"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 11:05
S13	10	S6 and @ad<"20060420"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 11:05
S14	15	S9 and (@ad<"20060420" or @rlad <"20060420")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 11:09

Trend Micro, Inc.
EX1002-50

S15	12	S6 and (@ad<"20060420" or @rlad <"20060420")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 11:09
S16	12	S15 and (period or time or interval or duration or period or periodically)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 11:14
S18	14	boney near matthew.inv.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 13:04
S19	10	boney near "matthew.inv.and" pestware with reference same (source or origin)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 13:05
S20	3	boney near matthew.inv. and pestware with reference same (source or origin)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 13:05
S28	73	webroot.as.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2011/12/09 12:45
S29	4	S28 and kernel with pestware same (boot or sequence or registr$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2011/12/09 12:47

Trend Micro, Inc.
EX1002-51

S30	4	S28 and kernel same pestware same (boot or sequence or registr$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2011/12/09 12:48
S31	9	S28 and pestware same (boot or sequence or registr $3 or kernel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2011/12/09 12:48
S41	1	malware with kernel with detection.ti.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2011/12/09 15:01
S42	20	S37 and (Time$1stamp$3 or time adj stamp$3 or period or date or duration or rang$3 or length or day) with (user or entr$3 or interface$3 or interest$3 or set $3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2011/12/09 15:14
S43	7	S42 and (pestware or malware or potential or suspicious) same (boot or sequence or registr$3 or kernel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2011/12/09 15:16

S44	23	(US-20090158430-$ or US-20070250928-$ or US-20070220043-$ or US-20070168694-$ or US-20070094725-$ or US-20070016953-$ or US-20060136720-$ or US-20050268112-$ or US-20040225877-$ or US-20040064515-$ or US-20040034794-$ or US-20040024864-$ or US-20030159070-$ or US-20100313006-$ or US-20080034429-$ or US-20050120242-$ or US-20020162015-$).did. or (US-7480683-$ or US-6633835-$ or US-6460060-$ or US-7565695-$ or US-6804780-$).did. or (WO-9845778-$).did.	US-PGPUB; USPAT; EPO	OR	OFF	2011/12/09 15:55
S45	16	S44 and (Time$1stamp$3 or time adj stamp$3 or period or date or duration or rang$3 or length or day) with (user or entr$3 or interface$3 or interest$3 or set $3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2011/12/09 15:56
S46	12	S45 and (pestware or malware or potential or suspicious) same (boot or sequence or registr$3 or kernel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2011/12/09 15:56
S47	12	S45 and (pestware or pest$5 or virus or malware or potential or suspicious) same (boot or sequence or registr$3 or kernel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2011/12/09 15:56
S67	6	(US-20080034429-$ or US-20040225877-$ or US-20090158430-$ or US-20060265761-$).did. or (US-8069487-$ or US-7698744-$).did.	US-PGPUB; USPAT	OR	OFF	2011/12/09 17:29

Trend Micro, Inc.
EX1002-53

S68	111954	(Time$1stamp$3 or time adj stamp$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2011/12/09 17:33
S69	3	S67 and (Time$1stamp$3 or time adj stamp$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2011/12/09 17:33
S79	25175	(726/5,22,23,24,27;709/224,713/100).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2011/12/21 18:15
S80	14817	S79 and (determin$5 or identif$4 or locat$3 or detect $3 or look$3 or find$3) with (source or origin$5 or network or outside or outsource or external$3 or remot$2 compromised or suspicious or suspected server or service or device or computer) with (Identification or identity$3 or id or identifier or address or name)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/12/21 18:15
S81	14817	S80 and (determin$5 or identif$4 or locat$3 or detect $3 or look$3 or find$3) with (source or origin$5 or network or outside or outsource or external$3 or remot$2 compromised or suspicious or suspected server or service or device or computer) with (Identification or identity$3 or id or identifier or address or name)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/12/21 18:21

S82	8373	S81 and (Time$1stamp$3 or time adj stamp$3 or period or date or duration or rang$3 or length or day) with (user or entr$3 or interface$3 or interest$3 or detect$3 or monitor$3 or log$5 or record$3 or event $3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2011/12/21 18:21
S83	8282	S82 and (period or time or interval or duration or period or periodically)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/12/21 18:22
S84	1	S83 and pestware with reference same (source or origin)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/12/21 18:22

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	23509	(726/5,23,24,27;709/224,713/100).ccls.	US-PGPUB; USPAT; UPAD	OR	ON	2011/12/21 19:27
L2	22393	1 and (period or time or interval or duration or period or periodically)	US-PGPUB; USPAT; UPAD	OR	ON	2011/12/21 19:28
L3	12115	2 and (Time$1stamp$3 or time adj stamp$3 or period or date or duration or rang$3 or length or day) with (user or entr$3 or interface$3 or interest$3 or detect$3 or monitor$3 or log$5 or record$3 or event$3)	US-PGPUB; USPAT; UPAD	OR	OFF	2011/12/21 19:28
L4	3	1 and pestware with reference same (source or origin)	US-PGPUB; USPAT; UPAD	OR	ON	2011/12/21 19:28

L5	1	4 and (Time$1stamp$3 or time adj stamp$3 or period or date or duration or rang$3 or length or day) with initiat$3 near6 issu$5	US-PGPUB; USPAT; UPAD	OR	OFF	2011/12/21 19:29
L6	0	((Time$1stamp$3 or time adj stamp$3 or period or date or duration or rang$3 or length or day) with initiat $3 near6 issu$5 and kernel with (monitor$3 or track$3) and (log or record or event)).clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2011/12/21 19:31
L7	5	((Time$1stamp$3 or time adj stamp$3 or period or date or duration or rang$3 or length or day) with initiat $3 and kernel with (monitor$3 or track$3)and (log or record or event)).clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2011/12/21 19:31
L8	5	7 and (@ad<"20060420" or rlad <"20060420")	US-PGPUB; USPAT; UPAD	OR	ON	2011/12/21 19:32
L9	0	8 and ((period or date or duration or rang$3 or length or day) with (initiat$3 or issu$5) near4 (Time$1stamp $3 or time adj stamp$3) and kernel with (monitor$3 or track$3)and (log or record or event)).clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2011/12/21 19:33

12/ 21/ 2011 8:29:22 PM
C:\ Documents and Settings\ mrahman4\ My Documents\ EAST\ Workspaces\ 31_Time Stamp to find Origin of Pestware_04202006_11408145\ 31_Exported from Tagged_RCE-1_Second Non Final_11408145.wsp

Issue Classification

Application/Control No.	Applicant(s)/Patent Under Reexamination
11408145	BONEY, MATTHEW L.
Examiner	**Art Unit**
MAHFUZUR RAHMAN	2438

ORIGINAL		INTERNATIONAL CLASSIFICATION	
CLASS	SUBCLASS	CLAIMED	NON-CLAIMED
726	22	G 0 6 F 21 / 00 (2006.01.01)	

CROSS REFERENCE(S)

CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
709	224				
713	100				
726	5	23	24	27	

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1		17												
2	2		18												
3	3		19												
4	4	14	20												
	5		21												
5	6	15	22												
	7	16	23												
6	8														
	9														
7	10														
8	11														
9	12														
10	13														
11	14														
12	15														
13	16														

/M.R./ Examiner.Art Unit 2438 (Assistant Examiner)	12/21/2011 (Date)	**Total Claims Allowed:** 16
/TAGHI ARANI/ Supervisory Patent Examiner.Art Unit 2438 (Primary Examiner)	12/22/2011 (Date)	O.G. Print Claim(s): 1 O.G. Print Figure: 1

Trend Micro, Inc.
EX1002-57

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:	BONEY, Matthew L.	Confirmation No.:	8007
Serial No.:	11/408,145	Group Art Unit:	2438
Filed:	April 20, 2006	Examiner:	RAHMAN, Mahfuzur

For: **BACKWARD RESEARCHING TIME STAMPED EVENTS TO FIND AN ORIGIN OF PESTWARE**

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

AMENDMENT/RESPONSE TO OFFICE ACTION

In response to the Official Action dated March 28, 2011 (the "Office Action"), please amend the above-identified patent application in the following manner:

Amendments to the Drawings begin on page 2 of this paper.

Amendments to the Specification begin on page 3 of this paper.

Amendments to the Claims are reflected on the listing of the claims which begins on page 8 of this paper.

Remarks/Arguments begin on page 13 of this paper.

AMENDMENTS TO THE DRAWINGS:

Figure 1 has been amended to correct the reference number for the activity log. The activity log of Figure 1 now has the reference number 121. Filed herewith are a Replacement Drawing Sheet for Figure 1 showing the corrected reference number and an Annotated Drawing Sheet for Figure 1 annotating the correction. No new matter has been added through the amendment to Figure 1.

AMENDMENTS TO THE SPECIFICATION:

Please replace the paragraph nos. [0003], [0005], [0015], [0016], [0018], [0031], [0034], [0035], [0037], [0041], and [0043] with the following paragraphs. The amendments to paragraph nos. [0003], [0005], [0015], [0016], [0018], [0031], [0034], [0035], [0037], [0041], and [0043] are indicated by strikethough and underlining.

[0003] Also shown is a file storage device 118 that is coupled to the research module 108 and an activity monitor 116. In this embodiment the file storage device includes an activity log ~~120~~121, a pestware file 124 and a collection of *N* files 130. The file storage device 118 is described herein in several implementations as hard disk drive for convenience, but this is certainly not required, and one of ordinary skill in the art will recognize that other storage media may be utilized without departing from the scope of the present invention. In addition, one of ordinary skill in the art will recognize that the storage device 118, which is depicted for convenience as a single storage device, may be realized by multiple (e.g., distributed) storage devices.

[0005] In accordance with several embodiments, the research module 108 is configured to receive an indication that either known pestware is residing on the computer or activities indicative of pestware have occurred or are occurring on the protected computer. In response, the research module 108 is configured to research the activity log ~~120~~121 and/or the *N* files 130, which include information (e.g., historical logs) relating to events on the computer 100, to identify a source of the pestware 122, 124 or pestware-related activities, which may be reported by the reporting module 114 to a centralized data store for subsequent pestware management purposes.

[0015] In yet other embodiments, the timestamp module 112 operates independently of the heuristics module 110. For example, the timestamp module 112 may prompt the research module 108 to initiate a review of the activity log ~~120~~121 and/or one or more of the *N* files in response to a user request.

[0016] The activity monitor 116 in several embodiments monitors activities on the computer and stores information about the activities in the activity log ~~120~~121 so as to assist the research module 108 in identifying activities associated with pestware and the source of the pestware. In some embodiments, for example, the activity log ~~120~~121 includes a list of processes that are running on the protected computer and the files that are associated with the processes. Although not depicted in FIGURE 1, the shields 120 may utilize the activity monitor 116 to detect pestware-related events and intercept efforts by pestware to spawn new processes or alter aspects of the protected computer 100.

[0018] In other embodiments, the activity monitor 116 is realized by a kernel-mode driver that may be loaded during a boot sequence for the protected computer or anytime later. In these embodiments, the activity monitor 116 is configured to log API calls in the activity log 121. In many variations for example, when a process (e.g., the pestware process) attempts to spawn a another pestware process or alter a registry entry, the API call utilized by the process is intercepted before it is carried out by an operating system of the protected computer. In this way, the attempt may be logged in the activity log ~~120~~121 and the process may be analyzed to determine whether it is known to be a pestware-related process. Additional details of use of a kernel-level driver in connection with pestware management may be found in the above identified application entitled: *System and Method for Kernel-Level Pestware Management.*

[0031] As shown in FIGURE 3, if pestware indicia is found, then recorded information (e.g., the activity log ~~120~~121 and/or the *N* files 130) that may include traces of the pestware is accessed (Block 304), and traversed to search for information leading to the identification of the source of the pestware (Block 306). In some instances, the origin of the pestware may be identified by simply referencing one piece of data that is stored in connection with the identification of the pestware source. In other instances, however, it may be necessary to access several pieces of referential data, which may be located in one or more of the files 220-256 before arriving at the identity of the source of the pestware.

[0034] Referring next to FIGURE 4, shown is a flowchart depicting a method in accordance with another embodiment of the present invention. Again, reference will be made to FIGURES 1 and 2 for exemplary purposes, but it should be recognized that the method described with reference to FIGURE 4 is certainly not limited to the specific embodiments described with reference to FIGURES 1 and 2. As shown, in this embodiment activity on a computer is monitored for indicia of pestware (Block 402), and if potential pestware-related activity is detected, recorded information related to the activity is searched to identify one or more suspicious objects (e.g., files and/or processes) that are related to the activity (Block 404). In some embodiments, the shields 120 (described with reference to FIGURE 1) may monitor the protected computer 100 for activities, and if the activity is identified as potential pestware activity (e.g., by the heuristics module 110), then the research module 108 searches the activity log ~~120~~121 and/or one or more of the *N* files for information relating to the pestware-related activity.

[0035] As shown in FIGURE 4, recorded information (e.g., one or more of the *N* files) is then traversed to trace through information related to the suspicious objects that leads to an origin of

the suspicious objects (Block 406). In one embodiment for example, the suspicious activity leads to a search for suspicious processes and/or files related to the activity (e.g., using the activity log ~~120~~121), which then leads to a search of one or more of the *N* files 130 (e.g., the cache index 243) for an indication of the source of the suspicious process and/or files.

[0037] As an example of pestware-related activity that may trigger the search for a source of the activity, if a series of particular API calls is made in a pattern known to be associated with pestware, the process(es) making the calls may be identified using, for example, the activity log ~~120~~121. In turn, the activity log ~~120~~121 may be used to identify the file(s) associated with the process(es), and the cache index 243 may be utilized to search for a source of the file(es). It should be recognized that this is merely one example of the type of activity that may trigger backwards researching of logs on a computer, and that patterns in process creation, downloaded files, changes to an operating system registry and browser settings, for example, may trigger a search of the computer's logs.

[0041] As shown in FIGURE 5, once a time of interest is established, suspicious activity is identified on the computer based upon the time of interest (Block 504). The time of interest may be established, for example, to include a time period before the time stamp is issued so that a search for suspicious activity is limited to a particular time period. In some embodiments, the activity log ~~120~~121 and/or one or more of the *N* files 130 are accessed and analyzed to determine whether any activity during the time of interest is suspicious (e.g., the activity indicates in some way that it may be associated with pestware). As an example, if any logged information (e.g., in the activity log ~~120~~121 and/or one or more of the *N* files 130) indicates that during the time of interest that, for example, access to the registry was carried out in connection with a downloaded

file or the launch of a process, the activities may identified as being suspect and further research relative to the process and the file may carried out.

[0043] As depicted in FIGURE 5, once one or more activities are identified as being suspicious (Block 504), one or more objects (e.g., processes or files) on the computer are associated with the suspicious activity (Block 506). For example, the research module 108 may search the activity log ~~120~~121 and/or one or more of the *N* files for information that associates the suspicious activity to one or more processes and the processes may be related to one or more files.

AMENDMENTS TO THE CLAIMS:

Set forth below in ascending order, with status identifiers, is a complete listing of all claims currently under examination. Changes to any amended claims are indicated by strikethrough and underlining. This listing also reflects any cancellation and/or addition of claims.

1. (currently amended) A method for identifying an origin of suspected pestware activity on a computer, the method comprising:

receiving, from a user via an interface of the computer, a time of interest relating to a suspicion of pestware on the computer, the suspicion of pestware comprising;

identifying, based upon the time of interest, indicia of pestware; and

accessing, using a hardware processor of the computer, at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify, based at least in part upon the identified indicia of pestware, a reference to an identity of an externally networked source that is suspected of originating pestware;

wherein the recorded history of externally networked sources is stored on a file storage device.

2. (original) The method of claim 1, wherein the identifying includes:

accessing at least one log of historical events on the computer;

locating at least one event in the at least one log that corresponds to the time of interest; and

determining that the at least one event is associated with the indicia of pestware.

3. (original) The method of claim 2, wherein the determining that the at least one event is associated with the indicia of pestware includes following references in the at least one log to a suspected pestware object.

4. (original) The method of claim 3, wherein following the references includes following at least one reference in an activity log from the event to a suspected pestware process.

5. (original) The method of claim 4, wherein the activity log is generated from a kernel-mode driver.

6. (original) The method of claim 2, wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs.

7. (canceled)

8. (previously presented) The method of claim 1, wherein the user input is in response to an alert provided to the user regarding a detected suspicious activity on the computer.

9. (canceled)

10. (currently amended) The method of claim 1, including:

reporting the identity of the externally networked source to [[a]]an externally networked pestware research entity so as to enable the pestware research entity to research whether the externally networked source is a source of pestware.

11. (previously presented) The method of claim 1, wherein the externally networked source is identified by an identifier selected from the group consisting of an I.P. address and a URL.

12. (currently amended) A system for identifying a source of suspected pestware on a computer, the system comprising:

a hardware processor;

a file storage device coupled to the hardware processor;

a timestamp module configured to be executed by the hardware processor and to generate a time of interest in response to detected activity on the computer that is indicative of pestware;

a research portion configured to be executed by the hardware processor and to access at least one log on a file storage device of the computer to relate the time of interest to at least one externally networked source of potential pestware activity on the computer; and

a reporting portion configured to be executed by the hardware processor and to generate a report that identifies the at least one externally networked source of potential pestware activity.

13. (previously presented) The system of claim 12, wherein the at least one log includes information that relates the time of interest to an event, and wherein the at least one log includes information that relates the event to a suspected pestware object, and wherein the at

least one log includes information that relates the suspected pestware object to the at least one externally networked source of potential pestware activity.

14. (currently amended) The system of claim 13, including:

a heuristics module configured to be executed by the hardware processor and to evaluate whether the event is a suspected pestware-related event before the research portion accesses information in the at least one log that relates the event to the suspected pestware object.

15. (original) The system of claim 14, wherein the heuristics module determines that the at least one event is suspected to be pestware-related by analyzing other events in connection with the event, wherein the other events are also related to the time of interest.

16. (original) The system of claim 12, wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs

17.-18. (canceled)

19. (previously presented) The system of claim 12, wherein the timestamp module is configured to generate the time of interest as a time interval.

20. (previously presented) The system of claim 12, wherein the timestamp module is configured to generate the time of interest as a point in time.

21. (original) The system of claim 12, including a kernel-mode driver adapted to monitor activity on the computer and to generate an activity log that is included within the at least one log.

22. (previously presented) The system of claim 12, wherein the at least one externally networked source of potential pestware activity is identified by an identifier selected from the group consisting of an I.P. address and a URL.

23. (original) The system of claim 12, wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs.

REMARKS

Each of claims 1, 10, 12, and 14 is currently amended. Each of claims 8, 11, 13, 19, 20, and 22 was previously amended. Each of claims 7, 9, 17, and 18 was previously canceled. No other claims are currently added, amended, or canceled. Each of claims 1-6, 8, 10-16, and 19-23 thus remains pending.

Amendments to the Specification

Each of Paragraphs [0003], [0005], [0015], [0016], [0018], [0031], [0034], [0035], [0037], [0041], and [0043] has been amended to reflect the amendment to Figure 1, that is, the correction to the reference number of the activity log. No new matter has been added through the amendments to Paragraphs [0003], [0005], [0015], [0016], [0018], [0031], [0034], [0035], [0037], [0041], and [0043].

Claim Amendments

Claim 1 has been currently amended to recite, among other things, "receiving, from a user via an interface of the computer, a time of interest relating to a suspicion of pestware on the computer, the suspicion of pestware comprising" and "accessing, using a hardware processor of the computer, at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify, based at least in part upon the identified indicia of pestware, a reference to an identity of an externally networked source that is suspected of originating pestware." Support for each of these amendments can be found, for example, at Figure 1 and Paragraphs [0012] and [0029] of the application as filed. No new matter has been added through these amendments.

Claim 10 has been currently amended to recite "reporting the identity of the externally networked source to an externally networked pestware research entity so as to enable the

pestware research entity to research whether the externally networked source is a source of pestware." Support for this amendment can be found, for example, at Paragraph [0054] in the application as filed. No new matter has been added through this amendment.

Claim 12 has been currently amended to recite, among other things, "a hardware processor," "a file storage device coupled to the hardware processor," "a timestamp module configured to be executed by the hardware processor and to generate a time of interest in response to detected activity on the computer that is indicative of pestware," "a research portion configured to be executed by the hardware processor and to access at least one log on a file storage device of the computer to relate the time of interest to at least one externally networked source of potential pestware activity on the computer," and "a reporting portion configured to be executed by the hardware processor and to generate a report that identifies the at least one externally networked source of potential pestware activity."

Support for each of these amendments can be found, for example, at Figure 1 and Paragraphs [0012] and [0029] of the application as filed. No new matter has been added through these amendments.

Claim 14 has been currently amended to recite "a heuristics module configured to be executed by the hardware processor and to evaluate whether the event is a suspected pestware-related event before the research portion accesses information in the at least one log that relates the event to the suspected pestware object." Support for this amendment can be found, for example, at Figure 1 and Paragraphs [0012] and [0029] of the application as filed. No new matter has been added through this amendment.

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

The Office Action rejects each of claims 1-6, 8, 10-16, and 19-23 under 35 U.S.C § 103 as being unpatentable over Porras et al. (U.S. Publ. No. 2004/0024864, hereinafter "Porras") in view of Borders (U.S. Publ. No. 2007/0094725, hereinafter "Borders"). Applicant respectfully traverses these rejections

Claim 1

Porras does not teach or suggest "receiving, from a user via an interface of the computer, a time of interest relating to a suspicion of pestware on the computer, the suspicion of pestware comprising." Currently-amended independent claim 1 now recites, among other things, "receiving, from a user via an interface of the computer, a time of interest relating to a suspicion of pestware on the computer, the suspicion of pestware comprising." The Office Action asserts that Porras, at Paragraph [0014], discloses "receiving, from a user . . . , a time of interest relating to a suspicion of pestware on the computer, the suspicion of pestware comprising." Office Action, p. 3. Applicant respectfully disagrees.

Porras describes several embodiments of an intrusion detection system ("IDS") in which certain audit record data is identified and associated for further analysis. Porras, Paragraph [0014]. First, Porras can associate IP addresses and session identifiers from audit records. *Id.* at Figure 3 and Paragraph [0015]. Second, Porras can associate application names and process identifiers from the audit records. *Id.* at Figure 4 and Paragraph [0016]. Third, Porras can associate an application name from the audit records to an alert. *Id.* at Figure 5 and Paragraph [0017]. Fourth, Porras can associate a remote IP address and a process ID from the audit records. *Id.* at Figure 6 and Paragraph [0018]. Lastly, Porras can associate an IP address from the audit records to an alert. *Id.* at Figure 7 and Paragraph [0019]. Porras' IDS can receive the

audit records from which it obtains its data for association either in realtime or as needed. *Id.* at Paragraph [0014].

None of Porras' embodiments include "receiving, from a user . . . a time of interest." The Office Action appears to argue that because Porras' IDS can be received in realtime, that it receives a "time of interest." However, Porras never describes a time as part of its audit records. Porras describes *when* audit records are received, not that a time is received. And no part of the IDS relies on when audit records are received. Even assuming the IDS received a "time of interest," it would not receive it from a user. The IDS receives its audit records from the system's kernel. Porras, Paragraph [0014]. Therefore, Porras neither teaches nor suggests "receiving, from a user via an interface of the computer, a time of interest relating to a suspicion of pestware on the computer, the suspicion of pestware comprising."

Porras does not teach or suggest "identifying, based upon the time of interest, indicia of pestware." Currently-amended independent claim 1 recites, among other things, "identifying, based upon the time of interest, indicia of pestware." The Office Action asserts that Porras, at Paragraphs [0017] and [0019], discloses this limitation. Office Action, p. 3. Applicant respectfully disagrees.

As discussed above, Porras fails to teach or suggest a "time of interest." Therefore, it cannot teach or suggest identifying anything, including indicia of pestware, "based upon the time of interest." Even assuming Porras discloses a "time of interest," it does not teach or suggest "identifying . . . indicia of pestware" based upon it. As discussed above, Porras discloses identifying and associating IP addresses, process IDs, application names, session identifiers, and alerts. Porras' IDS and its analysis engine use those data items to determine the existence of

pestware. Porras, Paragraph [0014]. None of those data items are a "time of interest" and Porras never mentions using a time to identify any of them.

Furthermore, Porras describes associating those data items after the "IDS identifies a process as suspicious." Porras, Paragraph [0017]. In other words, Porras assumes that a suspicious process is already identified before associating the data items. Porras never describes, beyond this short description in Paragraph [0017] how a process is identified as suspicious.

In short, Porras describes associating data items, other than a "time of interest," *after* a suspected attack has been identified so that the IDS can perform further analysis. Therefore, Porras neither teaches nor suggests "identifying, based upon the time of interest, indicia of pestware."

Each of claims 1-6, 8, and 10-11 is allowable. Neither Porras nor Borders, either alone or in combination, teach or suggest each and every limitation of currently-amended independent claim 1. Therefore, Applicant believes claim 1 to be allowable. Each of claims 2-6, 8, and 10-11 is thus allowable, at least by virtue of its depending from allowable claim 1. Applicant therefore respectfully request withdrawal of the rejection, under 35 U.S.C. § 103, of each of claims 1-6, 8, and 10-11.

Claim 2

Porras does not teach or suggest "locating at least one event in the at least one log that corresponds to the time of interest." Dependent claim 2 recites, among other things, "locating at least one event in the at least one log that corresponds to the time of interest." The Office Action asserts that Porras, at Paragraph [0015], discloses this limitation. Office Action, p. 5. As discussed above, Porras does not teach or suggest a "time of interest." Furthermore, it does not teach or suggest locating anything in a log based on a time. Instead, Porras describes identifying

IP addresses, process IDs, application names, and session identifiers in audit records. Porras, Paragraphs [0015]-[0019]. Porras never describes using a "time of interest" to find those data items. Therefore, Porras cannot teach or suggest "locating at least one event in the at least one log that corresponds to the time of interest."

Claim 2 is allowable. For at least the foregoing reasons, Applicant believes dependent claim 2 to be allowable. Applicant therefore respectfully requests withdrawal of the rejection, under 35 U.S.C. § 103, of claim 2.

Claim 10

Porras does not teach or suggest "reporting the identity of the externally networked source to an externally networked pestware research entity so as to enable the pestware research entity to research whether the externally networked source is a source of pestware." Currently-amended dependent claim now recites "reporting the identity of the externally networked source to an externally networked pestware research entity so as to enable the pestware research entity to research whether the externally networked source is a source of pestware." The Office Action asserts that Porras, at Paragraphs [0013] and [0019], discloses the limitation "reporting the identity of the externally networked source to a pestware research entity so as to enable the pestware research entity to research whether the externally networked source is a source of pestware." Office Action, p. 7.

Claim 10 has now been amended to make clear that the "pestware research entity" is "externally networked." Porras teaches an analysis engine that is an internal part of Porras' IDS. Porras, Figure 1 and Paragraph [0013] (describing the IDS of Figure 1 which includes the "IDS's analysis engine 107"). Because Porras requires a internal analysis engine, it cannot disclose an "externally networked pestware research entity." Therefore, Porras neither teaches nor suggests

"reporting the identity of the externally networked source to an externally networked pestware research entity so as to enable the pestware research entity to research whether the externally networked source is a source of pestware."

Claim 10 is allowable. For at least the foregoing reasons, Applicant believes currently-amended dependent claim 10 to be allowable. Applicant therefore respectfully requests withdrawal of the rejection, under 35 U.S.C. § 103, of claim 10.

Claim 12

Porras does not teach or suggest "a timestamp module configured to be executed by the hardware processor and to generate a time of interest in response to detected activity on the computer that is indicative of pestware." Currently-amended independent claim 12 now recites, among other things, "a timestamp module configured to be executed by the hardware processor and to generate a time of interest in response to detected activity on the computer that is indicative of pestware." The Office Action asserts that Porras, at Paragraph [0014], teaches "a timestamp module configured to generate a time of interest in response to detected activity on the computer that is indicative of pestware." Office Action, p. 7-8.

Claim 12 is distinguishable from Porras in several respects. First, as discussed above, Porras does not teach or suggest a "time of interest." Second, Porras receives its audit records in order to analyze the existence of an attack irrespective of a particular time. Porras, Paragraph [0014] (discussing alternatively receiving audit records in realtime or as needed). Third, Porras never discloses a timestamp module or any module that is configured to generate a time of interest. Moreover, Porras never discloses, either expressly or impliedly, that any portion of its IDS is configured to "generate a time of interest in response to detected activity." Porras states that the operating system kernel generates audit records. Porras, Paragraph [0014]. It is well

understood that the operating system will generate audit records during the normal course of operation. Porras never mentions that the audit records are generated, not in the normal course, but "in response to detected activity on the computer that is indicative of pestware." Therefore, Porras fails to teach or suggest this limitation.

Porras does not teach or suggest "a research portion configured to be executed by the hardware processor and to access at least one log on a file storage device of the computer to relate the time of interest to at least one externally networked source of potential pestware activity on the computer." Currently-amended independent claim 12 now recites, among other things, "a research portion configured to be executed by the hardware processor and to access at least one log on a file storage device of the computer to relate the time of interest to at least one externally networked source of potential pestware activity on the computer." The Office Action asserts that Porras, at Paragraphs [0013] and [0019], discloses the limitation "a research portion configured to access at least one log on a file storage device of the computer to relate the time of interest to at least one [externally networked source] of potential pestware activity on the computer." Office Action, p. 8. As discussed above, Porras does not teach or suggest a "time of interest." Nor does Porras teach or suggest relating a "time of interest" to any activity on its computer. Therefore, Porras cannot teach or suggest this limitation.

Each of claims 12-16 and 19-23 is allowable. Neither Porras nor Borders, either alone or in combination teach or suggest each and every limitation of currently-amended independent claim 1. Therefore, Applicant believes claim 12 to be allowable. Each of claims 13-16 and 19-23 is thus allowable, at least by virtue of its depending from allowable claim 12. Applicant therefore respectfully request withdrawal of the rejection, under 35 U.S.C. § 103, of each of claims 12-16 and 19-23.

CONCLUSION

In view of the foregoing, Applicant respectfully submits that no further impediments exist to the allowance of this application and, therefore, requests an indication of allowability. However, the Examiner is requested to call the undersigned if any questions or comments arise.

The Director is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.16, 1.17, and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 50-1283.

COOLEY LLP
ATTN: Patent Group
777 6th Street NW, Suite 1100
Washington, DC 20001

Tel: (720) 566-4106
Fax: (202) 842-7899

Respectfully submitted,
COOLEY LLP

By: /Mark Schafer/
Mark Schafer
Reg. No. 65,336

Replacement Drawing Sheet

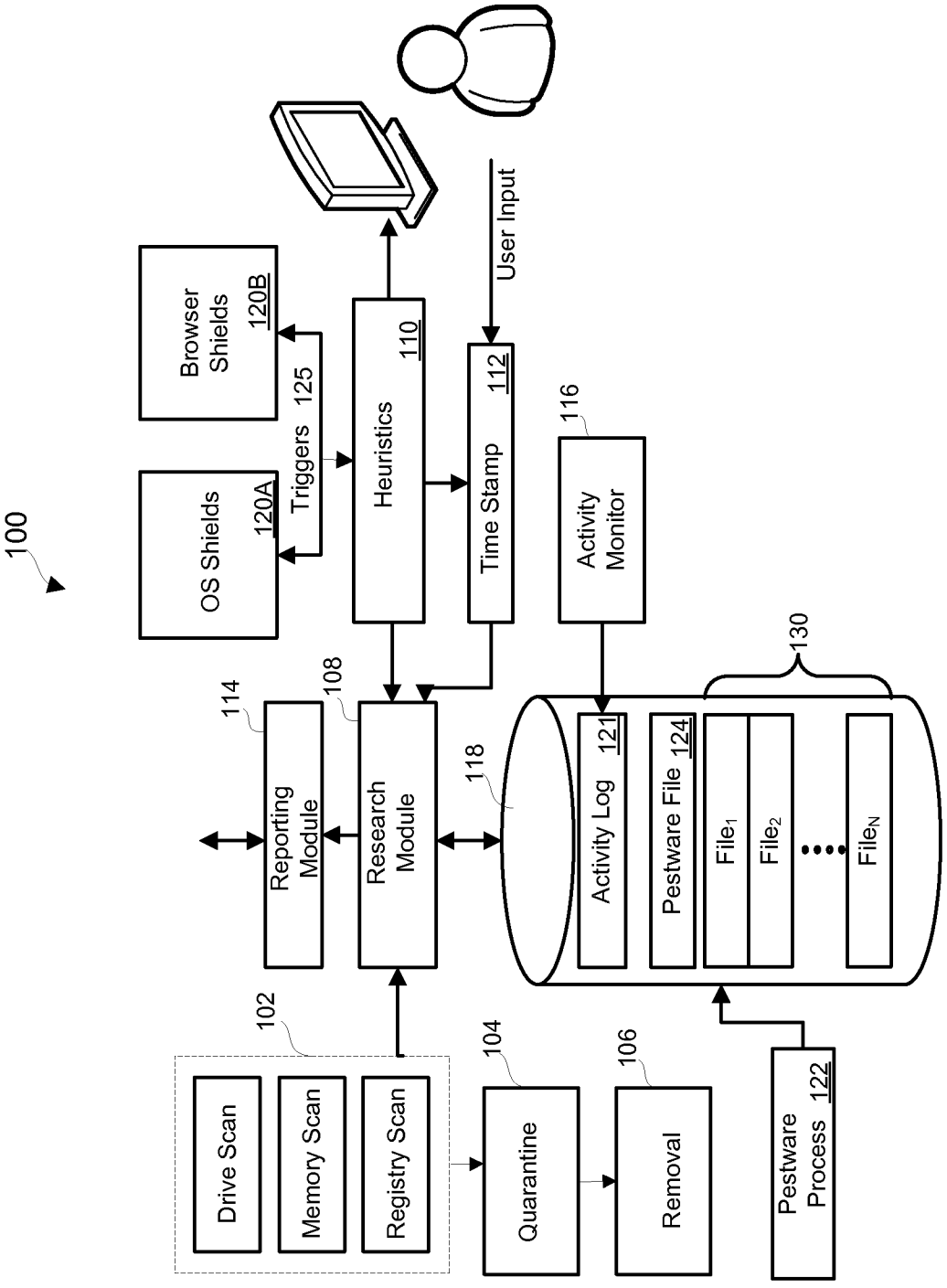


FIGURE 1

Annotated Drawing Sheet

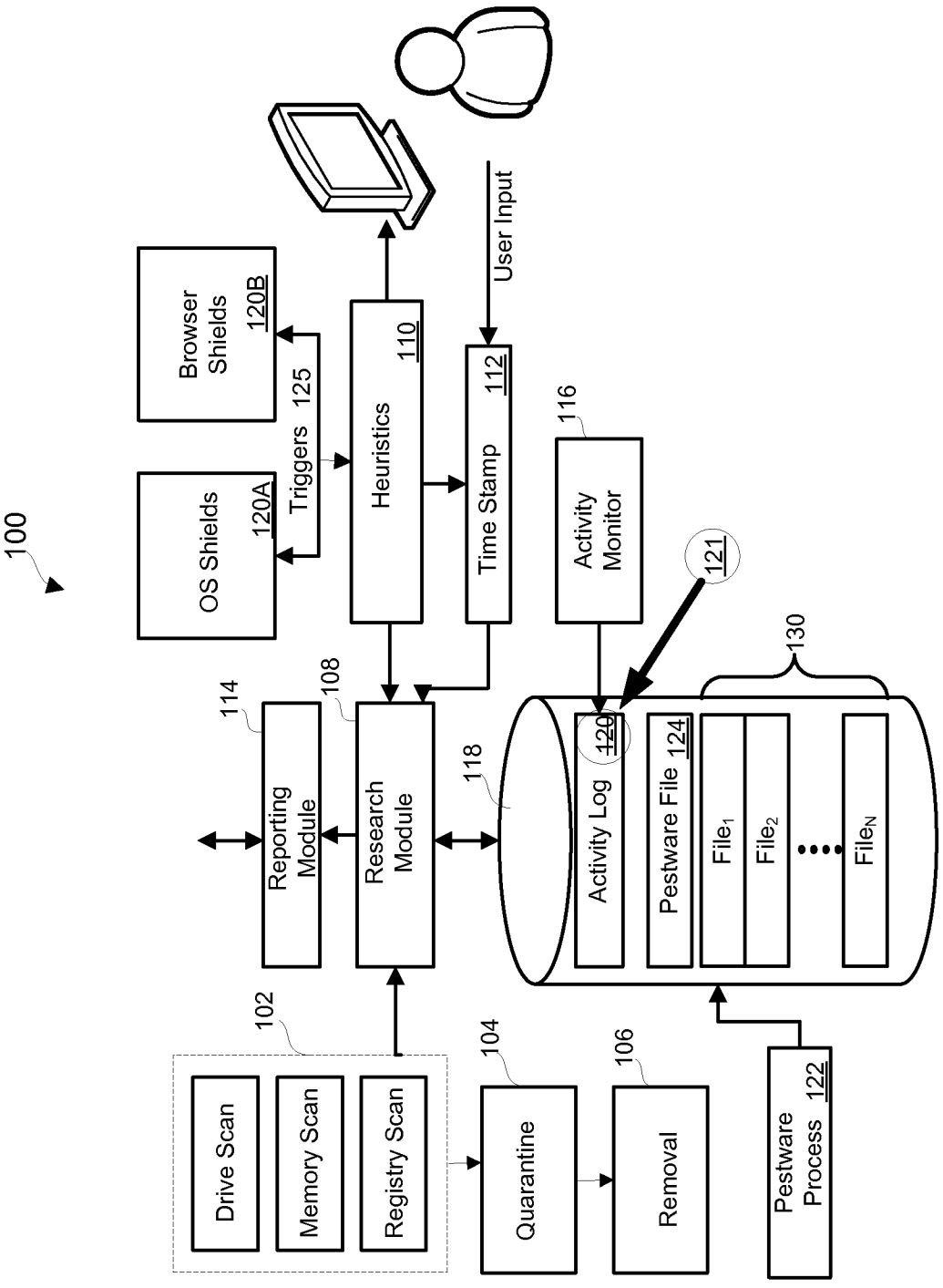


FIGURE 1

Electronic Patent Application Fee Transmittal

Application Number:	11408145
Filing Date:	20-Apr-2006
Title of Invention:	Backward researching time stamped events to find an origin of pestware
First Named Inventor/Applicant Name:	Matthew L. Boney
Filer:	Mark Randolph Schafer/Sherry Bitler
Attorney Docket Number:	WEBR-045/00US 303666-2050

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:				
Extension - 3 months with $0 paid	1253	1	1270	1270

Trend Micro, Inc.
EX1002-81

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**1270**

Electronic Acknowledgement Receipt

EFS ID:	11062612
Application Number:	11408145
International Application Number:	
Confirmation Number:	8007
Title of Invention:	Backward researching time stamped events to find an origin of pestware
First Named Inventor/Applicant Name:	Matthew L. Boney
Customer Number:	22903
Filer:	Mark Randolph Schafer/Sherry Bitler
Filer Authorized By:	Mark Randolph Schafer
Attorney Docket Number:	WEBR-045/00US 303666-2050
Receipt Date:	28-SEP-2011
Filing Date:	20-APR-2006
Time Stamp:	13:34:52
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1270
RAM confirmation Number	10478
Deposit Account	501283
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	Applicant Arguments/Remarks Made in an Amendment	WEBR04500US-roa.pdf	156828 12b3dd0dfc95e16c04c31cc337e24000ec78a0ee	no	21
Warnings:					
Information:					
2	Drawings-only black and white line drawings	WEBR04500US-Figure1-Replacement.pdf	48344 a726e533f38212e7582721b048ac4d3179a6d4e2	no	2
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30119 040e6fedb2bdb35a8e185660f72448d92abfaa9f	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	235291		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
11/408,145	04/20/2006	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☐ RATE ($)	SMALL ENTITY ☐ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), 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))							
			TOTAL			TOTAL	

* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED – PART II

AMENDMENT	09/28/2011	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 19	Minus	** 23	= 0	X $ =		OR	X $60=	0
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $ =		OR	X $250=	0
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	0

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) 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))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/KAREN VESTAL/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/408,145	04/20/2006	Matthew L. Boney	WEBR-045/00US 303666-2050	8007

22903 7590 03/28/2011

COOLEY LLP
ATTN: PATENT GROUP
Suite 1100
777 - 6th Street, NW
WASHINGTON, DC 20001

EXAMINER	
RAHMAN, MAHFUZUR	
ART UNIT	**PAPER NUMBER**
2438	

MAIL DATE	DELIVERY MODE
03/28/2011	PAPER

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.

Trend Micro, Inc.
EX1002-86

Office Action Summary	Application No.	Applicant(s)	
	11/408,145	BONEY, MATTHEW L.	
	Examiner	Art Unit	
	MAHFUZUR RAHMAN	2438	

-- 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 *24 January 2011*.

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

3)☐ 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

4)☒ Claim(s) *1-6,8,10-16 and 19-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8,10-16 and 19-23* is/are rejected.

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

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

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

10)☒ The drawing(s) filed on *20 April 2006* 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).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

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. _____.

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) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Trend Micro, Inc.
EX1002-87

DETAILED ACTION

Applicant's remark filed on 1/24/2011 is acknowledged. Claims 1-6, 8, 10-16, and 19-23 are presented for examination on the merits.

Response to Arguments

1. Applicant's arguments, filed 01/24/2011, with respect to the rejection(s) of claims 1-6, 8, 10-16, and 19-23 under 35 U.S.C. 103(a) have been considered. Therefore, the office action mailed on 09/1//2010 is withdrawn. However, upon further consideration, a new ground(s) of rejection is made over Porras et al. (US 2004/0024864 A1) in view of Borders (US 20070094725 A1) and THIS ACTION IS MADE NON-FINAL.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. 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.

4. Claims 1-6, 8, 10-16, and 19-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Porras et al. (US 2004/0024864 A1, hereinafter, Porras) in view of Borders (US 20070094725 A1).

Regarding claim 1, Porras discloses a method for identifying an origin of suspected pestware activity on a computer, the method comprising:

receiving, from a user, a time of interest relating to a suspicion of pestware on the computer (Paragraph 0014: generating audit records that are analyzed periodically or as needed basis to identify any suspicious activity that is responsible for a potential attack on a host a computer);

identifying, based upon the time of interest, [indicia] of pestware (Paragraph 0017: If an IDS identifies the process as suspicious, the pathnames of applications invoked by the process are associated with IDS alerts related to the suspicious process; Paragraph 0019: the IP address of a source of suspicious activity is acquired and then associated with IDS alerts related to the suspicious activity);

and accessing at least a portion of a recorded history of [externally networked] sources (Paragraph 0015: audit-record that records the IP address of the source)

that the computer received files from so as to identify, based at least in part upon the identified indicia of pestware, a reference to an identity of an externally networked source that is suspected of originating pestware (Paragraph 0019: the IP address of a source of suspicious activity is acquired and then associated with IDS alerts related to the suspicious activity).

Porras does not explicitly disclose but Borders from the same or similar fields of endeavor teaches an externally networked source (Borders, Paragraph 0187: a particular host inside a protected network to a particular host outside that network identified by URL; Paragraph 0118: a "wait for request on input stream" outputs to a "Does header contain suspicious values", a "Insert <time>-Previous <time> for same <source, destination> into delay list for <source, destination>", a "Size of contents> threshold?", a "Add size of contents to total bandwidth value for <source, destination> over the past 24 hours" of block 314, a "Add size of contents to bandwidth counter for 5-minute intervals for <source, destination>") wherein

an indicia of pestware is being analyzed (Borders, Paragraph 0028: Low variation in bandwidth usage is indicative of abnormal or non-human activity. The plot of the coefficient of variation measurements for an 8-hour time period can been seen; Paragraph 0078: monitoring the data stream to detect a security threat based on a set of heuristics).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to identify a reference of an externally networked source as taught by Borders in the teachings of Porras for the advantage of monitoring the data stream to

detect a security threat based on a set of heuristics related to legitimate, outbound, application layer messages, and generating a signal if a security threat is detected (Paragraph 0066).

Regarding claim 2, the combination of Porras and Borders discloses the method of claim 1, wherein the identifying includes: accessing at least one log of historical events on the computer; locating at least one event in the at least one log that corresponds to the time of interest; and determining that the at least one event is associated with the indicia of pestware (Porras, Paragraph 0015: audit record wherein network communication event and process session associated with a session identifier are recorded).

Regarding claim 3, the combination of Porras and Borders discloses the method of claim 2, wherein the determining that the at least one event is associated with the indicia of pestware includes following references in the at least one log to a suspected pestware object (Porras, Paragraph 0015: Intrusion Detection System determines that session is part of an attack via IP address of source or a session identifier).

Regarding claim 4, the combination of Porras and Borders discloses the method of claim 3, wherein following the references includes following at least one reference in an activity log from the event to a suspected pestware process (Porras, Paragraph

0015: source of the attack is identified using session identifier and IP address in the audit record or the record that is obtained from network communication events)

.

Regarding claim 5, the combination of Porras and Borders discloses the method of claim 4, wherein the activity log is generated from a kernel-mode driver (Porras , Paragraph 0015: session identifier of a suspicious activity is recorded as a log entry in kernel audit records, for example).

Regarding claim 6, the combination of Porras and Borders discloses the method of claim 2 wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs (Porras , Paragraph 0017: application pathnames related to the suspicious process is obtained where pathnames includes file information, for example).

Regarding claim 8, the combination of Porras and Borders discloses the method of claim 1, wherein the user input is in response to an alert provided to the user regarding a detected suspicious activity on the computer (Porras, Paragraph 0017: IDS operator or system administrator takes selective action once the alert is generated regarding any suspicious activity from attacker; Page 3 lines 20-23: response to a suspicious activity).

Regarding claim 10, the combination of Porras and Borders discloses the method of claim 1, including: reporting the identity of the externally networked source to a pestware research entity so as to enable the pestware research entity to research whether the externally networked source is a source of pestware (Porras , Paragraph 0013: preprocessor associates necessary information to audit record and reports it to the analysis engine so the source that is responsible for attack can be identified; Paragraph 0019: the IP address of a source of suspicious activity is acquired , and then associated with IDS alerts related to the suspicious activity).

Regarding claim 11, the combination of Porras and Borders discloses the method of claim 1, wherein the externally networked source is identified by an identifier selected from the group consisting of an I.P. address and a URL (Porras, Paragraph 0019: the IP address of a source of suspicious activity is acquired, and then associated with IDS alerts related to the suspicious activity).

Regarding claim 12, Porras discloses a system for identifying a source of suspected pestware on a computer, the system comprising:

a timestamp module configured to generate a time of interest in response to detected activity on the computer that is indicative of pestware (Paragraph 0014: generating audit records that are analyzed periodically or as needed basis to identify any suspicious activity that is responsible for a potential attack on a host a computer;

Paragraph 0019: the IP address of a source of suspicious activity is acquired and then associated with IDS alerts related to the suspicious activity)

a research portion configured to access at least one log on a file storage device of the computer to relate the time of interest to at least one [externally networked source] of potential pestware activity on the computer (Paragraph 0013: analysis engine determines if an intrusion or attack has taken place by analyzing audit records where analysis engine acts as a research portion of the Intrusion Detection System, for example; Paragraph 0019: the IP address of a source of suspicious activity is acquired and then associated with IDS alerts related to the suspicious activity); and

a reporting portion configured to generate a report that identifies the at least one externally networked source of potential pestware activity (Paragraph 0003: the analysis of audit records provides an exceptional degree of insight to determine what activity is "normal," and user actions can be compared against their expected roles within the system; Fig. 7: Obtain the IP address of a source of suspicious activity 701, 703).

Porras does not explicitly disclose but Borders from the same or similar fields of endeavor teaches an externally networked source (Borders, Paragraph 0187: a particular host inside a protected network to a particular host outside that network identified by URL; Paragraph 0118: a "wait for request on input stream" outputs to a "Does header contain suspicious values", a "Insert <time>-Previous <time> for same <source, destination> into delay list for <source, destination>", a "Size of contents> threshold?", a "Add size of contents to total bandwidth value for <source, destination>

over the past 24 hours" of block 314, a "Add size of contents to bandwidth counter for 5-minute intervals for <source, destination>") wherein

an indicia of pestware is being analyzed (Borders, Paragraph 0028: Low variation in bandwidth usage is indicative of abnormal or non-human activity. The plot of the coefficient of variation measurements for an 8-hour time period can been seen; Paragraph 0078: monitoring the data stream to detect a security threat based on a set of heuristics).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to identify a reference of an externally networked source as taught by Borders in the teachings of Porras for the advantage of monitoring the data stream to detect a security threat based on a set of heuristics related to legitimate, outbound, application layer messages, and generating a signal if a security threat is detected (Paragraph 0066).

Regarding claim 13, the combination of Porras and Borders discloses the system of claim 12, wherein the at least one log includes information that relates the time of interest to an event, and wherein the at least one log includes information that relates the event to a suspected pestware object, and wherein the at least one log includes information that relates the suspected pestware object to the at least one externally networked source of potential pestware activity (Porras, Paragraph 0015: source of the attack is identified using session identifier, IP address in the audit record or from the record that is obtained from network communication events).

Regarding claim 14, the combination of Porras and Borders discloses the system of claim 13, including: a heuristics module configured to evaluate whether the event is a suspected pestware-related event before the research portion accesses information in the at least one log that relates the event to the suspected pestware object (Porras, Paragraph 0013: based on the evaluation, preprocessor associates necessary information to the audit record before sending it to the IDS's (Intrusion Detection System) analysis engine where preprocessor functions as a heuristics module and analysis engine as a research portion, for example)

Regarding claim 15, the combination of Porras and Borders discloses the system of claim 14, wherein the heuristics module determines that the at least one event is suspected to be pestware-related by analyzing other events in connection with the event, wherein the other events are also related to the time of interest (Porras, Paragraph 0013: preprocessor associates related event information with suspected audit record and then provides the combined information to the analysis engine)

Regarding claim 16, the combination of Porras and Borders discloses the system of claim 12, wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs (Porras, Paragraph 0017: application

pathnames related to the suspicious process is obtained where pathnames includes file information, for example)

Regarding claim 19, the combination of Porras and Borders discloses the system of claim 12, wherein the timestamp module is configured to generate the time of interest as a time interval (Porras , Paragraph 0014: kernel audit records are received in real time and analyzed periodically to identify any suspicious activity from attacker).

Regarding claim 20, the combination of Porras and Borders discloses the system of claim 12, wherein the timestamp module is configured to generate the time of interest as a point in time (Porras , Paragraph 0014: kernel audit records are generated in real time, for example).

Regarding claim 21, the combination of Porras and Borders discloses the system of claim 12, including a kernel-mode driver adapted to monitor activity on the computer and to generate an activity log that is included within the at least one log (Porras, Paragraph 0014: kernel audit records are analyzed periodically or as needed basis to identify any suspicious activity from attacker; Paragraph 0015: session identifier recorded as a log entry in kernel audit records, for example).

Regarding claim 22, the combination of Porras and Borders discloses the system of claim 12, wherein the at least one externally networked source of potential

pestware activity is identified by an identifier selected from the group consisting of an I.P. address and a URL (Porras, Paragraph 0019: the IP address of a source of suspicious activity is acquired, and then associated with IDS alerts related to the suspicious activity)

Regarding claim 23, the combination of Porras and Borders discloses the system of claim 12, wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs (Porras, Paragraph 0017: network communication event in audit records; Paragraph 0017: application pathnames related to the suspicious process is obtained where pathnames includes file information, for example).

Conclusion

5. A reference to specific paragraphs, columns, pages, or figures in a cited prior art reference is not limited to preferred embodiments or any specific examples. It is well settled that a prior art reference, in its entirety, must be considered for all that it expressly teaches and fairly suggests to one having ordinary skill in the art. Stated differently, a prior art disclosure reading on a limitation of Applicant's claim cannot be ignored on the ground that other embodiments disclosed were instead cited. Therefore, the Examiner's citation to a specific portion of a single prior art reference is not intended to exclusively dictate, but rather, to demonstrate an exemplary disclosure

commensurate with the specific limitations being addressed. *In re Heck,* 699 F.2d 1331, 1332-33,216 USPQ 1038, 1039 (Fed. Cir. 1983) (quoting In re *Lemelson,* 397 F.2d 1006, 1009, 158 USPQ 275, 277 (CCPA 1968)). In re: *Upsher-Smith Labs. v. Pamlab, LLC,* 412 F.3d 1319, 1323, 75 USPQ2d 1213, 1215 (Fed. Cir. 2005); *In re Fritch,* 972 F.2d 1260, 1264, 23 USPQ2d 1780, 1782 (Fed. Cir. 1992); *Merck & Co. v. Biocraft Labs., Inc.,* 874 F.2d 804,807, 10 USPQ2d 1843, 1846 (Fed. Cir. 1989); *In re Fracalossi,* 681 F.2d 792,794 n.1,215 USPQ 569, 570 n.1 (CCPA 1982); *In re Lamberti, 545 F.2d 747, 750, 192 USPQ 278,280 (CCPA 1976); In re Bozek,* 416 F.2d 1385, 1390, 163 USPQ 545, 549 (CCPA 1969).

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

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 MAHFUZUR RAHMAN whose telephone number is (571)270-7638. The examiner can normally be reached on Monday thru Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T. Arani can be reached on (571)272-3787. 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.

/M. R./
Examiner, Art Unit 2438

/Thanhnga B. Truong/
Primary Examiner, Art Unit 2438
March 24, 2011

Notice of References Cited	Application/Control No. 11/408,145	Applicant(s)/Patent Under Reexamination BONEY, MATTHEW L.	
	Examiner MAHFUZUR RAHMAN	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,633,835 B1	10-2003	Moran et al.	702/190
*	B	US-2004/0064515 A1	04-2004	Hockey, Alyn	709/206
*	C	US-2004/0225877 A1	11-2004	Huang, Zezhen	713/100
*	D	US-2006/0136720 A1	06-2006	Armstrong et al.	713/164
*	E	US-2007/0094725 A1	04-2007	Borders, Kevin R.	726/022
	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.

Trend Micro, Inc.
EX1002-101

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11408145	BONEY, MATTHEW L.
	Examiner	Art Unit
	MAHFUZUR RAHMAN	2438

SEARCHED

Class	Subclass	Date	Examiner
726	22	3/22/2011	MR

SEARCH NOTES

Search Notes	Date	Examiner
East search, search terms used:(determin$5 or identif$4 or locat$3 or detect$3 or look$3 or find$3) with (source or origin$5 or network or outside or outsource or external$3 or remot$2 compromised or suspicious or suspected or abnormal or server or service or device or computer or outsource or resource) same (Identification or identity$3 or id or identifier or address or name)	3/23/2011	MR
Performed Inventor/Assignee name search	3/23/2011	MR
Keyword search of 726/22-25,13;713/187-188,193-194	3/23/2011	MR

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

/MAHFUZUR RAHMAN/ Examiner.Art Unit 2438	

Trend Micro, Inc.
EX1002-102

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	17	(US-20040024864-$ or US-20040064515-$ or US-20070016953-$ or US-20050268112-$ or US-20070250928-$ or US-20040225877-$ or US-20090158430-$ or US-20070094725-$ or US-20070168694-$ or US-20070220043-$ or US-20030159070-$ or US-20040034794-$ or US-20060136720-$).did. or (US-6633835-$ or US-6460060-$ or US-7480683-$).did. or (WO-9845778-$).did.	US-PGPUB; USPAT; EPO	OR	ON	2011/03/23 10:33
S2	17	(US-20090158430-$ or US-20070250928-$ or US-20070220043-$ or US-20070168694-$ or US-20070094725-$ or US-20070016953-$ or US-20060136720-$ or US-20050268112-$ or US-20040225877-$ or US-20040064515-$ or US-20040034794-$ or US-20040024864-$ or US-20030159070-$).did. or (US-7480683-$ or US-6633835-$ or US-6460060-$).did. or (WO-9845778-$).did.	US-PGPUB; USPAT; EPO	OR	ON	2011/03/23 10:33

S3	15	S2 and (determin$5 or identif$4 or locat$3 or detect$3 or look$3 or find $3) with (source or origin $5 or network or outside or outsource or external$3 or remot$2 compromised or suspicious or suspected server or service or device or computer) same (Identification or identity $3 or id or identifier or address or name)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 10:33
S4	14	S2 and (determin$5 or identif$4 or locat$3 or detect$3 or look$3 or find $3) with (source or origin $5 or network or outside or outsource or external$3 or remot$2 compromised or suspicious or suspected server or service or device or computer) with (Identification or identity $3 or id or identifier or address or name)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 10:33
S5	17	(US-20090158430-$ or US-20070250928-$ or US-20070220043-$ or US-20070168694-$ or US-20070094725-$ or US-20070016953-$ or US-20060136720-$ or US-20050268112-$ or US-20040225877-$ or US-20040064515-$ or US-20040034794-$ or US-20040024864-$ or US-20030159070-$).did. or (US-7480683-$ or US-6633835-$ or US-6460060-$).did. or (WO-9845778-$).did.	US-PGPUB; USPAT; EPO	OR	ON	2011/03/23 10:43

S6	14	S5 and (determin$5 or identif$4 or locat$3 or detect$3 or look$3 or find $3) with (source or origin $5 or network or outside or outsource or external$3 or remot$2 compromised or suspicious or suspected server or service or device or computer) with (Identification or identity $3 or id or identifier or address or name)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 10:43
S7	14	S6 and (@ad<"20060420" or rlad <"20060420")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 10:43
S8	14	S7 and (determin$5 or identif$4 or locat$3 or detect$3 or look$3 or find $3) with (source or origin $5 or network or outside or outsource or external$3 or remot$2 compromised or suspicious or suspected server or service or device or computer) with (Identification or identity $3 or id or identifier or address or name)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 10:45
S9	17	(US-20090158430-$ or US-20070250928-$ or US-20070220043-$ or US-20070168694-$ or US-20070094725-$ or US-20070016953-$ or US-20060136720-$ or US-20050268112-$ or US-20040225877-$ or US-20040064515-$ or US-20040034794-$ or US-20040024864-$ or US-20030159070-$).did. or (US-7480683-$ or US-6633835-$ or US-6460060-$).did. or (WO-9845778-$).did.	US-PGPUB; USPAT; EPO	OR	ON	2011/03/23 10:57
S10	17	S9 and (@ad<"20060420" or rlad <"20060420")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 11:01

S11	13	S9 and @ad<"20060420"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 11:05
S13	10	S6 and @ad<"20060420"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 11:05
S14	15	S9 and (@ad<"20060420" or @rlad <"20060420")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 11:09
S15	12	S6 and (@ad<"20060420" or @rlad <"20060420")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 11:09
S16	12	S15 and (period or time or interval or duration or period or periodically)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 11:14
S17	1	(US-20070094725-$).did.	US-PGPUB	OR	ON	2011/03/23 11:48
S18	14	boney near matthew.inv.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 13:04
S19	10	boney near "matthew.inv. and" pestware with reference same (source or origin)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 13:05
S20	3	boney near matthew.inv. and pestware with reference same (source or origin)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 13:05
S21	0	S20 and (@ad<"20060420" or @rlad <"20060420")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 13:05
S22	6	webroot.as. and pestware with reference same (source or origin)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 13:06
S23	0	S22 and (@ad<"20060420" or @rlad <"20060420")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 13:06
S24	1	726/22.ccls. and pestware with reference same (source or origin)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 13:07

S25	0	S24 and (@ad<"20060420" or @rlad <"20060420")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/03/23 13:07

EAST Search History (Interference)

< This search history is empty>

3/ 23/ 2011 4:33:00 PM
C:\ Documents and Settings\ mrahman4\ My Documents\ EAST\ Workspaces\ 31_Time Stamp to find Origin of Pestware_04202006_11408145\ 31_Exported from Tagged_RCE-1_Second Non Final_11408145.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11408145	BONEY, MATTHEW L.
	Examiner	**Art Unit**
	MAHFUZUR RAHMAN	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/15/2009	02/02/2010	09/08/2010	03/23/2011					
	1	✓	✓	✓	✓					
	2	✓	✓	✓	✓					
	3	✓	✓	✓	✓					
	4	✓	✓	✓	✓					
	5	✓	✓	✓	✓					
	6	✓	✓	✓	✓					
	7	✓	-	-	-					
	8	✓	✓	✓	✓					
	9	✓	-	-	-					
	10	✓	✓	✓	✓					
	11	✓	✓	✓	✓					
	12	✓	✓	✓	✓					
	13	✓	✓	✓	✓					
	14	✓	✓	✓	✓					
	15	✓	✓	✓	✓					
	16	✓	✓	✓	✓					
	17	✓	-	-	-					
	18	✓	-	-	-					
	19	✓	✓	✓	✓					
	20	✓	✓	✓	✓					
	21	✓	✓	✓	✓					
	22	✓	✓	✓	✓					
	23	✓	✓	✓	✓					

Trend Micro, Inc.
EX1002-108

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:	BONEY, Matthew L.	Confirmation No.:	8007
Serial No.:	11/408,145	Group Art Unit:	2438
Filed:	April 20, 2006	Examiner:	Mahfuzur RAHMAN

FOR: **BACKWARD RESEARCHING TIME STAMPED EVENTS TO FIND AN ORIGIN OF PESTWARE**

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

RESPONSE TO OFFICE ACTION

In response to the Official Action dated September 10, 2010 (the "Office Action"), please amend the above-identified patent application in the following manner:

Though no claims have been currently amended, a **Listing of Claims** has been included beginning on page 2 of this paper for the Examiner's convenience.

Remarks/Arguments begin on page 7 of this paper.

Trend Micro, Inc.
EX1002-109

LISTING OF CLAIMS:

Set forth below in ascending order, with status identifiers, is a complete listing of all claims currently under examination. This listing also reflects any cancellation and/or addition of claims.

1. (previously presented) A method for identifying an origin of suspected pestware activity on a computer, the method comprising:

receiving, from a user, a time of interest relating to a suspicion of pestware on the computer;

identifying, based upon the time of interest, indicia of pestware; and

accessing at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify, based at least in part upon the identified indicia of pestware, a reference to an identity of an externally networked source that is suspected of originating pestware.

2. (original) The method of claim 1, wherein the identifying includes:

accessing at least one log of historical events on the computer;

locating at least one event in the at least one log that corresponds to the time of interest; and

determining that the at least one event is associated with the indicia of pestware.

3. (original) The method of claim 2, wherein the determining that the at least one event is associated with the indicia of pestware includes following references in the at least one log to a suspected pestware object.

4. (original) The method of claim 3, wherein following the references includes following at least one reference in an activity log from the event to a suspected pestware process.

5. (original) The method of claim 4, wherein the activity log is generated from a kernel-mode driver.

6. (original) The method of claim 2, wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs.

7. (canceled)

8. (previously presented) The method of claim 1, wherein the user input is in response to an alert provided to the user regarding a detected suspicious activity on the computer.

9. (canceled)

10. (previously presented) The method of claim 1, including:

reporting the identity of the externally networked source to a pestware research entity so as to enable the pestware research entity to research whether the externally networked source is a source of pestware.

11. (previously presented) The method of claim 1, wherein the externally networked source is identified by an identifier selected from the group consisting of an I.P. address and a URL.

12. (previously presented) A system for identifying a source of suspected pestware on a computer, the system comprising:

a timestamp module configured to generate a time of interest in response to detected activity on the computer that is indicative of pestware;

a research portion configured to access at least one log on a file storage device of the computer to relate the time of interest to at least one externally networked source of potential pestware activity on the computer; and

a reporting portion configured to generate a report that identifies the at least one externally networked source of potential pestware activity.

13. (previously presented) The system of claim 12, wherein the at least one log includes information that relates the time of interest to an event, and wherein the at least one log includes information that relates the event to a suspected pestware object, and wherein the at least one log includes information that relates the suspected pestware object to the at least one externally networked source of potential pestware activity.

14. (original) The system of claim 13, including:

a heuristics module configured to evaluate whether the event is a suspected pestware-related event before the research portion accesses information in the at least one log that relates the event to the suspected pestware object.

15. (original) The system of claim 14, wherein the heuristics module determines that the at least one event is suspected to be pestware-related by analyzing other events in connection with the event, wherein the other events are also related to the time of interest.

16. (original) The system of claim 12, wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs

17.-18. (canceled)

19. (previously presented) The system of claim 12, wherein the timestamp module is configured to generate the time of interest as a time interval.

20. (previously presented) The system of claim 12, wherein the timestamp module is configured to generate the time of interest as a point in time.

21. (original) The system of claim 12, including a kernel-mode driver adapted to monitor activity on the computer and to generate an activity log that is included within the at least one log.

22. (previously presented) The system of claim 12, wherein the at least one externally networked source of potential pestware activity is identified by an identifier selected from the group consisting of an I.P. address and a URL.

23. (original) The system of claim 12, wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs.

REMARKS

No claims have been currently amended, added, or cancelled. Claims 7, 9, and 17-18 were canceled previously. Each of claims 1-6, 8, 10-16, and 19-23 thus remains pending.

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

The Office Action rejects claims 1-6, 8, 10-16, and 19-23 under 35 U.S.C. § 103(a) as being unpatentable over Porras et al. (U.S. Publ. No. 2004/0024864, hereinafter "Porras") in view of Maddaloni et al. (U.S. Publ. No. 2007/0168694, hereinafter "Maddaloni").

Maddaloni is disqualified as prior art under 35 U.S.C. § 103(c). All of the rejections above rely on the combination of Porras and Maddaloni. However, Maddaloni is not an eligible reference upon which a *prima facie* case of obviousness can be based. First, Applicant notes that Maddaloni qualifies as potential prior art only under § 102(e). Second, Maddaloni and the subject matter claimed in the instant application, at the time the instant invention was made, were both owned by the same entity—Webroot, Inc. Therefore, Maddaloni is disqualified as prior art under 35 U.S.C. § 103(c)(1). An assignment of the entire right, title, and interest in Maddaloni to Webroot is recorded at reel/frame 020706/0197. Likewise, an assignment of the entire right, title, and interest in the instant application to Webroot is recorded at reel/frame 017986/0435. Copies of the USPTO assignment recordation receipts for Maddaloni and the instant application are included herewith. The other applied reference, Porras, does not teach or suggest all of the limitations recited in the independent claims. Therefore, Porras can neither anticipate the claims nor render them obivous. Applicant respectfully requests withdrawal of the rejection, under § 103(a), of each of claims 1-6, 8, 10-16, and 19-23.

Trend Micro, Inc.
EX1002-115

CONCLUSION

In view of the foregoing, Applicant respectfully submits that no further impediments exist to the allowance of this application and, therefore, requests an indication of allowability. However, the Examiner is requested to call the undersigned if any questions or comments arise.

The Director is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.16, 1.17, and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 50-1283.

COOLEY LLP
ATTN: Patent Group
777 6th Street NW, Suite 1100
Washington, DC 20001

Tel: (720) 566-4106
Fax: (202) 842-7899

Respectfully submitted,
COOLEY LLP

By: _____
Mark R. Schafer
Reg. No. 65,336

Electronic Patent Application Fee Transmittal

Application Number:	11408145
Filing Date:	20-Apr-2006
Title of Invention:	Backward researching time stamped events to find an origin of pestware
First Named Inventor/Applicant Name:	Matthew L. Boney
Filer:	Mark Randolph Schafer/Sherry Bitler
Attorney Docket Number:	WEBR-045/00US 303666-2050

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:				
Extension - 2 months with $0 paid	1252	1	490	490

Trend Micro, Inc.
EX1002-117

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**490**

Electronic Acknowledgement Receipt

EFS ID:	9292635
Application Number:	11408145
International Application Number:	
Confirmation Number:	8007
Title of Invention:	Backward researching time stamped events to find an origin of pestware
First Named Inventor/Applicant Name:	Matthew L. Boney
Customer Number:	22903
Filer:	Mark Randolph Schafer/Sherry Bitler
Filer Authorized By:	Mark Randolph Schafer
Attorney Docket Number:	WEBR-045/00US 303666-2050
Receipt Date:	24-JAN-2011
Filing Date:	20-APR-2006
Time Stamp:	21:17:30
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$490
RAM confirmation Number	6852
Deposit Account	501283
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	Applicant Arguments/Remarks Made in an Amendment	WEBR04500US-2011-01-24-roa.pdf	257963 a93852a66cedcfdb291cdb1088b408623f7785c0	no	8
Warnings:					
Information:					
2	Fee Worksheet (PTO-875)	fee-info.pdf	30292 759bf80cb7519bd9426dad3e9f646b07c5a08335	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	288255		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
11/408,145	04/20/2006	

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☐ RATE ($)	SMALL ENTITY ☐ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
FOR	NUMBER FILED	NUMBER EXTRA					
☐ 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), (i), 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.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	01/24/2011	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 19	Minus	** 23	= 0	X $ =		OR	X $52=	0
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $ =		OR	X $220=	0
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	0

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) 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))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/ANNETTE SMITH/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/408,145	04/20/2006	Matthew L. Boney	WEBR-045/00US 303666-2050	8007

22903 7590 09/10/2010

COOLEY LLP
ATTN: PATENT GROUP
Suite 1100
777 - 6th Street, NW
WASHINGTON, DC 20001

EXAMINER	
RAHMAN, MAHFUZUR	

ART UNIT	PAPER NUMBER
2438	

MAIL DATE	DELIVERY MODE
09/10/2010	PAPER

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.

Office Action Summary	Application No.	Applicant(s)	
	11/408,145	BONEY, MATTHEW L.	
	Examiner	Art Unit	
	MAHFUZUR RAHMAN	2438	

-- 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 *20 August 2010*.

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

3)☐ 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

4)☒ Claim(s) *1-6,8,10-16 and 19-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8,10-16 and 19-23* is/are rejected.

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

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

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

10)☒ The drawing(s) filed on *20 April 2006* 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).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

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. _____.

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) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Trend Micro, Inc.
EX1002-123

DETAILED ACTION

Applicant's amendment filed 08/20/2010 is acknowledged. Claims 1, 10-13, and 22 have been amended. Claims 1-6, 8, 10-16, and 19-23 are examined and are pending.

Continued Examination Under 37 CFR 1.114

1. 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 10/30/2009 has been entered.

Response to Arguments

2. Applicants amendment to claims filed on August 20, 2010 necessitated a new ground of rejection presented in this Office Action. The previously presented rejections have changed because the new limitations “an externally networked source” have been added to the above mentioned claims. Thus applicant’s arguments filed on August 20, 2010 have been rendered moot in view of the new ground(s) of rejection. The reference

of Maddaloni has been introduced to the references of Porras to address the newly added limitations. The reasons of obviousness are included below in this office action.

Claims 1-6, 8, 10-16, and 19-23 are now rejected under 35 U.S.C. 103(a) as being unpatentable over Porras et al. (US 2004/0024864 A1, hereinafter, Porras) in view of Maddaloni et al. (US 2007/0168694 A1, hereinafter, Maddaloni).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. 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.

5. Claims 1-6, 8, 10-16, and 19-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Porras et al. (US 2004/0024864 A1, hereinafter, Porras) in view of Maddaloni et al. (US 2007/0168694 A1, hereinafter, Maddaloni).

Regarding claim 1, Porras discloses a method for identifying an origin of suspected pestware activity on a computer, the method comprising:

[receiving, from a user, a time of interest] relating to a suspicion of pestware on the computer (Paragraph 0014: generating audit records that are analyzed periodically or as needed basis to identify any suspicious activity that is responsible for a potential attack on a host a computer);

identifying, based upon the time of interest, [indicia] of pestware (Paragraph 0017: If an IDS identifies the process as suspicious, the pathnames of applications invoked by the process are associated with IDS alerts related to the suspicious process; Paragraph 0019: the IP address of a source of suspicious activity is acquired and then associated with IDS alerts related to the suspicious activity);

and accessing at least a portion of a recorded history of [externally networked] sources (Paragraph 0015: audit-record that records the IP address of the source)

that the computer received files from so as to identify, based at least in part upon the identified indicia of pestware, a reference to an identity of an externally networked source that is suspected of originating pestware (Paragraph 0019: the IP address of a source of suspicious activity is acquired and then associated with IDS alerts related to the suspicious activity).

Porras does not explicitly disclose but Maddaloni from the same or similar fields of endeavor teaches an indicia of pestware (Maddaloni, Paragraph 0028: identify any suspect entries that are indicia of potential pestware activity) and

an externally networked source (Maddaloni, Paragraph 0033: pestware definitions and/or updated anti-pestware code to be retrieved from the external memory source 130; Fig. 1 External Networked Source 130) wherein

time of interest is received by user (Maddaloni, Paragraph 0045: second anti-pestware module 342 scans at predetermined time intervals, when a predetermined event occurs, and/or in response to a user's direction)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use an indicia of pestware and externally networked source as taught by Maddaloni in the teachings of Porras for the advantage of identifying and remove pestware in a convenient manner such as managing pestware utilizing an operating system that is secondary to a primary operating system of a computer (Paragraphs 0005, 0016).

Regarding claim 2, the combination of Porras and Maddaloni discloses the method of claim 1, wherein the identifying includes: accessing at least one log of historical events on the computer; locating at least one event in the at least one log that corresponds to the time of interest; and determining that the at least one event is associated with the indicia of pestware (Porras, Paragraph 0015: audit record wherein network communication event and process session associated with a session identifier are recorded).

Regarding claim 3, the combination of Porras and Maddaloni discloses the method of claim 2, wherein the determining that the at least one event is associated with the indicia of pestware includes following references in the at least one log to a suspected pestware object (Porras, Paragraph 0015: Intrusion Detection System determines that session is part of an attack via IP address of source or a session identifier).

Regarding claim 4, the combination of Porras and Maddaloni discloses the method of claim 3, wherein following the references includes following at least one reference in an activity log from the event to a suspected pestware process (Porras, Paragraph 0015: source of the attack is identified using session identifier and IP address in the audit record or the record that is obtained from network communication events)

.

Regarding claim 5, the combination of Porras and Maddaloni discloses the method of claim 4, wherein the activity log is generated from a kernel-mode driver (Porras , Paragraph 0015: session identifier of a suspicious activity is recorded as a log entry in kernel audit records, for example).

Regarding claim 6, the combination of Porras and Maddaloni discloses the method of claim 2 wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser

settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs (Porras , Paragraph 0017: application pathnames related to the suspicious process is obtained where pathnames includes file information, for example).

Regarding claim 8, the combination of Porras and Maddaloni discloses the method of claim 1, wherein the user input is in response to an alert provided to the user regarding a detected suspicious activity on the computer (Porras, Paragraph 0017: IDS operator or system administrator takes selective action once the alert is generated regarding any suspicious activity from attacker; Page 3 lines 20-23: response to a suspicious activity).

Regarding claim 10, the combination of Porras and Maddaloni discloses the method of claim 1, including: reporting the identity of the externally networked source to a pestware research entity so as to enable the pestware research entity to research whether the externally networked source is a source of pestware (Porras , Paragraph 0013: preprocessor associates necessary information to audit record and reports it to the analysis engine so the source that is responsible for attack can be identified; Paragraph 0019: the IP address of a source of suspicious activity is acquired , and then associated with IDS alerts related to the suspicious activity).

Regarding claim 11, the combination of Porras and Maddaloni discloses the method of claim 1, wherein the externally networked source is identified by an identifier selected from the group consisting of an I.P. address and a URL (Porras, Paragraph 0019: the IP address of a source of suspicious activity is acquired, and then associated with IDS alerts related to the suspicious activity).

Regarding claim 12, Porras discloses a system for identifying a source of suspected pestware on a computer, the system comprising:

a timestamp module configured to generate a [time of interest] in response to detected activity on the computer that is indicative of pestware (Paragraph 0014: generating audit records that are analyzed periodically or as needed basis to identify any suspicious activity that is responsible for a potential attack on a host a computer; Paragraph 0019: the IP address of a source of suspicious activity is acquired and then associated with IDS alerts related to the suspicious activity)

a research portion configured to access at least one log on a file storage device of the computer to relate the time of interest to at least one [externally networked source] of potential pestware activity on the computer (Paragraph 0013: analysis engine determines if an intrusion or attack has taken place by analyzing audit records where analysis engine acts as a research portion of the Intrusion Detection System, for example; Paragraph 0019: the IP address of a source of suspicious activity is acquired and then associated with IDS alerts related to the suspicious activity); and

a reporting portion configured to generate a report that identifies the at least one externally networked source of potential pestware activity (Paragraph 0003: the analysis of audit records provides an exceptional degree of insight to determine what activity is "normal," and user actions can be compared against their expected roles within the system; Fig. 7: Obtain the IP address of a source of suspicious activity 701, 703).

Porras does not explicitly disclose but Maddaloni from the same or similar fields of endeavor teaches an externally networked source (Maddaloni, Paragraph 0033: pestware definitions and/or updated anti-pestware code to be retrieved from the external memory source 130; Fig. 1 External Networked Source 130) and

time of interest directed by a user (Maddaloni, Paragraph 0045: second anti-pestware module 342 scans at predetermined time intervals, when a predetermined event occurs, and/or in response to a user's direction) wherein

an activity that is indicative of pestware is detected (Maddaloni, Paragraph 0028: identify any suspect entries that are indicia of potential pestware activity)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use an indicia of pestware and externally networked source as taught by Maddaloni in the teachings of Porras for the advantage of managing pestware utilizing an operating system that is secondary to a primary operating system of a computer so the anti-pestware application or service is able to effectively carry out its functions using the secondary operating system (Paragraphs 0016, 0019).

Regarding claim 13, the combination of Porras and Maddaloni discloses the system of claim 12, wherein the at least one log includes information that relates the time of interest to an event, and wherein the at least one log includes information that relates the event to a suspected pestware object, and wherein the at least one log includes information that relates the suspected pestware object to the at least one externally networked source of potential pestware activity (Porras, Paragraph 0015: source of the attack is identified using session identifier, IP address in the audit record or from the record that is obtained from network communication events).

Regarding claim 14, the combination of Porras and Maddaloni discloses the system of claim 13, including: a heuristics module configured to evaluate whether the event is a suspected pestware-related event before the research portion accesses information in the at least one log that relates the event to the suspected pestware object (Porras, Paragraph 0013: based on the evaluation, preprocessor associates necessary information to the audit record before sending it to the IDS's (Intrusion Detection System) analysis engine where preprocessor functions as a heuristics module and analysis engine as a research portion, for example)

Regarding claim 15, the combination of Porras and Maddaloni discloses the system of claim 14, wherein the heuristics module determines that the at least one event is suspected to be pestware-related by analyzing other events in connection with the event, wherein the other events are also related to the time of interest (Porras,

Paragraph 0013: preprocessor associates related event information with suspected audit record and then provides the combined information to the analysis engine)

Regarding claim 16, the combination of Porras and Maddaloni discloses the system of claim 12, wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs (Porras, Paragraph 0017: application pathnames related to the suspicious process is obtained where pathnames includes file information, for example)

Regarding claim 19, the combination of Porras and Maddaloni discloses the system of claim 12, wherein the timestamp module is configured to generate the time of interest as a time interval (Porras , Paragraph 0014: kernel audit records are received in real time and analyzed periodically to identify any suspicious activity from attacker).

Regarding claim 20, the combination of Porras and Maddaloni discloses the system of claim 12, wherein the timestamp module is configured to generate the time of interest as a point in time (Porras , Paragraph 0014: kernel audit records are generated in real time, for example).

Regarding claim 21, the combination of Porras and Maddaloni discloses the system of claim 12, including a kernel-mode driver adapted to monitor activity on the computer and to generate an activity log that is included within the at least one log (Porras, Paragraph 0014: kernel audit records are analyzed periodically or as needed basis to identify any suspicious activity from attacker; Paragraph 0015: session identifier recorded as a log entry in kernel audit records, for example).

Regarding claim 22, the combination of Porras and Maddaloni discloses the system of claim 12, wherein the at least one externally networked source of potential pestware activity is identified by an identifier selected from the group consisting of an I.P. address and a URL (Porras, Paragraph 0019: the IP address of a source of suspicious activity is acquired, and then associated with IDS alerts related to the suspicious activity)

Regarding claim 23, the combination of Porras and Maddaloni discloses the system of claim 12, wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs (Porras, Paragraph 0017: network communication event in audit records; Paragraph 0017: application pathnames related to the suspicious process is obtained where pathnames includes file information, for example).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Oliver et al. US 2007/0220043 A1 discloses determination of related entities.
- Geis et al. US 2003/0065943 A1 discloses method and apparatus for recognizing and reacting to denial of service attacks on a computerized network.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MAHFUZUR RAHMAN whose telephone number is (571)270-7638. The examiner can normally be reached on Monday thru Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T. Arani can be reached on (571) - 272-3787. 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.

/M. R./

Examiner, Art Unit 2438

/Taghi T. Arani/
Supervisory Patent Examiner, Art Unit 2438

Notice of References Cited	Application/Control No. 11/408,145	Applicant(s)/Patent Under Reexamination BONEY, MATTHEW L.	
	Examiner MAHFUZUR RAHMAN	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2003/0065943 A1	04-2003	Geis et al.	713/201
*	B	US-2003/0159070 A1	08-2003	Mayer et al.	713/201
*	C	US-2007/0168694 A1	07-2007	Maddaloni et al.	714/004
*	D	US-2007/0220043 A1	09-2007	Oliver et al.	707/103.R
	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.

Trend Micro, Inc.
EX1002-137

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11408145	BONEY, MATTHEW L.
	Examiner	Art Unit
	MAHFUZUR RAHMAN	2438

SEARCHED

Class	Subclass	Date	Examiner
726	22	9/7/2010	MR

SEARCH NOTES

Search Notes	Date	Examiner
East search, search terms used: (origin$5 or source or target$ or destination or root) same (external or outside or network or inside or separate or outside or out adj side or inside or outer or third or remote); (pestware maleware spamware adware scumware) and (timestamp or duration or time or period) same (user or client) same event	9/7/2010	MR
Performed Inventor/Assignee name search	9/7/2010	MR
Keyword search of 726/22-25,13;713/187-188,193-194	9/7/2010	MR

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

/MAHFUZUR RAHMAN/ Examiner.Art Unit 2438	

Trend Micro, Inc.
EX1002-138

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	5	(US-20070168694-$ or US-20040024864-$ or US-20050268112-$ or US-20040225877-$ or US-20070220043-$).did.	US-PGPUB	OR	ON	2010/09/08 10:52
L5	5	1 and (origin$5 or source or target$ or destination or root) same (external or outside or network or inside or separate or outside or out adj side or inside or outer or third or remote)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2010/09/08 11:01
L6	109	(pestware maleware spamware adware scumware) and (timestamp or duration or time or period) same (user or client) same event	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2010/09/08 11:40
L7	2	5 and (pestware maleware spamware adware scumware) and (timestamp or duration or time or period) same (user or client) same event	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2010/09/08 11:40
L8	1	5 and indicia	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2010/09/08 11:52
L18	1	(US-20040024864-$).did.	US-PGPUB	OR	ON	2010/09/08 12:08
L19	1	18 and (timestamp or duration or time or period) same (user or client)	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2010/09/08 12:08
L20	1	18 and (timestamp or duration or time or period)	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2010/09/08 12:09
L30	24	zuta.in.	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2010/09/08 13:45

L149	105	("20020078381" | "20020162015" | "20020162017" | "20020166063" | "20030065943" | "20030074581" | "20030101381" | "20030159070" | "20030217287" | "20040024864" | "20040030914" | "20040034794" | "20040064515" | "20040064736" | "20040080529" | "20040143763" | "20040187023" | "20040225877" | "20050005160" | "20050038697" | "20050138433" | "20050154885" | "20050268112" | "20050268112" | "20060075494" | "20060075501" | "20060161988" | "5623600" | "5920696" | "5951698" | "6069628" | "6073241" | "6092194" | "6154844" | "6167520" | "6310630" | "6397264" | "6405316" | "6460060" | "6480962" | "6535931" | "6611878" | "6633835" | "6667751" | "6701441" | "6772345" | "6785732" | "6804780" | "6813711" | "6829654" | "6910134" | "6965968" | "7058822" | "7107617").PN.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2010/09/08 13:45
L150	2	(US-20040024864-$ or US-20050268112-$).did.	US-PGPUB	OR	ON	2010/09/08 13:45
L151	1	L150 and (respon$4 or provid$3 or generat$3) same request$3 same record	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2010/09/08 13:45
L152	1	L150 and (respon$4 or provid$3 or generat$3) same request$3	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2010/09/08 13:45
L153	2	L150 and user same (respon$4 or provid$3 or generat$3)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2010/09/08 13:45

L154	15	L149 and user same (request$3 or send$3 or receiv$3) same time same2 (respons$4 or generat$3 or provid$3)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2010/09/08 13:45
L162	64279	(user or client) near4 request$3 with time Identif $4 and suspici$3	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2010/09/08 13:45
L163	294	(user or client) near4 request$3 with time same Identif$4 and suspici$3	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2010/09/08 13:45
L164	294	L163 and (@ad<"20060420" or rlad <"20060420")	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2010/09/08 13:45
L165	146	L164 and intrusion	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2010/09/08 13:45
L166	7	L165 and (pestware or maleware or spyware)	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2010/09/08 13:45
S18	7684	726/22-25,13;713/187-188,193-194.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2009/06/15 14:27
S19	21	S18 and ((token indicia sign$5) same (pestware maleware spamware adware scumware))	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2009/06/15 14:30
S20	21	S19 and (@ad<"20060420" or rlad <"20060420")	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2009/06/15 14:32
S25	21	S18 and ((token indicia sign$5) same (pestware maleware spamware adware scumware))	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2009/06/15 15:03
S26	19	S20 and (time period)	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2009/06/15 15:03
S27	19	S25 and (time period)	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2009/06/15 15:04
S28	2	S27 and (time$1stamp "time stamp")	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2009/06/15 15:10
S54	58580	(user or client) near4 request$3 with time Identif $4 and suspici$3	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2010/02/02 19:16

S55	283	(user or client) near4 request$3 with time same Identif$4 and suspici$3	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2010/02/02 19:16
S56	283	S55 and (@ad<"20060420" or rlad<"20060420")	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2010/02/02 19:17
S57	143	S56 and intrusion	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2010/02/02 19:17
S58	7	S57 and (pestware or maleware or spyware)	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2010/02/02 19:18
S172	11	(US-20040024864-$ or US-20040064515-$ or US-20070016953-$ or US-20050268112-$ or US-20070250928-$ or US-20040225877-$ or US-20090158430-$ or US-20070094725-$).did. or (US-6633835-$ or US-6460060-$).did. or (WO-9845778-$).did.	US-PGPUB; USPAT; EPO	OR	ON	2010/09/07 18:52
S173	13524	"11" and (External or outside) same network same origin$5	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2010/09/07 18:53
S174	1	S172 and (External or outside) same network same origin$5	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2010/09/07 18:53
S175	61	("20020166063" | "20030065943" | "20030074581" | "20030101381" | "20030159070" | "20030217287" | "20040030914" | "20040034794" | "20040064736" | "20040080529" | "20040143763" | "20040187023" | "20040225877" | "20050138433" | "20050268112" | "20060074896" | "20060085528" | "20060272021" | "5442669" | "5485575" | "5623600" | "5696822" | "5826013" | "5951698" | "5987611" | "6069628" | "6073241" | "6092194" | "6154844" | "6167520" |	US-PGPUB; USPAT; USOCR	OR	ON	2010/09/07 18:54

		"6192512" | "6253258" | "6310630" | "6357008" | "6397264" | "6405316" | "6457174" | "6460060" | "6473406" | "6480962" | "6535931" | "6611878" | "6633835" | "6667751" | "6681972" | "6701441" | "6735703" | "6772345" | "6775780" | "6785732" | "6804780" | "6813711" | "6829654" | "6851057" | "6910134" | "6965968" | "7058822" | "7107617" | "7210168").PN. OR ("7480683").URPN.				
S176	4	S175 and (External or outside) same network same origin$5	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2010/09/07 18:54
S177	42	pestware and (External or outside or network or website or url) same (origin $5 or source)	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2010/09/07 19:08
S178	30	pestware and (External or outside or network or website or url) same (origin $5 or source)and (timestamp or duration or time or period) same (user or client)	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2010/09/07 19:10
S179	30	S178 and (@ad<"20060420" or rlad <"20060420")	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2010/09/07 19:11
S180	4	pestware and (External or outside or network or website or url) same (origin $5 or source)and (timestamp or duration or time or period) same (user or client) same event	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2010/09/07 19:12

EAST Search History (Interference)

< This search history is empty>

9/8/2010 2:00:26 PM
C:\ Documents and Settings\ mrahman4\ My Documents\ EAST\ Workspaces\ 31_Time Stamp to find Origin of Pestware_04202006_11408145\ 30_Time Stamp to find Origin of Pestware_04202006_11408145.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11408145	BONEY, MATTHEW L.
	Examiner	Art Unit
	MAHFUZUR RAHMAN	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/15/2009	02/02/2010	09/08/2010						
	1	✓	✓	✓						
	2	✓	✓	✓						
	3	✓	✓	✓						
	4	✓	✓	✓						
	5	✓	✓	✓						
	6	✓	✓	✓						
	7	✓	-	-						
	8	✓	✓	✓						
	9	✓	-	-						
	10	✓	✓	✓						
	11	✓	✓	✓						
	12	✓	✓	✓						
	13	✓	✓	✓						
	14	✓	✓	✓						
	15	✓	✓	✓						
	16	✓	✓	✓						
	17	✓	-	-						
	18	✓	-	-						
	19	✓	✓	✓						
	20	✓	✓	✓						
	21	✓	✓	✓						
	22	✓	✓	✓						
	23	✓	✓	✓						

Trend Micro, Inc.
EX1002-144

PTO/SB/30 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995. no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Request for Continued Examination (RCE) Transmittal

Address to:
Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Application Number	11/408,145
Filing Date	04/20/2006
First Named Inventor	BONEY, Matthew L.
Art Unit	2438
Examiner Name	RAHMAN, Mahfuzur
Attorney Docket Number	WEBR-045/00US 303666-2050

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. See Instruction Sheet for RCEs (not to be submitted to the USPTO) on page 2.

1. 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).

   a. ☐ 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.

      i. ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

      ii. ☐ Other _____

   b. ☒ Enclosed

      i. ☒ Amendment/Reply

      ii. ☐ Affidavit(s)/ Declaration(s)

      iii. ☐ Information Disclosure Statement (IDS)

      iv. ☐ Other _____

2. Miscellaneous

   Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a

   a. ☐ period of ___ months. (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

   b. ☐ Other _____

3. 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 the following fees any underpayment of fees or credit any overpayments to

   a. ☒ Deposit Account No. 50-1283 .

      i. ☒ RCE fee required under 37 CFR 1.17(e)

      ii ☒ Extension of time fee (37 CFR 1.136 and 1.17)

      iii ☐ Other _____

   b. ☐ Check in the amount of $ _____ enclosed

   c. ☐ Payment by credit card (Form PTO-2038 enclosed)

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.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Signature	/s. Thomas M. Croft/	Date	2010-08-20
Name (Print/Type)	Thomas M. Croft	Registration No.	44,051

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. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop RCE, 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.

American LegalNet, Inc.
www.FormsWorkFlow.com

Trend Micro, Inc.
EX1002-145

Attorney Docket No. WEBR-045/00US 303666-2050 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:	BONEY, Matthew L.	Confirmation No.:	8007
Serial No.:	11/408,145	Group Art Unit:	2438
Filed:	April 20, 2006	Examiner:	Mahfuzur RAHMAN

FOR: **BACKWARD RESEARCHING TIME STAMPED EVENTS TO FIND AN ORIGIN OF PESTWARE**

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

AMENDMENT/RESPONSE TO OFFICE ACTION

In response to the Final Official Action dated February 22, 2010, please amend the above-identified patent application in the following manner:

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

Remarks/Arguments begin on page 7 of this paper.

Trend Micro, Inc.
EX1002-146

AMENDMENTS TO THE CLAIMS:

Set forth below in ascending order, with status identifiers, is a complete listing of all claims currently under examination. Changes to any amended claims are indicated by strikethrough, brackets, and underlining. This listing also reflects any previous cancellation and/or addition of claims.

1. (currently amended) A method for identifying an origin of suspected pestware activity on a computer, the method comprising:

receiving, from a user, a time of interest relating to a suspicion of pestware on the computer;

identifying, based upon the time of interest, indicia of pestware; and

accessing at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify, based at least in part upon the identified indicia of pestware, a reference to an identity of [[a]] an externally networked source that is suspected of originating pestware.

2. (original) The method of claim 1, wherein the identifying includes:

accessing at least one log of historical events on the computer;

locating at least one event in the at least one log that corresponds to the time of interest; and

determining that the at least one event is associated with the indicia of pestware.

3. (original) The method of claim 2, wherein the determining that the at least one event is associated with the indicia of pestware includes following references in the at least one log to a suspected pestware object.

4. (original) The method of claim 3, wherein following the references includes following at least one reference in an activity log from the event to a suspected pestware process.

5. (original) The method of claim 4, wherein the activity log is generated from a kernel-mode driver.

6. (original) The method of claim 2, wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs.

7. (canceled)

8. (previously presented) The method of claim 1, wherein the user input is in response to an alert provided to the user regarding a detected suspicious activity on the computer.

9. (canceled)

10. (currently amended) The method of claim 1, including:

reporting the identity of the externally networked source to a pestware research entity so as to enable the pestware research entity to research whether the externally networked source is a source of pestware.

11. (currently amended) The method of claim 1, wherein the externally networked source is identified by an identifier selected from the group consisting of an I.P. address[[,]] and a URL~~, an email client and a program name~~.

12. (currently amended) A system for identifying a source of suspected pestware on a computer, the system comprising:

a timestamp module configured to generate a time of interest in response to detected activity on the computer that is indicative of pestware;

a research portion configured to access at least one log on a file storage device of the computer to relate the time of interest to at least one externally networked source of potential pestware activity on the computer; and

a reporting portion configured to generate a report that identifies the at least one externally networked source of potential pestware activity.

13. (currently amended) The system of claim 12, wherein the at least one log includes information that relates the time of interest to an event, and wherein the at least one log includes information that relates the event to a suspected pestware object, and wherein the at least one log includes information that relates the suspected pestware object to the at least one externally networked source of potential pestware activity.

14. (original) The system of claim 13, including:

a heuristics module configured to evaluate whether the event is a suspected pestware-related event before the research portion accesses information in the at least one log that relates the event to the suspected pestware object.

15. (original) The system of claim 14, wherein the heuristics module determines that the at least one event is suspected to be pestware-related by analyzing other events in connection with the event, wherein the other events are also related to the time of interest.

16. (original) The system of claim 12, wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs

17.-18. (canceled)

19. (previously presented) The system of claim 12, wherein the timestamp module is configured to generate the time of interest as a time interval.

20. (previously presented) The system of claim 12, wherein the timestamp module is configured to generate the time of interest as a point in time.

21. (original) The system of claim 12, including a kernel-mode driver adapted to monitor activity on the computer and to generate an activity log that is included within the at least one log.

22. (currently amended) The system of claim 12, wherein the at least one externally networked source of potential pestware activity is identified by an identifier selected from the group consisting of an I.P. address[[,]] and a URL~~, an email client and a program name~~.

23. (original) The system of claim 12, wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs.

REMARKS

Claims 1, 10-13, and 22 have been currently amended. No new claims have been added. Claims 1-6, 8, 10-16, and 19-23 thus remain pending in the application

Claim Rejections

The Office Action rejects claims 1-6, 8, 10-16, and 19-23 under 35 U.S.C. § 103(a) as being unpatentable over Porras et al. (U.S. 2004/0024864, hereinafter "Porras") in view of Wang et al. (U.S. 2005/0268112, hereinafter "Wang") and in further view of Huang (U.S. 2004/0225877, hereinafter "Huang").

Applicant believes that independent claims 1 and 12, as currently amended, recite limitations neither taught nor suggested by Porras, Wang, or Huang.

Claim 1. Currently amended independent claim 1 recites "accessing at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify, based at least in part upon the identified indicia of pestware, a reference to an identity of an externally networked source that is suspected of originating pestware." Porras, however, pertains to "host-based intrusion detection systems." Porras, Para. 001. Such host-based intrusion detection systems involve analyzing audit records which "include information about system calls (operating system routines executed on the host computer), and may include some information about sessions (the communications between a user or process and the host computer during a connection)." Porras, Para. 0002. More specifically, Porras relates to identifying "a user, process, or application" of a host computer and taking "action against *only* those sessions and applications that are related to an attack" on the host computer. Porras, Para. 0005 (emphasis added). In other words, Porras is expressly limited to finding and taking action, on the host computer, against only the host computer session that attacks the host computer. The

universe of activity in Porras is limited to the confines of the host computer and its user sessions and process sessions.

Currently amended claim 1, on the other hand, recites "to identify . . . a reference to an identity of an *externally networked source* that is suspected of *originating* pestware" (emphasis added). Porras is interested not in an externally networked source suspected of originating an attack (e.g., an Internet URL or Web site from which the pestware was downloaded), but in the internal network's user or process session through which the attack is made (i.e., the local "victim" of the attack). Porras, Wang, and Huang, whether separately or in combination, do not teach or suggest the above-quoted limitation. Applicant notes that the current amendments to claim 1 are amply supported at, e.g., Paragraphs 0016 and 0046 of the specification as originally filed. No new matter has been introduced by way of the current amendments.

Porras, Wang, and Huang, whether taken separately or in combination, fail to teach or suggest each and every limitation recited in currently amended claim 1. As a result, the cited references cannot render claim 1 obvious under § 103(a), and Applicant believes claim 1 to be allowable. Each of dependent claims 2-6, 8, and 10-11 is thus also allowable at least by virtue of its depending from allowable claim 1. Withdrawal of the rejection, under § 103(a), of claims 1-6, 9, and 10-11 is respectfully requested.

Claim 12. Currently amended independent claim 12 recites "a research portion configured to access at least one log on a file storage device of the computer to relate the time of interest to at least one externally networked source of potential pestware activity on the computer." Similar to the argument above in connection with claim 1, Porras is not interested in the actual source that is suspected of originating an attack. It is interested only in activity in the internal network, specifically the user sessions or process sessions within a host computer, and

limiting any action taken to those sessions. Porras is silent regarding the actual source suspected of originating potential pestware activity. Applicant notes that the current amendments to claim 12 are amply supported at, e.g., Paragraphs 0016 and 0046 of the specification as originally filed. No new matter has been introduced by way of the current amendments.

Porras, Wang, and Huang, whether taken separately or in combination, fail to teach or suggest each and every limitation recited in claim 12. As a result, the cited references cannot render claim 12 obvious under § 103(a), and Applicant believes claim 1 to be allowable. Each of dependent claims 13-16 and 19-23 is thus also allowable at least by virtue of its depending from allowable claim 12. Withdrawal of the rejection, under § 103(a), of claims 12-16 and 19-23 is respectfully requested.

Request for Continued Examination

Applicant has filed herewith a Request for Continued Examination (RCE) under 37 C.F.R. § 1.114.

CONCLUSION

In view of the foregoing, Applicant respectfully submits that no further impediments exist to the allowance of this application and, therefore, requests an indication of allowability. However, the Examiner is requested to call the undersigned if any questions or comments arise.

The Director is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.16, 1.17, and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 50-1283.

COOLEY LLP
ATTN: Patent Group
777 6th Street NW, Suite 1100
Washington, DC 20001

Tel: (720) 566-4044
Fax: (202) 842-7899

Respectfully submitted,
COOLEY LLP

By: Thomas M. Croft

Thomas M. Croft
Reg. No. 44,051

Electronic Patent Application Fee Transmittal

Application Number:	11408145
Filing Date:	20-Apr-2006
Title of Invention:	Backward researching time stamped events to find an origin of pestware
First Named Inventor/Applicant Name:	Matthew L. Boney
Filer:	Thomas M. Croft/Sherry Bitler
Attorney Docket Number:	WEBR-045/00US 303666-2050

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:				
Extension - 3 months with $0 paid	1253	1	1110	1110

Trend Micro, Inc.
EX1002-156

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Request for continued examination	1801	1	810	810
		Total in USD ($)		**1920**

Electronic Acknowledgement Receipt

EFS ID:	8262286
Application Number:	11408145
International Application Number:	
Confirmation Number:	8007
Title of Invention:	Backward researching time stamped events to find an origin of pestware
First Named Inventor/Applicant Name:	Matthew L. Boney
Customer Number:	22903
Filer:	Thomas M. Croft/Sherry Bitler
Filer Authorized By:	Thomas M. Croft
Attorney Docket Number:	WEBR-045/00US 303666-2050
Receipt Date:	20-AUG-2010
Filing Date:	20-APR-2006
Time Stamp:	20:06:39
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1920
RAM confirmation Number	5253
Deposit Account	501283
Authorized User	

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

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	WEBR04500US-RCE.pdf	123854 3cee4d5729eb1092f507b6eed12f2e4a3df46fe7	no	1
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
2	Amendment Submitted/Entered with Filing of CPA/RCE	WEBR04500US-2010-08-20-roa.pdf	365510 4c59b5bacfa7b5a74e7269c65a604ab09358c520	no	10
Warnings:					
Information:					
3	Fee Worksheet (PTO-875)	fee-info.pdf	32035 662feb4580a1036560957597d402aba2ecd33da0	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	521399		

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.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
11/408,145	04/20/2006	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), 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.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 08/20/2010	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 19	Minus	** 23	= 0	X $ =		OR	X $52=	0
Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $ =		OR	X $220=	0
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	0

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) 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))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/DONNA D. SMALLS LOGAN/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/408,145	04/20/2006	Matthew L. Boney	WEBR-045/00US 303666-2050	8007

22903 7590 02/22/2010

COOLEY GODWARD KRONISH LLP
ATTN: PATENT GROUP
Suite 1100
777 - 6th Street, NW
WASHINGTON, DC 20001

EXAMINER	
RAHMAN, MAHFUZUR	

ART UNIT	PAPER NUMBER
2438	

MAIL DATE	DELIVERY MODE
02/22/2010	PAPER

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.

Office Action Summary	Application No.	Applicant(s)	
	11/408,145	BONEY, MATTHEW L.	
	Examiner	Art Unit	
	MAHFUZUR RAHMAN	2438	

-- 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 *04 August 2009*.

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

3)☐ 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

4)☒ Claim(s) *1-6,8,10-16 and 19-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8,10-16 and 19-23* is/are rejected.

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

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

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

10)☒ The drawing(s) filed on *20 April 2006* 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).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

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. _____.

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) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *8/4/2009*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Trend Micro, Inc.
EX1002-162

DETAILED ACTION

Claims 1-6, 8, 10-16, and 19-23 are examined and are pending. Claims 1, 8, 12, and 19-20 have been currently amended. Claims 7, 9, and 17-18 have been canceled.

Response to Arguments

1. Applicant's amendments with respect to the claim objections filed on August 4, 2009 are acknowledged and the objection is withdrawn.

2. Applicants amendment to claims 1 and 12 filed on August 4, 2009 necessitated a new ground of rejection presented in this Office Action. The previously presented rejections have changed because the new limitations "receiving from a user" have been added to claim 1 and "to detected activity on the computer that is indicative of pestware" have been added to claim 12. Thus applicant's arguments filed on August 8, 2009 have been rendered moot in view of the new ground(s) of rejection. The reference of Huang has been introduced to the references of Porras and Wang to address the newly added limitations. The reasons of obviousness are included below in this office action.

Claims 1-23 are now rejected under 35 U.S.C. 103(a) as being unpatentable over Porras et al. (US 2004/0024864 A1, hereinafter, Porras) in view of Wang et al. (US

2005/0268112 A1, hereinafter, Wang), and further in view of Huang (US 2004/0225877 A1).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. 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.

5. Claims 1-6, 8, 10-16, and 19-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Porras et al. (US 2004/0024864 A1, hereinafter, Porras) in view of Wang et al. (US 2005/0268112 A1, hereinafter, Wang), and further in view of Huang (US 2004/0225877 A1).

Regarding claim 1, Porras discloses a method for identifying an origin of suspected pestware activity on a computer, the method comprising:

[receiving, from a user], a time of interest relating to a suspicion of pestware on the computer (Paragraph 0014: generating audit records that are analyzed periodically or as needed basis to identify any suspicious activity that is responsible for a potential attack on a host a computer);

and accessing at least a portion of a recorded history of sources (Paragraph 0015: audit-record that records the IP address of the source) that the computer received files from so as to identify, based at least in part upon the identified indicia of pestware, a reference to an identity of a source that is suspected of originating pestware (Paragraph 0015: Intrusion Detection System (DS) identifies the source of intrusion based on the IP address associated with session identifier).

Porras does not explicitly disclose identifying, based upon the time of interest, indicia of pestware;

Wang from the same or similar fields of endeavor teaches that a browser component is configured to record timestamps along with an event log (Paragraph 0041: Gatekeeper Browser Helper Object (BHO) is provided for monitoring activity and to record the timestamp of a suspicious event) to identify and trace the process or application that is responsible for an attack (Paragraph 0050: Browser Helper Object (BHO) is customized such that the source of a suspected process or application can be identified).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention, to use time of interest such as timestamp and event log to identify any suspicious event that takes place on a host computer as taught by Wang et al. in the teaching of Porras for the advantage of identifying potential unwanted software through timestamp records and tracing the source, so appropriate actions can be taken against those sessions and applications that are responsible for originating pestwares.

The combination of Porras and Wang does not disclose but Huang from the same or similar fields of endeavor teaches that [receiving, from a user], a time of interest relating to a suspicion of pestware on the computer (Paragraph 0029: The time window length is set by the user. It may sufficient to account the number of user activities in time slots, instead of logging the content of every user activities in the process buffer; Fig. 4: Block 410, Retrieve User Activities that Occurred in a Time Window).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to receive a time of interest from a user as taught by Huang in the teachings of Porras and Wang for the advantage of matching a plurality of attributes including the user initiation attribute derived from a system activity and take security action specified by the best matched security policy against the system activity (Paragraph 0007) wherein user activities is received in a time window initiated by a user (Paragraph 0006).

Regarding claim 2, the combination of Porras, Wang and Huang discloses the method of claim 1, wherein the identifying includes: accessing at least one log of historical events on the computer; locating at least one event in the at least one log that corresponds to the time of interest; and determining that the at least one event is associated with the indicia of pestware (Porras, Paragraph 0015: audit record wherein network communication event and process session associated with a session identifier are recorded).

Regarding claim 3, the combination of Porras, Wang and Huang discloses the method of claim 2, wherein the determining that the at least one event is associated with the indicia of pestware includes following references in the at least one log to a suspected pestware object (Porras, Paragraph 0015: Intrusion Detection System determines that session is part of an attack via IP address of source or a session identifier).

Regarding claim 4, the combination of Porras, Wang and Huang discloses the method of claim 3, wherein following the references includes following at least one reference in an activity log from the event to a suspected pestware process (Porras, Paragraph 0015: source of the attack is identified using session identifier and IP address in the audit record or the record that is obtained from network communication events)

.

Regarding claim 5, the combination of Porras, Wang and Huang discloses the method of claim 4, wherein the activity log is generated from a kernel-mode driver (Porras , Paragraph 0015: session identifier of a suspicious activity is recorded as a log entry in kernel audit records, for example).

Regarding claim 6, the combination of Porras, Wang and Huang discloses the method of claim 2 wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs (Porras , Paragraph 0017: application pathnames related to the suspicious process is obtained where pathnames includes file information, for example).

Regarding claim 8, the combination of Porras, Wang and Huang discloses the method of claim 1, wherein the user input is in response to an alert provided to the user regarding a detected suspicious activity on the computer (Porras, Paragraph 0017: IDS operator or system administrator takes selective action once the alert is generated regarding any suspicious activity from attacker; Page 3 lines 20-23: response to a suspicious activity).

Regarding claim 10, the combination of Porras, Wang and Huang discloses the method of claim 1, including: reporting the identity of the source to a pestware research

entity so as to enable the pestware research entity to research whether the source is a source of pestware (Porras , Paragraph 0013: preprocessor associates necessary information to audit record and reports it to the analysis engine so the source that is responsible for attack can be identified)

Regarding claim 11, the combination of Porras, Wang and Huang discloses the method of claim 1, wherein the at least one source of potential pestware activity is identified by an identifier selected from the group consisting of an I.P. address, a URL, an email client and a program name (Porras, Paragraph 0015: IP address or a session identifier associated with the source of a user in the audit record).

Regarding claim 12, Porras discloses a system for identifying a source of suspected pestware on a computer, the system comprising:

[a timestamp] module configured to generate a [time of interest] in response to detected activity on the computer that is indicative of pestware (Page 3 lines 20-23: response to a suspicious activity)

a research portion configured to access at least one log on a file storage device of the computer to relate the time of interest to at least one source of potential pestware activity on the computer (Paragraph 0013: analysis engine determines if an intrusion or attack has taken place by analyzing audit records where analysis engine acts as a research portion of the Intrusion Detection System); and

a reporting portion configured to generate a report that identifies the at least one source of potential pestware activity (Paragraph 0003: audit record provides a report of what activities are normal and what are unusual as a reporting component, for example).

Porras does not but Wang from the same or similar fields of endeavor teaches, a timestamp module configured to generate a [time of interest] in response to detected activity on the computer (Paragraph 0041: Gatekeeper Browser Helper Object (BHO) is provided for monitoring activity and to record the timestamp of a suspicious event) that is indicative of pestware (Paragraph 0050: Browser Helper Object (BHO) is customized such that the source of a suspected process or application can be identified).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention, to use a component that is configured to record timestamps related to a suspicious event on a host computer as taught by Wang et al. in the teaching of Porras for the advantage of identifying potential unwanted software through timestamp records and tracing the source that is suspected of originating pestware so appropriate actions can be taken against those sessions and applications that are responsible for potential attacks.

The combination of Porras and Wang does not disclose but Huang from the same or similar fields of endeavor teaches generating a time of interest in response to detected activity on the computer (Paragraph 0029: program generating system activity for a time window. The time window length can be set the user, it can also be set dynamically by the system according to the software program)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to generate a time of interest in response to detected activity on computer that is indicative of suspicious activity as taught by Huang in the teachings of Porras and Wang for the advantage of detecting anomalous activity, monitoring system, event, and security log files generated in the operating system to look for attack signatures, specific patterns that usually indicate malicious intent (paragraph 0004) and providing the control of computer virus, Trojan Horse program, or any malicious software (Paragraph 0002).

Regarding claim 13, the combination of Porras, Wang and Huang discloses the system of claim 12, wherein the at least one log includes information that relates the time of interest to an event, and wherein the at least one log includes information that relates the event to a suspected pestware object, and wherein the at least one log includes information that relates the suspected pestware object to the at least one source of potential pestware activity (Porras, Paragraph 0015: source of the attack is identified using session identifier, IP address in the audit record or from the record that is obtained from network communication events).

Regarding claim 14, the combination of Porras, Wang and Huang discloses the system of claim 13, including: a heuristics module configured to evaluate whether the

event is a suspected pestware-related event before the research portion accesses information in the at least one log that relates the event to the suspected pestware object (Porras, Paragraph 0013: based on the evaluation, preprocessor associates necessary information to the audit record before sending it to the IDS's (Intrusion Detection System) analysis engine where preprocessor functions as a heuristics module and analysis engine as a research portion, for example)

Regarding claim 15, the combination of Porras, Wang and Huang discloses the system of claim 14, wherein the heuristics module determines that the at least one event is suspected to be pestware-related by analyzing other events in connection with the event, wherein the other events are also related to the time of interest (Porras, Paragraph 0013: preprocessor associates related event information with suspected audit record and then provides the combined information to the analysis engine)

Regarding claim 16, the combination of Porras, Wang and Huang discloses the system of claim 12, wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs (Porras, Paragraph 0017: application pathnames related to the suspicious process is obtained where pathnames includes file information, for example)

Regarding claim 19, the combination of Porras, Wang and Huang discloses the system of claim 12, wherein the timestamp module is configured to generate the time of interest as a time interval (Porras , Paragraph 0014: kernel audit records are received in real time and analyzed periodically to identify any suspicious activity from attacker).

Regarding claim 20, the combination of Porras, Wang and Huang discloses the system of claim 12, wherein the timestamp module is configured to generate the time of interest as a point in time (Porras , Paragraph 0014: kernel audit records are generated in real time, for example).

Regarding claim 21, the combination of Porras, Wang and Huang discloses the system of claim 12, including a kernel-mode driver adapted to monitor activity on the computer and to generate an activity log that is included within the at least one log (Porras, Paragraph 0014: kernel audit records are analyzed periodically or as needed basis to identify any suspicious activity from attacker; Paragraph 0015: session identifier recorded as a log entry in kernel audit records, for example).

Regarding claim 22, the combination of Porras, Wang and Huang discloses the system of claim 12, wherein the at least one source of potential pestware activity is identified by an identifier selected from the group consisting of an I.P. address, a URL,

an email client and a program name (Porras, Paragraph 0015: IP address or a session identifier associated with the source of a user in the audit record)

Regarding claim 23, the combination of Porras, Wang and Huang discloses the system of claim 12, wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs (Porras, Paragraph 0017: network communication event in audit records; Paragraph 0017: application pathnames related to the suspicious process is obtained where pathnames includes file information, for example).

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

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

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MAHFUZUR RAHMAN whose telephone number is (571)270-7638. The examiner can normally be reached on Monday thru Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on (571) - 272-3787. 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.

/M. R./
Examiner, Art Unit 2438

/Taghi T. Arani/
Supervisory Patent Examiner, Art Unit 2438

Notice of References Cited	Application/Control No. 11/408,145	Applicant(s)/Patent Under Reexamination BONEY, MATTHEW L.	
	Examiner MAHFUZUR RAHMAN	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2004/0024864	02-2004	Porras et al.	709/224
*	B	US-2005/0268112	12-2005	Wang et al.	713/188
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S18	7684	726/22-25,13;713/187-188,193-194.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2009/06/15 14:27
S19	21	S18 and ((token indicia sign$5) same (pestware maleware spamware adware scumware))	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2009/06/15 14:30
S20	21	S19 and (@ad<"20060420" or rlad <"20060420")	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2009/06/15 14:32
S21	19	S20 and (time period)	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2009/06/15 14:48
S41	105	("20020078381" | "20020162015" | "20020162017" | "20020166063" | "20030065943" | "20030074581" | "20030101381" | "20030159070" | "20030217287" | "20040024864" | "20040030914" | "20040034794" | "20040064515" | "20040064736" | "20040080529" | "20040143763" | "20040187023" | "20040225877" | "20050005160" | "20050038697" | "20050138433" | "20050154885" | "20050268112" | "20050268112" | "20060075494" | "20060075501" | "20060161988" | "5623600" | "5920696" | "5951698" | "6069628" | "6073241" | "6092194" | "6154844" | "6167520" | "6310630" | "6397264" | "6405316" | "6460060" |	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2010/02/02 18:01

		"6480962" | "6535931" | "6611878" | "6633835" | "6667751" | "6701441" | "6772345" | "6785732" | "6804780" | "6813711" | "6829654" | "6910134" | "6965968" | "7058822" | "7107617").PN.				
S46	15	S41 and user same (request$3 or send$3 or receiv$3) same time same2 (respons$4 or generat$3 or provid$3)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2010/02/02 18:28
S48	4	(user or client) near6 request$3 with time and pestware	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2010/02/02 19:12
S49	4	S48 and (@ad<"20060420" or rlad<"20060420")	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2010/02/02 19:12
S50	3	S49 and respon$4	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2010/02/02 19:12
S51	4	(user or client) with request$3 with time and pestware	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2010/02/02 19:14
S52	6	(user or client) same request$3 with time and pestware	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2010/02/02 19:14
S53	6	S52 and (@ad<"20060420" or rlad<"20060420")	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2010/02/02 19:14
S55	283	(user or client) near4 request$3 with time same Identif$4 and suspici$3	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2010/02/02 19:16
S56	283	S55 and (@ad<"20060420" or rlad<"20060420")	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2010/02/02 19:17
S57	143	S56 and intrusion	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2010/02/02 19:17
S58	7	S57 and (pestware or maleware or spyware)	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2010/02/02 19:18
S76	3	(US-20040024864-$ or US-20050268112-$ or US-20070094725-$).did.	US-PGPUB	OR	ON	2010/02/02 20:04

S77	2	S76 and (user or client) same time same (request $3 or search$3 or look)	US-PGPUB	OR	ON	2010/02/02 20:04
S78	2	S76 and (user or client or administrator) same time same (request$3 or search $3 or look)	US-PGPUB	OR	ON	2010/02/02 20:04

EAST Search History (Interference)

<This search history is empty>

2/4/2010 7:04:02 PM
C:\Documents and Settings\mrahman4\My Documents\EAST\Workspaces\31_Time Stamp to find Origin of Pestware_04202006_11408145\30_Time Stamp to find Origin of Pestware_04202006_11408145.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11408145	BONEY, MATTHEW L.
	Examiner	Art Unit
	MAHFUZUR RAHMAN	2438

SEARCHED

Class	Subclass	Date	Examiner
726	22	2/2/2010	MR

SEARCH NOTES

Search Notes	Date	Examiner
East search, search terms used: user or client or administrator, respons$3, activit$3, suspicious, generat$3, request$3 or send$3 or receiv$3 or search$3 or look, time or period, respons$4 or generat$3 or provid$3, pestware or maleware or spyware, log, event, alert, history	2/4/2010	MR
Performed Inventor/Assignee name search	2/4/2010	MR
Keyword search of 726/22-25,13;713/187-188,193-194	2/4/2010	MR

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

/MAHFUZUR RAHMAN/ Examiner.Art Unit 2438	

Trend Micro, Inc.
EX1002-180

Receipt date: 08/04/2009

Please type a plus sign (+) inside this box → [+]

PTO/SB/08A (07-05)
Approved for use through 07/31/2006. OMB 0651-0031

Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(use as many sheets as necessary)*		***Complete if Known***	
		Application Number	11/408,145
		Filing Date	04/20/2006
		First Named Inventor	Matthew L. BONEY
		Group Art Unit	2438
		Examiner Name	Mahfuzur RAHMAN
Sheet	1 of 1	Attorney Docket Number	WEBR-045/00US 303666-2050

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
		US-2002/0078381	06-20-2002	Farley	

Examiner Signature	/Mahfuzur Rahman/	Date Considered	02/04/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Unique citation designation number (optional). [2]See attached Kinds of U.S. Patent Documents. This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours 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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R./

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11408145	BONEY, MATTHEW L.
	Examiner	Art Unit
	MAHFUZUR RAHMAN	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/15/2009	02/02/2010							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	-							
	8	✓	✓							
	9	✓	-							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16	✓	✓							
	17	✓	-							
	18	✓	-							
	19	✓	✓							
	20	✓	✓							
	21	✓	✓							
	22	✓	✓							
	23	✓	✓							

Trend Micro, Inc.
EX1002-182

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:	Matthew L. BONEY	Confirmation No.:	8007
Serial No.:	11/408,145	Group Art Unit:	2438
Filed:	04/20/2006	Examiner:	Mahfuzur RAHMAN

FOR: **BACKWARD RESEARCHING TIME STAMPED EVENTS TO FIND AN ORIGIN**

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

INFORMATION DISCLOSURE STATEMENT UNDER 37 C.F.R. §1.97(c)

In accordance with the duty of disclosure set forth in 37 C.F.R. §1.56, Applicant(s) hereby submits the following information in conformance with 37 C.F.R. §§1.97 and 1.98.

[x] Pursuant to 37 C.F.R. §1.98, a copy of each non-US patent document cited in the attached Form PTO/SB/08 is enclosed.

[] No copies of any U.S. patents or U.S. patent application publications listed on the attached Form PTO/SB/08 are being provided pursuant to 37 C.F.R. §1.98.

This Information Disclosure Statement is filed after the period specified in 37 C.F.R. § 1.97(b), but before the mailing of any of the following:

[x] a final action under 37 C.F.R. §1.113;

[] a notice of allowance under 37 C.F.R. §1.311; or

[] an action that otherwise closes prosecution in this application.

In accordance with 37 C.F.R. §1.97(c) also enclosed is:

[x] Fee under 37 C.F.R. §1.17(p) in the amount of $180.00; or

[] Statement as specified in 37 C.F.R. §1.97(e):

[] Each item of information contained in the Information Disclosure Statement cited herein was first cited in a

communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing date of the Information Disclosure Statement; or

[] No item of information contained in the Information Disclosure Statement submitted herewith was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned, having made a reasonable inquiry, no item of information contained in the 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 date of the Information Disclosure Statement.

It is respectfully requested that the Examiner consider the above-noted information and return an initialed copy of the attached Form PTO/SB/08 to the undersigned.

COOLEY GODWARD KRONISH LLP
ATTN: Patent Group
777 6th Street NW, Suite 1100
Washington, DC 20001

Tel: (720) 566-4044
Fax: (202) 842-7899

Respectfully submitted,
COOLEY GODWARD KRONISH LLP

By: Thomas M. Croft
Thomas M. Croft
Reg. No. 44,051

Please type a plus sign (+) inside this box → [+]

PTO/SB/08A (07-05)
Approved for use through 07/31/2006. OMB 0651-0031

Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(use as many sheets as necessary)*		***Complete if Known***	
		Application Number	11/408,145
		Filing Date	04/20/2006
		First Named Inventor	Matthew L. BONEY
		Group Art Unit	2438
		Examiner Name	Mahfuzur RAHMAN
Sheet	1 of 1	Attorney Docket Number	WEBR-045/00US 303666-2050

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
		US-2002/0078381	06-20-2002	Farley	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Unique citation designation number (optional). [2]See attached Kinds of U.S. Patent Documents. This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Electronic Patent Application Fee Transmittal

Application Number:	11408145
Filing Date:	20-Apr-2006
Title of Invention:	Backward researching time stamped events to find an origin of pestware
First Named Inventor/Applicant Name:	Matthew L. Boney
Filer:	Thomas M. Croft/Sherry Bitler
Attorney Docket Number:	WEBR-045/00US 303666-2050

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:	5789873
Application Number:	11408145
International Application Number:	
Confirmation Number:	8007
Title of Invention:	Backward researching time stamped events to find an origin of pestware
First Named Inventor/Applicant Name:	Matthew L. Boney
Customer Number:	22903
Filer:	Thomas M. Croft/Sherry Bitler
Filer Authorized By:	Thomas M. Croft
Attorney Docket Number:	WEBR-045/00US 303666-2050
Receipt Date:	04-AUG-2009
Filing Date:	20-APR-2006
Time Stamp:	12:54:18
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	8847
Deposit Account	501283
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	Applicant Arguments/Remarks Made in an Amendment	WEBR04500USroa.pdf	381749 b3c9a81c2675fb0ecd4caebd1acdb9daf4ff4e73	no	11
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Filed (SB/08)	WEBR04500USIDS.pdf	124770 ba1d1109c8e2693a09bbd28ce6bbffaf153bfd41	no	3
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Fee Worksheet (PTO-875)	fee-info.pdf	30304 ccffa2aafe644e45f842428c8615a5485ea449c4	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	536823		

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 Application of:	Matthew L. BONEY	Confirmation No.:	8007
Serial No.:	11/408,145	Group Art Unit:	2438
Filed:	04/20/2006	Examiner:	Mahfuzur RAHMAN

FOR: **BACKWARD RESEARCHING TIME STAMPED EVENTS TO FIND AN ORIGIN**

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

AMENDMENT/RESPONSE TO OFFICE ACTION

In response to the Official Action dated June 22, 2009 (the "Office Action"), please amend the above-identified patent application in the following manner:

Amendments to the Specification begin on page 2 of this paper.

Amendments to the Claims are reflected in the listing of the claims that begins on page 4 of this paper.

Remarks/Arguments begin on page 9 of this paper.

Trend Micro, Inc.
EX1002-190

Amendments to the Specification:

Please replace paragraph no. [0001] with the following paragraph. The amendments to paragraph no. [0001] are indicated by strikethrough and underlining.

[0001] The present application is related to commonly owned and assigned Application No. 10/956,573, ~~Attorney Docket No. WEBR-003/00US~~now U.S. Patent No. 7,480,683, entitled *System and Method For Heuristic Analysis to Identify Pestware*; Application No. 10/956,574, ~~Attorney Docket No. WEBR-005/00US~~now U.S. Patent No. 7,533,131, entitled *System and Method for Pestware Detection and Removal*; Application No. ~~11/237,291~~10/956,818, ~~Attorney Docket No. WEBR-006/00US,~~ entitled *System and Method for Locating Malware and Generating Malware Definitions*; Application No. 11/257,609, ~~Attorney Docket No. WEBR-015/00US,~~ entitled *System and Method for Kernel-Level Pestware Management*; Application No. 11/237,291, ~~Attorney Docket No. WEBR-020/00US,~~ entitled *Client Side Exploit Tracking*; Application No. ~~[unassigned]~~11/408,146, ~~Attorney Docket No. WEBR-044/00US,~~ entitled *Backwards researching Activity Indicative of Pestware*, filed herewith; and Application No. ~~[unassigned]~~11/408,215, ~~Attorney Docket No. WEBR-043/00US,~~ entitled *Backward Researching Existing Pestware*, filed herewith, which are incorporated herein by reference.

Please replace paragraph no. [0051] with the following paragraph. The amendments to paragraph no. [0051] are indicated by strikethrough and underlining.

[0051] As shown in FIGURE 5, once a time of interest is established, suspicious activity is identified on the computer based upon the time of interest (Block 504). The time of interest may be established, for example, to include a time period before the time stamp is issued so that a search for suspicious activity is limited to a particular time period. In some embodiments, the activity log ~~130~~120 and/or one or more of the *N* files 130 are accessed and analyzed to determine whether any activity during the time of interest is suspicious (e.g., the activity indicates in some way that it may be associated with pestware). As an example, if any logged information (e.g., in the activity log ~~130~~120 and/or one or more of the *N* files 130) indicates that during the time of interest that, for example, access to the registry was carried out in connection with a downloaded file or the launch of a process, the activities may identified as being suspect and further research relative to the process and the file may carried out.

Amendments to the Claims:

Set forth below in ascending order, with status identifiers, is a complete listing of all claims currently under examination. Changes to any amended claims are indicated by strikethrough and underlining. This listing also reflects any cancellation and/or addition of claims.

1. (currently amended) A method for identifying an origin of suspected pestware activity on a computer, the method comprising:

receiving, from a user, ~~establishing~~ a time of interest relating to a suspicion of pestware on the computer;

identifying, based upon the time of interest, indicia of pestware; and

accessing at least a portion of a recorded history of sources that the computer received files from so as to identify, based at least in part upon the identified indicia of pestware, a reference to an identity of a source that is suspected of originating pestware.

2. (original) The method of claim 1, wherein the identifying includes:

accessing at least one log of historical events on the computer;

locating at least one event in the at least one log that corresponds to the time of interest; and

determining that the at least one event is associated with the indicia of pestware.

3. (original) The method of claim 2, wherein the determining that the at least one event is associated with the indicia of pestware includes following references in the at least one log to a suspected pestware object.

4. (original) The method of claim 3, wherein following the references includes following at least one reference in an activity log from the event to a suspected pestware process.

5. (original) The method of claim 4, wherein the activity log is generated from a kernel-mode driver.

6. (original) The method of claim 2, wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs.

7. (canceled)

8. (currently amended) The method of claim [[5]]1, wherein the user input is in response to an alert provided to the user regarding a detected suspicious activity on the computer.

9. (canceled)

10. (original) The method of claim 1, including:

reporting the identity of the source to a pestware research entity so as to enable the pestware research entity to research whether the source is a source of pestware.

11. (original) The method of claim 1, wherein the source is identified by an identifier selected from the group consisting of an I.P. address, a URL, an email client and a program name.

12. (currently amended) A system for identifying a source of suspected pestware on a computer, ~~including~~the system comprising:

a timestamp module configured to generate a time of interest in response to detected activity on the computer that is indicative of pestware~~a suspicion of pestware on the computer~~;

a research portion configured to access at least one log on a file storage device of the computer ~~that~~to relate[[s]] the time of interest to at least one source of potential pestware activity on the computer; and

a reporting portion configured to generate a report that identifies the at least one source of potential pestware activity.

13. (original) The system of claim 12, wherein the at least one log includes information that relates the time of interest to an event, and wherein the at least one log includes information that relates the event to a suspected pestware object, and wherein the at least one log includes information that relates the suspected pestware object to the at least one source of potential pestware activity.

14. (original) The system of claim 13, including:

a heuristics module configured to evaluate whether the event is a suspected pestware-related event before the research portion accesses information in the at least one log that relates the event to the suspected pestware object.

15. (original) The system of claim 14, wherein the heuristics module determines that the at least one event is suspected to be pestware-related by analyzing other events in connection with the event, wherein the other events are also related to the time of interest.

16. (original) The system of claim 12, wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs

17.-18. (canceled)

19. (currently amended) The system of claim 12, wherein the timestamp module is configured to generate the time of interest as a time interval.

20. (currently amended) The system of claim 12, wherein the timestamp module is configured to generate the time of interest as a point in time.

21. (original) The system of claim 12, including a kernel-mode driver adapted to monitor activity on the computer and to generate an activity log that is included within the at least one log.

22. (original) The system of claim 12, wherein the at least one source of potential pestware activity is identified by an identifier selected from the group consisting of an I.P. address, a URL, an email client and a program name.

23. (original) The system of claim 12, wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs.

REMARKS

Claims 1, 8, 12, and 19-20 have been currently amended. Claims 7, 9, and 17-18 have been canceled. No new claims have been added. Claims 1-6, 8, 10-16, and 19-23 thus remain pending in the application.

Claim Objections

The Office Action objects to claims 19 and 20 because of typographical errors in the claim references ("system of claim 1" instead of "system of claim 12"). These typographical errors have been corrected by amendment. Withdrawal of the objections is respectfully requested.

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

The Office Action rejects claims 1-23 under 35 U.S.C. § 103(a) as being unpatentable over Porras et al. (U.S. 2004/0024864, hereinafter "Porras") in view of Wang et al. (U.S. 2005/0268112, hereinafter "Wang").

Applicant believes that independent claims 1 and 12, as currently amended, recite limitations that are not taught or suggested in Porras or Wang.

Claim 1. Currently amended independent method claim 1 recites, among other things, the limitation "receiving, from a user, a time of interest relating to a suspicion of pestware on the computer." This "time of interest" received from the user serves as a basis for "identifying . . . indicia of pestware" on the computer. At least a portion of a recorded history of sources from which the computer received files is accessed to identify, based at least in part upon the identified indicia of pestware, a reference to an identity of a source that is suspected of originating pestware. In short, the method of claim 1 uses a user-supplied "time of interest" to guide an automated (computer-implemented) process for researching and identifying the source

from which the pestware originated. Neither Porras nor Wang teaches or suggests such a method, whether those references are considered separately or in combination. Applicant notes that the current amendments to claim 1 are amply supported at, e.g., Paragraph 0049 of the specification. No new matter has been introduced by way of the current amendments to claim 1.

Because Porras and Wang, whether taken separately or in combination, fail to teach or suggest each and every limitation recited in currently amended claim 1, they cannot render claim 1 obvious under § 103(a), and Applicant believes claim 1 to be allowable. Each of dependent claims 2-6, 8, and 10-11 is thus also allowable at least by virtue of its depending from allowable claim 1. Withdrawal of the rejection, under § 103(a), of claims 1-6, 8, and 10-11 is respectfully requested.

Claim 12. Currently amended independent system claim 12 recites, among other things, the limitation "a timestamp module configured to generate a time of interest in response to detected activity on the computer that is indicative of pestware." Neither Porras nor Wang teaches or suggests this limitation. Though Paragraph 0050 of Wang discusses using a customized Browser Helper Object ("BHO") to record accessed URLs and their associated timestamps, it is clear from the context of Paragraph 0050 that this is done for *all* URLs accessed. Therefore, Wang does not teach generating a "time of interest" "*in response to* detected activity on the computer that is indicative of pestware" (emphasis added). The timestamps associated with the accessed URLs are not generated "in response to" anything. There is ample support for the current amendments to claim 12 at, e.g., Paragraph 0024 of the specification. No new matter has been introduced by way of the current amendments to claim 12.

Because Porras and Wang, whether taken separately or in combination, fail to teach or suggest each and every limitation recited in currently amended claim 12, they cannot render

claim 12 obvious under § 103(a), and Applicant believes claim 12 to be allowable. Each of dependent claims 13-16 and 19-23 is thus also allowable at least by virtue of its depending from allowable claim 12. Withdrawal of the rejection, under § 103(a), of claims 12-16 and 19-23 is respectfully requested.

CONCLUSION

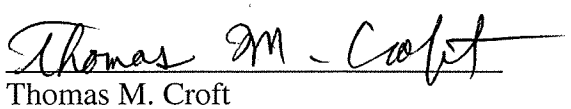
In view of the foregoing, Applicant respectfully submits that no further impediments exist to the allowance of this application and, therefore, requests an indication of allowability. However, the Examiner is requested to call the undersigned if any questions or comments arise.

The Director is hereby authorized to charge any appropriate fees under 37 C.F.R. §§1.16, 1.17, and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 50-1283.

COOLEY GODWARD KRONISH LLP
ATTN: Patent Group
777 6th Street NW, Suite 1100
Washington, DC 20001

Tel: (720) 566-4044
Fax: (202) 842-7899

Respectfully submitted,
COOLEY GODWARD KRONISH LLP

By: 
Thomas M. Croft
Reg. No. 44,051

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
11/408,145	04/20/2006	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), 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.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 08/04/2009	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 19	Minus	** 23	= 0	X $ =		OR	X $52=	0
Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $ =		OR	X $220=	0
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	0

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) 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))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/AUDRIS SIAS/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/408,145	04/20/2006	Matthew L. Boney	WEBR-045/00US 303666-2050	8007

22903 7590 06/22/2009

COOLEY GODWARD KRONISH LLP
ATTN: PATENT GROUP
Suite 1100
777 - 6th Street, NW
WASHINGTON, DC 20001

EXAMINER	
RAHMAN, MAHFUZUR	
ART UNIT	**PAPER NUMBER**
2438	

MAIL DATE	DELIVERY MODE
06/22/2009	PAPER

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.

Office Action Summary	Application No.	Applicant(s)	
	11/408,145	BONEY, MATTHEW L.	
	Examiner	Art Unit	
	MAHFUZUR RAHMAN	2438	

-- 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 *20 April 2006*.

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

3)☐ 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

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

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

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

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

10)☒ The drawing(s) filed on *20 April 2006* 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).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

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. _____.

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) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *4/18/2007, 11/21/2007, 5/22/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Trend Micro, Inc.
EX1002-203

DETAILED ACTION

Claims 1-23 are examined and are pending.

Claim Objections

1. Claims 19 and 20 are objected to because of the following informalities: claim 19 recites "The system of claim 1" is interpreted by examiner as typographical error and should read as "The system of claim 12". Claim 20 recites "The system of claim 1" is interpreted by examiner as typographical error and should read as "The system of claim 12". Appropriate correction is requested.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. 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.

4. Claims 1-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Porras et al. (US 2004/0024864 A1, hereinafter, Porras) in view of Wang et al. (US 2005/0268112 A1, hereinafter, Wang).

Regarding claim 1, Porras discloses a method for identifying an origin of suspected pestware activity on a computer comprising:

establishing a time of interest relating to a suspicion of pestware on the computer (Paragraph 0014: generating audit records that are analyzed periodically or as needed basis to identify any suspicious activity that is responsible for a potential attack on a host a computer);

accessing at least a portion of a recorded history of sources (Paragraph 0015: audit-record that records the IP address of the source) that the computer received files from so as to identify, based at least in part upon the identified indicia of pestware, a reference to an identity of a source that is suspected of originating pestware (Paragraph 0015: Intrusion Detection System (DS) identifies the source of intrusion based on the IP address associated with session identifier).

Porras does not explicitly disclose identifying, based upon the time of interest, indicia of pestware;

Wang from the same or similar fields of endeavor teaches that a browser component is configured to record timestamps along with an event log (Paragraph 0041: Gatekeeper Browser Helper Object (BHO) is provided for monitoring activity and to record the timestamp of a suspicious event) to identify and trace the process or application that is responsible for an attack (Paragraph 0050: Browser Helper Object (BHO) is customized such that the source of a suspected process or application can be identified).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention, to use time of interest such as timestamp and event log to identify any suspicious event that takes place on a host computer as taught by Wang et al. in the teaching of Porras for the advantage of identifying potential unwanted software through timestamp records and tracing the source, so appropriate actions can be taken against those sessions and applications that are responsible for originating pestwares.

Regarding claim 2, the combination of Porras and Wang discloses the method of claim 1, wherein the identifying includes: accessing at least one log of historical events on the computer; locating at least one event in the at least one log that corresponds to the time of interest; and determining that the at least one event is associated with the indicia of pestware (Porras, Paragraph 0015: audit record wherein network communication event and process session associated with a session identifier are recorded).

Regarding claim 3, the combination of Porras and Wang discloses the method of claim 2, wherein the determining that the at least one event is associated with the indicia of pestware includes following references in the at least one log to a suspected pestware object (Porras, Paragraph 0015: Intrusion Detection System determines that session is part of an attack via IP address of source or a session identifier).

Regarding claim 4, the combination of Porras and Wang discloses the method of claim 3, wherein following the references includes following at least one reference in an activity log from the event to a suspected pestware process (Porras, Paragraph 0015: source of the attack is identified using session identifier and IP address in the audit record or the record that is obtained from network communication events)

.

Regarding claim 5, the combination of Porras and Wang discloses the method of claim 4, wherein the activity log is generated from a kernel-mode driver (Porras , Paragraph 0015: session identifier of a suspicious activity is recorded as a log entry in kernel audit records, for example).

Regarding claim 6, the combination of Porras and Wang discloses the method of claim 2 wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs (Porras , Paragraph 0017: application pathnames related

to the suspicious process is obtained where pathnames includes file information, for example)

Regarding claim 7, the combination of Porras and Wang discloses the method of claim 1, wherein the time of interest is established from a user input (Porras , Paragraph 0017: IDS operator or system administrator provides input such as takes selective action once an alert corresponding to a suspicious activity is generated where the alert is related to a time of interest, for example).

Regarding claim 8, the combination of Porras and Wang discloses the method of claim 5, wherein the user input is in response to an alert provided to the user (Porras, Paragraph 0017: IDS operator or system administrator takes selective action once the alert is generated regarding any suspicious activity from attacker).

Regarding claim 9, the combination of Porras and Wang discloses the method of claim 1, wherein the time of interest is established from a time stamp of a substantially instant moment in time (Porras, Paragraph 0014: analysis is performed periodically or as needed basis on kernel audit records for any potential attack on host computer where the periodic analysis is related to the time of interest, for example)

Regarding claim 10, the combination of Porras and Wang discloses the method of claim 1, including: reporting the identity of the source to a pestware research entity so as to enable the pestware research entity to research whether the source is a source of pestware (Porras , Paragraph 0013: preprocessor associates necessary information to audit record and reports it to the analysis engine so the source that is responsible for attack can be identified)

Regarding claim 11, the combination of Porras and Wang discloses the method of claim 1, wherein the at least one source of potential pestware activity is identified by an identifier selected from the group consisting of an I.P. address, a URL, an email client and a program name (Porras, Paragraph 0015: IP address or a session identifier associated with the source of a user in the audit record).

Regarding claim 12, Porras et al. discloses a system for identifying a source of suspected pestware on a computer including:

a research portion configured to access at least one log on the computer that relates the time of interest to at least one source of potential pestware activity on the computer (Paragraph 0013: analysis engine determines if an intrusion or attack has taken place by analyzing audit records where analysis engine acts as a research portion of the Intrusion Detection System); and

a reporting portion configured to generate a report that identifies the at least one source of potential pestware activity (Paragraph 0003: audit record provides a report of

what activities are normal and what are unusual as a reporting component, for example).

Porras does not disclose,

a timestamp module configured to generate a time of interest in response to a suspicion of pestware on the computer;

Wang from the same or similar fields of endeavor teaches that a browser component is configured to record timestamps along with an event log (Paragraph 0041: Gatekeeper Browser Helper Object (BHO) is provided for monitoring activity and to record the timestamp of a suspicious event) and trace the process or application that is responsible for an attack (Paragraph 0050: Browser Helper Object (BHO) is customized such that the source of a suspected process or application can be identified).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention, to use a component that is configured to record timestamps related to a suspicious event on a host computer as taught by Wang et al. in the teaching of Porras for the advantage of identifying potential unwanted software through timestamp records and tracing the source that is suspected of originating pestware so appropriate actions can be taken against those sessions and applications that are responsible for potential attacks.

Regarding claim 13, the combination of Porras and Wang discloses the system of claim 12, wherein the at least one log includes information that relates the time of

interest to an event, and wherein the at least one log includes information that relates the event to a suspected pestware object, and wherein the at least one log includes information that relates the suspected pestware object to the at least one source of potential pestware activity (Porras, Paragraph 0015: source of the attack is identified using session identifier, IP address in the audit record or from the record that is obtained from network communication events).

Regarding claim 14, the combination of Porras and Wang discloses the system of claim 13, including: a heuristics module configured to evaluate whether the event is a suspected pestware-related event before the research portion accesses information in the at least one log that relates the event to the suspected pestware object (Porras, Paragraph 0013: based on the evaluation, preprocessor associates necessary information to the audit record before sending it to the IDS's (Intrusion Detection System) analysis engine where preprocessor functions as a heuristics module and analysis engine as a research portion, for example)

Regarding claim 15, the combination of Porras and Wang discloses the system of claim 14, wherein the heuristics module determines that the at least one event is suspected to be pestware-related by analyzing other events in connection with the event, wherein the other events are also related to the time of interest (Porras, Paragraph 0013: preprocessor associates related event information with suspected audit record and then provides the combined information to the analysis engine)

Regarding claim 16, the combination of Porras and Wang discloses the system of claim 12, wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs (Porras, Paragraph 0017: application pathnames related to the suspicious process is obtained where pathnames includes file information, for example)

Regarding claim 17, the combination of Porras and Wang discloses the system of claim 12, wherein the timestamp module configured to generate a time of interest in response to user input, which indicates the suspicion of pestware on the computer (Porras, Paragraph 0014: kernel audit records are received in real time and analyzed periodically to identify any suspicious activity from attacker).

Regarding claim 18, the combination of Porras and Wang discloses the system of claim 17, wherein the user input is in response to an alert provided to the user (Porras, Paragraph 0017: IDS operator or system administrator takes selective action once the alert is generated regarding any suspicious activity from attacker).

Regarding claim 19, the combination of Porras and Wang discloses the system of claim 12, wherein the timestamp module configured to generate the time of interest

as a time interval (Porras , Paragraph 0014: kernel audit records are received in real time and analyzed periodically to identify any suspicious activity from attacker).

Regarding claim 20, the combination of Porras and Wang discloses the system of claim 12, wherein the timestamp module is configured to generate the time of interest as a point in time (Porras , Paragraph 0014: kernel audit records are generated in real time, for example).

Regarding claim 21, the combination of Porras and Wang discloses the system of claim 12, including a kernel-mode driver adapted to monitor activity on the computer and to generate an activity log that is included within the at least one log (Porras, Paragraph 0014: kernel audit records are analyzed periodically or as needed basis to identify any suspicious activity from attacker; Paragraph 0015: session identifier recorded as a log entry in kernel audit records, for example).

Regarding claim 22, the combination of Porras and Wang discloses the system of claim 12, wherein the at least one source of potential pestware activity is identified by an identifier selected from the group consisting of an I.P. address, a URL, an email client and a program name (Porras, Paragraph 0015: IP address or a session identifier associated with the source of a user in the audit record)

Regarding claim 23, the combination of Porras and Wang discloses the system of claim 12, wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs (Porras, Paragraph 0017: network communication event in audit records; Paragraph 0017: application pathnames related to the suspicious process is obtained where pathnames includes file information, for example).

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- MARC ZUTA (WO009845778A2) discloses ANTIVIRUS SYSTEM AND METHOD.
- Hockey (US 2004/0064515 A1) discloses Monitoring electronic mail message digests.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MAHFUZUR RAHMAN whose telephone number is (571)270-7638. The examiner can normally be reached on Monday thru Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on (571)272-3787. 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.

/MAHFUZUR RAHMAN/
Examiner, Art Unit 4124

/Taghi T. Arani/
Supervisory Patent Examiner, Art Unit 2438

Notice of References Cited	Application/Control No. 11/408,145	Applicant(s)/Patent Under Reexamination BONEY, MATTHEW L.	
	Examiner MAHFUZUR RAHMAN	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2004/0024864	02-2004	Porras et al.	709/224
*	B	US-2005/0268112	12-2005	Wang et al.	713/188
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Trend Micro, Inc.
EX1002-217

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11408145	BONEY, MATTHEW L.
	Examiner	Art Unit
	MAHFUZUR RAHMAN	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/15/2009								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								

Trend Micro, Inc.
EX1002-218

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11408145	BONEY, MATTHEW L.
	Examiner	**Art Unit**
	MAHFUZUR RAHMAN	2438

SEARCHED

Class	Subclass	Date	Examiner
726	22-25, 13	6/15/2009	MR
713	187-188, 193-194	6/15/2009	MR

SEARCH NOTES

Search Notes	Date	Examiner
East Search, search terms used: token, indicia, signature, identifier, pestware, maleware, spamware, adware, scumware, event log, history, source, time stamp	6/15/2009	MR
Used Primary provided search classes	6/15/2009	MR
Performed Inventor/Assignee name search on PALM	6/15/2009	MR
Google Patent using session, maleware, spamware, adware, attack, timestamp, event log, source, origin, trace	6/16/2009	MR

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

/MAHFUZUR RAHMAN/ Examiner.Art Unit 4124	

Trend Micro, Inc.
EX1002-219

Please type a plus sign (+) inside this box → [+]

PTO/SB/08A (08-00)

Substitute for form 1449A/PTO		*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT		Application Number	11/408,145
		Filing Date	04/20/2006
		First Named Inventor	Matthew L. Boney
(use as many sheets as necessary)		Group Art Unit	2154
		Examiner Name	Not Yet Assigned
Sheet	1 of 3	Attorney Docket Number	WEBR-045/00US

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	U.S. Patent Document Number	Kind Code[2] (*if known*)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY
		5,623,600		JI, ET AL.	04/22/97
		5,920,696		BRANDT ET AL.	07/1999
		5,951,698		CHEN ET AL.	09/1999
		6,069,628		FARRY, ET AL.	05/30/00
		6,073,241		ROSENBERG, ET AL.	06/06/00
		6,092,194		TOUBOUL	07/18/00
		6,154,844		TOUBOUL	11/28/00
		6,167,520		TOUBOUL	12/26/00
		6,310,630		KULKARNI, ET AL.	10/30/01
		6,397,264		STASNICK, ET AL.	05/28/02
		6,405,316		KRISHNAN ET AL.	06/2002
		6,460,060		MADDALOZZO, JR., ET AL.	10/01/02
		6,480,962		TOUBOUL	11/12/02
		6,535,931		CELI, JR.	03/18/03
		6,611,878		DE ARMAS, ET AL.	08/26/03
		6,633,835		MORAN ET AL.	10/14/03
		6,667,751		WYNN, ET AL.	12/23/03
		6,701,441		BALASUBRAMANIAM, ET AL.	03/02/04
		6,772,345		SHETTY	08/2004
		6,785,732		BATES, ET AL.	08/31/04
		6,804,780		TOUBOUL	10/12/04
		6,813,711		DIMENSTEIN	11/02/04
		6,829,654		JUNGEK	12/07/04
		6,910,134		MAHER ET AL.	06/2005
		6,965,968		TOUBOUL	11/15/05
		7,058,822		EDERY ET AL.	06/06/06
		7,107,617		HURSEY ET AL.	09/2006
		US 2002/0162015		TANG	10/2002
		US 2002/0166063		LACHMAN ET AL.	11/2002
		US 2003/0065943		GEIS ET AL.	04/2003
		US 2003/0074581		HURSEY ET AL.	04/2003
		US 2003/0101381		MATEEV ET AL.	05/2003
		US 2003/0159070		MAYER ET AL.	08/2003
		US 2003/0217287	A1	KRUGLENKO	11/20/03
		US 2004/0030914	A1	KELLEY, ET AL.	02/12/04
		US 2004/0034794	A1	MAYER ET AL.	02/19/04
		US 2004/0064736	A1	OBRECHT, MARK ERIC, ET AL.	04/01/04
		US 2004/0080529	A1	WOJCIK, PAUL KAZIMIERZ	04/29/04
		US 2004/0143763	A1	RADATTI	07/22/04

Examiner Signature	06/17/2009	Date Considered	06/17/2009

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

[1] Unique citation designation number.
[2] See attached Kinds of U.S. Patent Documents.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH./M.R./

Hitachi Micros., Inc.
EX1002-220

Please type a plus sign (+) inside this box → [+]

PTO/SB/08A (08-00)

Substitute for form 1449A/PTO		*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT		Application Number	11/408,145
		Filing Date	04/20/2006
		First Named Inventor	Matthew L. Boney
		Group Art Unit	2154
(use as many sheets as necessary)		Examiner Name	Not Yet Assigned
Sheet	2 of 3	Attorney Docket Number	WEBR-045/00US

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	U.S. Patent Document Number	Kind Code[2] (*if known*)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY
		US 2004/0187023	A1	ALAGNA, MICHAEL ANTHONY, ET AL.	09/23/04
		US 2004/0225877	A1	HUANG	11/11/04
		US 2005/0038697	A1	JEFFREY	02/2005
		US 2005/0154885		VISCOMI ET AL.	07/2005
		US 2005/0138433	A1	LINETSKY, GENE	06/23/05
		2006/0075494		BERTMAN ET AL.	04/2006
		2006/0075501		THOMAS ET AL.	04/2006
		2006/0161988		COSTEA ET AL.	07/2006
		10/956,573		STEVE THOMAS	N/A Filed: 10/01/04
		10/956,574		STEVE THOMAS	N/A Filed: 10/01/04
		10/956,818		MATTHEW BONEY	N/A Filed: 10/01/04
		11/257,609		MICHAEL BURTSCHER	N/A Filed: 10/25/05
		11/237,291		PHILIP MADDALONI	N/A Filed: 09/28/05
		11/408,215		MATTHEW BONEY	N/A Filed: 04/20/06
		11/408,146		MATTHEW BONEY	N/A Filed: 04/20/06

Examiner Signature	/Mahfuzur Rahman/	Date Considered	06/17/2009

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

[1] Unique citation designation number.
[2] See attached Kinds of U.S. Patent Documents.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH./M.R./

Hitachi Micro, Inc.
EX1002-221

Please type a plus sign (+) inside this box → [+]

PTO/SB/08A (08-00)

Substitute for form 1449A/PTO		*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT		Application Number	11/408,145
		Filing Date	04/20/2006
		First Named Inventor	Matthew L. Boney
		Group Art Unit	2154
(use as many sheets as necessary)		Examiner Name	Not Yet Assigned
Sheet	3 of 3	Attorney Docket Number	WEBR-045/00US

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document			Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	T[4]
		Office[1]	Number[2]	Kind Code[3] (if known)			

OTHER – 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[2]
	I.	Codeguru, Three Ways to Inject Your Code Into Another Process, by Robert Kuster, August 4, 2003, 22 pgs.	
	II.	Codeguru, Managing Low-Level Keyboard Hooks With The Windows API for VB .Net, by Paul Kimmel, April 18, 2004, 10 pgs.	
	III.	Codeguru, Hooking The Keyboard, by Anoop Thomas, December 13, 2001, 6 pgs.	
	IV.	Illusive Security, Wolves In Sheep's Clothing: malicious DLLs Injected Into trusted Host Applications, Author Unknown, http://home.arcor.de/scheinsicherheit/dll.htm 13 pgs.	
	V.	DevX.com, Intercepting Systems API Calls, by Seung-Woo Kim, May 13, 2004, 6 pgs.	
	VI.	Microsoft.com, How To Subclass A Window in Windows 95, Article ID 125680, July 11, 2005, 2 pgs.	
	VII.	MSDN, Win32 Hooks by Kyle Marsh, July 29, 1993, 15 pgs.	
	VII.	PCT Search Report, PCT/US05/34874, 07/05/06, 7 Pages	
	VIII	Yurcik, William et al., "A Planning Framework for Implementing Virtual Private Networks, June 2001, IT Pro, IEEE, pages 41-44	

Examiner Signature	/Mahfuzur Rahman/	Date Considered	06/17/2009

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

[1] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3).
[2] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document.
[3] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible.
[4] Applicant is to place a check mark here if English language Translation is attached.

[1] Unique citation designation number.
[2] Applicant is to place a check mark here if English language Translation attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH./M.R./

Finjan Microsystems, Inc.
EX1002-222

Please type a plus sign (+) inside this box → [+]

PTO/SB/08A (07-05)
Approved for use through 07/31/2006. OMB 0651-0031

Substitute for form 1449A/PTO		*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT		Application Number	11/408,145
		Filing Date	04/20/2006
		First Named Inventor	Mathew L. BONEY
(use as many sheets as necessary)		Group Art Unit	2154
		Examiner Name	Not yet assigned
Sheet	1 of 1	Attorney Docket Number	WEBR-045/00US 303666-2050

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
		US-2002/0162017-A1	10-31-2002	Sorkin	
		US-2005/0005160-A1	01-06-2005	Bates	
		US-2005/0268112-A1	12-01-2005	Wang	

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[2]
		PCT/US2006/025378	09-18-2007	Piccard	Search Report and Written Opinion	
		PCT/US2007/067076	11-02-2007	Boney	Search Report and Written Opinion	
		PCT/US2007/067084	11-05-2007	Boney	Search Report and Written Opinion	

Examiner Signature	/Mahfuzur Rahman/	Date Considered	06/17/2009

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Unique citation designation number (optional). [2]See attached Kinds of U.S. Patent Documents. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours 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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH./M.R./

Hirtd Micro, Inc.
EX1002-223

Please type a plus sign (+) inside this box → [+]

PTO/SB/08A (07-05)
Approved for use through 07/31/2006. OMB 0651-0031

Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(use as many sheets as necessary)*		***Complete if Known***	
		Application Number	11/408,145
		Filing Date	04/20/2006
		First Named Inventor	Matthew L. BONEY
		Group Art Unit	2154
		Examiner Name	
Sheet	1 of 1	Attorney Docket Number	WEBR-045/00US 303666-2050

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
		US-2004/0024864 A1	02-05-2004	Phillip Andrew PORRAS	
		US-2004/0064515 A1	04-01-2004	Alyn HOCKEY	

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[2]
		WO 98/45778	10-15-1998	Marc ZUTA		
		PCT/US2007/067078	04-20-2007 (Filed)	Webroot Software, Inc.	International Search Report and Written Opinion of the International Searching Authority mailed 11/02/2007	

Examiner Signature	/Mahfuzur Rahman/	Date Considered	06/17/2009

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Unique citation designation number (optional). [2]See attached Kinds of U.S. Patent Documents. This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours 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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH./M.R./

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	"11408145"	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2009/06/15 09:56
S18	7684	726/22-25,13;713/187-188,193-194.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2009/06/15 14:27
S19	21	S18 and ((token indicia sign$5) same (pestware maleware spamware adware scumware))	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2009/06/15 14:30
S20	21	S19 and (@ad<"20060420" or rlad<"20060420")	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2009/06/15 14:32
S21	19	S20 and (time period)	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2009/06/15 14:48
S25	21	S18 and ((token indicia sign$5) same (pestware maleware spamware adware scumware))	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2009/06/15 15:03
S27	19	S25 and (time period)	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2009/06/15 15:04
S28	2	S27 and (time$1stamp "time stamp")	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2009/06/15 15:10

S29	2	S28 and (log history)	US-PGPUB; USPAT; FPRS; EPO; JPO	OR	OFF	2009/06/15 15:12

6/17/2009 12:31:02 PM
C:\Documents and Settings\mrahman4\My Documents\EAST\Workspaces\30_Time Stamp to find Origin of Pestware_04202006_11408145\30_Time Stamp to find Origin of Pestware_04202006_11408145.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

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

BIB DATA SHEET

CONFIRMATION NO. 8007

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
11/408,145	04/20/2006	709	2438	WEBR-045/00US 303666-2050

APPLICANTS
Matthew L. Boney, Longmont, CO;

**** CONTINUING DATA ***************************

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****
05/16/2006

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /MAHFUZUR RAHMAN/ Examiner's Signature	☐ Met after Allowance MR Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CO	5	23	2

ADDRESS

COOLEY GODWARD KRONISH LLP
ATTN: PATENT GROUP
Suite 1100
777 - 6th Street, NW
WASHINGTON, DC 20001
UNITED STATES

TITLE

Backward researching time stamped events to find an origin of pestware

FILING FEE RECEIVED		
1280	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

Trend Micro, Inc.
EX1002-227

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:	Mathew L. BONEY	Confirmation No.:	8007
Serial No.:	11/408,145	Group Art Unit:	2154
Filed:	04/20/2006	Examiner:	Not yet assigned

FOR: **BACKWARD RESEARCHING TIME STAMPED EVENTS TO FIND AN ORIGIN**

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

INFORMATION DISCLOSURE STATEMENT UNDER 37 C.F.R. §1.97(b)

In accordance with the duty of disclosure set forth in 37 C.F.R. §1.56, Applicant(s) hereby submits the following information in conformance with 37 C.F.R. §§1.97 and 1.98.

[x] Pursuant to 37 C.F.R. §1.98, a copy of each non-US patent document cited in the attached Form PTO/SB/08 is enclosed.

[x] No copies of any U.S. patents or U.S. patent application publications listed on the attached Form PTO/SB/08 are being provided pursuant to 37 C.F.R. §1.98.

This Information Disclosure Statement is filed within any one of the following time periods:

[] within three months from the filing date of this national application other than a CPA under 37 C.F.R. § 1.53(d);

[] within three months from the date of entry of the national stage as set forth in 37 C.F.R. §1.491 in this international application;

[x] 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 C.F.R. § 1.114.

It is respectfully requested that the Examiner consider the above-noted information and return an initialed copy of the attached Form PTO/SB/08 to the undersigned.

COOLEY GODWARD KRONISH LLP
ATTN: Patent Group
777 6th Street NW, Suite 1100
Washington, DC 20001

Tel: (720) 566-4044
Fax: (202) 842-7899

Respectfully submitted,
COOLEY GODWARD KRONISH LLP

By: Thomas M. Croft
Thomas M. Croft
Reg. No. 44,051

Please type a plus sign (+) inside this box → [+]

PTO/SB/08A (07-05)
Approved for use through 07/31/2006. OMB 0651-0031

Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(use as many sheets as necessary)*		***Complete if Known***	
		Application Number	11/408,145
		Filing Date	04/20/2006
		First Named Inventor	Mathew L. BONEY
		Group Art Unit	2154
		Examiner Name	Not yet assigned
Sheet	1 of 1	Attorney Docket Number	WEBR-045/00US 303666-2050

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
		US-2002/0162017-A1	10-31-2002	Sorkin	
		US-2005/0005160-A1	01-06-2005	Bates	
		US-2005/0268112-A1	12-01-2005	Wang	

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[2]
		PCT/US2006/025378	09-18-2007	Piccard	Search Report and Written Opinion	
		PCT/US2007/067076	11-02-2007	Boney	Search Report and Written Opinion	
		PCT/US2007/067084	11-05-2007	Boney	Search Report and Written Opinion	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Unique citation designation number (optional). [2]See attached Kinds of U.S. Patent Documents. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours 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.

PATENT COOPERATION TREATY

3036666-2015

From the INTERNATIONAL SEARCHING AUTHORITY

To:
SEAN R. O'DOWD
COOLEY GODWARD, LLP
ATTN: PATENT GROUP
THE BOWEN BUILDING
875 15TH STREET, NW, SUITE 800
WASHINGTON, DC 20005-2221

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

	Date of mailing (*day/month/year*)
Applicant's or agent's file reference WEBR01700WO	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US06/25378	International filing date (*day/month/year*) 29 June 2006 (29.06.2006)
Applicant WEBROOT SOFTWARE, INC.	

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

   When? The time limit for filing such amendments is normally twomonths from the date of transmittal of the international search report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: (41-22) 338.82.70.

   For more detailed instructions, see the notes on the accompanying sheet.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the Intenational Searching Authority are transmitted herewith.

3. ☐ **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

   ☐ no decision has been made yet on the protest; theapplicant will be notified as soon as a decision is made.

4. **Reminders**

   Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90*bis*.1 and 90*bis*.3, respectively, before the completion of the technical preparations for international publication.

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of**30 months** (or later) will apply even ifno demand is filed within 19 months.

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address ofthe ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Nasser Moazzami Telephone No. (571)272-2100

Jean Proctor
Paralegal Specialist

Form PCT/ISA/220 (January 2004) *(See notes on accompanying sheet)*

RECEIVED
SEP 24 2007
COOLEY GODWARD KRONISH LLP

ENTERED
DUE:
EOL: Written Opinion 12/18/07
Abstract 10/18/07
Article 19 Amendment 11/18/07

Trend Micro, Inc.
EX1002-231

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
SEAN R. O'DOWD
COOLEY GODWARD, LLP
ATTN: PATENT GROUP
THE BOWEN BUILDING
875 15TH STREET, NW, SUITE 800
WASHINGTON, DC 20005-2221

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

	Date of mailing (*day/month/year*) 18 SEP 2007
Applicant's or agent's file reference WEBR01700WO	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US06/25378	International filing date (*day/month/year*) 29 June 2006 (29.06.2006)
Applicant WEBROOT SOFTWARE, INC.	

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

   When? The time limit for filing such amendments is normally twomonths from the date of transmittal of the international search report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: (41-22) 338.82.70.

   For more detailed instructions, see the notes on the accompanying sheet.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the Intenational Searching Authority are transmitted herewith.

3. ☐ **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

   ☐ no decision has been made yet on the protest; theapplicant will be notified as soon as a decision is made.

4. **Reminders**

   Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90*bis*.1 and 90*bis*.3, respectively, before the completion of the technical preparations for international publication.

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of**30 months** (or later) will apply even ifno demand is filed within 19 months.

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address ofthe ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Nasser Moazzami Telephone No. (571)272-2100

Jean Proctor
Paralegal Specialist

Form PCT/ISA/220 (January 2004) *(See notes on accompanying sheet)*

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference WEBR01700WO	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below
International application No. PCT/US06/25378	International filing date (*day/month/year*) 29 June 2006 (29.06.2006)	(Earliest) Priority Date (*day/month/year*) 30 June 2005 (30.06.2005)
Applicant WEBROOT SOFTWARE, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the Report**
   a. With regard to the **language**, the international search was carried out on the basis of:
      ☒ the international application in the language in which it was filed.
      ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. ☐ **Certain claims were found unsearchable** (See Box No. II)
3. ☐ **Unity of invention is lacking** (See Box No. III)
4. With regard to the **title**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,
   a. the figure of the **drawings** to be published with the abstract is Figure No. 1
      ☒ as suggested by the applicant.
      ☐ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figures is to be published with the abstract.

Trend Micro, Inc.
EX1002-233

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US06/25378

A. CLASSIFICATION OF SUBJECT MATTER

IPC: **G06F 12/14**(2006.01)

USPC: 726/24

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 726/24

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

ACM/IEEE?Springer/Altavista/Google/Scholar/Archive

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	US 2006/0075468 A1 (BONEY et al) 6 April 2006 (06.04.2006)	1-18
X	US 6,785,732 B1 (BATES et al) 31 August 2004 (31.08.2004)	1-18
X	US 2005/0005160 A1 (BATES et al) 6 January 2005 (06.01.2005)	1-18
X,P	US 2006/0080637 A1 (TREIT et al) 13 April 2006 (13.04.2006)	1-18

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

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

"E" earlier application or patent published on or after the international filing date

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

02 August 2007 (02.08.2007)

Date of mailing of the international search report

18 SEP 2007

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Facsimile No. (571) 273-3201

Authorized officer

Nasser Moazzami

Jean Proctor
Paralegal Specialist

Telephone No. (571)272-2100

Form PCT/ISA/210 (second sheet) (April 2005)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
SEAN R. O'DOWD
COOLEY GODWARD, LLP
ATTN: PATENT GROUP
THE BOWEN BUILDING
875 15TH STREET, NW, SUITE 800
WASHINGTON, DC 20005-2221

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing (*day/month/year*)	18 SEP 2007
Applicant's or agent's file reference WEBR01700WO	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date (*day/month/year*)	Priority date (*day/month/year*)
PCT/US06/25378	29 June 2006 (29.06.2006)	30 June 2005 (30.06.2005)

International Patent Classification (IPC) or both national classification and IPC

IPC: **G06F 12/14**(2006.01)
USPC: 726/24

Applicant

WEBROOT SOFTWARE, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I — Basis of the opinion
- ☐ Box No. II — Priority
- ☐ Box No. III — Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV — Lack of unity of invention
- ☒ Box No. V — Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI — Certain documents cited
- ☐ Box No. VII — Certain defects in the international application
- ☐ Box No. VIII — Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis(b)* that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	11 August 2007 (11.08.2007)	Nasser Moazzami Jean Proctor Paralegal Specialist Telephone No. (571)272-2100

Form PCT/ISA/237 (cover sheet) (April 2005)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US06/25378

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

☒ the international application in the language in which it was filed

☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

a. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ on paper

☐ in electronic form

c. time of filing/furnishing

☐ contained in the international application as filed.

☐ filed together with the international application in electronic form.

☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

Trend Micro, Inc.
EX1002-236

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US06/25378

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims NONE	YES
	Claims 1-18	NO
Inventive step (IS)	Claims NONE	YES
	Claims 1-18	NO
Industrial applicability (IA)	Claims 1-18	YES
	Claims NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

Trend Micro, Inc.
EX1002-237

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient.**

V. 2. Citations and Explanations:
Claims 1-18 lack novelty under PCT Article 33(2) as being anticipated by Bates et al (US Patent 6,785,732, hereinafter Bates).

Regarding claim 1, Bates teaches a method of identifying a malware distribution site, comprising: analyzing a file to determine that the file includes potential malware (abstract); searching a download history log to identify a Web site from which the file was downloaded (abstract); and generating an indication that the Web site corresponds to a potential malware distribution site (abstract, col. 3, lines 35-67, col. 6, lines 1-40).

Regarding claim 7, Bates teaches a computer-readable medium comprising executable instructions to: compare a file with a set of malware definitions; based on determining that the file matches one of the set of malware definitions, determine a Web address from which the file was received; and generate an indication that the Web address is associated with malware (abstract, col. 3, lines 35-67, col. 6, lines 1-40).

Regarding claim 13, Bates teaches a system of managing malware, comprising: a malware detection module configured to analyze a file of a protected computer to determine that the file is associated with malware; and a Web site identification module configured to search a download history log of the protected computer to identify a Web site from which the file was downloaded (abstract, col. 3, lines 35-67, col. 6, lines 1-40).

Regarding claim 2, Bates teaches wherein the analyzing the file includes determining that the file matches one of a set of malware definitions (col. 12, lines 1-60).

Regarding claims 3, 10, and 14, Bates teaches wherein the download history log corresponds to a Web browser's history log (abstract, col. 6, lines 1-40).

Regarding claims 4, 11, and 15, Bates teaches generating the download history log based on a Web browser's history log (abstract, col. 6, lines 1-40).

Regarding claims 5 and 9, Bates teaches wherein the searching the download history log includes searching the download history log to identify a Web address associated with the Web site (abstract, col. 6, lines 1-40).

International application No.
PCT/US06/25378

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient.**

Regarding claims 6 and 18, Bates teaches wherein the analyzing the file, the searching the download history log, and the generating the indication are performed at a protected computer, the method further comprising: directing the protected computer to convey the indication to a remotely-located computer (abstract, col. 6, lines 1-40).

Regarding claim 8, Bates teaches wherein the executable instructions to compare the file with the set of malware definitions include executable instructions to compare a hash value of the file with a set of hash values of malware (col. 12, lines 1-60).

Regarding claim 12, Bates teaches wherein the Web address corresponds to a Universal Resource Locator associated with a Web site (abstract, col. 6, lines 1-40).

Regarding claim 16, Bates teaches wherein the Web site identification module is configured to search the download history log to identify a Universal Resource Locator associated with the Web site (abstract, col. 6, lines 1-40).

Regarding claim 17, Bates teaches a reporting module configured to generate an indication that the Web site corresponds to a potential malware distribution site (col. 11, lines 5-67).

NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under Article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the *PCT Applicant's Guide*, a publication of WIPO.

In these Notes, "Article," "Rule" and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions, respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report and the written opinion of the International Searching Authority, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims, description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only (see *PCT Applicant's Guide*, Volume I/A, Annexes B1 and B2).

The attention of the applicant is drawn to the fact that amendments to the claims under Article 19 are not allowed where the International Searching Authority has declared, under Article 17(2), that no international search report would be established (see *PCT Applicant's Guide*, Volume I/A, paragraph 296).

What parts of the international application may be amended ?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Preliminary Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

When ? Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

Where not to file the amendments ?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

How ? Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet must be submitted for each sheet of the claims which, on account of an amendment or amendments, differs from the sheet originally filed.

All the claims appearing on a replacement sheet must be numbered in Arabic numerals. Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively (Section 205(b)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments ?

Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

Trend Micro, Inc.
EX1002-240

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
WEBR04300WO		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2007/067084	20/04/2007	20/04/2006
Applicant		
WEBROOT SOFTWARE, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 5 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language,** the international search was carried out on the basis of:
      [X] the international application in the language in which it was filed
      [ ] a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. [ ] **Certain claims were found unsearchable** (See Box No. II)

3. [ ] **Unity of invention is lacking** (see Box No III)

4. With regard to the **title,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings,**
   a. the figure of the **drawings** to be published with the abstract is Figure No. 3
      [ ] as suggested by the applicant
      [ ] as selected by this Authority, because the applicant failed to suggest a figure
      [X] as selected by this Authority, because this figure better characterizes the invention
   b. [ ] none of the figures is to be published with the abstract

Trend Micro, Inc.
EX1002-241

International application No
PCT/US2007/067084

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98/45778 A (ZUTA MARC [IL]) 15 October 1998 (1998-10-15) page 16, line 7 - line 18 page 18, line 9 - line 12 page 26, line 1 - last line	1-4, 7-19,22, 23
X	US 2005/268112 A1 (WANG YI-MIN [US] ET AL) 1 December 2005 (2005-12-01) page 6, paragraph 50	1,9,16
A	US 2006/074896 A1 (THOMAS STEVE [US] ET AL) 6 April 2006 (2006-04-06) page 2, paragraph 20	
A	US 2004/064515 A1 (HOCKEY ALYN [GB]) 1 April 2004 (2004-04-01) page 6, paragraph 116	

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

☒ See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 October 2007	05/11/2007

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Arbutina, Ljiljana

Trend Micro, Inc.
EX1002-242

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

Continuation of Box II.2

Claims Nos.: 5,6,20,21

Method claim 5 has been drafted as dependent on claim 1. It is not clear from the wording of these claims whether the steps of monitoring and recording (claim 5) are performed before, or after, or interleaved with steps of identifying and accessing (claim 1).
According to the description, once a pestware presence is established, existing logs are accessed and analysed in order to identify the source of the pestware. This would imply that the steps of monitoring and recording (claim 5) are performed before the steps of identifying and accessing (claim 1). However, the steps of monitoring and recording refer to a pestware process, implying that a process is already identified as a pestware. This means that the step of identifying (claim 1) is performed first, which contradicts previous conclusion.
Since the scope of claim 5 could not be defined neither from the wording of claims 5 and 1 alone, nor trying to interpret it in the light of the description, no meaningful search for claim 5, dependent claim 6, and corresponding claims 20 and 21 could be done.

The applicant's attention is drawn to the fact that claims relating to inventions in respect of which no international search report has been established need not be the subject of an international preliminary examination (Rule 66.1(e) PCT). The applicant is advised that the EPO policy when acting as an International Preliminary Examining Authority is normally not to carry out a preliminary examination on matter which has not been searched. This is the case irrespective of whether or not the claims are amended following receipt of the search report or during any Chapter II procedure. If the application proceeds into the regional phase before the EPO, the applicant is reminded that a search may be carried out during examination before the EPO (see EPO Guideline C-VI, 8.5), should the problems which led to the Article 17(2) declaration be overcome.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2007/067084

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos.: 5,6,20,21
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
see FURTHER INFORMATION sheet PCT/ISA/210

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers allsearchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search reportcovers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

Trend Micro, Inc.
EX1002-244

Information on patent family members

International application No
PCT/US2007/067084

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9845778 A	15-10-1998	AU 6850798 A	30-10-1998
US 2005268112 A1	01-12-2005	EP 1605332 A2	14-12-2005
		JP 2005339565 A	08-12-2005
		KR 20060046231 A	17-05-2006
US 2006074896 A1	06-04-2006	NONE	
US 2004064515 A1	01-04-2004	AU 8235901 A	13-03-2002
		EP 1368719 A2	10-12-2003
		GB 2366706 A	13-03-2002
		WO 0219069 A2	07-03-2002

Trend Micro, Inc.
EX1002-245

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2007/067084	20.04.2007	20.04.2006

International Patent Classification (IPC) or both national classification and IPC
INV. G06F21/00

Applicant
WEBROOT SOFTWARE, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☒ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

JN
ENTERED 1st 34 Dmend.
DUE:
EOL: 2-5-2008.

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	see form PCT/ISA/210	Arbutina, Ljiljana Telephone No. +31 70 340-4522

Trend Micro, Inc.
EX1002-246

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

   a. type of material:

      ☐ a sequence listing

      ☐ table(s) related to the sequence listing

   b. format of material:

      ☐ on paper

      ☐ in electronic form

   c. time of filing/furnishing:

      ☐ contained in the international application as filed.

      ☐ filed together with the international application in electronic form.

      ☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non obvious), or to be industrially applicable have not been examined in respect of

☐ the entire international application

☒ claims Nos. 5,6,20,21

because:

☐ the said international application, or the said claims Nos. relate to the following subject matter which does not require an international search *(specify)*:

☐ the description, claims or drawings *(indicate particular elements below)* or said claims Nos. are so unclear that no meaningful opinion could be formed *(specify)*:

☐ the claims, or said claims Nos. are so inadequately supported by the description that no meaningful opinion could be formed *(specify)*:

☒ no international search report has been established for the whole application or for said claims Nos. 5,6,20,21

☐ a meaningful opinion could not be formed without the sequence listing; the applicant did not, within the prescribed time limit:

- ☐ furnish a sequence listing on paper complying with the standard provided for in Annex C of the Administrative Instructions, and such listing was not available to the International Searching Authority in a form and manner acceptable to it.
- ☐ furnish a sequence listing in electronic form complying with the standard provided for in Annex C of the Administrative Instructions, and such listing was not available to the International Searching Authority in a form and manner acceptable to it.
- ☐ pay the required late furnishing fee for the furnishing of a sequence listing in response to an invitation under Rules 13*ter*.1(a) or (b).

☐ a meaningful opinion could not be formed without the tables related to the sequence listings; the applicant did not, within the prescribed time limit, furnish such tables in electronic form complying with the technical requirements provided for in Annex C-*bis* of the Administrative Instructions, and such tables were not available to the International Searching Authority in a form and manner acceptable to it.

☐ the tables related to the nucleotide and/or amino acid sequence listing, if in electronic form only, do not comply with the technical requirements provided for in Annex C-*bis* of the Administrative Instructions.

☐ See Supplemental Box for further details

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	2,10,11,12,13,17
	No:	Claims	1,3,4,7,8,9,14,15,16,18,19,22,23
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-4,7-19,22,23
Industrial applicability (IA)	Yes:	Claims	1-4,7-19,22,23
	No:	Claims	

2. Citations and explanations

see separate sheet

Trend Micro, Inc.
EX1002-249

Re Item III.

No opinion is established for claims 5, 6, 20 and 21 because no international search report has been established for these claims. No meaningful search for these claims could be done for the following reason:

Method claim 5 has been drafted as dependent on claim 1. It is not clear from the wording of these claims whether the steps of monitoring and recording (claim 5) are performed before, or after, or interleaved with steps of identifying and accessing (claim 1). According to the description, once a pestware is detected on a computer, existing logs are accessed and analysed in order to identify the source of the pestware. This would imply that the steps of monitoring and recording (claim 5) are performed before steps of identifying and accessing (claim 1). However, the steps of monitoring and recording refer to a pestware process, implying that a process is already identified as a pestware. This means that the step of identifying (claim 1) is performed first, which contradicts previous conclusion.

Since the scope of claim 5 could not be defined neither from the wording of claims 5 and 1 alone, nor trying to interpret it in the light of the description, no meaningful search for claim 5, dependent claim 6, and corresponding claims 20 and 21 could be done.

Re Item V.

1 Reference is made to the following document:
D1 : WO 98/45778 A (ZUTA MARC [IL]) 15 October 1998 (1998-10-15)

2 INDEPENDENT CLAIMS 1, 9 AND 16

2.1. The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of claim 1 is not new in the sense of Article 33(2) PCT.

Trend Micro, Inc.
EX1002-250

Document D1 discloses (the references in parentheses applying to this document):
a method for identifying an origin of pestware residing on computer comprising:
- identifying pestware on the computer (page 18, lines 9-12 and page 26, line 3, "a sensitive instruction or sequence of instructions took place");
- accessing recorded information on the computer relating to a history of the pestware, and traversing at least a subset of the recorded information, wherein the traversing includes accessing data within recorded information that provides a reference to an identity of a source of the pestware (page 26, lines 17-18: "logging the virus activity and tracing it to source").

2.2. Regarding corresponding computer program claim 16, it should be noted that, although the monitoring part itself in D1 is done by the hardware, this hardware is initiated by processor-executable instructions (D1, page 16, line 14). Therefore, the reasoning here above also applies, mutatis mutandis, to independent claim 16.

2.3. The additional feature of claim 9, namely a reporting portion configured to report the source of the pestware to a pestware research entity is also disclosed in D1, page 26, lines 16-17. Therefore, the subject-matter of claim 1 is not new (Article 33(2) PCT).

3 DEPENDENT CLAIMS 2-4, 7, 8, 10-15, 17-19, 22, 23

Dependent claims 2-4, 7, 8, 10-15, 17-19, 22, 23 do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of novelty and/or inventive step (Article 33(2) and (3) PCT), see the passages cited in the search report. It should be noted that D1 discloses in the cited passages a general idea of detecting a presence of a pestware in a computer and using activity log to trace the pestware to the source. A skilled person would, following this idea, implement a variety of detection methods and a variety of history logs present in the computer, depending on a specific computer and operating system used. Such modifications of D1 cannot be considered as involving an inventive step.

Trend Micro, Inc.
EX1002-251

Trend Micro, Inc.
EX1002-252

Possible steps after receipt of the international search report (ISR) and written opinion of the International Searching Authority (WO-ISA)

General information	For all international applications filed on or after 01/01/2004 the competent ISA will establish an ISR. It is accompanied by the WO-ISA. Unlike the former written opinion of the IPEA (Rule 66.2 PCT), the WO-ISA is not meant to be responded to, but to be taken into consideration for further procedural steps. This document explains about the possibilities.
Amending claims under Art. 19 PCT	Within 2 months after the date of mailing of the ISR and the WO-ISA the applicant may file amended claims under Art. 19 PCT directly with the International Bureau of WIPO. The PCT reform of 2004 did not change this procedure. For further information please see Rule 46 PCT as well as form PCT/ISA/220 and the corresponding Notes to form PCT/ISA/220.
Filing a demand for international preliminary examination	In principle, the WO-ISA will be considered as the written opinion of the IPEA. This should, in many cases, make it unnecessary to file a demand for international preliminary examination. If the applicant nevertheless wishes to file a demand this must be done before expiry of 3 months after the date of mailing of the ISR/ WO-ISA or 22 months after priority date, whichever expires later (Rule 54bis PCT). Amendments under Art. 34 PCT can be filed with the IPEA as before, normally at the same time as filing the demand (Rule 66.1 (b) PCT). If a demand for international preliminary examination is filed and no comments/amendments have been received the WO-ISA will be transformed by the IPEA into an IPRP (International Preliminary Report on Patentability) which would merely reflect the content of the WO-ISA. The demand can still be withdrawn (Art. 37 PCT).
Filing informal comments	After receipt of the ISR/WO-ISA the applicant may file informal comments on the WO-ISA directly with the International Bureau of WIPO. These will be communicated to the designated Offices together with the IPRP (International Preliminary Report on Patentability) at 30 months from the priority date. Please also refer to the next box.
End of the international phase	At the end of the international phase the International Bureau of WIPO will transform the WO-ISA or, if a demand was filed, the written opinion of the IPEA into the IPRP, which will then be transmitted together with possible informal comments to the designated Offices. The IPRP replaces the former IPER (international preliminary examination report).
Relevant PCT Rules and more information	Rule 43 PCT, Rule 43bis PCT, Rule 44 PCT, Rule 44bis PCT, PCT Newsletter 12/2003, OJ 11/2003, OJ 12/2003

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
WEBR04400WO		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2007/067076	20/04/2007	20/04/2006
Applicant		
WEBROOT SOFTWARE, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language,** the international search was carried out on the basis of:
      [X] the international application in the language in which it was filed
      [ ] a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. [ ] **Certain claims were found unsearchable** (See Box No. II)

3. [ ] **Unity of invention is lacking** (see Box No III)

4. With regard to the **title,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings,**
   a. the figure of the **drawings** to be published with the abstract is Figure No. 1
      [X] as suggested by the applicant
      [ ] as selected by this Authority, because the applicant failed to suggest a figure
      [ ] as selected by this Authority, because this figure better characterizes the invention
   b. [ ] none of the figures is to be published with the abstract

Trend Micro, Inc.
EX1002-254

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/268112 A1 (WANG YI-MIN [US] ET AL) 1 December 2005 (2005-12-01) page 6, paragraph 50	1,3,4,7, 8,17,19, 22
Y	WO 98/45778 A (ZUTA MARC [IL]) 15 October 1998 (1998-10-15) page 26, line 1 - last line	1-22
Y	US 2004/064515 A1 (HOCKEY ALYN [GB]) 1 April 2004 (2004-04-01) page 6, paragraph 116	1-22

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

☒ See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 October 2007	02/11/2007

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Arbutina, Ljiljana

1

Form PCT/ISA/210 (second sheet) (April 2005)

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005268112 A1	01-12-2005	EP 1605332 A2	14-12-2005
		JP 2005339565 A	08-12-2005
		KR 20060046231 A	17-05-2006
WO 9845778 A	15-10-1998	AU 6850798 A	30-10-1998
US 2004064515 A1	01-04-2004	AU 8235901 A	13-03-2002
		EP 1368719 A2	10-12-2003
		GB 2366706 A	13-03-2002
		WO 0219069 A2	07-03-2002

Trend Micro, Inc.
EX1002-256

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)* see form PCT/ISA/210 (second sheet)	
Applicant's or agent's file reference see form PCT/ISA/220	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2007/067076	20.04.2007	20.04.2006

International Patent Classification (IPC) or both national classification and IPC
INV. G06F21/00

Applicant
WEBROOT SOFTWARE, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

jew 10 SR
ENTERED Written Opinion
DUE:
EOL: 2/2/08

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	See form PCT/ISA/210	Arbutina, Ljiljana Telephone No. +31 70 340-4522

Form (PCT/ISA/237) (Cover Sheet) (April 2005)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

   a. type of material:

      ☐ a sequence listing

      ☐ table(s) related to the sequence listing

   b. format of material:

      ☐ on paper

      ☐ in electronic form

   c. time of filing/furnishing:

      ☐ contained in the international application as filed.

      ☐ filed together with the international application in electronic form.

      ☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

Trend Micro, Inc.
EX1002-258

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	2,5,6,9-16,18,20,21
	No:	Claims	1,3,4,7,8,17,19,22
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-22
Industrial applicability (IA)	Yes:	Claims	1-22
	No:	Claims	

2. Citations and explanations

see separate sheet

Trend Micro, Inc.
EX1002-259

Re Item V.

1 Reference is made to the following documents:

D1 : US 2005/268112 A1 (WANG YI-MIN [US] ET AL) 1 December 2005 (2005-12-01)

D2 : WO 98/45778 A (ZUTA MARC [IL]) 15 October 1998 (1998-10-15)

D3 : US 2004/064515 A1 (HOCKEY ALYN [GB]) 1 April 2004 (2004-04-01)

2 INDEPENDENT CLAIMS 1 AND 17, DOCUMENT D1

2.1. The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of claim 1 is not new in the sense of Article 33(2) PCT.

Document D1 discloses (the references in parentheses applying to this document):
a method for identifying an origin of activity on a computer that is indicative of pestware comprising
- monitoring the computer for activity that is indicative of pestware (page 6, left-hand col., last line - right-hand col. 1st line: "if any of the files is later instantiated to create more ASEP hooks", creating a hook being an activity indicative of pestware);
- identifying, based upon the activity, an object residing on the computer that is a suspected pestware object (page 6, right-hand col, lines 2-4), and
- accessing at least a portion of a recorded history of sources that the computer received files from so as to identify a reference to an identity of a particular source that the suspected pestware object originated from (page 6, left-hand col., lines 21-25 of par.[50]).

The same reasoning applies, mutatis mutandis, to corresponding claim 17.

3 INDEPENDENT CLAIMS 1, 9 AND 17, DOCUMENTS D2 AND D3

3.1. The present application does not meet the criteria of Article 33(1) PCT, because the subject matter of claim 1 does not involve an inventive step in the sense of Article 33(3)PCT.

Trend Micro, Inc.
EX1002-260

Document D2 discloses (the references in parentheses applying to this document):
a method for identifying an origin of activity on a computer that is indicative of pestware comprising
- monitoring the computer for activity that is indicative of pestware (page 26, lines 5-12: "monitors execution since init... writing to files without some processing or user input");
- identifying, based upon the activity, an object residing on the computer that is a suspected pestware object (page 26, lines 17-18: "logging the virus activity and tracing it to source").

The subject-matter of independent claim 1 differs from the disclosure of D2 in
- accessing at least a portion of a recorded history of sources that the computer received files from so as to identify a reference to an identity of a particular source that the suspected pestware object originated from.

The problem to be solved by the present invention may therefore be regarded as how to track the pestware back to the originator.

This problem was solved in D3, see page 6, lines 1-2 of par.[116], giving the same solution as the one proposed in the present claim, see lines 3-7 of par.[116].

Therefore the features disclosed in D2 and D3 would be combined by the skilled person, without exercise of any inventive skills in order to solve the problem posed. The proposed solution in independent claim 1 thus cannot be considered inventive (Article 33(3) PCT).

The same reasoning applies, mutatis mutandis, to corresponding claim 17.

3.2. Regarding additional features of claim 9, D2 also discloses a heuristic module configured to identify activity on the computer that is indicative of pestware residing on the computer (page 26, lines 9-12), and a reporting portion configured to generate a report that identifies the source of the file (page 26, lines 16-17: "reports which program initiated, introduced virus in our PC"; in the view of the reasoning here above, a skilled person would report also the source of the program as a matter of a routine activity.

Therefore. the subject matter of claim 9 cannot be considered inventive (Article 33(3)

Trend Micro, Inc.
EX1002-261

PCT).

4 DEPENDENT CLAIMS 2-8, 10-16, 18-22

Dependent claims 2-8, 10-16, 18-22 do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of novelty and/or inventive step (Article 33(2) and (3) PCT), see the passages cited in the search report.

Trend Micro, Inc.
EX1002-262

Possible steps after receipt of the international search report (ISR) and written opinion of the International Searching Authority (WO-ISA)

General information	For all international applications filed on or after 01/01/2004 the competent ISA will establish an ISR. It is accompanied by the WO-ISA. Unlike the former written opinion of the IPEA (Rule 66.2 PCT), the WO-ISA is not meant to be responded to, but to be taken into consideration for further procedural steps. This document explains about the possibilities.
Amending claims under Art. 19 PCT	Within 2 months after the date of mailing of the ISR and the WO-ISA the applicant may file amended claims under Art. 19 PCT directly with the International Bureau of WIPO. The PCT reform of 2004 did not change this procedure. For further information please see Rule 46 PCT as well as form PCT/ISA/220 and the corresponding Notes to form PCT/ISA/220.
Filing a demand for international preliminary examination	In principle, the WO-ISA will be considered as the written opinion of the IPEA. This should, in many cases, make it unnecessary to file a demand for international preliminary examination. If the applicant nevertheless wishes to file a demand this must be done before expiry of 3 months after the date of mailing of the ISR/WO-ISA or 22 months after priority date, whichever expires later (Rule 54bis PCT). Amendments under Art. 34 PCT can be filed with the IPEA as before, normally at the same time as filing the demand (Rule 66.1 (b) PCT). If a demand for international preliminary examination is filed and no comments/amendments have been received the WO-ISA will be transformed by the IPEA into an IPRP (International Preliminary Report on Patentability) which would merely reflect the content of the WO-ISA. The demand can still be withdrawn (Art. 37 PCT).
Filing informal comments	After receipt of the ISR/WO-ISA the applicant may file informal comments on the WO-ISA directly with the International Bureau of WIPO. These will be communicated to the designated Offices together with the IPRP (International Preliminary Report on Patentability) at 30 months from the priority date. Please also refer to the next box.
End of the international phase	At the end of the international phase the International Bureau of WIPO will transform the WO-ISA or, if a demand was filed, the written opinion of the IPEA into the IPRP, which will then be transmitted together with possible informal comments to the designated Offices. The IPRP replaces the former IPER (international preliminary examination report).
Relevant PCT Rules and more information	Rule 43 PCT, Rule 43bis PCT, Rule 44 PCT, Rule 44bis PCT, PCT Newsletter 12/2003, OJ 11/2003, OJ 12/2003

BNSDOCID: <XS_____20070401OCK_I_>

Trend Micro, Inc.
EX1002-263

From the INTERNATIONAL SEARCHING AUTHORITY

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

To:
COOLEY GODWARD KRONISH LLP
Attn. O'Dowd, Sean R.
1200 19th Street NW, Suite 500
Washington DC 20036
ETATS-UNIS D'AMERIQUE

Date of mailing *(day/month/year)*	02/11/2007
Applicant's or agent's file reference: WEBR04400WO 303666-2095	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No.: PCT/US2007/067076	International filing date *(day/month/year)*: 20/04/2007
Applicant: WEBROOT SOFTWARE, INC.	

1. [x] The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the International Search Report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Fascimile No.: (41-22) 338.82.70

   For more detailed instructions, see the notes on the accompanying sheet.

2. [ ] The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. [ ] **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   [ ] the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

   [ ] no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90*bis*.1 and 90*bis*.3, respectively, before the completion of the technical preparations for international publication.

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

RECEIVED
NOV 05 2007
COOLEY GODWARD KRONISH LLP

Name and mailing address of the International Searching Authority: European Patent Office, P.B. 5818 Patentlaan 2, NL-2280 HV Rijswijk, Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer: Anja Brüger

ENTERED Comment on Abstract
DUE:
EOL: 12/6/07

Form PCT/ISA/220 (October 2005) *(See notes on accompanying sheet)*

NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the *PCT Applicant's Guide*, a publication of WIPO.

In these Notes, "Article", "Rule", and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions, respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report and the written opinion of the International Searching Authority, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims,description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only (see *PCT Applicant's Guide*, Volume I/A, Annexes B1 and B2).

The attention of the applicant is drawn to the fact that amendments to the claims under Article 19 are not allowed where the International Searching Authority has declared, under Article 17(2), that no international search report would be established (see *PCT Applicant's Guide*, Volume I/A, paragraph 296).

What parts of the international application may be amended?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

When? Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

Where not to file the amendments?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

How? Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet must be submitted for each sheet of the claims which, on account of an amendment or amendments, differs from the sheet originally filed.

All the claims appearing on a replacement sheet must be numbered in Arabic numerals. Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively (Section 205(b)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments?

Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

Trend Micro, Inc.
EX1002-265

Electronic Acknowledgement Receipt

EFS ID:	3347414
Application Number:	11408145
International Application Number:	
Confirmation Number:	8007
Title of Invention:	Backward researching time stamped events to find an origin of pestware
First Named Inventor/Applicant Name:	Matthew L. Boney
Customer Number:	22903
Filer:	Thomas M. Croft/Sherry Bitler
Filer Authorized By:	Thomas M. Croft
Attorney Docket Number:	WEBR-045/00US 303666-2050
Receipt Date:	22-MAY-2008
Filing Date:	20-APR-2006
Time Stamp:	20:37:15
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed	WEBR04500USids.pdf	107245 707af6b53e1857b021ed04a8ffc7c04c411eee1a	no	3

Warnings:	
Information:	

This is not an USPTO supplied IDS fillable form					
2	Foreign Reference	WEBR04500US-01700WOsrwo.pdf	509169 8d2f44dead9594a4e15f0cd847acf4d5edb10340	no	10
Warnings:					
Information:					
3	Foreign Reference	WEBR04500US-04300WOsrwo.pdf	519256 da50e397d6dbd8f070c29b550e9f535899d88f53	no	13
Warnings:					
Information:					
4	Foreign Reference	WEBR04500US-04400WOsrwo.pdf	530395 d84a39d8c3f82b444001fde677835cfb2d147195	no	12
Warnings:					
Information:					
			Total Files Size (in bytes):	1666065	

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 Application of Matthew L. BONEY	Confirmation No.: 8007
Serial No.: 11/408,145	Group Art Unit: 2154
Filed: 04/20/2006	Examiner: Not Yet Assigned

FOR: BACKWARD RESEARCHING TIME STAMPED EVENTS TO FIND AN ORIGIN

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

INFORMATION DISCLOSURE STATEMENT UNDER 37 C.F.R. §1.97(b)

In accordance with the duty of disclosure set forth in 37 C.F.R. §1.56, Applicant(s) hereby submits the following information in conformance with 37 C.F.R. §§1.97 and 1.98.

[x] Pursuant to 37 C.F.R. §1.98, a copy of each non-US patent document cited in the attached Form PTO/SB/08 is enclosed.

[x] No copies of any U.S. patents or U.S. patent application publications listed on the attached Form PTO/SB/08 are being provided pursuant to 37 C.F.R. §1.98.

[x] Publications listed on the attached Form PTO/SB/08 were cited in a foreign search or examination report corresponding to PCT application no. PCT/US2007/067078 mailed on November 2, 2007.

This Information Disclosure Statement is filed within any one of the following time periods:

[] within three months from the filing date of this national application other than a CPA under 37 C.F.R. § 1.53(d);

[] within three months from the date of entry of the national stage as set forth in 37 C.F.R. §1.491 in this international application;

[x] 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 C.F.R. § 1.114.

Trend Micro, Inc.
EX1002-268

It is respectfully requested that the Examiner consider the above-noted information and return an initialed copy of the attached Form PTO/SB/08 to the undersigned.

Dated: November 21, 2007

Respectfully submitted,
COOLEY GODWARD KRONISH LLP

COOLEY GODWARD KRONISH LLP
ATTN: Patent Group
777 6th Street NW, Suite 1100
Washington, DC 20001

Tel: (720) 566-4044
Fax: (202) 842-7899

By: Thomas M. Croft
Thomas M. Croft
Reg. No. 44,051

Please type a plus sign (+) inside this box → [+]

PTO/SB/08A (07-05)
Approved for use through 07/31/2006. OMB 0651-0031

Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(use as many sheets as necessary)*		***Complete if Known***	
		Application Number	11/408,145
		Filing Date	04/20/2006
		First Named Inventor	Matthew L. BONEY
		Group Art Unit	2154
		Examiner Name	
Sheet	1 of 1	Attorney Docket Number	WEBR-045/00US 303666-2050

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
		US-2004/0024864 A1	02-05-2004	Phillip Andrew PORRAS	
		US-2004/0064515 A1	04-01-2004	Alyn HOCKEY	

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[2]
		WO 98/45778	10-15-1998	Marc ZUTA		
		PCT/US2007/067078	04-20-2007 (Filed)	Webroot Software, Inc.	International Search Report and Written Opinion of the International Searching Authority mailed 11/02/2007	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Unique citation designation number (optional). [2]See attached Kinds of U.S. Patent Documents. This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours 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.

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 11/00 | A2

(11) International Publication Number: WO 98/45778

(43) International Publication Date: 15 October 1998 (15.10.98)

(21) International Application Number: PCT/IL98/00170

(22) International Filing Date: 8 April 1998 (08.04.98)

(30) Priority Data:
120632 8 April 1997 (08.04.97) IL

(71)(72) Applicant and Inventor: ZUTA, Marc [IL/IL]; Ben Yehuda Street 19, 49373 Petah Tikva (IL).

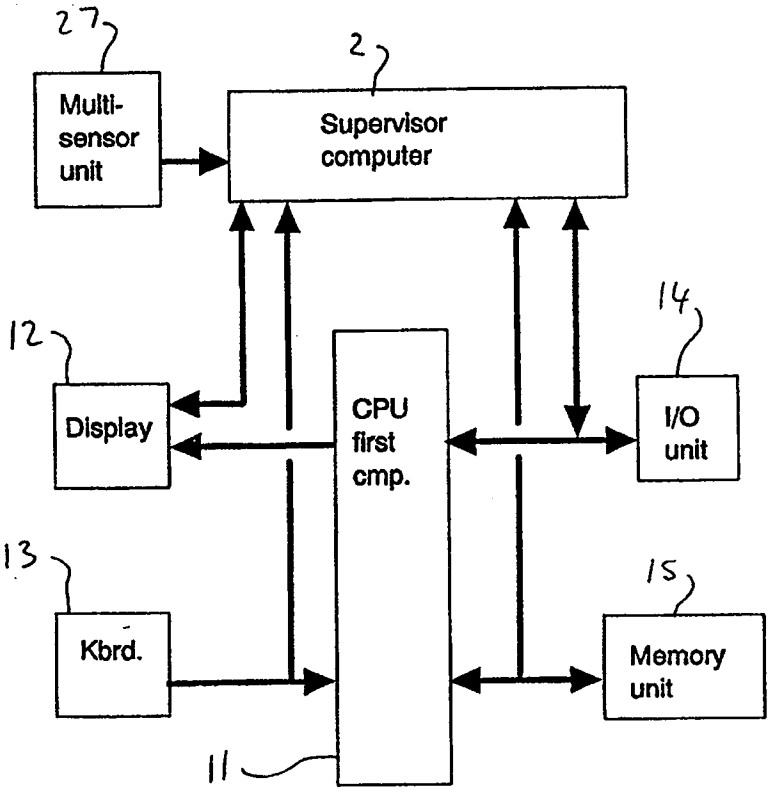
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: ANTIVIRUS SYSTEM AND METHOD

(57) Abstract

In an antivirus multiprocessor system, a second processor attached to a first processor for monitoring its performance and intervening if predefined behaviour thereof is detected. The second processor includes means for continuously supervising the operation of the first processor to detect virus-related activities therein by comparing actual performed instructions in the first processor with instruction sequences corresponding to known viruses or to predefined suspect behaviour. It will stop the first processor after a virus detection. A plurality of sensors is used to detect suspect activity in various media like radio frequency or wireless RF, serial or parallel communication channels, ultrasound, sonic or subsonic waves, power lines and/or optical media including infrared, visible light and/or ultraviolet. An antivirus protection method includes the steps of: A. connecting a second processor to an applications processor; B. using the second processor to continuously monitor the activities on the first processor and to compare to predefined forbidden activities; and C. taking actions in real time when a forbidden activity takes place, to prevent damage to the applications processor.



Trend Micro, Inc.
EX1002-271

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Trend Micro, Inc.
EX1002-272

Antivirus System and Method

Technical Field

This invention concerns antivirus protection systems and methods. The invention relates in particular to such systems in which a second (supervisor) processor is added to a first (applications) processor to continuously monitor its operation so as to prevent damage from viruses or software errors.

Bakground Art

With the proliferation of personal computers and of software therefor, there is a tendency for the hardware to become more and more powerful, and for the software packages to become more and more complex. Software packages nowadays take large disk space, in the range of megabytes to tens of megabytes each.

Heretofore, in this new environment, the computer has become less "personal", in the sense that the user cannot supervise the operation of the computer, or have a reasonable measure of assurance about what the computer is actually doing.

The result is that there are occurences of the computer not doing what its owner intended it to do. Rather, sometimes, the computer is doing something else, which causes damage to the user. The user usually learns too late of the damage, and sometimes may not know about it at all.

The very advantages of the computer have become its greatest weakness: Since the computer is fast and powerful, much damage can be done in a very short time. Before the user can intervene, in a time span of miliseconds, a virus can delete hundreds of files and megabytes of memory.

Presently used software packages are very large, including hundreds of files each, in tens of subdirectories, and taking tens to hundreds of megabytes. It is practically impossible for the user to verify all these files to detect a virus or to assess the damage done to these files.

Computers are used for communications. Much information and many programs are available in the INTERNET, for example. How is one to be sure that the information or programs are not contaminated?
The widely used E-Mail messages may include viruses therein.

The problem is much aggravated in computer networks. A network includes tens to hundreds of computers, each vulnerable to attack and capable of transmitting a virus to other computers. Moreover, a network is usually open to access from the outside, so that a malicious person can connect to a network without physically breaking into the victim's facilities. Much harm can be done from far away.

Following are several examples of computer malfunction instances.

1. Computer viruses. These are programs maliciously introduced into the user's computer, with the express purpose of causing damage.

Sometimes the virus erases information stored in the computer. Other times the virus alters the information without the user's permission. Viruses are known to create dummy files or enlarge existing files, which clutter the memory storage unit, so that the user may not have enough memory left for their purposes.

The name "virus" apparently came from a property of these programs to copy themselves to other media like diskettes, and therefrom to other computers, so that the "virus" is actually "spreading" to "contaminate" other computers.

One approach to the computer virus is the "antivirus" software, which stores digital patterns, each characteristic to a known virus. When starting the computer or inserting a diskette, the antivirus program scans the memory and compares the patterns therein with the stored patterns.

An alarm is activated if the patterns correspond, this indicating the presence of a virus.

The big problem with this approach is that only known viruses, that is viruses whose characteristics are stored in the program, can be detected. It appears that new viruses are continuously created, which are not detected nor protected against by the antivirus programs. In this war between virus and antivirus, the virus will always win, by its time lead. Thus, antivirus programs cannot prevent damage from new viruses which are not included therein.

Another problem with this approach is that the memory is only scanned prior to its use. A self-changing virus can become active after it was scanned, while the antivirus is no longer active.

If an antivirus program is used concurrently with the application, then there is a deterioration in performance, since the same processor is used to alternately perform instructions pertaining to the antivirus and the application. Thus, the application will take more time to run.

Moreover, antivirus programs do not indicate the source of the virus, that is which program contains it. At present, the user does not know which program caused the damage or inserted the virus, thus action cannot be taken at source, to stop that source of viruses and/or to claim damage compensation. The required evidence to prosecute the culprit is not available.

Antivirus programs do not help the user regain control of his/her computer. The program only demands to "clean" the virus, without reporting to its user which files are contaminated and what are the consequences of the cleanup, or allowing any choices to the user.

It is believed by the present inventor that software means cannot be used to protect from another software. A virus can tamper with the antivirus program itself, so that further actions by the user and/or updates of the antivirus are meaningless and useless.

Brute force approaches like denying access to disk or forbidding write operations make the computer practically useless, since a large part of the activity with computers is to read/write files and operate on information. Such a measure may be taken for a limited time. When the user can take it no more and disables the protection, the computer is completely vulnerable to attack.

2. Backdoors, for example a communication program including a routine to allow unauthorized access to another's computer by an outsider. Remote diagnostic programs are a needed feature in computers and networks; the same programs can be used by unauthorized people as backdoors to gain access to the victim computer.

Thus, unauthorized person A can remotely connect to the computer of user B. The trapdoor in user's B computer, of which B is not aware, allows A to access confidential files in that computer, to read them or make changes or to otherwise do damage. It is even possible for user B to connect to a remote computer, without that user being aware of the fact that the other party may use that trapdoor during that same session.

Trapdoors can also be used to introduce viruses, possibly with delayed action, or to access privileged information.

It was stated that most of the damage to computers to any firm is done by employees or former employees at that firm.

The inside knowledge gained during employment there may be used to bypass safequards and do damage.

3. Undesired TSRs (Terminate and Stay Resident programs).

A personal computer, during the several seconds it takes to prepare itself at turn-on until it is ready to accept user's commands, may perform tens to hundreds of millions of instructions. Some programs instruct the computer to be left and active in the memory, thus influencing the computer operation thereafter. This is basically a desirable action, for example a TSR to detect the activation of the mouse and to respond accordingly.

Unfortunately, with the advent of viruses, some TSRs come to perform undesired functions. For example, a maliciously introduced TSR may slow down the computer, by repeatedly performing an unnecessary piece of useless code, without user's knowledge.

The end result is that the computer performs slower than is to be expected, thus preventing the user from getting the full performance from the computer.

4. Unorganized or conflicting TSRs .

Nowadays a personal computer contains tens of different programs, each with its own TSR, all competing for the same computer resources and giving sometimes contradicting instructions to the computer. No software provider takes responsibility for the coexistence of the various programs in the computer.

The user is helpless and cannot intervene, since he/she does not know what is actually going on inside the computer.

5. Uninstall of software packages. It is sometimes difficult to remove a package which is no longer desired. Today software packages are large, tens of megabytes each, with hundreds of files being created on disk and changes performed on existing files. It is sometimes difficult to remove files scattered all over a large disk and to undo changes to existing files.

The problem is that the user sometimes is not completely aware of actions performed by the software package during installation. Sometimes, even with the most friendly install routine, the user will not bother to record all the actions performed, for each package installed, this being a tedious task. Human factors are as important as technical ones, and should be given careful attention.

Moreover, means for protection agains viruses should provide reliable protection, without leaving any doubt as to whether the protection device itself is secure or was compromised by a virus.

The protection means should provide the desired protection without a sizable degradation in the overall performance of the computer.

The protection means should perform its tasks without demanding too much of user's attention or intervention. Eventually, any protection means which is not easy to use will be disposed of.

It is an objective of the present invention to provide for an antivirus system and method using a first and a second processor means for overcoming the abovedetailed disadvantages.

Disclosure of Invention

It is an object of the present invention to provide an antivirus system and method using a multiprocessor system comprising a first processor for performing application programs and a second processor for continuously supervising the operation of the first, to protect it from misuse.

The object is achieved by an antivirus system as disclosed in claim 1.
In accordance with the invention a second processor, the supervisor, is attached to the first processor, the application processor, so that the supervisor includes means to continuously monitor the activity in the application processor, to detect viruses and abnormal operations.

The supervisor further includes means for intervening to stop the applications processor and/or to issue a warning when the virus is detected, to prevent damage.

According to a second object of the present invention, the supervisor itself is protected from attack. It has its own computer and memory, which are independent from the application processor and are protected from any attack by a virus in the application processor. Additional means protect from physical attack.

According to a third object of the present invention, the supervisor computer includes a combination of fast monitoring means in hardware, with smart verification means in a programmed device. These means operate together to protect from known viruses as well as from unknown viruses according to their suspect behavior.

According to a fourth object of the present invention, the supervisor method of operation allows both for detection of viruses in real time, and for smart monitoring of sensitive operations without a sizable decrease in performance. Operation at several levels of complexity is disclosed.

According to a fifth object of the present invention, the supervisor performs a smart verification method, to detect potentially dangerous activities.

According to a sixth object of the present invention, means are detailed for the supervisor to detect viruses without slowing down the applications processor.

According to a seventh object of the present invention, the supervisor includes a multisensor unit which monitors everything going on, in and around the application processor, including a plurality of sensors for sensing the various effects indicative of the presence of a virus.

Further objects, advantages and other features of the present invention will become obvious to those skilled in the art upon reading the disclosure set forth hereinafter.

Brief Description of Drawings

The invention will now be described by way of example and with reference to the accompanying drawings in which:

Fig. 1 is a simplified functional diagram, illustrating the attachment of a supervisor computer to an application computer.

Fig. 2 is a simplified electrical diagram illustrating the attachment of a supervisor computer to an application computer.

1

Fig. 3 details the functional structure of supervisor computer

Fig. 4 details the structure of real time monitoring means

Fig. 5 details the omparator structure and operation

Fig. 6 illustrates the structure of monitoring means using digital signature

Modes for Carrying out the Invention

A preferred embodiment of the present invention will now be described by way of example and with reference to the accompanying drawings.

Fig. 1 illustrates the attachment of supervisor computer 2 to an application computer. The application computer, in this simplified functional diagram, includes a Central Processor Unit CPU 11, connected to display means 12, keyboard 13, Input/Output unit (I/O) 14 and memory unit 15.

The application computer is the original computer which provides the computer functions desired by the user, and to which is added the supervisor 2 to ensure that indeed it will perform the desired functions, without the interference of viruses or malevolent programs.

One function of the supervisor 2 is to monitor activity on busses of CPU 11, like data, control and address between CPU 11 and memory 15, and input/output activity between CPU 11 and I/O means 14. Supervisor 2 connects to these busses to watch instructions and check if some forbidden activity is about to take place. It searches for known viruses patterns or privileged instructions which require authorization.

The monitoring is done concurrently with normal operation of the application computer, without slowind it down. Supervisor 2 reads commands and data "on-the-fly" in real time.

Another function of supervisor 2 is to act to stop or prevent forbidden activity, after detecting a virus as mentioned above. This is done by: activating a signal to CPU 11 to Reset processor or bring it to Wait state or stop CPU 11 and put its activities under closer scrutiny or log the activities performed.

A third function of supervisor 2 is to perform protected, direct dialog with the user, using the application computer resources like the keyboard 13 and display 12. Supervisor 2 has direct access to these devices, and it can also immobilize the CPU 11 during the dialog with the user. This is used to reliably notify the user of virus problems, to ask questions regarding permitted operations and to accept instructions from the user, like the subdirectories it is permitted to read and/or write files therein.

Moreover, the information in computer 2 can be updated by reading from a diskette (not shown), for example to update the list of viruses. Again, this is preferably done while CPU 11 is not active, to avoid interference with, or eavesdropping to, these activities by a potential virus or ilegitimate program in the applications processor.

The applications computer is deactivated using, for example, its RESET or HOLD or WAIT while supervisor 2 is using the resources therein like the diskette or keyboard or I/O channel.

Thus, the functions of supervisor 2 is to watch and report, prevent disaster, help recover from problem, let the user know how disaster happened, and who caused it.

The multisensor unit 27 supports the monitoring function of supervisor 2, by providing additional information relating to possible effects of viruses.

Thus, a virus can establish a communication link with an unauthorized outsider using any of a wide variety of media, for example through a wireless or RF link, ultrasonic or sonic or subsonic waves, signals on the power lines etc. High frequency signals can be transmitted over power lines to outside the firm or the user's home.

Other possible links may include existing serial or parallel communication channels, like an RS-232 link to a modem or a local net or a phone dialer. These links may be activated under a virus control without the permission or knowledge of the legitimate user. Other possible links may include optical media including infrared, visible light and/or ultraviolet.

Unit 27 includes a plurality of sensors for monitoring the various media for any potential undesired activity. The user may not be able to otherwise sense these activities which may go on about their computer.

Thus, the antivirus system and method uses a first processor, including CPU 11 and related units, for performing application programs and a second processor 2 for continuously supervising the operation of the first, to protect it from misuse. The supervisor 2 is attached to the application processor, wherein supervisor 2 includes means to continuously monitor the activity in the application processor, to detect viruses and abnormal operations. The monitoring is done in real time.

The supervisor further includes means for intervening to stop the applications processor and/or to issue a warning to user when the virus or abnormal operation is detected, to prevent damage to the application processor.

Fig. 2 details the electrical attachment of a supervisor computer 2 to an application computer, in a simplified biock diagram.

The supervisor computer 2 connects, or couples to a first processor, that is the applications computer. The multisensor unit 27 gives the supervisor 2 the ability to monitor the various media around the applications computer, as detailed below.

The applications computer includes the CPU 11, display means 12, keyboard 13, Input/Output unit (I/O) 14, memory unit 15 and other resources 16. All these devices are connected to each other through control/data/address bus 17, as known in the art.

Supervisor 2 connects to bus 17, thus gaining access to all the resources of the application computer. Whereas supervisor 2 monitors activity on the applications computer through bus 17 and exercises control over the application computer if need be, it does not use the memory 15 of the applications computer to store its programs or data.

By including (not shown) its own, separate processor and memory with programs and data, supervisor 2 is protected from attack by virus in the applications computer.

Supervisor 2 includes means to protect from physical attack, tampering with, removal from bus 17. Its board (not shown) is encased in hard plastic, to prevent access to its components. Mechanical means may be included (not shown) to lock to motherboard or bus 17 of applications computer.

Additional physical protection means include the supervisor 2 board being soldered to the connector of bus 17, or the supervisor being produced as an integral part of the motherboard of the applications computer.

In another embodiment, the supervisor 2 is manufactured as an integral part of the CPU 11. This achieves a CPU which is protected from viruses, and is practically impossible to separate between the actual CPU and its protection means.

Thus, the supervisor 2 itself is protected from attack. It has its own (not shown) computer and memory, which are independent from the application processor and are protected from any attack by a virus in the application processor. Additional means protect from physical attack.

Fig. 3 Illustrates one embodiment of the functional structure of the supervisor 2 mentioned in Figs. 1 and 2 above. The supervisor includes a combination of fast, real time monitoring means including units 22, 23, 24 and a slower, smart unit comprising controller 21.

Following is a detailed description of the structure and operation of the supervisor.

The supervisor structure includes the following means:

1. monitoring means, including registers 22 and 23 and comparators 24, to evaluate operation of first processor in real time for detecting abnormal operation, to stop first computer and issue alarm or warning or indication to controller 21. A shift register 22 continuously receives and shifts in real time instructions read in the first, or the supervised, computer. A plurality of comparators 24 each compares the instruction string with the string of a known virus or a predefined suspect behavior, to detect viruses in real time.

2. controller means 21 to: initiate the monitoring means at start–up, take actions when alarm is issued, dialog with user, program/update internal memory, log and analyze activities performed prior to an alarm or a virus attack. A smart analysis is done to detect suspect behaviour, indicative of virus, after receiving indication from monitoring means.

3. internal memory 25 – for virus patterns and forbidden/ privileged instructions, log of activity prior to virus, allowances in each application program (different set of allowances and masks for each application, according to user's instructions).

The memory can be implemented in the controller IC itself or in a separate IC or ICs or on disk, if adequate safeguards are taken to protect that disk area.

4. multisensor unit 27

The bus 17 of the applications computer, including control, data, address is coupled to comparator shift register 22. Various embodiments are possible, with corresponding levels of performance and circuit complexity. The simplest is to couple only the data bus to shift register 22, using part of the control signals to strobe the data in at the correct timing, as known in the art.

Control signals on bus 17 indicate when an instruction is on the bus, whether this is a memory or I/O operation, whether it is a Read or Write. Register 22 can be wired accordingly to accept a new sample for each new instruction, or only for memory read, or for all data bytes on the bus. This embodiment is suitable for recognizing instructions and various routines.

A more complex embodiment reads into register 22 the data together with the address and the control signals. This enables to search for instructions relating to specific addresses in RAM, like reading from the interrupt vectors area or the DOS sections, or writing to these locations, which are privileged locations. This embodiment requires a wider register 22, that is each stage contains more bits.

Register 22 includes a plurality of stages (not shown), each k bits in parallel. As a new sample is read in from bus 17, all the previous samples are shifted one stage to the right. The oldest sample is transferred out of register 22, to log shift register/FIFO 23.

The samples in the various stages of register 22 are output to extended processor bus 220. Thus, bus 220 contains the data bus and optionally also control and address, for a plurality of times: the last sample, the sample a clock ago, then two clocks ago etc...to 100 or several hundred samples.

Bus 220 contains the words or bytes for the last instructions on the bus 17. These instructions are compared in comparator unit 24 with the instructions for a specific virus, or the instructions sequence for a sensitive operation which demands scrutiny by contoller 21. The monitoring unit contains a plurality of comparator units 24, each programmed to detect one virus or privileged instruction, as detailed below. All the comparators 24 operate concurrently in real time. Each comparator 24 includes a string of a specific virus or instruction sequence, and possibly an ignore mask to ignore irrelevant parameters in the instruction string.

The comparators 24 issue an alarm/warning/action on bus 28, which includes busses 241 and 247. Thus, alarm/warning /action bus 28 is used to issue the alarm/warning if a suspect string or instruction was detected. The bus 28 combines with similar busses from the other comparator units, all connected in parallel.

Bus 28 contains action signals, comprising command bus 247, to take immediate action (fast) if a dangerous string is detected, to RESET or HOLD in wait the applications computer for example. Bus 28 also includes the report alarm bus 241, to report to controller 21 that an alarm/warning or other virus-related activity took place. The specific word on bus 241 can indicate the type of action or virus which was detected.

Thus, according to preprogrammed parameters, when an expected instructions sequence is detected in one of the comparators 24, then the application computer can be immediately stopped if necessary, and the controller 21 notified. If a less dangerous instruction is detected, then controller 21 can be notified without stopping or resetting the applications computer.

Supervisor controller 21 includes nonvolatile memory means 25 holding its programs and parameters, like the virus list. This information is protected from access from the applications computer through bus 17. Thus, programs in supervisor computer are protected from access from outside. The programs for controller are not changeable, to prevent tampering with. No software or virus in PC can affect the second processor. No event in PC can change the programs in second computer, including the user or a virus or any program or occurence in PC.

The internal storage is tamper-proof by application processor. Preferably the programs, parameters (whatever influences operation) are stored in internal ROM/PROM/ CMOS RAM/ Flash Memory.

Time/ date unit 26 serves to perform time-sensitive functions. For example, controller 21 can check the number of different files addressed by an application per second. Too many files acessed in a short time is a suspect activity, suggesting a virus. Time can also be used to log activities, to provide evidence for subsequent legal action.

Controller 21 also reads the report activity bus 231, to read past instructions from register 23, so as to reconstruct activity prior to alarm.
Log shift register/FIFO 23 can be longer than register 22, since only the final stage output goes to an output bus 231. It can keep log of thousands to hundreds of thousands of the last instructions. This allows controller 21 to inspect and find what events took place prior to the virus attack, or where the virus come from.

Controller 21 can take direct control over the application computer through bus 217. This bus can include (not shown) lines to Hold that computer inactive, or to Reset it, together with control, data and address lines to gain access to the application computer and its resources, for example using DMA.

Load parameters bus 29 is used by controller 21 to load parameters into comparators 24, each with a different instruction or instruction string and a corresponding "ignore" mask for each byte or bit, and a desired action to take if that string is detected.

It is possible to update the information/parameters in memory 25, while updates are done under controller 21 supervision. Encrypted messages may be used to program new virus patterns. It is preferred not to allow programming controller while the application is operational, but only with applications stopped by controller 21.

In another embodiment, monitoring means includes means (not shown) for computing digital signature or CRC (Cyclic Redundancy Code) and comparing with signature of viruses, instead of directly comparing bytes. This saves hardware. The embodiment is illustrated in Fig. 6. It is possible (not shown) to use one comparator, while multiplexing virus signatures and masks, to save hardware.

Another embodiment (not shown) uses a DSP (Digital Signal Processor) means or other programmed device instead of hardware, to compute signatures or directly compare with string of bytes and/or to perform masking operations. Very fast processors may be used to perform comparison with virus string as detailed above using a microprogrammed implementation of the abovedetailed structure and its operation method, as detailed with reference to shift register 22 and the comparators 24.

Thus, the supervisor computer includes a combination of fast monitoring means in hardware, with smart verification means in a programmed device. These means operate together to protect from known viruses as well as from unknown viruses according to their suspect behavior.

The controller 21 performs the following functions, in addition to the smart verification which is detailed in the following chapter:

1. Loader, at power-up loads all patterns and ignore to all registers from a mass storage like a Flash Memory.

2. Programmer to accept updates, check validity, then write update in nonvolatile memory. Memory is nonvolatile, like flash or cmos or similar, or magnetic. Internal in supervisor.

3. Update programs, data in internal memory. Can be changed only when entered with special format and CRC and/or encrypted, to enable update of virus list, programs etc by responsible provider. Responsible to user as to integrity of program. PC is in reset or wait during this update, so no virus or nonhonest user can watch, record or tamper with program update in second computer.

Supervisor Computer Operation

There are several possible embodiments, from the simple to complex. These are made possible with the structure detailed above, with monitoring unit including registers 22 and 23 and comparators 24 (fast comparison) under the supervision of the controller 21 (smart analysis):

1. Simple operation, virus pattern detection. At power-up the controller 21 loads known viruses into the monitoring means hardware, that is in comparators 24.

During the subsequent operation of the first computer (the application computer or PC or computer network), the monitoring means act to continuously detect viruses and stop the PC to prevent damage. Controller 21 is inactive, except to display the log of instructions prior to alarm, to report to user what happened there.

2. Guided scan protection: the monitoring means is programmed to detect the activity in the application PC of a piece of code being loaded to RAM for execution. When this activity is detected, the application CPU is stopped and the controller 21 is prompted accordingly. The controller 21 then reads all the instructions which are in RAM and ready for execution in the PC, just prior to their execution, by using bus 217.

While the instructions are thus read, the monitoring means reads samples through bus 17 into register 22 as detailed above and searches in real time, in hardware, for all the known viruses which are programmed therein. Thus, even viruses with self-changing code are detected, since this method verifies each piece of code just prior to its execution.

3. Two-stage protection: comprises fast real-time verification using the monitoring monitoring means, and a higher level, slower, smart verification using the controller 21, for sensitive operations.

At power–up the controller 21 loads known viruses pattern as well as sensitive operations which demand further scrutiny, like interrupts or file operations or I/O. The smart verification is detailed below.

During normal operation thereafter, if a virus is detected then the monitoring means act promptly to stop the applications CPU through bus 247, to prevent damage. If a sensitive operation is detected in the monitoring unit, then the CPU is temporarily stopped and the controller 21 is prompted through bus 241 to perform a smart, in–depth analysis of the situation.

This may be done in addition to controller 21 acting to report virus activity, as for the simple operation detailed above. This embodiment includes the simple hardware protection and further, the second level of verification/protection.

Advantage: protects from attack by yet unknown viruses, with unknown patterns, by detecting suspect activities. These are activities expected from viruses, like writing to files, changing files and more.

Rational: smart tests are difficult to perform in hardware, but are easier to implement in software, in the programmed controller. This, however, takes time and cannot be performed in real time, while the PC operates as normal. According to the present invention, the smart tests are performed for sensitive operations in the PC, which operations are slower than the rest. For example, disk operations are slow since they involve the mechanical movements of the disk head and platter, and take time in the order of milliseconds.

The PC is preferably stopped during the smart test performance.
Thus, the additional time it takes to perform the smart test has no considerable effect on the overall performance of the PC, since smart test can be peformed in about 10 – 100 microseconds, this time being so much shorter than the sensitive operation in the PC, that the overall performance is not much affected.

The smart test can be peformed is such a short time, for example using a 16-bit controller like the Intel 80196.
Similarly, I/O operations like a modem have a relatively slow bit rate, and take overall time in the order of seconds to minutes. Thus, a smart verification prior to the actual performance of the I/O function has no sizable effect on overall PC performance.

4. Active protection: may be performed in addition to the two-stage method. The controller 21 initiates activities in the PC, which are expected to stimulate or provoke viruses into action. Thus the virus is detected, by its activity.
The controller creates a controlled environment, wherein the activity of the PC can be completely predicted; any deviations from the expected activity are the result of a virus, thus the virus is detected before it has a chance to attack.
This is an offensive method of operation, wherein the protection means strikes first to provoke the virus, then to detect it and neutralize it.

Thus, the supervisor method of operation allows both for detection of viruses in real time, and for smart monitoring of sensitive operations without a sizable decrease in performance. Operation at several levels of complexity was disclosed.

Smart Verification Method

This method is performed by controller 21, after it is prompted through bus 241 that a sensitive instruction or sequence of instructions took place. It includes various routines for analyzing the activities in the PC from several aspects.

1. Monitors execution since init or reset. Logs TSR loading, disk access, communications access, especially in the initial stages of the application computer or PC operation. Logs autoexec.bat and config.sys execution, with the actual performance taking place.

2. Pays attention to special instruction or access to specific locations like access to directory or to boot sector, writing to exe, com , bat or sys files, reading too many different files in a short time, accessing files outside a permitted subdirectory, writing to files without some processing or user input (without apparent reason or prompting to do so).

3. Logs install or setup performance, to allow delete install

4. Logs TSR installation, and verifies TSR execution in actual life

5. Tracks virus to source; reports which program initiated, introduced virus in our PC, to take legal action again those responsible for virus. Logging the virus activity and tracing it to source can provide the required evidence to prosecute the culprit.

6. Communicates with user through keyboard, display, diskette, I/O

7. Keeps records in PC disk. May encrypt to preserve on disk. Prevents PC from access to those areas, like from a virus.

8. Logs creation of files on disk. In previous art computers, various applications create *.tmp, or temporary files, of size 5 – 15 megabytes, which clutter disk. If deleted, may interfere with applications. If this is malicious – user may want to know which program did it. If it is an error by programmer – user may want to know , to ask why there are retainted files to clutter disk. A notification may be issued like:

"you forgot a file or 100 files ... in my computer.." .

9. Reports to user by RS–232 or other I/O, while keeping PC inactive to prevent a virus therein from tampering with the transfer or to log it, for later misuse of information, keys or communication protocol.

10. Define illegal activities, or those which require user's manual approval. If detected– stop it and report. for example– request of information by LAN. Prompt from LAN or I/O or Internet to read file or to change it or delete information.

11. Read part of each TSR loading at init/reset into comparator units, to check how often they execute. If it is done too ofter– maybe virus. Report all TSRs being loaded; by whom; memory RAM occupied.

12. Log, monitor disk/diskette access. Too often is unnecessary, results in wear and tear of mechanical parts. Maybe reading information which is not really necessary, or doing damage to many files.

13. Log, monitor access to too many files at once, during short time period. In normal use, computer works with limited number of files. Monitor access to too many subdirectories. User can limit operation to several or few subdirs or to specific areas of disk.

14. Define forbidden combination of activities: ie communications + access to specific subdirs. or comm + printing. or comm + access to other than one subdir, where we deposited a file to read or write. Then load these to comparator units 24, to report back to controller 21 if detected.

15. Special adaptive comparator unit (or several such): freezes a pattern of executed instructions from SR 22 to registers, to compare with itself later on. Detects a virus which creates dummy loops, repetitive execution of unnecessary programs. Method of use: From time to time, at random, controller 21 reads pattern of instructions now executing through bus 231, and load through bus 29 into comparators 24.

The comparator then checks for repetitions of this patterns, and reports to controller. If the pattern repeats too often, it may be a virus. If not, then after a set time a new instructions string is read at random and compared with thereafter.

This solves the problem of a virus slowing down computer operation by initiating it to do unnecessary, dummy commands. It performs an adaptive monitoring and detection of unnecessary repetitions of code.

16. Correlator between program executing and disturbances monitored by sensors (multi-sensor unit 27). If there is correlation - stop and report to user. The user may be unaware that activity in his/her computer are a result of commands received from the LAN or Internet or a bug operated by radio for example, or with ultrasonic waves.

Thus, the supervisor performs a smart verification method, to detect potentially dangerous activities.

Fig. 4 details the structure of real time monitoring means in one embodiment, in simplified block diagram. This is the monitoring means hardware, used to monitor without slowing down the PC or application computer.

Data multiplexer and latches means 222 is used to read information from the applications computer bus, including data bus 172, control bus 173 and address bus 174. These are part of control/data/address of applications computer 17. Means 222 may read all or part of these busses. The PC bus uses data, address, control on 8 or 16 or 32 bit bus. Means 222 aligns the bus by bytes for proper analysis of programs execution, or brings into other uniform form the input samples.

The result is samples of instruction/data bus 223, which are transferred to comparator shift register 22. After input, these samples are shifted to present an instructions sequence for the comparators 24, to compare with existing viruses.

Bus 223 may contain, in addition to data and commands, also the status, strobe etc– the CPU controls issued on the bus. This provides the context of data issued or read: rd/wr, IO/memory, bus width.

These are specific to each CPU like the Intel 386 or Pentium, Motorola 68020, Analog Devices DSP 21020, 21060, and should be interpreted as such.

The shift register includes two parts:
comparator shift register 22, including stages like 224, 225. It shifts the data, commands all the time to the right, then to output bus 229;
and
log shift register/FIFO 23 , which shifts all the time as well, with its output bus 231 connected to controller (not shown).

Register 22 is used for comparison with patterns to search. It is small, about 100– 200 samples with outputs at every stage/sample (internal to supervisor). The first output is the data bus latest output C0 226, with subsequent outputs for previous samples. Thus, data bus i–th output Ci 227 represents one of the n stages in SR 22, and data bus earliest output Cn 228 is the oldest sample in register 22. The busses 226, 227, 228 comprise the abovementioned bus 220.

Register 23 keeps log of last operations, to track virus to source, by reconstruction of activity performed prior to virus attack/detection large, about 10 – 100 ksamples. Contains only output total 231, to controller 21.

Output busses from register 22, including bus 226, 227, 228 are connected in parallel (the same data) to a multitude of comparator units 24, each including:

1. instruction/data reference register 31, which is fixed after initial loading from controller. It includes a plurality of stages, corresponding to the stages of register 22, and with output bus at each stage, of which are shown the reference bus latest value R0 316, the reference bus i–th value Ri 317 which represents one of the n stages in register 31, and the reference bus earliest value Rn 318. The load reference bus 291, part of parameters bus 29, is used to load the initial values into register 31 at power–up.

This programmed structure allows for flexible operation, to load various viruses or instruction strings to be searched for.

2. a plurality of comparator stages in parallel. Illustrated is the comparator first stage 331, for last instruction value. It compares latest output C0 226 with corresponding reference R0 316, using AND mask from bus M0 326. The comparison is bitwise, that is each of k bits of bus C0 226 is compared with a corresponding bit of bus R0 316, with mask bit from M0 326 being applied to allow or ignore the result, then all the partial bit results are collected to result in result of comparison 361, which is detailed below.

Similarly the comparator stage 333, is used for earlies instruction value. Compares earliest output Cn 228 with corresponding reference Rn 318, using AND mask from bus Mn 328. The result of comparison 363 is the output.

AND gate 334 sums up all the results of comparison 361, 363 and all the results in between (n in all), to issue alarm strobe 335 if all the comparison results are positive, indicating the complete detection of a virus string.

3. Mask register 32 . Is fixed after initial loading through load mask bus 292, part of parameters bus 29, at power up. Like register 31, there are outputs at each stage, illustrated with mask bus latest value M0 326, mask bus i-th value Mi 327 represents one of the n stages in register 32, and mask bus earliest value Rn 328.

4. action register 34 holds a digital value indicating the type of action to take, which is related to the virus or event stored in register 31. The action may include Reset the CPU, Hold or only a warning to the controller 21 (see Fig. 3) of the supervisor processor. It is loaded through action bus 293, part of parameters bus 29, used to load the action parameters at power-up, from controller 21 (see Fig. 3).

Alarm/warning /action bus 28 is used to issue the alarm/warning if a suspect string or instruction was detected.

It is combined with similar bus from other comparator units (not shown) operating concurrently with that detailed in Fig. 4, and with their bus 28 connected in parallel to this one to form report alarm bus 241, to report to controller 21 that an alarm/warning or suspect activity took place.

Operation of the unit: This is a pipeline structure, with each instruction or sample of a long string being compared concurrently with all the other samples, using the comparator stages 331 ... 333. Thus, for each new instruction entered into register 22 from bus 17, that instruction together with the previous instructions, are compared with an instruction string pertaining to a virus or sensitive instruction stored in register 31, using mask in register 32.

The operation of the unit is synchronous, in that all the stages of register 22 are shifted at the same time, and the operation of the comparators is synchronized with that shift.

Thus, it was detailed how a string of bytes/ instructions are compared with a reference, by sliding the instructions intercepted from the PC busses past the fixed reference in register 31, using register 22.

What is compared, is shifted in SR 22 – only data or only instructions or also (optional) address or also (optional) control bus. Address information in register 22 allows to relate to specific address range, like interrupt vectors in RAM of PC, or to first instructions (from fixed address) after RESET.

Control information in register 22 allows to relate, or wait for specific instruction types, like only READ, or READ and I/O, or READ and MEMORY, or WRITE and I/O, or DMA, or other combinations.

Control of CPU in applications processor, examples for several CPUs:

1. For the Intel Model i486, or 80486, used in Personal Computers (PC) "compatibles":

RESET – the reset input forces the CPU to abandon all tasks, and restart from the beginning, as in power-up. Can be used where real danger is eminent, and no risks can be taken to preserve status or tasks in progress

HOLD – the hold input causes the CPU to float most of its output and input/output pins, thus allowing access to the supervisor to the address, control and data busses. That is, full control over the PC and its resources. After deactivating the HOLD signal, the CPU will continue its tasks as usual.

To float the outputs means that the outputs go into a tri-state or high impedance state, allowing other devices to control the logic state for the bits on the bus, either 1 or 0.

BOFF – the backoff input forces the CPU to float its bus in the next clock, having an effect similar to HOLD.

2. For the Intel Model Pentium, used in Personal Computers (PC) "compatibles":

RESET – the reset input forces the CPU to abandon all tasks, and restart from the beginning, as in power–up. Like in i486.

HOLD – the Hold Request input causes the CPU to float most of its output and input/output pins.

BOFF – the Back Off input forces the CPU to float its bus in the next clock, having an effect similar to HOLD.

BRDY – indicates that the external device is ready to transfer data.

3. For the Motorola Model 68020 CPU:

RESET – the reset input forces the CPU to abandon all tasks, and restart from the beginning, as in power–up.

HALT – this input stops all processor bus activity, and the bus is floated, to tri–state.

Mask bytes example, for Intel 8086/80486 family:

Structure of instruction "Jump within segment or group" :

Three bytes: Op Code, Disp Low , Disp High ;

Op Code= E9 hexa

Suppose that we aim to detect the "Jump" instruction, where the actual address is irrelevant. Maybe in different computers will load to different addresses. Then the first byte is enabled, and the next two bytes are completely disabled or masked out.

The result: any program including the "Jump" instruction of this type, with whatever parameters, will be detected reliably.

Mask bits example, for Intel 8086/80486 family:

Structure of instruction "Jump on condition" :

Two bytes: Op Code, Displacement ;

Op Code= 70 hexa Jump if overflow

Op Code= 71 hexa Jump if no overflow

Op Code= 72 hexa Jump if below

Op Code= 73 hexa Jump if above

Suppose we desire to detect all of these instructions with one comparator unit. The difference between the op codes is in the lowest two bits, (D1 D0) .

By using a mask 1111 1100 binary and an AND operation with the opcode, the lowest bits are masked out, to be always zero.

The masked opcode is the same for the four instructions, which can be detected with one comparator. Compare with 70 hexa.

If the displacement is irrelevant, then all its bits can be masked out as well (for example by performing AND with 0000 0000 binary).

Thus, means are detailed for the supervisor to detect viruses without slowing down the applications processor.

Fig. 5 details an embodiment of the comparator structure and operation. It details, for example, one embodiment of comparator 331, mentioned with reference to Fig. 4 above. Comparator 331 operates on busses C0 226, R0 316 and M0 326, each k bits wide latest output C0 226, the corresponding reference R0 316 and mask from bus M0 326.

Fig. 5 details the operations on one bit, say bit j. This is representative of the operation of the other bits as well.
One bit of the instruction C0(j) 412 is compared with one bit of the reference R0(j) 413, in XOR gate 41. It compares latest output C0 226 with corresponding reference R0 316, using AND mask from bus M0 326.

The comparison is bitwise, that is each of k bits of bus C0 226 is compared with a corresponding bit of bus R0 316, with mask bit from M0 326 being applied to allow or ignore the result, then all the partial bit results are collected to result in result 361.

The operations on one bit, say bit j, are detailed. This is representative of the operation of the other bits as well.
Thus, one bit of the instruction C0(j) 412 is compared with one bit of the reference R0(j) 413 in XOR gate 41. The output 414 of gate 41 is zero if the bits are equal (either both are 0 or both are 1 logic).
If the mask bit M0(j) 423 is HIGH or ENABLE, then AND gate 42 is transparent, so that its output 424 is identical to signal 414. Similarly, the other comparators (not shown) operate on the other bits of the busses C0, R0, M0 to issue the other input lines 425 to NOR gate 43.

If, and only if, all these input lines 424 and 425 are at ZERO state, then the output 361 of NOR gate 43 goes HIGH, indicating an ALARM or identity for that stage in comparison.

The above description relates to a bit for which the corresponding mask bit 423 is ENABLE, or M0(j)= HIGH. If the mask state is IGNORE or MASK, that is ZERO, then the output 424 of AND gate 42 is always ZERO, regardless of the result of the comparison in gate 41. Thus, the bit j is ignored and assumed equal to the reference, to allow the issuing of an ALARM if the other bits (those which are not ignored) are equal to the reference.

The result of comparison 361 at the output of NOR gate 43 is combined (not shown) with corresponding results from the other stages of comparison, to arrive at a decision regarding a specific virus pattern which is sought after.

The logic circuit of Fig. 5 and the corresponding explanation are just one embodiment of the bitwise comparison process.
Other embodiments will become apparent to persons in the art, like a PAL or FPLA or microcontrolled implementation to perform logical operation or a multiplexed comparison to perform sequential operation on the bits and/or the bytes or word of the relevant busses.

In another embodiment of the abovedetailed structure and method, a digital signal processor like the ANALOG DEVICES INC. DSP21000 family may be used to perform the bitwise logic and other functions as detailed above.

Fig. 6 details another structure of monitoring means, using digital signatures in lieu of direct comparison of all samples of an instruction string.

Data multiplexer and latches means 222 reads instructions from the input bus and generates instruction/data bus 223, which is transferred to comparator shift register 22, and thence to log shift register/FIFO 23. These registers shift all the time, to move the instructions past the comparation unit. The log shift register/FIFO output bus 231 is connected to the controller (not shown).

Thus, for example, register 22 outputs data bus latest output C0 226, and previous samples including data bus i-th output Ci 227 which represents one of the n stages in SR 22, and data bus earliest output Cn 228.

There are also a multitude of comparator units operating concurrently, each receiving the outputs from register 22 in parallel, and each including:

1. signature computing means 51, which receives a data bus 512 from SR 22 and a mask bus 513 from a register (not shown). The output is issued on the digital signature bus 515.

2. comparator 52, compares signature on bus 514 with reference of virus or other event, stored in signature reference register 53 . This is a fixed value, after initial loading. It is loaded through load signature reference bus 291, part of parameters bus 29.

The mask register (not shown) is serial or parallel, as known in the art. It is fixed after initial loading. An alarm strobe 335 is issued (active) if the signatures correspond, indicating the complete detection of a virus string. The alarm strobe 335 connects to an action register (not shown) similar to that in Fig. 4, or similar.

The comparator unit includes a plurality of such comparators, each with a signature computing means 51, comparator 52 and reference 53, and each issuing an alarm strobe 335.

Each may issue a different type of Alarm or Warning or Notice, as programmed by the controller (not shown) in the supervisor processor. All the comparators operate concurrently on the data/instructions supplied to all of them, in parallel, from SR 22.

Example of use of digital signatures:

Time to error – for 200 MHz clock, that is, one comparison and decision is performed each 5 nanoseconds interval.

Time to error: until the accumulated probability of error Pr is Pr=0.5. That is the probability for at least one error (the probability that not a single error occurred is too = 0.5), see Table 1.

Table 1

Number of bytes	Max. value 2^n	Probability of one error	Time to error, seconds	Time to error, years
2	65536	1.52E-05	1.63E-04	5.19E-12
3	1.67E+07	5.96E-08	4.19E-02	1.33E-09
4	4.29E+09	2.32E-10	11.	3.40E-07
5	1.09E+12	9.09E-13	2748.	8.71E-05
6	2.81E+14	3.55E-15	703687.	2.23E-02
7	7.20E+16	1.38E-17	1.80E+08	5.7
8	1.84E+19	5.42E-20	4.61E+10	1462.

Thus, using a signature of eight bytes, the 50% cumulative probability of error is achieved after continuous operation for 1,462 years, at a clock of 200 Megahertz. Thus signatures may be used to achieve a very reliable verification, while concurrently achieving a significant saving in cost and circuit complexity.

According to another aspect of the present invention, the supervisor includes a multisensor unit 27 which monitors everything going on, in and around the application processor, including (not shown) a plurality of sensors for sensing the various effects indicative of the presence of a virus.

The multisensor unit– monitors everything going on, including processor commands, I/O port activity, RS–232, modem/telephone output, ethernet, Internet, LAN, optical (visible/IR/UV), ultrasonic/sonic/subsonic, RF and microwaves, electrical and magnetic fields, disturbance on power line of 50 Hz or 60Hz. Its function: look everywhere, every medium is suspect; anything moving, bring in for inspection.

Part of the sensors are fixed, to continuously sense in and around the PC. Part of the sensors are portable, detachable, like a pen for example, so as to allow the user to bring it to suspect areas or busses.

Various implementations and other embodiments of the present invention will become apparent to persons skilled in the art upon reading the abovedetailed disclosure.

It will be recognized that the foregoing is but one example of an apparatus and method within the scope of the present invention and that various modifications will occur to those skilled in the art upon reading the disclosure set forth hereinbefore.

Claims

What is claimed is:

1. An antivirus protection system comprising a second processor attached to a first processor for monitoring its performance and intervening if predefined behaviour thereof is detected, wherein said second processor includes means for continuously supervising the operation of the first processor to detect virus-related activities therein by comparing actual performed instructions in the first processor with instruction sequences corresponding to known viruses or to predefined suspect behaviour therein, and to stop said activity in the first processor after its detection.

2. The antivirus system according to claim 1, further including means for protection from attack by virus in said first processor and including a separate computer and memory, which are independent from said processor.

3. The antivirus system according to claim 1, wherein said supervising means includes a combination of fast monitoring means in hardware, with smart verification means in a programmed device, with these means operating together to protect from known viruses as well as from unknown viruses according to their suspect behavior.

4. The antivirus system according to claim 1, further including a plurality of sensors to detect suspect activity in various media like radio frequency or wireless RF, serial or parallel communication channels, ultrasound, sonic or subsonic waves, power lines and/or optical media including infrared, visible light and/or ultraviolet.

5. An antivirus multiprocessor system comprising a first processor for performing application programs and a second processor for continuously supervising the operation of the first, wherein said second processor is connected to the bus of said first processor and includes means to monitor activity of the first processor to detect virus-related activities therein by comparing actual performed instructions in the first processor with instruction sequences corresponding to known viruses or to predefined suspect behaviour therein, and to stop said activity in the first processor after its detection.

6. The antivirus system according to claim 5, further including means for protection from attack by virus in the first processor and including a separate computer and memory, which are independent from said processor.

7. The antivirus system according to claim 5, wherein said supervising means includes a combination of fast monitoring means in hardware, with smart verification means in a programmed device, with these means operating together to protect from known viruses as well as from unknown viruses according to their suspect behavior.

8. The antivirus system according to claim 5, further including a plurality of sensors to detect suspect activity in various media like radio frequency or wireless Rf, ultrasound, sonic or subsonic waves, power lines and/or optical media including infrared, visible light and/or ultraviolet.

9. In a multiprocessor system, an antivirus protection method including the steps of:

A. connecting a second processor to a first applications processor;

B. using the second processor to continuously monitor the activities performed on the first processor and to compare to predefined forbidden activities; and

C. when the second processor detects a forbidden activity taking place in the first processor, then the second processor takes predefined actions to prevent damage to the second or applications processor.

10. The antivirus protection method according to claim 9, further including in step (B) the monitoring by the second processsor of a multisensor unit connected thereto.

11. The antivirus protection method according to claim 10, wherein the multisensor unit includes a plurality of sensors to detect suspect activity in various media like radio frequency or wireless Rf, ultrasound, sonic or subsonic waves, power lines and/or optical media including infrared, visible light and/or ultraviolet.

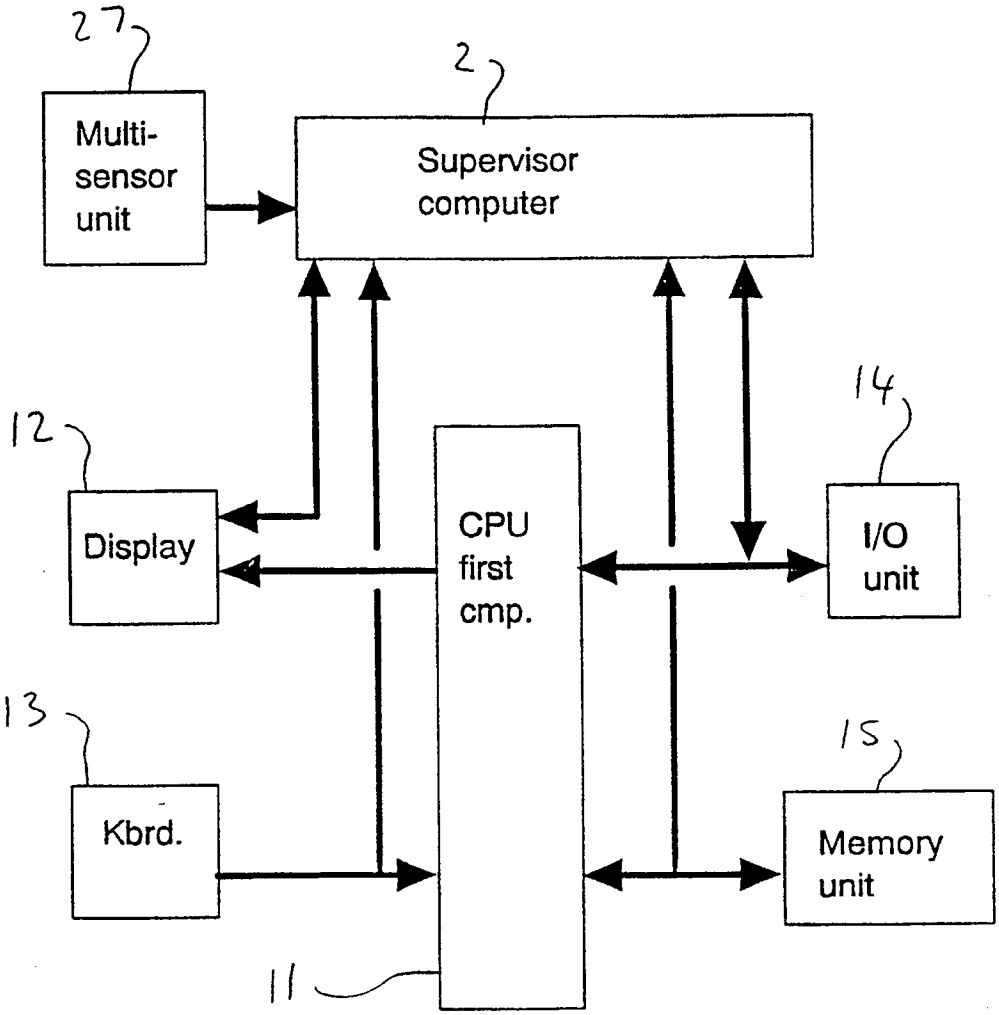

27
Multi-
sensor
unit
2
Supervisor
computer
12
Display
CPU
first
cmp.
14
I/O
unit
13
Kbrd.
15
Memory
unit
11

Fig. 1

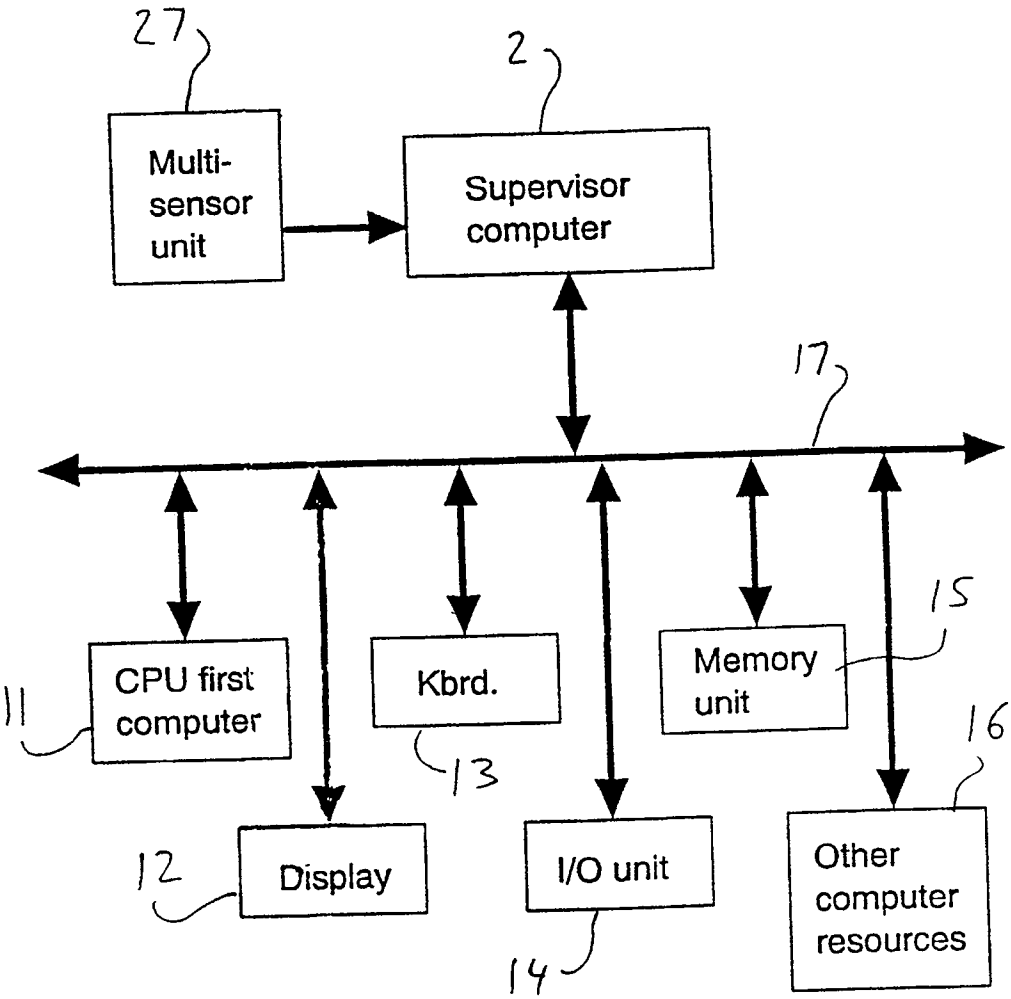

27
2
Multi-sensor unit
Supervisor computer
17
15
CPU first computer
11
Kbrd.
13
Memory unit
16
12
Display
I/O unit
14
Other computer resources

Fig. 2

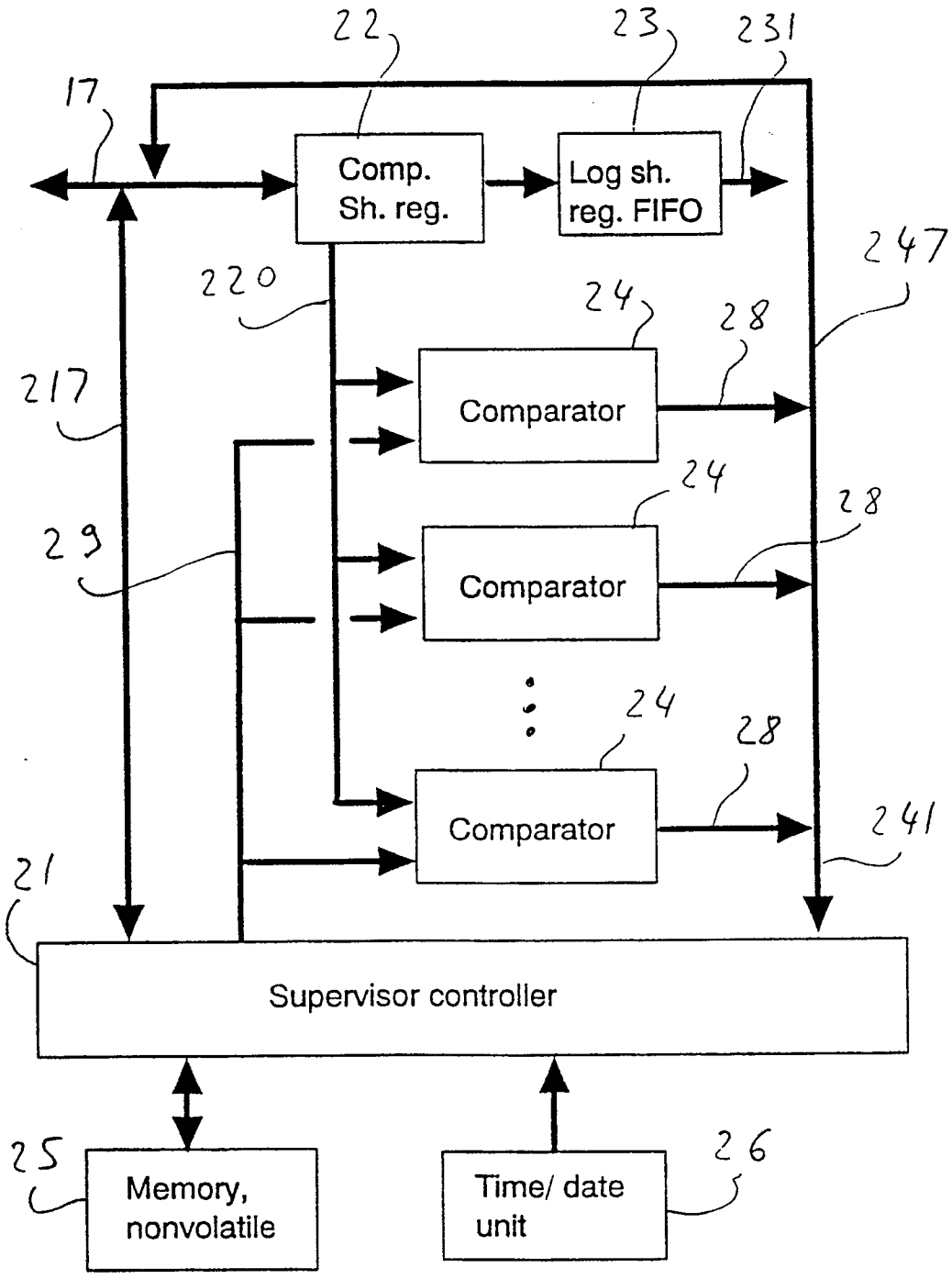
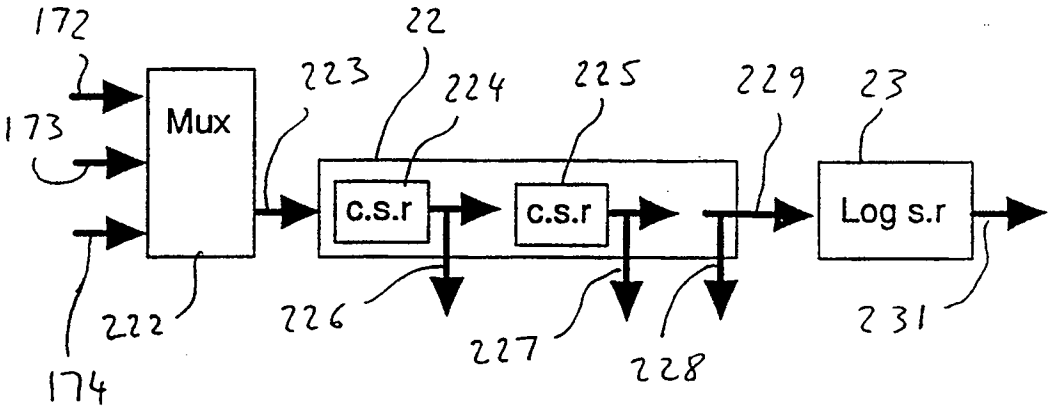


Fig. 3

Trend Micro, Inc.
EX1002-321


172
173
174
Mux
222
223
22
224
225
c.s.r
c.s.r
226
227
228
229
23
Log s.r
231

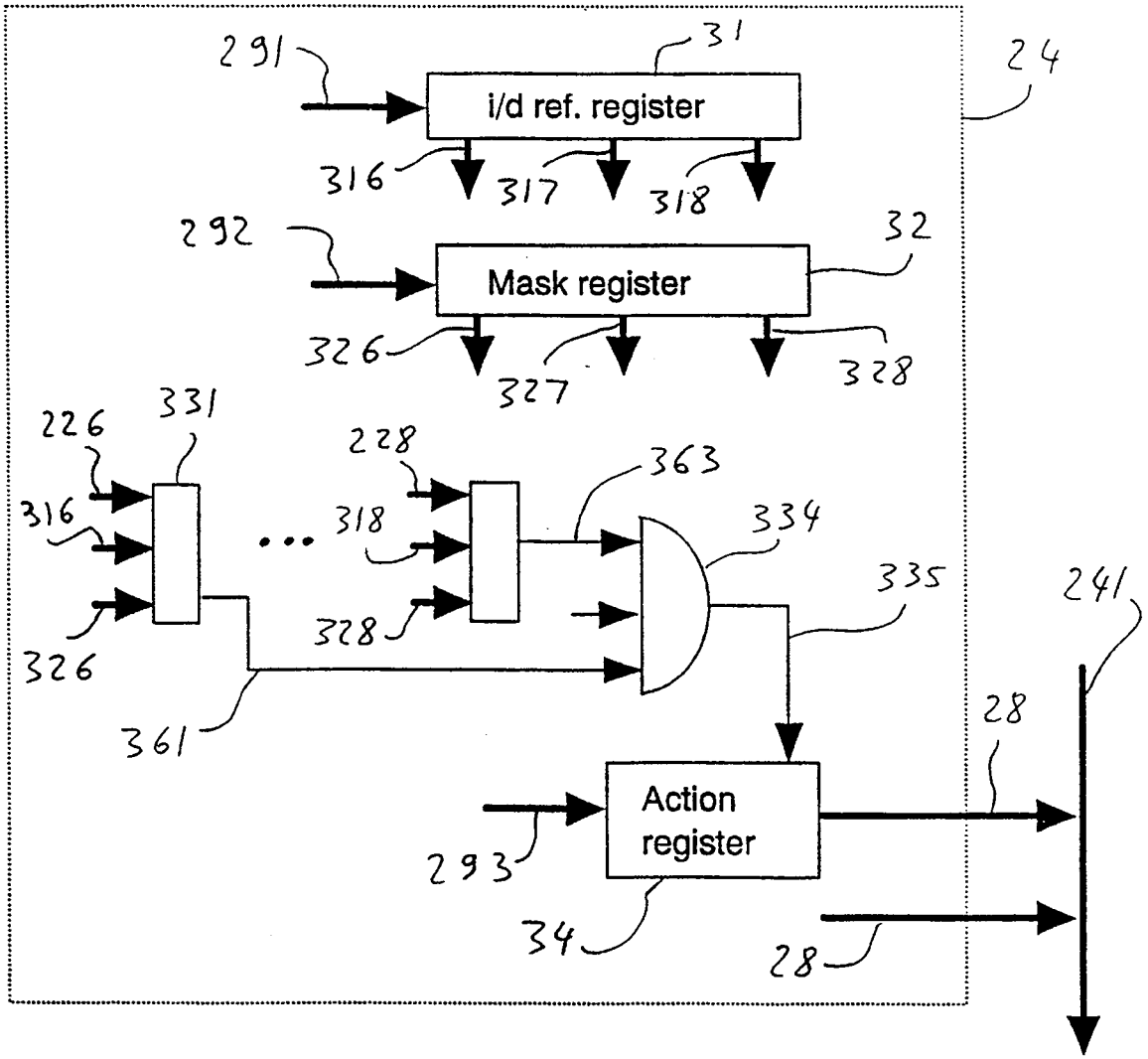

24
291
31
i/d ref. register
316
317
318
292
32
Mask register
326
327
328
226
331
316
326
228
318
328
363
334
335
241
361
28
Action register
293
34
28

Fig. 4

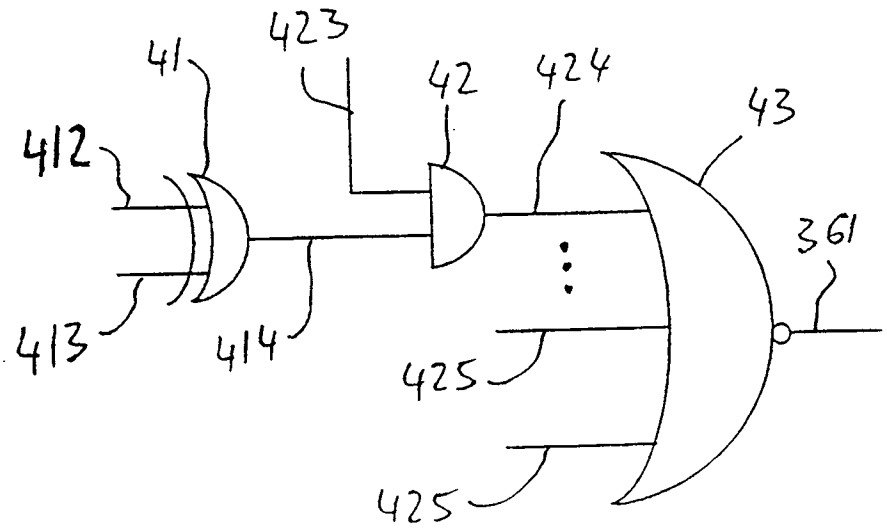


Fig. 5

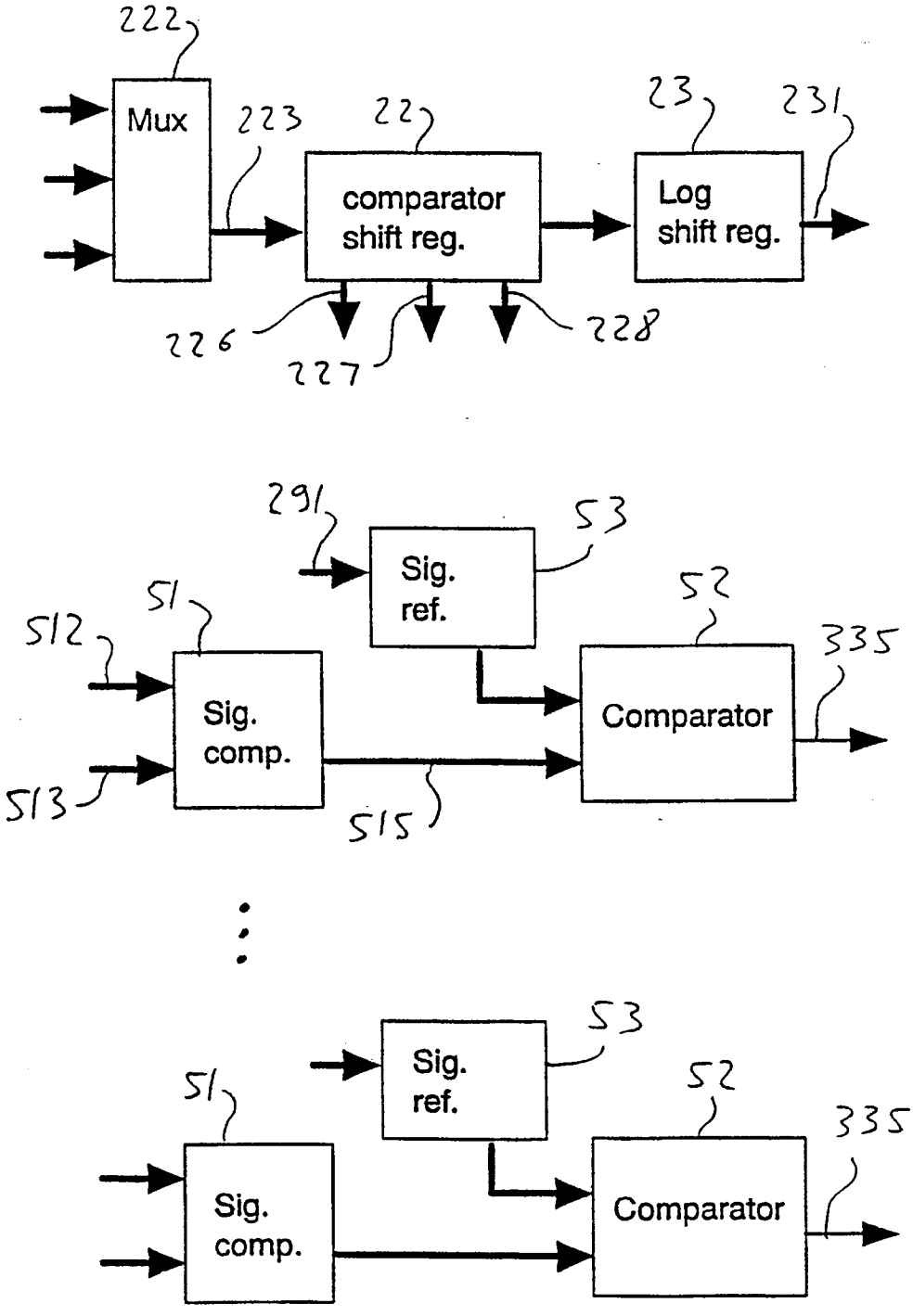

222
Mux
223
22
comparator
shift reg.
23
231
Log
shift reg.
226
227
228
291
53
Sig.
ref.
51
512
Sig.
comp.
513
52
335
Comparator
515
53
Sig.
ref.
51
Sig.
comp.
52
335
Comparator

Fig. 6

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 13/00, H04K 1/00

A3

(11) International Publication Number: WO 98/45778

(43) International Publication Date: 15 October 1998 (15.10.98)

(21) International Application Number: PCT/IL98/00170

(22) International Filing Date: 8 April 1998 (08.04.98)

(30) Priority Data:
120632 8 April 1997 (08.04.97) IL

(71)(72) Applicant and Inventor: ZUTA, Marc [IL/IL]; Ben Yehuda Street 19, 49373 Petah Tikva (IL).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

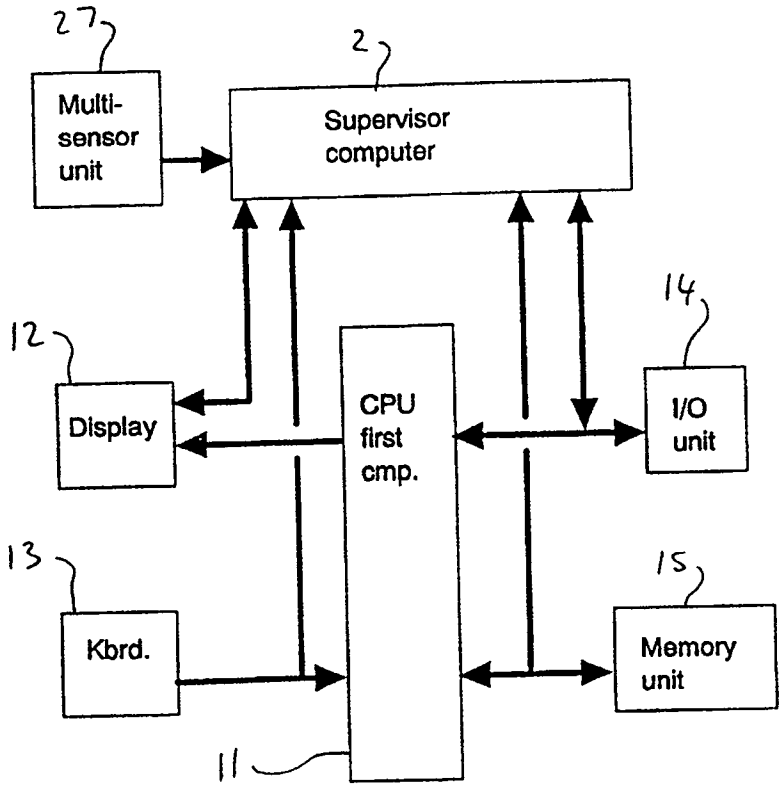
Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(88) Date of publication of the international search report:
30 December 1998 (30.12.98)

(54) Title: ANTIVIRUS SYSTEM AND METHOD

(57) Abstract

In an antivirus multiprocessor system, a second processor (2) is attached to a first processor (11) for monitoring its performance and intervening if predefined behaviour thereof is detected. The second processor (2) includes means for continuously supervising the operation of the first processor (11) to detect virus-related activities therein by comparing therein actual performed instructions in the first processor (11) with instruction sequences corresponding to known viruses or to predefined suspect behaviour, to prevent damage to the application processor. A plurality of sensors is used to detect suspect activity in various media like radio frequency or wireless RF, serial or parallel communication channels.



Trend Micro, Inc.
EX1002-325

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Trend Micro, Inc.
EX1002-326

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL98/00170

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) : G06F 13/00; H04K 1/00
US CL : 395/186, 183.14, 184.01, 185.01
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 395/186, 183.14, 184.01, 185.01, 183.07, 187.01; 380/3, 22

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y,P	US 5,657,473 A (KILEAN ET AL.) 12 August 1997, entire document.	1-3, 5-7, 9-11
Y	US 5,440,723 A (ARNOLD ET AL.) 08 August 1995, entire document.	1-3, 5-7, 9-11
Y	US 5,414,833 A (HERSHEY ET AL.) 09 May 1995, see entire document.	1-3, 5-7, 9-11
Y	US 5,491,791 A (GLOWNY ET AL.) 13 February 1996, see entire document.	1-3, 5-7, 9-11
X -- Y	LADKIN P. ET AL. "Comments on a paper by Voas...A model for detecting the existence of software corruption in real time", Computers and security 1994, pages 5-27-530	4, 8 ---- 1-11

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search
25 SEPTEMBER 1998

Date of mailing of the international search report
29 OCT 1998

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Authorized officer
NORMAN WRIGHT

Trend Micro, Inc.
EX1002-327

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL98/00170

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	COHEN F. "Current Best Practice Against Computer Viruses", IEEE, Carnahan Conf. on Security Technonlgy 1991, pages 261-269.	1-11
A	QASEM, I. ET AL., "Computer Viruses: Detection and prevention techniques", IEEE Proceedings 1990 Southeast Conf., pages 199-200.	1-11

Trend Micro, Inc.
EX1002-328

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

APS, STN, IEEE, search terms: virus monitor?, processor, computer, viral, abnorman operation, detect?, supervis?, antivirus, service processor, maintainence, protection, hardware, compare instructions.

Trend Micro, Inc.
EX1002-329

Electronic Acknowledgement Receipt

EFS ID:	2495487
Application Number:	11408145
International Application Number:	
Confirmation Number:	8007
Title of Invention:	Backward researching time stamped events to find an origin of pestware
First Named Inventor/Applicant Name:	Matthew L. Boney
Customer Number:	22903
Filer:	Thomas M. Croft/Sherry Bitler
Filer Authorized By:	Thomas M. Croft
Attorney Docket Number:	WEBR-045/00US
Receipt Date:	21-NOV-2007
Filing Date:	20-APR-2006
Time Stamp:	12:55:32
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed	WEBR04500USids.pdf	106280 11c858fc87b71bccf9e5768784dfd3f16ea98b79	no	3

Warnings:	
Information:	

This is not an USPTO supplied IDS fillable form					
2	Foreign Reference	WEBR04500WOsrwo1.pdf	346464 0c36b749f22c05024ae6e38d5fa288dea9b0ffcb	no	9
Warnings:					
Information:					
3	Foreign Reference	WEBR04500WO-wo9845778.pdf	1737248 701272a701acc940b8b75d59f3ba946739b8ad1e	no	59
Warnings:					
Information:					
			Total Files Size (in bytes):	2189992	

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

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

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(c) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/408,145	04/20/2006	Matthew L. Boney	WEBR-045/00US

CONFIRMATION NO. 8007

22903
COOLEY GODWARD KRONISH LLP
ATTN: PATENT GROUP
Suite 1100
777 - 6th Street, NW
WASHINGTON, DC20001

Title: Backward researching time stamped events to find an origin of pestware

Publication No. US-2007-0250928-A1
Publication Date: 10/25/2007

NOTICE OF PUBLICATION OF APPLICATION

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

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

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

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

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

Pre-Grant Publication Division, 703-605-4283

Please type a plus sign (+) inside this box → [+]

PTO/SB/08A (08-00)

Substitute for form 1449A/PTO		*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT		Application Number	11/408,145
		Filing Date	04/20/2006
		First Named Inventor	Matthew L. Boney
(use as many sheets as necessary)		Group Art Unit	2154
		Examiner Name	Not Yet Assigned
Sheet	1 of 3	Attorney Docket Number	WEBR-045/00US

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	U.S. Patent Document Number	Kind Code[2] (*if known*)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY
		5,623,600		JI, ET AL.	04/22/97
		5,920,696		BRANDT ET AL.	07/1999
		5,951,698		CHEN ET AL.	09/1999
		6,069,628		FARRY, ET AL.	05/30/00
		6,073,241		ROSENBERG, ET AL.	06/06/00
		6,092,194		TOUBOUL	07/18/00
		6,154,844		TOUBOUL	11/28/00
		6,167,520		TOUBOUL	12/26/00
		6,310,630		KULKARNI, ET AL.	10/30/01
		6,397,264		STASNICK, ET AL.	05/28/02
		6,405,316		KRISHNAN ET AL.	06/2002
		6,460,060		MADDALOZZO, JR., ET AL.	10/01/02
		6,480,962		TOUBOUL	11/12/02
		6,535,931		CELI, JR.	03/18/03
		6,611,878		DE ARMAS, ET AL.	08/26/03
		6,633,835		MORAN ET AL.	10/14/03
		6,667,751		WYNN, ET AL.	12/23/03
		6,701,441		BALASUBRAMANIAM, ET AL.	03/02/04
		6,772,345		SHETTY	08/2004
		6,785,732		BATES, ET AL.	08/31/04
		6,804,780		TOUBOUL	10/12/04
		6,813,711		DIMENSTEIN	11/02/04
		6,829,654		JUNGEK	12/07/04
		6,910,134		MAHER ET AL.	06/2005
		6,965,968		TOUBOUL	11/15/05
		7,058,822		EDERY ET AL.	06/06/06
		7,107,617		HURSEY ET AL.	09/2006
		US 2002/0162015		TANG	10/2002
		US 2002/0166063		LACHMAN ET AL.	11/2002
		US 2003/0065943		GEIS ET AL.	04/2003
		US 2003/0074581		HURSEY ET AL.	04/2003
		US 2003/0101381		MATEEV ET AL.	05/2003
		US 2003/0159070		MAYER ET AL.	08/2003
		US 2003/0217287	A1	KRUGLENKO	11/20/03
		US 2004/0030914	A1	KELLEY, ET AL.	02/12/04
		US 2004/0034794	A1	MAYER ET AL.	02/19/04
		US 2004/0064736	A1	OBRECHT, MARK ERIC, ET AL.	04/01/04
		US 2004/0080529	A1	WOJCIK, PAUL KAZIMIERZ	04/29/04
		US 2004/0143763	A1	RADATTI	07/22/04

Examiner Signature		Date Considered	

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

[1] Unique citation designation number.
[2] See attached Kinds of U.S. Patent Documents.

Trend Micro, Inc.
EX1002-333

Please type a plus sign (+) inside this box → [+]

PTO/SB/08A (08-00)

Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(use as many sheets as necessary)*		*Complete if Known*	
		Application Number	11/408,145
		Filing Date	04/20/2006
		First Named Inventor	Matthew L. Boney
		Group Art Unit	2154
		Examiner Name	Not Yet Assigned
Sheet	2 of 3	Attorney Docket Number	WEBR-045/00US

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	U.S. Patent Document Number	Kind Code[2] (*if known*)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY
		US 2004/0187023	A1	ALAGNA, MICHAEL ANTHONY, ET AL.	09/23/04
		US 2004/0225877	A1	HUANG	11/11/04
		US 2005/0038697	A1	JEFFREY	02/2005
		US 2005/0154885		VISCOMI ET AL.	07/2005
		US 2005/0138433	A1	LINETSKY, GENE	06/23/05
		2006/0075494		BERTMAN ET AL.	04/2006
		2006/0075501		THOMAS ET AL.	04/2006
		2006/0161988		COSTEA ET AL.	07/2006
		10/956,573		STEVE THOMAS	N/A Filed: 10/01/04
		10/956,574		STEVE THOMAS	N/A Filed: 10/01/04
		10/956,818		MATTHEW BONEY	N/A Filed: 10/01/04
		11/257,609		MICHAEL BURTSCHER	N/A Filed: 10/25/05
		11/237,291		PHILIP MADDALONI	N/A Filed: 09/28/05
		11/408,215		MATTHEW BONEY	N/A Filed: 04/20/06
		11/408,146		MATTHEW BONEY	N/A Filed: 04/20/06

Examiner Signature		Date Considered	

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

[1] Unique citation designation number.
[2] See attached Kinds of U.S. Patent Documents.

Please type a plus sign (+) inside this box → [+]

PTO/SB/08A (08-00)

Substitute for form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(use as many sheets as necessary)*		***Complete if Known***	
		Application Number	11/408,145
		Filing Date	04/20/2006
		First Named Inventor	Matthew L. Boney
		Group Art Unit	2154
		Examiner Name	Not Yet Assigned
Sheet	3 of 3	Attorney Docket Number	WEBR-045/00US

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document			Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	T[4]
		Office[1]	Number[2]	Kind Code[3] (if known)			

OTHER – 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[2]
	I.	Codeguru, Three Ways to Inject Your Code Into Another Process, by Robert Kuster, August 4, 2003, 22 pgs.	
	II.	Codeguru, Managing Low-Level Keyboard Hooks With The Windows API for VB .Net, by Paul Kimmel, April 18, 2004, 10 pgs.	
	III.	Codeguru, Hooking The Keyboard, by Anoop Thomas, December 13, 2001, 6 pgs.	
	IV.	Illusive Security, Wolves In Sheep's Clothing: malicious DLLs Injected Into trusted Host Applications, Author Unknown, http://home.arcor.de/scheinsicherheit/dll.htm 13 pgs.	
	V.	DevX.com, Intercepting Systems API Calls, by Seung-Woo Kim, May 13, 2004, 6 pgs.	
	VI.	Microsoft.com, How To Subclass A Window in Windows 95, Article ID 125680, July 11, 2005, 2 pgs.	
	VII.	MSDN, Win32 Hooks by Kyle Marsh, July 29, 1993, 15 pgs.	
	VII.	PCT Search Report, PCT/US05/34874, 07/05/06, 7 Pages	
	VIII	Yurcik, William et al., "A Planning Framework for Implementing Virtual Private Networks, June 2001, IT Pro, IEEE, pages 41-44	

Examiner Signature		Date Considered	

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

[1] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3).
[2] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document.
[3] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible.
[4] Applicant is to place a check mark here if English language Translation is attached.

[1] Unique citation designation number.
[2] Applicant is to place a check mark here if English language Translation attached.

Electronic Acknowledgement Receipt

EFS ID:	1692583
Application Number:	11408145
International Application Number:	
Confirmation Number:	8007
Title of Invention:	Backward researching time stamped events to find an origin of pestware
First Named Inventor/Applicant Name:	Matthew L. Boney
Customer Number:	22903
Filer:	Sean Ryan Odowd/Daxmara Sanchez
Filer Authorized By:	Sean Ryan Odowd
Attorney Docket Number:	WEBR-045/00US
Receipt Date:	18-APR-2007
Filing Date:	20-APR-2006
Time Stamp:	13:00:27
Application Type:	Utility

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part /.zip	Pages (if appl.)
1		IDS.pdf	237005	yes	5

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Miscellaneous Incoming Letter	1	2
	Information Disclosure Statement (IDS) Filed	3	5

Warnings:					
Information:					
2	NPL Documents	WEBR-003-00US.pdf	1087355	no	32
Warnings:					
Information:					
3	NPL Documents	WEBR-005-00US.pdf	1212931	no	38
Warnings:					
Information:					
4	NPL Documents	WEBR-006-00US.pdf	991454	no	32
Warnings:					
Information:					
5	NPL Documents	WEBR-015-00US.pdf	765879	no	24
Warnings:					
Information:					
6	NPL Documents	WEBR-020-00US.pdf	782212	no	24
Warnings:					
Information:					
7	NPL Documents	WEBR-043-00US.pdf	1153335	no	35
Warnings:					
Information:					
8	NPL Documents	WEBR-044-00US.pdf	1134038	no	35
Warnings:					
Information:					

9	NPL Documents	Article-oa-002-00US.pdf	460799	no	4
Warnings:					
Information:					
10	NPL Documents	Articles.pdf	4504142	no	88
Warnings:					
Information:					
			Total Files Size (in bytes):	12329150	

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.

Attorney Docket No. WEBR-045/00US **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Matthew L. Boney	**Confirmation No.:**	8007
Serial No.:	11/408,145	**Art Unit No.:**	2154
Filed:	04/20/2006	**Examiner:**	Not Yet Assigned

Title: BACKWARDS RESEARCHING TIME STAMPED EVENTS TO FIND AN ORIGIN OF PESTWARE

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

INFORMATION DISCLOSURE STATEMENT UNDER 37 C.F.R. §1.97(b)

In accordance with the duty of disclosure set forth in 37 C.F.R. §1.56, Applicant(s) hereby submits the following information in conformance with 37 C.F.R. §§1.97 and 1.98.

[X] Pursuant to 37 C.F.R. §1.98, a copy of each non-US patent document cited in the attached Form PTO/SB/08 is enclosed.

[] Pursuant to 37 C.F.R. §1.98, a copy of each document cited in the attached Form PTO/SB/08 is enclosed.

[] No copies of the publications listed on the attached Form PTO/SB/08A are being provided pursuant to 37 C.F.R. §1.98(d) because the publications were previously cited by or submitted to the Office in prior Application Serial No. ___ to which the above-identified application claims priority under 35 U.S.C. §120.

[X] No copies of any U.S. patents or U.S. patent application publications listed on the attached Form PTO/SB/08A are being provided pursuant to 37 C.F.R. §1.98 because this application was filed after June 30, 2003.

[] Publication(s) ___ listed on the attached Form PTO/SB/08A were cited in a foreign search or examination report corresponding to ___ application serial no. ___ and mailed on ___.

[] Enclosed is a copy of a non-English publication(s) ___. Pursuant to §609 of the M.P.E.P., Applicant submits the attached foreign search or examination report, which cites such non-English language publication(s).

[] Enclosed is a copy of a non-English publication(s) ___. English language publication ___ (copy enclosed) claims priority from this non-English publication.

This Information Disclosure Statement is filed within any one of the following time periods:

[] within three months from the filing date of this national application other than a CPA under 37 C.F.R. § 1.53(d);

[] within three months from the date of entry of the national stage as set forth in 37 C.F.R. §1.491 in this international application;

[X] 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 C.F.R. § 1.114.

It is respectfully requested that the Examiner consider the above-noted information and return an initialed copy of the attached Form PTO/SB/08A to the undersigned.

Cooley Godward Kronish LLP
ATTN: Patent Group
1200 19th Street, NW
5th Floor
Washington, DC 20036
Telephone: (720) 566-4035
Facsimile: (202) 842-7899

Respectfully submitted,
COOLEY GODWARD KRONISH LLP

By: _____
Sean R. O'Dowd
Reg. No. 53,403

OIPE IAP18 JUN 15 2006 PATENT AND TRADEMARK OFFICE

06/16/06

CTFW

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	ATTORNEY DOCKET NUMBER
11/408,145	04/20/2006	Matthew L. Boney	WEBR-045/00US

CONFIRMATION NO. 8007
FORMALITIES LETTER

22903
COOLEY GODWARD LLP
ATTN: PATENT GROUP
11951 FREEDOM DRIVE, SUITE 1600
ONE FREEDOM SQUARE- RESTON TOWN CENTER
RESTON, VA 20190-5656

Date Mailed: 05/17/2006

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

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

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

The applicant needs to satisfy supplemental fees problems indicated below.

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

- To avoid abandonment, a surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of $130 for a non-small entity, must be submitted with the missing items identified in this letter.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is **$130** for a Large Entity

- **$130** Surcharge.

Replies should be mailed to: Mail Stop Missing Parts

06/20/2006 JBALINAN 00000008 501283 11408145
01 FC:1051 130.00 DA

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

A copy of this notice MUST be returned with the reply.

Office of Initial Patent Examination (571) 272-4000, or 1-800-PTO-9199, or 1-800-972-6382
PART 2 - COPY TO BE RETURNED WITH RESPONSE



Attorney Docket No. WEBR-045/00US **PATENT**

Express Mail Label Number: EV778911587US
Date of Deposit: 6/15/06

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as Express Mail in an envelope addressed to the Mail Stop Missing Parts, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

By: _____
Daxmara Sanchez

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Matthew L. Boney	**Confirmation No.:**	8007
Serial No.:	11/408,145	**Art Unit No.:**	2154
Filed:	04/20/06	**Examiner:**	Not yet Assigned

Title: BACKWARDS RESEARCHING TIME STAMPED EVENTS TO FIND AN ORIGIN OF PESTWARE

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

RESPONSE TO NOTICE TO FILE MISSING PARTS OF APPLICATION

In response to the Notice to File Missing Parts of Application under 37 C.F.R. § 1.53(e) or (f) mailed May 17, 2006, enclosed are:

[X] Copy of the Notice to File Missing Parts of Application
[X] Executed Declaration
[] Power to Prosecute
[] Assertion of Entitlement to Small Entity Status
[] Application Data Sheet
[X] Other: Executed Assignment and Recordation Form
[] A copy of the Official Filing Receipt marked in red to show corrections that are needed. Please make the following corrections in the Official Filing Receipt:

Issuance of a corrected filing receipt is respectfully requested.

and the payment of the following fee(s):

[X] Filing fee of $130.00
[] Surcharge fee for Late Filing of Declaration of $
[X] Other fees: $40.00 (Assignment)

Total Fee due: $170.00.

[] Check No. ___ in the amount of $___ for the total fee is attached.

[X] Please charge $170.00 to Deposit Account No. 50-1283 for the total fee. This paper is being submitted in duplicate.

The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §§1.16, 1.17, and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 50-1283.

Cooley Godward LLP
ATTN: Patent Group
The Bowen Building
875 15th Street NW
Suite 800
Washington, DC 20005-2221
Telephone: (720) 566-4035
Facsimile: (720) 566-4099

Respectfully submitted,
COOLEY GODWARD LLP

By: _____
Sean R. O'Dowd
Reg. No. 53,403

OIPE IAP18
JUN 15 2006
PATENT & TRADEMARK OFFICE

DECLARATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

BACKWARDS RESEARCHING TIME STAMPED EVENTS TO FIND AN ORIGIN OF PESTWARE

the specification of which:

(check one)

[] is attached hereto;

[X] was filed as United States Application Serial No. 11/408,145 on 04/20/06.

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 to the U.S. Patent and Trademark Office all information which is known to me to be material to the patentability of said invention in accordance with 37 C.F.R. §1.56;

I hereby claim the benefit under 35 U.S.C. §119(e) of any United States provisional application(s) listed below:

_____ _____
(Application Number) (Filing Date) (day, month, year)

_____ _____
(Application Number) (Filing Date) (day, month, year)

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 willful 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 willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of third inventor: Matthew L. Boney

Inventor's signature _____ Date June 7, 2006
Residence: 1100 E. 17th Ave., E303, Longmont, Colorado 80501
Citizen of: USA
Post Office Address: Same as Above

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	ATTORNEY DOCKET NUMBER
11/408,145	04/20/2006	Matthew L. Boney	WEBR-045/00US

CONFIRMATION NO. 8007

FORMALITIES LETTER

22903
COOLEY GODWARD LLP
ATTN: PATENT GROUP
11951 FREEDOM DRIVE, SUITE 1600
ONE FREEDOM SQUARE- RESTON TOWN CENTER
RESTON, VA 20190-5656

Date Mailed: 05/17/2006

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

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

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

The applicant needs to satisfy supplemental fees problems indicated below.

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

- To avoid abandonment, a surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of $130 for a non-small entity, must be submitted with the missing items identified in this letter.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is **$130** for a Large Entity

- **$130** Surcharge.

Replies should be mailed to: Mail Stop Missing Parts

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

A copy of this notice MUST be returned with the reply.

Freshwat

Office of Initial Patent Examination (571) 272-4000, or 1-800-PTO-9199, or 1-800-972-6382
PART 3 - OFFICE COPY

18351 U.S. PTO
042006

Attorney Docket No. WEBR-045/00US **PATENT**

Express Mail Label Number: EV778911445US Date of Deposit: 4/20/06

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as Express Mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

By: _____
Daxmara Sanchez

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

112991 U.S. PTO
11/408145
042006

UTILITY PATENT APPLICATION TRANSMITTAL

Transmitted herewith for filing is a U.S. Non-Provisional Utility Patent Application entitled:

BACKWARD RESEARCHING TIME STAMPED EVENTS TO FIND AN ORIGIN OF PESTWARE

naming as inventors: Matthew L. Boney

and including:

[X] (22) pages of description (before the claims);
[X] (05) pages of claims ((23) total claims; (02) independent claims);
[X] One (1) Sheet of Abstract;
[X] (05) sheets of drawing(s) including Figures 1-5.

1. Also enclosed are:
   - [] Executed Declaration
   - [] Application Data Sheet
   - [] Assignment and Assignment Recordation Cover Sheet
   - [] Power by Assignee
   - [] Assertion of Entitlement to Small Entity Status
   - [] Information Disclosure Statement
   - [] Preliminary Amendment
   - [] CD-ROM or CD-R in duplicate, large table or Computer Program (Appendix)
   - [] Nucleotide and/or Amino Acid Sequence Submission
     - [] Computer Readable Form (CRF) on 3 ½" floppy disk
     - [] Specification Sequence Listing on:

[] CD-ROM or CD-R (2 copies); or
[] paper

[] The content of the copy in computer readable form is identical to the content of the paper, CD-ROM, or CD-R copy of the Sequence Listing.

[] Nonpublication Request and Certification

[] Check No. XXX in the amount of $XXX for the total fee as calculated below

[X] Return receipt postcard

[] Other: XXX

2. Applicant claims small entity status. See 37 CFR 1.27.

3. The filing fee has been calculated as follows [] and in accordance with the enclosed preliminary amendment:

	NO. OF CLAIMS		EXTRA CLAIMS	RATE	FEE
Basic Application Fee (including filing fee of $300, search fee of $500, examination fee of $200)					$1,000.00
Total Claims	23	- 20 =	03	x $50.00	$150.00
Independent Claims	02	- 3 =	0	x $200.00	$0.0
If multiple dependent claims are presented, add $360.00					
Total Application Fee					$1,150.00
If an Assertion of Entitlement to Small Entity Status is asserted, subtract 50% of Total Application Fee					0
Other fees: (specify)					
TOTAL FEE DUE					$1,150.00

[] This application is being filed without a filing fee. Issuance of a Notice to File Missing Parts of Application is respectfully requested.

[] A check for the total fee is attached.

[X] Please charge $$1,150.00 to Deposit Account No. **50-1283** for the total fee. This paper is being submitted in duplicate.

[X] The Director is hereby authorized to charge any appropriate fees under 37 C.F.R. §§1.16, 1.17, and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. **50-1283**.

Trend Micro, Inc.
EX1002-350

4. Please direct all correspondence concerning this application to:

COOLEY GODWARD LLP
ATTN: Patent Group
One Freedom Square
Reston Town Center
11951 Freedom Drive
Reston, VA 20190-5656
Tel: (720) 566-4035
Fax: (720) 566-4099

CUSTOMER NUMBER: **22903**

COOLEY GODWARD LLP
ATTN: Patent Group
One Freedom Square
Reston Town Center
11951 Freedom Drive
Reston, VA 20190-5656
Tel: (720) 566-4035
Fax: (720) 566-4099

Respectfully submitted,
COOLEY GODWARD LLP

By: _____
Sean R. O'Dowd
Reg. No. 53,403

COOLEY GODWARD LLP
ATTORNEY DOCKET NO.: WEBR-045/00US
CLIENT NO.: 303666-2050

EXPRESS MAIL NO. EV778911445US

APPLICATION FOR PATENT

TITLE: BACKWARD RESEARCHING TIME STAMPED EVENTS TO FIND AN ORIGIN OF PESTWARE

Trend Micro, Inc.
EX1002-352

RELATED APPLICATIONS

[0001] The present application is related to commonly owned and assigned Application No. 10/956,573, Attorney Docket No. WEBR-003/00US, entitled *System and Method For Heuristic Analysis to Identify Pestware*; Application No. 10/956,574, Attorney Docket No. WEBR-005/00US, entitled *System and Method for Pestware Detection and Removal*; Application No. 11/237,291, Attorney Docket No. WEBR-006/00US, entitled *System and Method for Locating Malware and Generating Malware Definitions*; Application No. 11/257,609, Attorney Docket No. WEBR-015/00US, entitled *System and Method for Kernel-Level Pestware Management*; Application No. 11/237,291, Attorney Docket No. WEBR-020/00US, entitled *Client Side Exploit Tracking*; Application No. [unassigned], Attorney Docket No. WEBR-044/00US, entitled *Backwards researching Activity Indicative of Pestware*, filed herewith; and Application No. [unassigned], Attorney Docket No. WEBR-043/00US, entitled *Backward Researching Existing Pestware*, filed herewith, which are incorporated herein by reference.

COPYRIGHT

[0002] A portion of the disclosure of this patent document contains material that is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent disclosure, as it appears in the Patent and Trademark Office patent files or records, but otherwise reserves all copyright rights whatsoever.

FIELD OF THE INVENTION

[0003] The present invention relates to computer system management. In particular, but not by way of limitation, the present invention relates to systems and methods for detecting, controlling and/or removing pestware.

BACKGROUND OF THE INVENTION

[0004] Personal computers and business computers are continually attacked by trojans, spyware, and adware, collectively referred to as "malware," "spyware" or "pestware." These types of programs generally act to gather information about a person or organization—often without the person or organization's knowledge. Some pestware is highly malicious. Other pestware is non-malicious but may cause issues with privacy or system performance. And yet other pestware is actually beneficial or wanted by the user. Unless specified otherwise, "pestware" as used herein refers to any of these programs that collects information about a person or an organization.

[0005] Software is presently available to detect and remove pestware. But as it evolves, the software to detect and remove it must also evolve. Accordingly, current techniques and software for removing pestware are not always satisfactory and will most certainly not be satisfactory in the future. Additionally, because some pestware is actually valuable to a user, pestware-detection software should, in some cases, be able to handle differences between wanted and unwanted pestware.

Trend Micro, Inc.
EX1002-354

[0006] Current pestware removal software uses definitions of known pestware to search for and remove files on a protected system. These definitions are often slow and cumbersome to create. Additionally, it is often difficult to initially locate the pestware in order to create the definitions. Accordingly, a system and method are needed to address the shortfalls of present technology and to provide other new and innovative features.

SUMMARY OF THE INVENTION

[0007] Exemplary embodiments of the present invention that are shown in the drawings are summarized below. These and other embodiments are more fully described in the Detailed Description section. It is to be understood, however, that there is no intention to limit the invention to the forms described in this Summary of the Invention or in the Detailed Description. One skilled in the art can recognize that there are numerous modifications, equivalents and alternative constructions that fall within the spirit and scope of the invention as expressed in the claims.

[0008] The present invention can provide a system and method for identifying an origin of suspected pestware activity on a computer. One embodiment includes establishing a time of interest relating to a suspicion of pestware on the computer, identifying, based upon the time of interest, indicia of pestware and accessing at least a portion of a recorded history of sources that the computer received files from so as to identify, based at least in part upon the identified indicia of pestware, a reference to an identity of a source that is suspected of originating pestware.

Trend Micro, Inc.
EX1002-355

[0009] As previously stated, the above-described embodiments and implementations are for illustration purposes only. Numerous other embodiments, implementations, and details of the invention are easily recognized by those of skill in the art from the following descriptions and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] Various objects and advantages and a more complete understanding of the present invention are apparent and more readily appreciated by reference to the following Detailed Description and to the appended claims when taken in conjunction with the accompanying Drawings wherein:

FIGURE 1 illustrates a block diagram of one implementation of the present invention;

FIGURE 2 is a block diagram depicting an embodiment of the file storage device of FIGURE 1;

FIGURE 3 is a flowchart depicting a method according to an exemplary embodiment;

FIGURE 4 is a flowchart depicting another method according to another embodiment;

FIGURE 5 is a flowchart depicting yet another method according to yet another embodiment.

Trend Micro, Inc.
EX1002-356

DETAILED DESCRIPTION

[0011] Referring now to the drawings, where like or similar elements are designated with identical reference numerals throughout the several views, and referring in particular to FIGURE 1, it illustrates a block diagram of one implementation of the present invention. Shown is a protected computer 100 that includes a detection module 102, quarantine module 104, removal module 106, and shields 120. In addition, a research module 108 is shown coupled to a heuristics module 110, a time stamp module 112 and a reporting module 114.

[0012] Each of these modules can be implemented in software or hardware. And if implemented in software, the modules can be implemented in a single software package or in multiple software packages. In addition, one of ordinary skill in the art will recognize that the software can be designed to operate on any type of computer system including WINDOWS and Linux-based systems. Additionally, the software can be configured to operate on personal computers and/or servers. For convenience, embodiments of the present invention are generally described herein with relation to WINDOWS-based systems. Those of skill in the art can easily adapt these implementations for other types of operating systems or computer systems.

[0013] Also shown is a file storage device 118 that is coupled to the research module 108 and an activity monitor 116. In this embodiment the file storage device includes an activity log 120, a pestware file 124 and a collection of *N* files 130. The file storage

Trend Micro, Inc.
EX1002-357

device 118 is described herein in several implementations as hard disk drive for convenience, but this is certainly not required, and one of ordinary skill in the art will recognize that other storage media may be utilized without departing from the scope of the present invention. In addition, one of ordinary skill in the art will recognize that the storage device 118, which is depicted for convenience as a single storage device, may be realized by multiple (e.g., distributed) storage devices.

[0014] In the exemplary embodiment, the pestware file 124, corresponds to (e.g., includes data relating to) a pestware process 122 operating in memory. The pestware process 122 is exemplary of pestware processes that are configured to make one or more unauthorized alterations to the computer 100. For example, the pestware process 122 may make changes to either or both of the browser settings and/or operating system (OS) settings without approval and/or the knowledge of the user.

[0015] In accordance with several embodiments, the research module 108 is configured to receive an indication that either known pestware is residing on the computer or activities indicative of pestware have occurred or are occurring on the protected computer. In response, the research module 108 is configured to research the activity log 120 and/or the *N* files 130, which include information (e.g., historical logs) relating to events on the computer 100, to identify a source of the pestware 122, 124 or pestware-related activities, which may be reported by the reporting module 114 to a centralized data store for subsequent pestware management purposes.

[0016] For example, the identities (e.g., I.P. address, URL, email client or program name) of sources (e.g., web sites, email or program) of the pestware may be collected in a centralized data store (not shown) and then subsequently reported to other users. In addition, the sources of the pestware or suspected pestware may be visited to further research how the pestware is being distributed from the URLs and/or to generate new definitions for pestware discovered at these sources.

[0017] As described further with reference to FIGURE 2, the *N* files 130 include one or more files with information that assist the research module 108 in tracing information in the *N* files 130 to an identity (e.g., URL) of the source of pestware 122, 124 on the computer 100. One or more of the *N* files 130 may be associated with an operating system of the protected computer and/or one or more applications of the protected computer, and may include information such as process IDs, registry entries, file names, cookies and URLs among other information that is used to trace from an identified pestware file, pestware process and/or pestware activity to an originating source (e.g., URL or IP address) of the infection. In one embodiment, one or more of the *N* files 130 is generated from an application that generates a log of data after examining the computer. An example of such an application is an application distributed under the name HijackThis.

[0018] In the exemplary embodiment depicted in FIGURE 1, the research module 108 is configured to receive indications that pestware may be present on the computer from each of the detection engine 102, the heuristics engine 110 and the time stamp module

Trend Micro, Inc.
EX1002-359

112, but this is certainly not required. In other embodiments, for example, the research module 108 may be configured to communicate only with the detection engine 102 or only with the heuristics engine. In yet other embodiments, the research module 108 may be configured to receive only a time stamp from the time stamp module 112.

[0019] According to several embodiments, pestware-detection functions operating on the protected computer 100 are represented by the detection engine 102, the quarantine engine 104, the removal engine 106, the shields 120 and the heuristic engine 110. The basic functions of the detection engine 102 is to compare files, processes and registry entries on the protected computer against known pestware definitions and characteristics. When a match is found, in addition to quarantining and removing a pestware object, the detection engine 102 informs the research module 108 of the pestware. Details associated with several embodiments of sweep, quarantine, and removal engines are found in the above-identified application entitled *System and Method for Pestware Detection and Removal.*

[0020] Pestware and pestware activity can also be identified by the shields 120, which generally run in the background on the computer system. In the exemplary embodiment depicted in FIGURE 1, the shields 120 are divided into the operating system shields 120A and the browser shields 120B. The shields 120 are designed to watch for pestware and for typical pestware activity and includes two types of shields: behavior-monitoring shields and definition-based shields.

[0021] As an example, the shields 120 monitor the protected computer 100 for certain types of activities that generally correspond to pestware behavior. Particular examples of some of the types of activities that are monitored include a process spawning another process, an alteration to registry entries, communications with remote sites via the Internet, alterations to a start up folder, injection of a DLL into another process, and a change to the browser's home page and/or bookmarks. Some specific examples of shields are disclosed in the above-identified application entitled *System and Method for Locating Malware and Generating Malware Definitions*. In the exemplary embodiment, the shields 120 inform the heuristics engine 108 about the activities and the heuristics engine 108 determines whether the research module 108 should be informed and/or whether the activity should be blocked.

[0022] As an example, the heuristics module 110 may compare the activities on the computer with weighted factors to make decisions relative to activities at the protected computer. Each of these factors may be, for example, associated with a particular activity and each factor may be weighted by the likelihood that the activity is associated with pestware. If the sum of the weighted factors that match the activity history exceed a threshold, then the activity is identified as pestware activity and the heuristics module 110 prompts the research module 108 to initiate research into the origin of the pestware initiating the activity. It should be recognized that this type of heuristics operation is merely one example, and that the heuristics module 110 may use other techniques to analyze activity on the computer. Additional information related to heuristics-based

scanning is found in the above-identified applications entitled *System and Method For Heuristic Analysis to Identify Pestware* and *Client Side Exploit Tracking.*

[0023] In the exemplary embodiment depicted in FIGURE 1, the time stamp module 112 is configured to send a time stamp to the research module 108 in response to a request from a user and/or in response to the heuristics module 108. In some embodiments for example, the heuristics module 108 provides the user with information about suspect activity on the computer 100 so that the user has the option as to whether or not the research module 108 will attempt to identify the source of the activity.

[0024] In other embodiments, the heuristics module 110 prompts the time stamp module 112 to initiate the generation of a time stamp, without user intervention, in response to activity that is indicative of pestware activity. In one implementation, for example, the heuristics module 110 prompts the research module 108 to initiate tracing of the pestware activity to an origin of the pestware that is associated with the activity, and the heuristics module 110 also prompts the time stamp module 112 to send a time stamp 112 to the research module 108 so that the research module 108 is provided with a time reference as well as information about the pestware activities.

[0025] In yet other embodiments, the timestamp module 112 operates independently of the heuristics module 110. For example, the timestamp module 112 may prompt the research module 108 to initiate a review of the activity log 120 and/or one or more of the *N* files in response to a user request.

[0026] The activity monitor 116 in several embodiments monitors activities on the computer and stores information about the activities in the activity log 120 so as to assist the research module 108 in identifying activities associated with pestware and the source of the pestware. In some embodiments, for example, the activity log 120 includes a list of processes that are running on the protected computer and the files that are associated with the processes. Although not depicted in FIGURE 1, the shields 120 may utilize the activity monitor 116 to detect pestware-related events and intercept efforts by pestware to spawn new processes or alter aspects of the protected computer 100.

[0027] In some variations, the activity monitor 116 may inject code into existing processes so that when a process attempts to call a function of the computer's 100 operating system (not shown) the injected code can check the process to be started and raise a flag if the existing process is attempting to create a new pestware process or attempting to alter one or more settings (e.g., a registry setting) of the protected computer 100.

[0028] In other embodiments, the activity monitor 116 is realized by a kernel-mode driver that may be loaded during a boot sequence for the protected computer or anytime later. In these embodiments, the activity monitor 116 is configured to log API calls in the activity log. In many variations for example, when a process (e.g., the pestware process) attempts to spawn a another pestware process or alter a registry entry, the API call utilized by the process is intercepted before it is carried out by an operating system of the protected computer. In this way, the attempt may be logged in the activity log 120 and

the process may be analyzed to determine whether it is known to be a pestware-related process. Additional details of use of a kernel-level driver in connection with pestware management may be found in the above identified application entitled: *System and Method for Kernel-Level Pestware Management.*

[0029] It should be recognized that the block diagram in FIGURE 1 depicts functional capabilities associated with several embodiments of the present invention. One of ordinary skill in the art will recognize that the functions described with reference to FIGURE 1 may be realized by various implementations of software in connection with hardware or hardware alone. In these implementations several functions may be consolidated into a single module, for example, and as a consequence, may appear different from the block diagram in FIGURE 1 without departing from the scope of the present invention.

[0030] Referring next to FIGURE 2, shown are exemplary resources, also referred to herein as historical logs, that are available to the research module 108 in accordance with one embodiment of the present invention. In general, these resources are logs of historical events that occurred on the computer, and each of the logs includes information that may be used to reference other information when, for example, activities, processes and files are traced so as to determine an origin of the pestware or suspected pestware. As shown, a file storage device 218 in this embodiment includes an activity log 220, which may be generated by an activity monitor (e.g., the activity monitor 116) and may include information about processes running on the computer 100 and files corresponding

Trend Micro, Inc.
EX1002-364

to the processes. In variations, the activity log 220 includes a history of API calls and respective times made by processes running on the protected computer, but this is certainly not required.

[0031] In addition, the file storage device 218 includes a browser history 240, browser cache 242, browser settings 244, OS settings 246, an event log 248, a debugging log 250, a firewall log 252, file information 254 and monitoring software logs 256. One or more of these exemplary files 240-256 may be implemented for one or more of the *N* files 130 described with reference to FIGURE 1.

[0032] The browser history 240 in this embodiment includes a listing of web sites and respective times that the web sites were visited by the user. The browser cache 242 in this embodiment includes files, cookies, and other objects cached in connection with use of a browser of the protected computer(e.g., Internet Explorer or Mozilla (not shown)). As depicted, the browser cache 242 includes a cache index 243 that includes a listing, which associates the content of the browser cache 242 with URLs and time stamps. As discussed further herein, the cache index 243 provides an efficient means for identifying the times objects were retrieved and the URLs that the objects were retrieved from.

[0033] The browser settings 244 include information about settings associated with a browser and may include a home page setting and list of user favorites. The browser settings 244 are monitored by the shields 120 for changes. Those settings also contain URLs that may be referenced in time stamped logs, firewall logs, browser histories, etc.

[0034] The operating system (OS) settings 246 may include registry entries, a start up folder and other information utilized by an operating system of the protected computer. As discussed further herein, data included in the OS settings 246 may include time stamps, which indicate when changes were made to the settings.

[0035] The event log 248 in this embodiment includes a log of events that is maintained by an operating system of the protected computer 100. For example, the event log 248 may include event information including errors, user log-in history, a listing of processes that have been launched (and the users that launched the processes), path information, information about which process (and which users) accessed a secure area and other information relating to operations of the computer 100.

[0036] Also shown in FIGURE 2 is a debugging log 250 that includes application errors, which point to a process and the address where the error occurred. Some techniques employed by pestware forcibly shut down applications, or cause applications to crash when their memory space is injected with pestware code. The infected applications like "explorer.exe" will crash, or some times restart spontaneously. These events/occurrences show up in debugging logs. These are time stamped events, that also reference files on the system.

[0037] The firewall log 252 is this embodiment is a collection of information relating to network-related events on the protected computer. The firewall log 252, may for

example, include time stamps of network activities on the protected computer, which may be utilized by the research module 108 to locate pestware or indicia of pestware.

[0038] Also shown in the data storage device 218 is a collection of file information 254, also known as the file system, which includes a database that the operating system uses to locate and store information about files. For example, the file information 254 may include the date and time a file is created, a date and time the file was last modified, the date and time the files was last accessed and the size of the file.

[0039] The monitoring-software logs 256 includes information collected from one or more pieces of monitoring software that are configured to monitor activity on the computer. As an example, the monitoring logs 256 may be generated from a filter driver, a module interfacing with a layer service provider and/or browser helper objects. It should be recognized that the logs 220, 240-256 depicted in FIGURE 2 are merely exemplary and these logs are by no means representative all the potential logs that may be accessed to research origins of pestware and/or suspected-pestware.

[0040] Referring next to FIGURE 3, shown is a flowchart depicting a method in accordance with one embodiment. Although reference will be made to FIGURES 1 and 2 for exemplary purposes, it should be recognized that the method described with reference to FIGURE 3 is certainly not limited to the specific embodiments described with reference to FIGURES 1 and 2. As shown, in this embodiment a scan of a computer (e.g., the computer 100) for pestware is initially carried out (Block 302). In several

Trend Micro, Inc.
EX1002-367

embodiments for example, the detection engine 102 scans the file storage device 118, the operating system registry and executable memory of the protected computer for indicia of pestware (e.g., processes or files matching pestware definitions and/or alterations to a registry entry that are consistent with pestware).

[0041] As shown in FIGURE 3, if pestware indicia is found, then recorded information (e.g., the activity log 120 and/or the *N* files 130) that may include traces of the pestware is accessed (Block 304), and traversed to search for information leading to the identification of the source of the pestware (Block 306). In some instances, the origin of the pestware may be identified by simply referencing one piece of data that is stored in connection with the identification of the pestware source. In other instances, however, it may be necessary to access several pieces of referential data, which may be located in one or more of the files 220-256 before arriving at the identity of the source of the pestware.

[0042] As an example, if a pestware file is found on the file storage device 118, then the cache index 243 of the browser cache 242 may be searched to identify the name of the file, and if the originating URL is stored in connection with the file, the URL is identified as the source of the file. As another example, if a pestware process is identified, a search of the activity log 220 may lead to the identity of a second process that spawned the pestware process, and additional searching of the activity log 220 using the name of the second process may lead to the identification of a pestware file associated with the

second process. In turn, a search of the cache index 243 for the name of the pestware file may lead to the URL from which the pestware file was downloaded.

[0043] As shown in FIGURE 3, if the source of the pestware is identified (Block 308), then the source of the pestware is reported (Block 310). In some embodiments, it is contemplate that several other computers configured in accordance with the protected computer 100 depicted in FIGURE 1 may also report sources of pestware to a centralized location where the URLs may be added to a list of "bad URLs." In addition, the identified URLs may be actively searched to learn more about the pestware generated at the sites, which may help generate definitions for the pestware and may provide information about how pestware infections occur.

[0044] Referring next to FIGURE 4, shown is a flowchart depicting a method in accordance with another embodiment of the present invention. Again, reference will be made to FIGURES 1 and 2 for exemplary purposes, but it should be recognized that the method described with reference to FIGURE 4 is certainly not limited to the specific embodiments described with reference to FIGURES 1 and 2. As shown, in this embodiment activity on a computer is monitored for indicia of pestware (Block 402), and if potential pestware-related activity is detected, recorded information related to the activity is searched to identify one or more suspicious objects (e.g., files and/or processes) that are related to the activity (Block 404). In some embodiments, the shields 120 (described with reference to FIGURE 1) may monitor the protected computer 100 for activities, and if the activity is identified as potential pestware activity (e.g., by the

Trend Micro, Inc.
EX1002-369

heuristics module 110), then the research module 108 searches the activity log 120 and/or one or more of the *N* files for information relating to the pestware-related activity.

[0045] As shown in FIGURE 4, recorded information (e.g., one or more of the *N* files) is then traversed to trace through information related to the suspicious objects that leads to an origin of the suspicious objects (Block 406). In one embodiment for example, the suspicious activity leads to a search for suspicious processes and/or files related to the activity (e.g., using the activity log 120), which then leads to a search of one or more of the *N* files 130 (e.g., the cache index 243) for an indication of the source of the suspicious process and/or files.

[0046] As depicted in FIGURE 4, if the source of the suspicious object(s) is identified (Block 408), then the source of the suspicious object(s) is then reported (e.g., to a pestware research entity). In this way, the suspicious objects and the web sites originating the suspicious objects may be further researched to establish the extent to which they may be a threat.

[0047] As an example of pestware-related activity that may trigger the search for a source of the activity, if a series of particular API calls is made in a pattern known to be associated with pestware, the process(es) making the calls may be identified using, for example, the activity log 120. In turn, the activity log 120 may be used to identify the file(s) associated with the process(es), and the cache index 243 may be utilized to search for a source of the file(es). It should be recognized that this is merely one example of the

type of activity that may trigger backwards researching of logs on a computer, and that patterns in process creation, downloaded files, changes to an operating system registry and browser settings, for example, may trigger a search of the computer's logs.

[0048] Referring next to FIGURE 5, shown is a flowchart depicting yet another method in accordance with another embodiment of the present invention. While referring to FIGURE 5, simultaneous reference will be made to FIGURES 1 and 2 for exemplary purposes, but it should be recognized that the method described with reference to FIGURE 5 is certainly not limited to the specific embodiments described with reference to FIGURES 1 and 2.

[0049] As shown, in this embodiment a time of interest is initially established based upon a suspicion that pestware has infected a computer (Block 502). In some embodiments, for example, a user may establish the time of interest based upon events the user observed (e.g., pop-ups or a system crash). In one embodiment, as discussed with reference to FIGURE 1, in response to a user request, the time stamp module 112 may issue a time stamp and initiate research that is related to activity occurring at or around the time of the time stamp. In variations, the user is provide with an alert in response to the heuristics module 110 identifying an activity that is suspicious and the user is given an option to initiate research at or around the time of interest.

Trend Micro, Inc.
EX1002-371

[0050] In other embodiments, the time stamp module 112 automatically generates a time stamp in response to a report of suspicious activity (e.g., from the shields 120 or heuristics module 110).

[0051] As shown in FIGURE 5, once a time of interest is established, suspicious activity is identified on the computer based upon the time of interest (Block 504). The time of interest may be established, for example, to include a time period before the time stamp is issued so that a search for suspicious activity is limited to a particular time period. In some embodiments, the activity log 130 and/or one or more of the *N* files 130 are accessed and analyzed to determine whether any activity during the time of interest is suspicious (e.g., the activity indicates in some way that it may be associated with pestware). As an example, if any logged information (e.g., in the activity log 130 and/or one or more of the *N* files 130) indicates that during the time of interest that, for example, access to the registry was carried out in connection with a downloaded file or the launch of a process, the activities may identified as being suspect and further research relative to the process and the file may carried out.

[0052] Beneficially, many of the logs accessed include time-stamped information, which enables an activity that occurred during the time of interest to be readily identified and analyzed either alone or in connection with other activities occurring during the time of interest. As an example, the activity log 220, the browser history 240, browser cache 242, operating system setting 246, the event log 248, the debugging log 250 the firewall log 252, the file information 254 and the monitoring software logs 256 include time

stamped information that provides insight into the activities that occurred on the computer during the time of interest.

[0053] As depicted in FIGURE 5, once one or more activities are identified as being suspicious (Block 504), one or more objects (e.g., processes or files) on the computer are associated with the suspicious activity (Block 506). For example, the research module 108 may search the activity log 120 and/or one or more of the *N* files for information that associates the suspicious activity to one or more processes and the processes may be related to one or more files.

[0054] As shown in FIGURE 5, recorded information on the computer is then traversed in order to trace to an origin of one or more of the objects (Block 508). For example, a search of one or more of the *N* files 130 (e.g., the cache index 243) may be carried out to identify the source of a suspicious process and/or files. Once the source of the suspicious object(s) is identified (Block 510), the source is then reported (e.g., to a remote research entity)(Block 512).

[0055] It should be recognized that the methods described with reference to FIGURES 3, 4 and 5 are merely exemplary and are certainly not the only modes of operation that are contemplated. As an example, the establishment of a time of interest, as discussed with reference to FIGURE 5, may be useful in the method described with reference to FIGURES 3 and 4 for identifying information that leads to the source of the pestware or

pestware-related activities. Moreover, it is contemplated that aspects from all three of the methods described with reference to FIGURES 3, 4 and 5 may be combined.

[0056] In conclusion, the present invention provides, among other things, a system and method for identifying a source of pestware or suspected pestware on a computer. Those skilled in the art can readily recognize that numerous variations and substitutions may be made in the invention, its use and its configuration to achieve substantially the same results as achieved by the embodiments described herein. Accordingly, there is no intention to limit the invention to the disclosed exemplary forms. Many variations, modifications and alternative constructions fall within the scope and spirit of the disclosed invention as expressed in the claims.

WHAT IS CLAIMED IS:

1. A method for identifying an origin of suspected pestware activity on a computer comprising:

establishing a time of interest relating to a suspicion of pestware on the computer;

identifying, based upon the time of interest, indicia of pestware;

accessing at least a portion of a recorded history of sources that the computer received files from so as to identify, based at least in part upon the identified indicia of pestware, a reference to an identity of a source that is suspected of originating pestware.

2. The method of claim 1, wherein the identifying includes:

accessing at least one log of historical events on the computer;

locating at least one event in the at least one log that corresponds to the time of interest; and

determining that the at least one event is associated with the indicia of pestware.

3. The method of claim 2, wherein the determining that the at least one event is associated with the indicia of pestware includes following references in the at least one log to a suspected pestware object.

4. The method of claim 3, wherein following the references includes following at least one reference in an activity log from the event to a suspected pestware process.

Trend Micro, Inc.
EX1002-375

5. The method of claim 4, wherein the activity log is generated from a kernel-mode driver.

6. The method of claim 2, wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs.

7. The method of claim 1, wherein the time of interest is established from a user input.

8. The method of claim 5, wherein the user input is in response to an alert provided to the user.

9. The method of claim 1, wherein the time of interest is established from a time stamp of a substantially instant moment in time.

10. The method of claim 1, including:

reporting the identity of the source to a pestware research entity so as to enable the pestware research entity to research whether the source is a source of pestware.

11. The method of claim 1, wherein the source is identified by an identifier selected from the group consisting of an I.P. address, a URL, an email client and a program name.

12. A system for identifying a source of suspected pestware on a computer including:

a timestamp module configured to generate a time of interest in response to a suspicion of pestware on the computer;

a research portion configured to access at least one log on the computer that relates the time of interest to at least one source of potential pestware activity on the computer; and

a reporting portion configured to generate a report that identifies the at least one source of potential pestware activity.

13. The system of claim 12, wherein the at least one log includes information that relates the time of interest to an event, and wherein the at least one log includes information that relates the event to a suspected pestware object, and wherein the at least one log includes information that relates the suspected pestware object to the at least one source of potential pestware activity.

14. The system of claim 13, including:

a heuristics module configured to evaluate whether the event is a suspected pestware-related event before the research portion accesses information in the at least one log that relates the event to the suspected pestware object.

15. The system of claim 14, wherein the heuristics module determines that the at least one event is suspected to be pestware-related by analyzing other events in connection with the event, wherein the other events are also related to the time of interest.

16. The system of claim 12, wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs

17. The system of claim 12, wherein the timestamp module configured to generate a time of interest in response to user input, which indicates the suspicion of pestware on the computer.

18. The system of claim 17, wherein the user input is in response to an alert provided to the user.

19. The system of claim 1, wherein the timestamp module configured to generate the time of interest as a time interval.

20. The system of claim 1, wherein the timestamp module is configured to generate the time of interest as a point in time.

21. The system of claim 12, including a kernel-mode driver adapted to monitor activity on the computer and to generate an activity log that is included within the at least one log.

22. The system of claim 12, wherein the at least one source of potential pestware activity is identified by an identifier selected from the group consisting of an I.P. address, a URL, an email client and a program name.

23. The system of claim 12, wherein the at least one log includes at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs.

ABSTRACT

A system and method for identifying an origin of suspected pestware activity on a computer is described. One embodiment includes establishing a time of interest relating to a suspicion of pestware on the computer, identifying, based upon the time of interest, indicia of pestware and accessing at least a portion of a recorded history of sources that the computer received files from so as to identify, based at least in part upon the identified indicia of pestware, a reference to an identity of a source that is suspected of originating pestware.

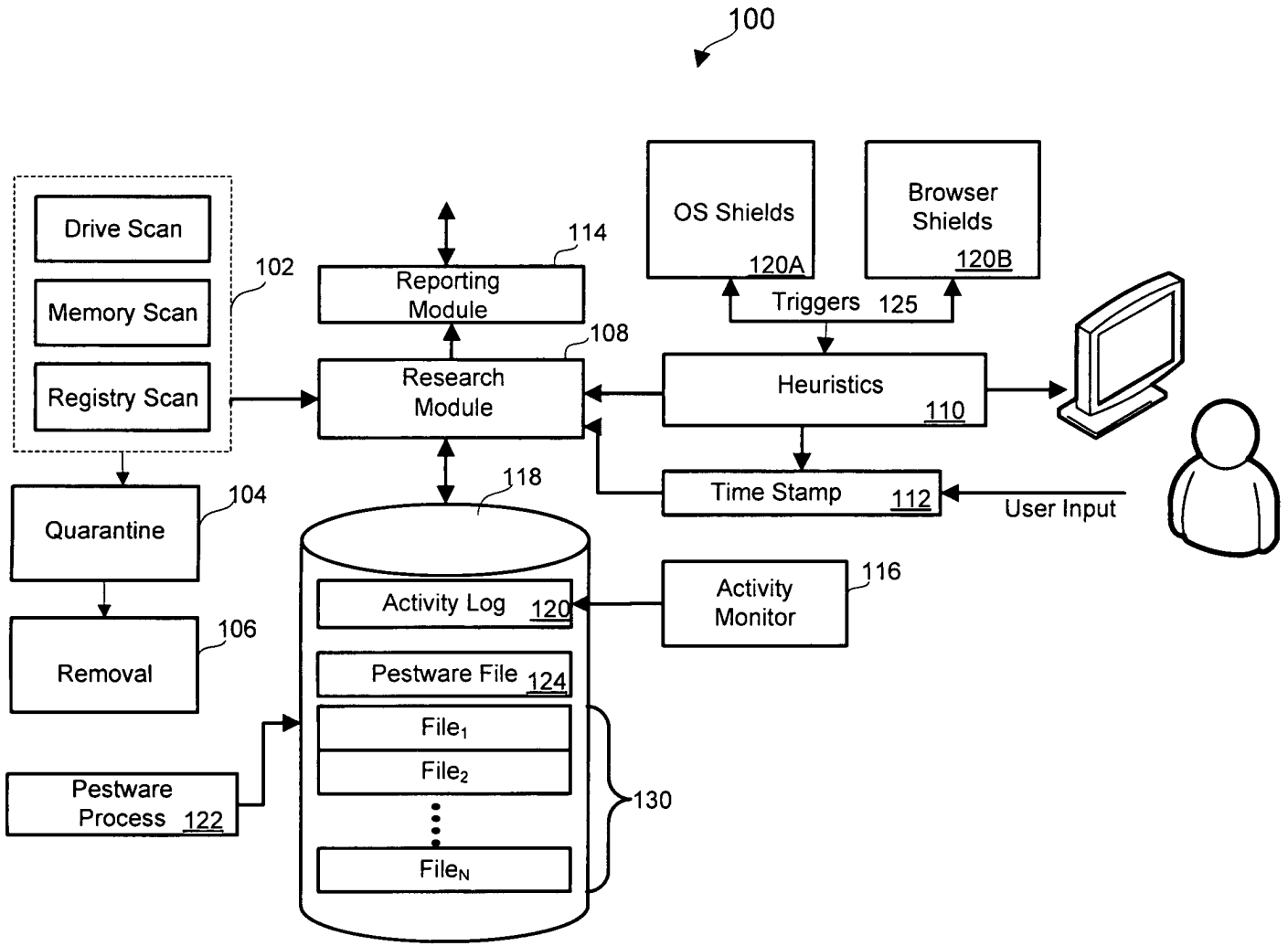


FIGURE 1

ATTORNEY DOCKET NO. WEBR-045/00US
EXPRESS MAIL NO. EV778911445US

Trend Micro, Inc.
EX1002-381

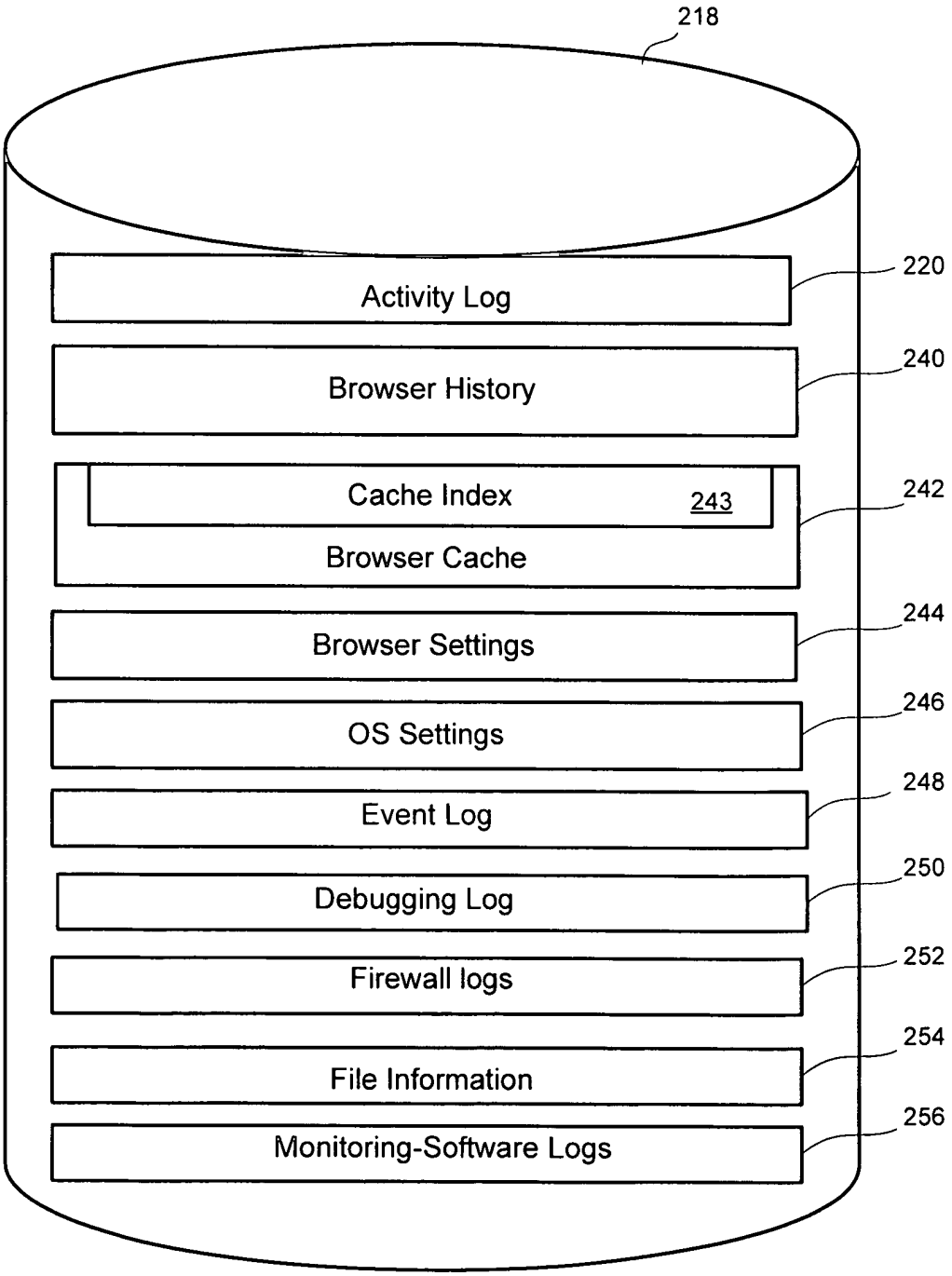


FIGURE 2

ATTORNEY DOCKET NO. WEBR-045/00US
EXPRESS MAIL NO. EV778911445US

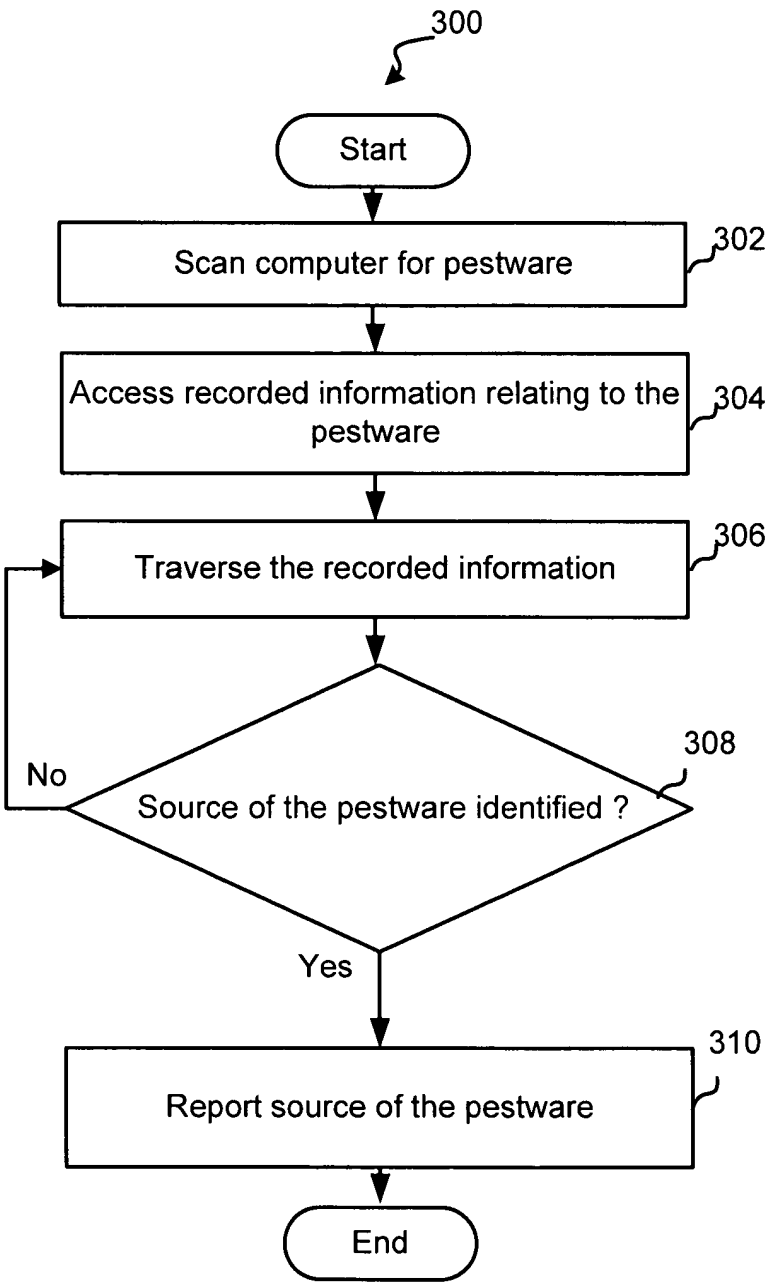


FIGURE 3

ATTORNEY DOCKET NO. WEBR-045/00US
EXPRESS MAIL NO. EV778911445US

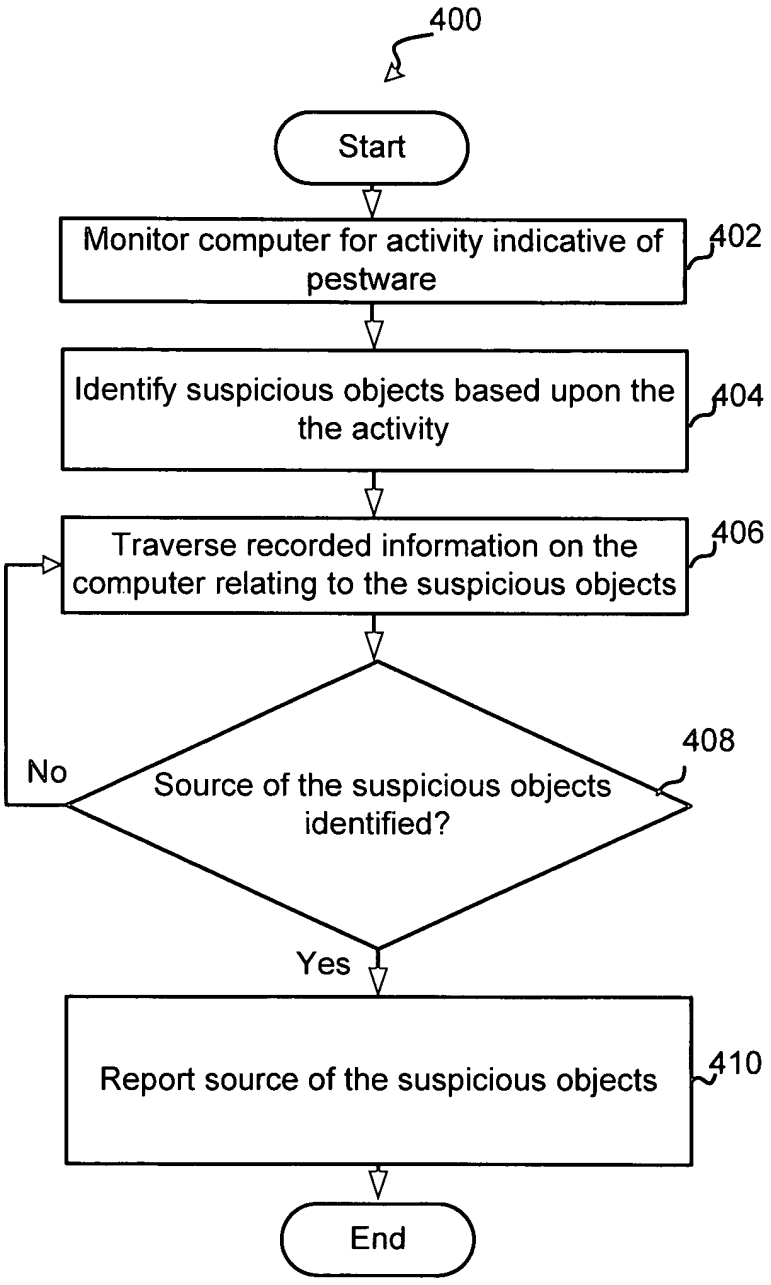


FIGURE 4

ATTORNEY DOCKET NO. WEBR-045/00US
EXPRESS MAIL NO. EV778911445US

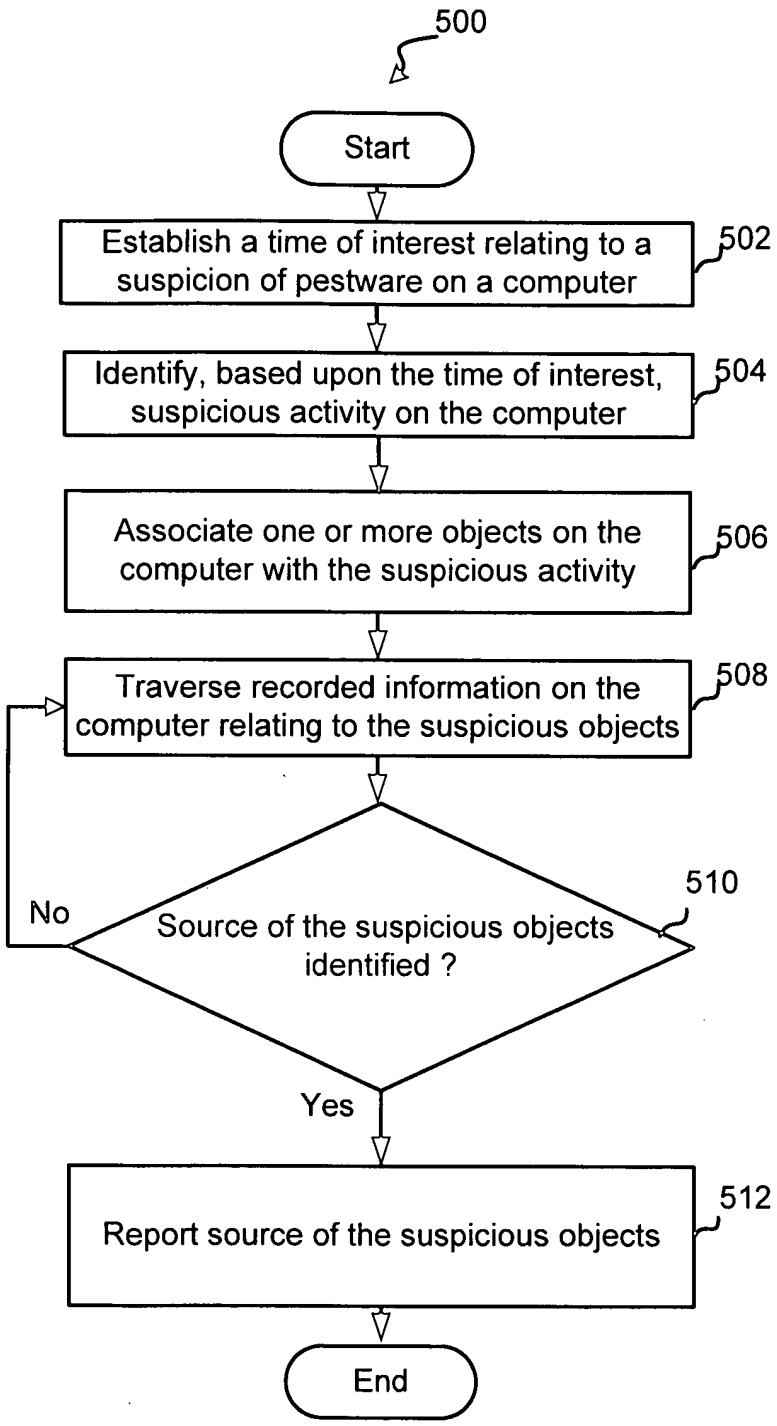


FIGURE 5

ATTORNEY DOCKET NO. WEBR-045/00US
EXPRESS MAIL NO. EV778911445US

PATENT APPLICATION SERIAL NO. _____

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

04/24/2006 HTECKLU1 00000074 501283 11408145

01 FC:1011 300.00 DA
02 FC:1111 500.00 DA
03 FC:1311 200.00 DA
04 FC:1202 150.00 DA

PTO-1556
(5/87)

*U.S. Government Printing Office: 2002 — 469-287/69033

18351 U.S. PTO
042006

Attorney Docket No. WEBR-045/00US **PATENT**

Express Mail Label Number: EV778911445US Date of Deposit: 4/20/06

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as Express Mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

By: _____
Daxmara Sanchez

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

112991 U.S. PTO
11/408145
042006

UTILITY PATENT APPLICATION TRANSMITTAL

Transmitted herewith for filing is a U.S. Non-Provisional Utility Patent Application entitled:

BACKWARD RESEARCHING TIME STAMPED EVENTS TO FIND AN ORIGIN OF PESTWARE

naming as inventors: Matthew L. Boney

and including:

[X] (22) pages of description (before the claims);
[X] (05) pages of claims ((23) total claims; (02) independent claims);
[X] One (1) Sheet of Abstract;
[X] (05) sheets of drawing(s) including Figures 1-5.

1. Also enclosed are:
   - [] Executed Declaration
   - [] Application Data Sheet
   - [] Assignment and Assignment Recordation Cover Sheet
   - [] Power by Assignee
   - [] Assertion of Entitlement to Small Entity Status
   - [] Information Disclosure Statement
   - [] Preliminary Amendment
   - [] CD-ROM or CD-R in duplicate, large table or Computer Program (Appendix)
   - [] Nucleotide and/or Amino Acid Sequence Submission
     - [] Computer Readable Form (CRF) on 3 ½" floppy disk
     - [] Specification Sequence Listing on:

[] CD-ROM or CD-R (2 copies); or
[] paper

[] The content of the copy in computer readable form is identical to the content of the paper, CD-ROM, or CD-R copy of the Sequence Listing.

[] Nonpublication Request and Certification

[] Check No. XXX in the amount of $XXX for the total fee as calculated below

[X] Return receipt postcard

[] Other: XXX

2. Applicant claims small entity status. See 37 CFR 1.27.

3. The filing fee has been calculated as follows [] and in accordance with the enclosed preliminary amendment:

	NO. OF CLAIMS		EXTRA CLAIMS	RATE	FEE
Basic Application Fee (including filing fee of $300, search fee of $500, examination fee of $200)					$1,000.00
Total Claims	23	- 20 =	03	x $50.00	$150.00
Independent Claims	02	- 3 =	0	x $200.00	$0.0
If multiple dependent claims are presented, add $360.00					
Total Application Fee					$1,150.00
If an Assertion of Entitlement to Small Entity Status is asserted, subtract 50% of Total Application Fee					0
Other fees: (specify)					
TOTAL FEE DUE					$1,150.00

[] This application is being filed without a filing fee. Issuance of a Notice to File Missing Parts of Application is respectfully requested.

[] A check for the total fee is attached.

[X] Please charge $$1,150.00 to Deposit Account No. **50-1283** for the total fee. This paper is being submitted in duplicate.

[X] The Director is hereby authorized to charge any appropriate fees under 37 C.F.R. §§1.16, 1.17, and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. **50-1283**.

Trend Micro, Inc.
EX1002-388

4. Please direct all correspondence concerning this application to:

COOLEY GODWARD LLP
ATTN: Patent Group
One Freedom Square
Reston Town Center
11951 Freedom Drive
Reston, VA 20190-5656
Tel: (720) 566-4035
Fax: (720) 566-4099

CUSTOMER NUMBER: **22903**

COOLEY GODWARD LLP
ATTN: Patent Group
One Freedom Square
Reston Town Center
11951 Freedom Drive
Reston, VA 20190-5656
Tel: (720) 566-4035
Fax: (720) 566-4099

Respectfully submitted,
COOLEY GODWARD LLP

By: _____
Sean R. O'Dowd
Reg. No. 53,403