AO 120 (Rev. 08/10)

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

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Western District of Texas, 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: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Western District of Texas, 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 8/31/2022	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.

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
13/490,294	06/06/2012	Matthew L. Boney	6890-61-CON

CONFIRMATION NO. 1064

POWER OF ATTORNEY NOTICE

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

OC000000116329858

Date Mailed: 04/20/2020

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 04/14/2020.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/tmwilliams/

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/490,294	06/06/2012	Matthew L. Boney	6890-61-CON

CONFIRMATION NO. 1064

POA ACCEPTANCE LETTER

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

OC000000116329872

Date Mailed: 04/20/2020

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 04/14/2020.

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

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/tmwilliams/

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:	39153797
Application Number:	13490294
International Application Number:	
Confirmation Number:	1064
Title of Invention:	BACKWARDS RESEARCHING ACTIVITY INDICATIVE 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:	6890-61-CON
Receipt Date:	14-APR-2020
Filing Date:	06-JUN-2012
Time Stamp:	14:20:29
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

PATENT
IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Number: 13/490,294 **Current Date: July 20, 2017**

Filing Date: June 6, 2012

Patent Number: 8,719,932

Issue Date: May 6, 2014

CHANGE OF ENTITY STATUS PURSUANT TO 37 C.F.R. §1.27 (g)(2)

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

Sir:

This communication hereby notifies the United States Patent and Trademark Office that small entity status is no longer applicable for the above-identified patent.

COMPANY or FIRM NAME AND ADDRESS:

Webroot Inc.
385 Interlocken Crescent, Suite 800
Broomfield, Colorado 80021

Respectfully submitted,

Signature
Ryan Howe
Printed Name
General Counsel
Title

OR
Reg. # if US Attorney

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/490,294	05/06/2014	8719932	6890-61-CON	1064

22442 7590 04/16/2014
Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

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

The Patent Term Adjustment is 142 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;

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

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

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

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

Leslie M. Roberts	(Depositor's name)
/Leslie M. Roberts/	(Signature)
March 24, 2014	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/490,294	06/06/2012	Matthew L. Boney	6890-61-CON	1064

TITLE OF INVENTION: BACKWARDS RESEARCHING ACTIVITY INDICATIVE OF PESTWARE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$890	$300	$0	$1190	03/26/2014

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 Sheridan Ross P.C.
2
3

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

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

(A) NAME OF ASSIGNEE: WEBROOT INC.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): BROOMFIELD, 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 credits any overpayment, to Deposit Account Number 19-1970 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ☐ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ☐ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ☐ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Bradley M. Knepper/ Date March 24, 2014

Typed or printed name Bradley M. Knepper Registration No. 44,189

Sophos Ex. 1002
Page 10 of 120

Electronic Patent Application Fee Transmittal

Application Number:	13490294
Filing Date:	06-Jun-2012
Title of Invention:	BACKWARDS RESEARCHING ACTIVITY INDICATIVE OF PESTWARE
First Named Inventor/Applicant Name:	Matthew L. Boney
Filer:	Bradley M. Knepper/Leslie Roberts
Attorney Docket Number:	6890-61-CON

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	2501	1	480	480
Extension-of-Time:				

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

Electronic Acknowledgement Receipt

EFS ID:	18558833
Application Number:	13490294
International Application Number:	
Confirmation Number:	1064
Title of Invention:	BACKWARDS RESEARCHING ACTIVITY INDICATIVE OF PESTWARE
First Named Inventor/Applicant Name:	Matthew L. Boney
Customer Number:	22442
Filer:	Bradley M. Knepper/Leslie Roberts
Filer Authorized By:	Bradley M. Knepper
Attorney Docket Number:	6890-61-CON
Receipt Date:	24-MAR-2014
Filing Date:	06-JUN-2012
Time Stamp:	12:07:02
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$480
RAM confirmation Number	10466
Deposit Account	191970
Authorized User	

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

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

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

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

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

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	ISSUE_FEE.pdf	81703 cea8cc79fef0a30741dc2590ec9470db5d0a9fce	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30673 e4ecf364dd36ce11ace746c68dc2e9fac8b65eea	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	112376		

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

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

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

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

EXAMINER
RAHMAN, MAHFUZUR

ART UNIT	PAPER NUMBER
2438	

DATE MAILED: 12/26/2013

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/490,294	06/06/2012	Matthew L. Boney	6890-61-CON	1064

TITLE OF INVENTION: BACKWARDS RESEARCHING ACTIVITY INDICATIVE OF PESTWARE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$890	$300	$0	$1190	03/26/2014

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PTOL-85 (Rev. 02/11)

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

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

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/490,294	06/06/2012	Matthew L. Boney	6890-61-CON	1064

TITLE OF INVENTION: BACKWARDS RESEARCHING ACTIVITY INDICATIVE OF PESTWARE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$890	$300	$0	$1190	03/26/2014

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 credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
❑ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
❑ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
❑ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

Sophos Ex. 1002
Page 16 of 120

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/490,294	06/06/2012	Matthew L. Boney	6890-61-CON	1064

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

EXAMINER
RAHMAN, MAHFUZUR

ART UNIT	PAPER NUMBER
2438	

DATE MAILED: 12/26/2013

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

The Patent Term Adjustment to date is 142 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 142 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

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

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

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

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

(Addendum to PTOL-85)

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

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

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

Notice of Allowability	Application No. 13/490,294	Applicant(s) BONEY, MATTHEW L.	
	Examiner MAHFUZUR RAHMAN	Art Unit 2438	AIA (First Inventor to File) Status No

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

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *06/06/2012*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1,3-6,8-14 and 16-18*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

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

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☒ Interview Summary (PTO-413), Paper No./Mail Date *12/12/2013* .
5. ☒ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/MAHFUZUR RAHMAN/
Primary Examiner, Art Unit 2438

DETAILED ACTION

This Office Action is in response to the application filed on 06/06/2012 in which claims 1-18 are presented for examination on the merits. Claims 1-18, now re-numbered as claims 1-15 are pending.

Terminal Disclaimer

The terminal disclaimer filed on 12/12/2013 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of U.S. Patent No. 8,201,243 B2 has been reviewed and is accepted. The terminal disclaimer has been recorded.

Oath/Declaration

The Oath/Declaration filed on 06/06/2012 is accepted by the examiner.

Drawings

The drawings filed on 06/06/2012 are accepted by the examiner.

Priority

The application is filed on 06/06/2012 and this is a continuation of application no. 11/408,146 filed on 04/20/2006.

Examiner Notes

1. This application is a continuation of and claims priority to US Application no. 11/408,146 (now U.S. Patent No. 8,201,243 B2). Examiner initiated an interview with applicant's representative on the record, Bradley M. Knepper, on December 12, 2013,

and indicated that claims 1, 3-6, 8-14, and 16-18 of instant application raise a nonstatutory obviousness-type double patenting issue over claims 1-14 of U.S. Patent No. 8,201,243 B2. In response, the Applicant filed a terminal disclaimer electronically on 12/12/2013 which is sufficient to overcome obviousness-type double patenting rejection.

EXAMINER'S AMENDMENT

2. 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 Bradley M. Knepper on December 12, 2013. The examiner-initiated interview summary (PTO 413B) is attached herein.

Amendment to the Claims

3. CLAIMS:

Please amend the claims below as follows:

1. (Currently Amended) A method for identifying an origin of activity on a computer that is indicative of pestware comprising:

monitoring, using a kernel-mode driver, API call activity on the computer;

storing information related to the API call activity in a log;

analyzing, heuristically, the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold;

identifying, based upon the API call activity, a suspected pestware object on the computer;

identifying, in response to the identifying the suspected pestware object, a reference to an identity of an externally networked source of the suspected pestware object; and

reporting the identity of the externally networked source to an externally networked pestware research entity, wherein

the identity of the externally networked source is selected from a group consisting of an I.P. address, a URL, an email client and a program.

2. (Cancelled)

6. (Currently Amended) A system for identifying a source of activity on a computer that is indicative of pestware including:

a kernel-level monitor configured to monitor API call activity on the computer and to store information related to the API call activity in a log;

a heuristics module configured to analyze the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold;

a research portion configured to identify, in response to a prompt from the heuristics module, a suspected pestware object on the computer; and

a reporting portion configured to generate a report including a reference to an identity of an externally networked source of the suspected pestware object and to report the identity of the externally networked source to an externally networked pestware research entity, wherein

the kernel-level monitor is configured to store information about a relationship between at least one API call of the API call activity and a file.

7. (Cancelled)

8. The system of claim [[7]] 6, wherein the information comprises an identity of at least one process that made at least one API call in the log.

14. (Currently Amended) A non-transitory computer-readable medium including processor-executable instructions for identifying an origin of activity on a computer that

is indicative of pestware, the instructions including instructions for:

monitoring, using a kernel-mode driver, API call activity on the computer;

storing information related to the API call activity in a log;

analyzing, heuristically, the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold;

identifying, based upon the API call activity, a suspected pestware object on the computer;

identifying, in response to the identifying the suspected pestware object, a reference to an identity of an externally networked source of the suspected pestware object; and

reporting the identity of the externally networked source to an externally networked pestware research entity, wherein

the identity of the externally networked source is selected by an identifier selected from a group consisting of an I.P. address, a URL, an email client and a program.

15. (Cancelled)

16. (Currently Amended) The ~~method~~ non-transitory computer-readable medium of claim 14, wherein the instructions for identifying the suspected pestware object include instructions for accessing an activity log that includes information that relates the activity to the suspected pestware object.

17. (Currently Amended) The non-transitory computer-readable medium of claim 14, wherein the instructions for identifying a reference include instructions for accessing at least a portion of a recorded history of externally networked sources.

18. (Currently Amended) The non-transitory computer-readable medium of claim 17, wherein the recorded history resides in 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.

Allowable Subject Matter

4. Claims 1, 3-6, 8-14, and 16-18 are allowed

Reasons for Allowance

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

Newly amended independent claims 1, 6, and 14 are allowed in view of the above examiner's amendment and dependent claims 3-5, 8-13, and 16-18 depend upon one the above-mentioned allowed claim and are therefore allowed by virtue of their dependencies.

Applicant's invention is directed towards computer system management for detecting, controlling and/or removing pestware where the subject matters of independent claim 1 recites "monitoring, using a kernel-mode driver, API call activity on the computer…. identifying, based upon the API call activity, a suspected pestware object on the computer; identifying, in response to the identifying the suspected pestware object, a reference to an identity of an externally networked source of the suspected pestware object".

Further, the limitations in claim 1, with respect to detecting, controlling and/or removing pestware, include "the identity of the externally networked source is selected from the group consisting of an I.P. address, a URL, an email client and a program".

Independent claim 14 recites the similar limitations as to those in claim 1.

Independent claim 6 recites similar subject matters and further includes "the kernel-level monitor is configured to store information about a relationship between at least one API call of the API call activity and a file"

The claimed subject matters are novel and non-obvious in scope over the prior art of records as the combination of prior-art references fails to teach each and every element of the independent claim including the limitations set forth above.

Further, the scope of claimed subject matters renders the invention patentably distinct as none of the prior art of record, either taken by itself or in any combination, would have anticipated or made obvious the invention of the present application at or before the time it was filed .Therefore, claims 1, 3-6, 8-14, and 16-18 are hereby allowed in view of above examiner's amendments presented above.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

6. 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/

Primary Examiner, Art Unit 2438

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	13/490,294	BONEY, MATTHEW L.	
	Examiner	Art Unit	
	MAHFUZUR RAHMAN	2438	

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

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

(2) *Bradley M. Knepper*. (4)_____.

Date of Interview: *12 December 2013*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☐103 ☒Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1-18*.

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...)

It was agreed to amend independent claims 1, 6, and 14 to include the subject matters of dependent claims 2, 7, and 15 respectively and thereby cancel dependent claims 2, 7, and 15 for the purpose of allowability. It was also agreed to incorporate appropriate claim limitations to overcome 101 issues of claim 14.

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

/MAHFUZUR RAHMAN/
Primary Examiner, Art Unit 2438

Notice of References Cited	Application/Control No. 13/490,294	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-2005/0273858 A1	12-2005	Zadok et al.	726/024
*	B	US-2007/0016914 A1	01-2007	Yeap, Yuen-Pin	719/328
*	C	US-2007/0174911 A1	07-2007	Kronenberg et al.	726/22
*	D	US-7,490,352 B2	02-2009	Kramer et al.	726/22
*	E	US-2011/0167050 A1	07-2011	Fanton et al.	707/698
*	F	US-8,312,479 B2	11-2012	Boillot, Marc Andre	719/328
	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	The ethical and legal concerns of spyware|http://utopia.csis.pace.edu/dps/2007/jkile/2005%20-%20Spring/DCS823/Spyware/sipior.pdf|2005|Sipior et al.|Pages 39-49
	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.

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. 1064

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/490,294	06/06/2012 **RULE**	726	2438	6890-61-CON

APPLICANTS

INVENTORS

Matthew L. Boney, Longmont, CO;

**** CONTINUING DATA ***************************

This application is a CON of 11/408,146 04/20/2006 PAT 8201243 *

(*)Data provided by applicant is not consistent with PTO records.

**** FOREIGN APPLICATIONS ****************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
06/14/2012

			STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
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	CO	5	18	3

ADDRESS

Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202
UNITED STATES

TITLE

BACKWARDS RESEARCHING ACTIVITY INDICATIVE OF PESTWARE

FILING FEE RECEIVED 1250	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S249	2909	H04L63/1416.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/13 16:42
S250	532	S249 and (outside or external or remote) with (source or originat$3)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/13 16:44
S251	1	S250 and (identity with source) and (pestware maleware spamware adware scumware)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/13 16:54
S252	1189	G06F21/56.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/13 16:55
S253	3	S252 and ((source or origin$5) and (malware or pestware or virus) and (kernel with API adj call)).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/13 16:56
S254	6	"9" and ((source or origin$5) and (malware or pestware or virus) and (kernel with API adj call)).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/13 16:59
S255	2	S254 and (@ad< "20060420" or @rlad <"20060420")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/13 17:00
S256	6	S254 AND ((G06F21/56 OR G06F21/51 OR G06F2221/2141 OR G06F21/566 OR G06F2221/2151 OR H04L63/1416).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/13 17:01
S257	9327	((G06F21/56 OR G06F21/51 OR	US-PGPUB;	OR	ON	2013/12/13

		G06F2221/2141 OR G06F21/566 OR G06F2221/2151 OR H04L63/1416).CPC.)	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			17:02
S258	6	S257 and ((source or origin$5) and (malware or pestware or virus) and (kernel with API adj call)).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/13 17:02
S259	35	S257 and ((source or origin$5) and (malware or pestware or virus) and (kernel with API adj call))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/13 17:02
S260	25	S259 and (@ad< "20060420" or @rlad <"20060420")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/13 17:02
S261	0	S260 and (identity with source) and (pestware maleware spamware adware scumware)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/13 17:02
S262	2	S260 and (monitor$3 or identify$3) same (source or origin$4) same (record or history)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/13 17:03
S263	3	(US-20040024864-$ or US-20050268112-$ or US-20040225877-$).did.	US-PGPUB	OR	ON	2013/12/13 17:52
S264	2	S263 and reference	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/13 17:52
S265	20065	726/22-25,13;713/187-188,193-194.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/13 18:04
S266	2327	S265 AND ((G06F21/56 OR G06F21/577 OR G06F21/50 OR G06F21/55 OR G06F2221/2129 OR H04B7/18593).CPC.)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/13 18:12
S267	88	S266 and (monitor$3 or identify$3) same (source or origin$4) same (record or history)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/13 18:12
S268	3	S267 and ((source or origin$5) and (malware or pestware or virus) and	US-PGPUB; USPAT;	OR	ON	2013/12/13 18:12

		(kernel with API adj call))	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S269	0	S268 and (@ad< "20060420" or @rlad <"20060420")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/13 18:13
S270	9	S267 and (source or origin$5) and (malware or pestware or virus) and kernel same API	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/13 18:14
S271	3	S270 and (@ad< "20060420" or @rlad <"20060420")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/13 18:14
S273	30	(US-20040064515-$ or US-20040024864-$ or US-20050268112-$ or US-20040225877-$ or US-20070168694-$ or US-20070220043-$ or US-20030065943-$ or US-20030159070-$ or US-20060031680-$ or US-20070169198-$ or US-20060085528-$ or US-20060230290-$ or US-20070074289-$ or US-20070094725-$ or US-20050154900-$ or US-20030167153-$ or US-20080086775-$ or US-20100083382-$ or US-20060265746-$ or US-20050120242-$ or US-20050086524-$ or US-20040131056-$ or US-20040034794-$ or US-20030154399-$).did. or (US-7849185-$ or US-7539736-$ or US-7352280-$ or US-7089428-$ or US-7058976-$).did. or (WO-9845778-$).did.	US-PGPUB; USPAT; EPO	OR	ON	2013/12/13 18:18
S274	10	S273 and (determin$5 or identif$4 or locat$3 or detect$3 or look$3 or find$3) with (source or originating or originator or origin) with (outside or external or remote) with (zone or network$3 or zone)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/13 18:18
S275	696	(outside or outsource or external$3 or remot$ or zone) with report$3 with (audit$3 or inspect$3 or research$3)	USPAT	OR	OFF	2013/12/13 18:34
S276	42	S275 and (outside or outsource or external$3 or remot$ or zone) with (audit$3 or inspect$3 or research$3) with (indicia or suspicious or suspected or abnormal or potential)	USPAT	OR	OFF	2013/12/13 18:34
S277	9	webroot.as. and ((source or origin$5) with (malware or pestware or virus) same kernel and (API or call))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2013/12/13 18:51

			IBM_TDB			
S278	0	S277 and (@ad< "20060420" or @rlad <"20060420")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/13 18:52
S279	19	webroot.as. and ((source or origin$5) with (malware or pestware or virus) same2 (API or call))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/13 18:52
S280	0	S261 and (@ad< "20060420" or @rlad <"20060420")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/13 18:52
S281	18	boney near3 matthew.inv.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/13 18:53
S282	696	(outside or outsource or external$3 or remot$ or zone) with report$3 with (audit$3 or inspect$3 or research$3)	USPAT	OR	OFF	2013/12/13 18:57
S283	42	S282 and (outside or outsource or external$3 or remot$ or zone) with (audit$3 or inspect$3 or research$3) with (indicia or suspicious or suspected or abnormal or potential)	USPAT	OR	OFF	2013/12/13 18:57
S284	22	S283 and (outside or outsource or external$3 or remot$ or zone) near6 source	USPAT	OR	OFF	2013/12/13 18:57
S285	1	S263 and (history same source)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/13 19:08
S286	34	(source or origin$5) with pestware same2 (indication or indicia or reference or map$4 or link$3)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/13 19:09
S298	30	(US-20040064515-$ or US-20040024864-$ or US-20050268112-$ or US-20040225877-$ or US-20070168694-$ or US-20070220043-$ or US-20030065943-$ or US-20030159070-$ or US-20060031680-$ or US-20070169198-$ or US-20060085528-$ or US-20060230290-$ or US-20070074289-$ or US-20070094725-$ or US-20050154900-$ or US-20030167153-$ or US-20080086775-$ or US-20100083382-$ or US-20060265746-$ or US-20050120242-$ or US-20050086524-$ or US-20040131056-$ or US-20040034794-$ or US-20030154399-$).did. or (US-7849185-$ or US-7539736-$ or US-7352280-$ or US-7089428-$ or US-7058976-$).did. or (WO-9845778-$).did.	US-PGPUB; USPAT; EPO	OR	ON	2013/12/13 19:30

S299	10	S298 and (determin$5 or identif$4 or locat$3 or detect$3 or look$3 or find$3) with (source or originating or originator or origin) with (outside or external or remote) with (zone or network$3 or zone)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/13 19:30
S300	6	S299 AND ((H04L63/1458 OR H04L63/1416 OR H04L63/1433 OR H04L12/2602 OR H04L41/0893 OR H04L43/00 OR H04L43/16 OR H04L63/12 OR H04L63/1408 OR H04L63/1441 OR H04L41/065 OR H04L41/0686 OR H04L41/28 OR H04L43/0882 OR H04L63/02 OR H04L63/0227 OR H04L63/0254 OR H04L63/0263 OR H04L63/0428 OR H04L63/083 OR H04L63/1425 OR H04L63/1466).CPC.)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/13 19:30
S301	38156	((H04L63/1458 OR H04L63/1416 OR H04L63/1433 OR H04L12/2602 OR H04L41/0893 OR H04L43/00 OR H04L43/16 OR H04L63/12 OR H04L63/1408 OR H04L63/1441 OR H04L41/065 OR H04L41/0686 OR H04L41/28 OR H04L43/0882 OR H04L63/02 OR H04L63/0227 OR H04L63/0254 OR H04L63/0263 OR H04L63/0428 OR H04L63/083 OR H04L63/1425 OR H04L63/1466).CPC.)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/13 19:30
S302	161	S301 and ((determin$5 or identif$4 or locat$3 or detect$3 or look$3 or find$3) with (source or originating or originator or origin) with (outside or external or remote) with (zone or network$3 or zone)).clm.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/13 19:31
S303	0	S302 and (identity with source) and (pestware maleware spamware adware scumware)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/13 19:31
S304	0	S302 and source same (pestware maleware spamware adware scumware)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/13 19:31
S305	0	S302 and (source or origin$5) same (pestware maleware spamware adware scumware)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/13 19:32
S306	20065	726/22-25,13;713/187-188,193-194.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/13 22:10
S307	39	S306 and (identity with source) and (pestware maleware spamware adware scumware)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/13 22:10
S308	5	S307 and (source or origin$5) with pestware same2 (indication or indicia or reference or map$4 or link$3)	US-PGPUB; USPAT; FPRS; EPO; JPO;	OR	ON	2013/12/13 22:28

			DERWENT			
S309	34	(source or origin$5) with pestware same2 (indication or indicia or reference or map$4 or link$3)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/13 22:28
S310	7	(US-20030154399-$ or US-20030065943-$ or US-20060265746-$ or US-20050120242-$).did. or (US-7089428-$ or US-7058976-$ or US-7849185-$).did.	US-PGPUB; USPAT	OR	ON	2013/12/13 23:03
S311	3	S310 and reference with (compromise$3 or suspici$4 or suspected or abnormal or anomal$4 or unauthorized or potential or behavior$2 or attack$3 or intrusion)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/13 23:03
S312	7	(US-20030154399-$ or US-20030065943-$ or US-20060265746-$ or US-20050120242-$).did. or (US-7089428-$ or US-7058976-$ or US-7849185-$).did.	US-PGPUB; USPAT	OR	ON	2013/12/14 10:09
S313	3	S312 and reference with (compromise$3 or suspici$4 or suspected or abnormal or anomal$4 or unauthorized or potential or behavior$2 or attack$3 or intrusion)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/14 10:09
S315	38298	((H04L63/1458 OR H04L63/1416 OR H04L63/1433 OR H04L12/2602 OR H04L41/0893 OR H04L43/00 OR H04L43/16 OR H04L63/12 OR H04L63/1408 OR H04L63/1441 OR H04L41/065 OR H04L41/0686 OR H04L41/28 OR H04L43/0882 OR H04L63/02 OR H04L63/0227 OR H04L63/0254 OR H04L63/0263 OR H04L63/0428 OR H04L63/083 OR H04L63/1425 OR H04L63/1466).CPC.)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/14 10:34
S316	9	S315 and (outside or outsource or external$3 or remot$ or zone) with (audit$3 or inspect$3 or research$3) with (indicia or suspicious or suspected or abnormal or potential)	USPAT	OR	OFF	2013/12/14 10:35
S317	1	(US-20050268112-$).did.	US-PGPUB	OR	ON	2013/12/14 11:12
S318	0	S317 and analy$4 same (record$2 or computer)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/14 11:12
S319	0	S317 and analy$4 same activit$3 same record$2 same computer	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/14 11:12
S320	1	(US-20050268112-$).did.	US-PGPUB	OR	ON	2013/12/14 11:12
S321	1	S320 and (detect$3 or identify$3) same activit$3	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/14 11:12
S322	1	S321 AND ((G06F21/51 OR G06F21/554).CPC.)	US-PGPUB; USPAT;	OR	ON	2013/12/14 11:12

			FPRS; EPO; JPO; DERWENT			
S323	3002	((G06F21/51 OR G06F21/554).CPC.)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/14 11:13
S324	8	S323 and (source or origin$5) with (pestware or malware or virus or suspect$3) same (indication or indicia or reference or map$4 or link$3) with (kernel or memory)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/14 11:13
S336	116	webroot.as.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/12/14 14:34
S337	5	S336 and (monitor$3 or identif$5) with (source or origin$4) with (kernel or memory)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/14 14:35
S338	6	S336 and (monitor$3 or identif$5) with (source or origin$4) same (kernel or memory)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/14 14:35
S339	13	S336 and (monitor$3 or identif$5 or detect$3 or determin$5) with (source or origin$4) same (kernel or memory)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2013/12/14 14:36

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	44553	(713/164,202,188;709/206,224;380/279;370/386;726/27).ccls.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/15 14:51
L3	44540	"1" and L2	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/15 14:51
S238	27	(kernel with API adj call).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2012/02/06 12:49
S240	0	((source or origin$5) with (external$3 or outside or central$5) near4 network$3 and (kernel with API adj call)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2012/02/06 12:52
S241	0	((source or origin$5) with network$3 and (kernel with API adj call)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2012/02/06 12:52
S242	8	((source or origin$5) and (kernel with API adj call)).clm.	US-	OR	ON	2012/02/06

			PGPUB; USPAT; UPAD			12:53
S243	4	((source or origin$5) and (malware or pestware or virus) and (kernel with API adj call)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2012/02/06 12:54
S244	0	S243 and ((source or origin$5) with network and (malware or pestware or virus) and (kernel with API adj call)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2012/02/06 12:55
S245	0	((source or origin$5) with network and (malware or pestware or virus) and (kernel with API adj call)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2012/02/06 12:55
S246	2	((source or origin$5) with (network or computer or host) and (malware or pestware or virus) and (kernel with API adj call)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2012/02/06 12:55
S247	0	S246 and (@ad< "20060420" or @rlad <"20060420")	US-PGPUB; USPAT; UPAD	OR	ON	2012/02/06 12:55
S248	0	webroot.as. and ((source or origin$5) with network and (malware or pestware or virus) and (kernel with API adj call))	US-PGPUB; USPAT; UPAD	OR	ON	2012/02/06 12:57
S287	1	"13490294"	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/13 16:32
S288	3730	(H04L63/145 G06F21/56 G06F21/566 G06F21/564 G06F21/562).cpc.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/13 16:57
S289	2	S288 and ((source or origin$5) with (external$3 or outside or central$5) near4 network$3 and (kernel with API adj call)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/13 16:57
S290	3730	(H04L63/145 G06F21/56 G06F21/566 G06F21/564 G06F21/562).cpc.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/13 16:59
S291	0	S290 and ((source or origin$5) with network and (malware or pestware or virus) and (kernel with API adj call)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/13 16:59
S292	4	S290 and ((source or origin$5) and (malware or pestware or virus) and (kernel with API adj call)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/13 16:59
S293	17456	726/22-25,13;713/187-188,193-194.ccls.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/13 18:15
S294	0	S293 and ((source or origin$5) with network and (malware or pestware or virus) and (kernel with API adj call)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/13 18:16
S295	2034	S293 AND ((G06F21/56 OR G06F21/577 OR G06F21/50 OR	US-	OR	ON	2013/12/13

		G06F21/55 OR G06F2221/2129 OR H04B7/18593).CPC.)	PGPUB; USPAT; UPAD			18:16
S296	2	S295 and ((source or origin$5) with (malware or pestware or virus or infect$5) and kernel same (API or call)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/13 18:17
S297	0	S296 and (@ad< "20060420" or @rlad <"20060420")	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/13 18:18
S314	17	((kernel or memory) with (monitor$3 or trac$5) with (API or (program or application) near6 call) with (origin$5 or source)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 10:24
S325	1	((kernel or memory) with (monitor$3 or trac$5) with (API or (program or application) near6 call) with (origin$5 or source) with (reference or object)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 10:26
S326	0	((kernel or memory) with (monitor$3 or trac$5) with (API or (program or application) near6 call) with (origin$5 or source) with (reference or object) with (pestware or malware or virus or abnormal or suspicious or suspected)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 10:28
S327	17	((kernel or memory) with (monitor$3 or trac$5) with (API or (program or application) near6 call) with (origin$5 or source)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 10:29
S328	10	S327 AND ((G06F11/3466 OR G06F11/366 OR G06F17/30371 OR G06F21/56 OR G06F9/4426 OR G06F11/3636 OR G06F3/0304).CPC.)	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 10:30
S329	7543	((G06F11/3466 OR G06F11/366 OR G06F17/30371 OR G06F21/56 OR G06F9/4426 OR G06F11/3636 OR G06F3/0304).CPC.)	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 10:30
S330	1	S329 and ((kernel or memory) with (monitor$3 or trac$5) with (API or (program or application) near6 call) with (origin$5 or source) with (reference or object)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 10:30
S331	0	S330 and ((kernel or memory) with (monitor$3 or trac$5) with (API or (program or application) near6 call) with (origin$5 or source) with (reference or object) with (pestware or malware or virus or abnormal or suspicious or suspected)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 10:31
S332	10254	(H04L63/1416 H04L63/1408 H04L63/145 H04L63/1441 H04L63/1458 or G06F21/56 or H04L63/145 G06F21/566 G06F21/564 G06F21/562).cpc.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 10:33
S334	0	S332 and ((kernel or memory) with (monitor$3 or trac$5) with (API or (program or application) near6 call) with (origin$5 or source) with (reference or object)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 10:33
S335	0	S332 and ((kernel or memory) with (monitor$3 or trac$5) with (API or (program or application) near6 call) with (origin$5 or source) with (reference or object) with (pestware or malware or virus or abnormal or suspicious or suspected)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 10:34
S340	17	((kernel or memory) with (monitor$3 or trac$5) with (API or (program or application) near6 call) with (origin$5 or source)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 19:13
S341	10	S340 AND ((G06F11/3466 OR G06F11/366 OR G06F17/30371	US-	OR	ON	2013/12/14

		OR G06F21/56 OR G06F9/4426 OR G06F11/3636 OR G06F3/0304).CPC.)	PGPUB; USPAT; UPAD			19:13
S342	8	S341 and ((monitor$3 or identif$5 or detect$3 or determin$5) with (source or origin$4) same (kernel or memory)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 19:13
S343	12	"s323" and ((monitor$3 or identif$5 or detect$3 or determin$5) with (source or origin$4) same (kernel or memory)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 19:13
S344	44553	(713/164,202,188;709/206,224;380/279;370/386;726/27).ccls.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 19:23
S345	504	S344 and ((monitor$3 or identif$5 or detect$3 or determin$5) with (source or origin$4) same (kernel or memory)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 19:23
S346	0	S345 and ((kernel or memory) with (monitor$3 or trac$5) with (API or (program or application) near6 call) with (origin$5 or source) with (reference or object) with (pestware or malware or virus or abnormal or suspicious or suspected)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 19:23
S347	0	S346 and ((kernel or memory) with (monitor$3 or trac$5) with (API or (program or application) near6 call) with (origin$5 or source) with (reference or object) with (pestware or malware or virus or abnormal or suspicious or suspected)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 19:23
S348	1	S345 and (source or origin$5) with (pestware or malware or virus or suspect$3) same (indication or indicia or reference or map$4 or link$3) with (kernel or memory)	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 19:24
S349	1	S348 and (@ad< "20060420" or @rlad <"20060420")	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 19:25
S350	23	S345 AND ((G06Q10/0635 OR H04L51/18 OR H04L63/126 OR H04L63/1433 OR H04L63/1441 OR H04L12/26).CPC.)	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 19:32
S351	7425	((G06Q10/0635 OR H04L51/18 OR H04L63/126 OR H04L63/1433 OR H04L63/1441 OR H04L12/26).CPC.)	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 19:32
S352	1	S351 and (source or origin$5) with (pestware or malware or virus or suspect$3) same (indication or indicia or reference or map$4 or link$3) with (kernel or memory)	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 19:33
S353	1	"13490294"	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 19:38
S354	17456	726/22-25,13;713/187-188,193-194.ccls.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 22:30
S355	39	(kernel with API adj call).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 22:30
S356	28	S355 and (@ad< "20060420" or @rlad <"20060420")	US-	OR	ON	2013/12/14

			PGPUB; USPAT; UPAD			22:30
S357	15	S356 AND ((G06F21/10 OR G06F21/53 OR G06F21/554).CPC.)	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 22:31
S358	0	S357 and ((source or origin$5) with (kernel or memory)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 22:32
S360	0	S357 and ((kernel or memory) with (monitor$3 or trac$5) with (API or (program or application) near6 call) with (origin$5 or source))	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 22:34
S361	12026	((G06F21/10 OR G06F21/53 OR G06F21/554).CPC.)	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 22:34
S362	9	S361 and ((kernel or memory) with (monitor$3 or trac$5) with (API or (program or application) near6 call) with (origin$5 or source))	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/14 22:34
S363	39	(kernel with API adj call).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/15 10:40
S364	21	S363 AND ((G06F21/51 OR G06F21/52 OR G06F21/577 OR G06F21/56 OR G06F11/3636).CPC.)	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/15 10:50
S365	6124	((G06F21/51 OR G06F21/52 OR G06F21/577 OR G06F21/56 OR G06F11/3636).CPC.)	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/15 10:50
S366	21	S365 and (kernel with API adj call).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/15 10:50
S367	1	"8201243".pn.	US-PGPUB; USPAT; UPAD	OR	ON	2013/12/15 10:50

12/15/2013 3:23:52 PM
C:\Users\mrahman4\Documents\EAST\Workspaces\71_211_ackward researching existing pestware_11408146_13490294\71_211_ackward researching existing pestware_11408146_13490294.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13490294	BONEY, MATTHEW L.
	Examiner	**Art Unit**
	MAHFUZUR RAHMAN	2438

CPC- SEARCHED

Symbol	Date	Examiner
H04L63/1416, G06F21/56	12/14/2013	MR

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner
(H04L63/1416 H04L63/1408 H04L63/145 H04L63/1441 H04L63/1458).cpc.	12/14/2013	MR
(G06F21/56 or H04L63/145 G06F21/566 G06F21/564 G06F21/562).cpc.	12/14/2013	MR
((G06Q10/0635 OR H04L51/18 OR H04L63/126 OR H04L63/1433 OR H04L63/1441 OR H04L12/26).CPC.)	12/14/2013	MR
((G06F11/3466 OR G06F11/366 OR G06F17/30371 OR G06F21/56 OR G06F9/4426 OR G06F11/3636 OR G06F3/0304).CPC.)	12/14/2013	MR

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner
726	22	12/14/2013	MR

SEARCH NOTES

Search Notes	Date	Examiner
Searched EAST databases, keywords include: (kernel or memory) with (monitor$3 or trac$5) with (API or (program or application) near6 call) with (origin$5 or source) with (reference or object) with (pestware or malware or virus or abnormal or suspicious or suspected); (monitor$3 or identif$5 or detect$3 or determin$5); (research$3 or audit$3)	12/14/2013	MR
Text limited search of (713/164,202,188;709/206,224;380/279;370/386;726/27)	12/14/2013	MR
Inventor/Assignee Search in EAST	12/14/2013	MR
Searched Google and IEEE Xplore	12/14/2013	MR

	/MAHFUZUR RAHMAN/ Primary Examiner.Art Unit 2438

INTERFERENCE SEARCH			
US Class/ CPC Symbol	**US Subclass / CPC Group**	**Date**	**Examiner**
713	164, 202, 188	12/14/2013	MR
709	206, 224	12/14/2013	MR
380	279	12/14/2013	MR
370	386	12/14/2013	MR
H04L63/1416	H04L63	12/14/2013	MR
G06F21/56	G06F21	12/14/2013	MR
G06Q10/063	G06Q10	12/14/2013	MR
	((kernel or memory) with (monitor$3 or trac$5) with (API or (program or application) near6 call) with (origin$5 or source) with (reference or object) with (pestware or malware or virus or abnormal or suspicious or suspected)).clm.	12/14/2013	MR
	((source or origin$5) with (external$3 or outside or central$5) near4 network$3 and (kernel with API adj call)).clm.	12/14/2013	MR

	/MAHFUZUR RAHMAN/ Primary Examiner.Art Unit 2438

Sophos Ex. 1002
Page 45 of 120

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13490294	BONEY, MATTHEW L.
	Examiner	**Art Unit**
	MAHFUZUR RAHMAN	2438

CPC						
Symbol					Type	Version
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			

CPC Combination Sets							
Symbol					Type	Set	Ranking	Version
			/					
			/					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	15	
/MAHFUZUR RAHMAN/ Primary Examiner.Art Unit 2438	12/14/2013	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13490294	BONEY, MATTHEW L.
	Examiner	**Art Unit**
	MAHFUZUR RAHMAN	2438

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION										
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED					
726	22	G	0	6	F	21 / 56 (2013.01.01)						

CROSS REFERENCE(S)					
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
713	164	202	188		
709	206	224			
380	279				
370	386				
726	27				

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 15	
/MAHFUZUR RAHMAN/ Primary Examiner.Art Unit 2438 (Primary Examiner)	12/14/2013 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 3

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13490294	BONEY, MATTHEW L.
	Examiner	**Art Unit**
	MAHFUZUR RAHMAN	2438

☒ **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	14	17												
	2	15	18												
2	3														
3	4														
4	5														
5	6														
	7														
6	8														
7	9														
8	10														
9	11														
10	12														
11	13														
12	14														
	15														
13	16														

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 15	
/MAHFUZUR RAHMAN/ Primary Examiner.Art Unit 2438 (Primary Examiner)	12/14/2013 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 3

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13490294	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	12/14/2013								
1	1	=								
	2	-								
2	3	=								
3	4	=								
4	5	=								
5	6	=								
	7	-								
6	8	=								
7	9	=								
8	10	=								
9	11	=								
10	12	=								
11	13	=								
12	14	=								
	15	-								
13	16	=								
14	17	=								
15	18	=								

Doc Code: DIST.E.FILE Document Description: Electronic Terminal Disclaimer - Filed	PTO/SB/26 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT**
Application Number	13490294
Filing Date	06-Jun-2012
First Named Inventor	Matthew Boney
Attorney Docket Number	6890-61-CON
Title of Invention	BACKWARDS RESEARCHING ACTIVITY INDICATIVE OF PESTWARE

☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action

☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent Interest
WEBROOT INC.	100%

The owner(s) with percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)

8201243

as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:
- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

◉ Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request.

○ I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.

Applicant claims the following fee status:

◉ Small Entity

○ Micro Entity

○ Regular Undiscounted

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.

THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

◉ An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application

Registration Number 44189

○ A sole inventor

○ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors

○ A joint inventor; all of whom are signing this request

○ The assignee of record of the entire interest that has properly made itself of record pursuant to 37 CFR 3.71

Signature	/Bradley M Knepper/
Name	Bradley M Knepper

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Electronic Patent Application Fee Transmittal

Application Number:	13490294
Filing Date:	06-Jun-2012
Title of Invention:	BACKWARDS RESEARCHING ACTIVITY INDICATIVE OF PESTWARE
First Named Inventor/Applicant Name:	Matthew L. Boney
Filer:	Bradley M. Knepper/Leslie Roberts
Attorney Docket Number:	6890-61-CON

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Statutory or Terminal Disclaimer	1814	1	160	160
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($)
Miscellaneous:				
			Total in USD ($)	**160**

Doc Code: DISQ.E.FILE
Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 13490294

Filing Date: 06-Jun-2012

Applicant/Patent under Reexamination: Boney et al.

Electronic Terminal Disclaimer filed on December 12, 2013

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt

EFS ID:	17646543
Application Number:	13490294
International Application Number:	
Confirmation Number:	1064
Title of Invention:	BACKWARDS RESEARCHING ACTIVITY INDICATIVE OF PESTWARE
First Named Inventor/Applicant Name:	Matthew L. Boney
Customer Number:	22442
Filer:	Bradley M. Knepper/Leslie Roberts
Filer Authorized By:	Bradley M. Knepper
Attorney Docket Number:	6890-61-CON
Receipt Date:	12-DEC-2013
Filing Date:	06-JUN-2012
Time Stamp:	17:23:28
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$160
RAM confirmation Number	5905
Deposit Account	191970
Authorized User	

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

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

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

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

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

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Electronic Terminal Disclaimer-Filed	eTerminal-Disclaimer.pdf	33750 a8ee209b284819629671da1faa4469d8fbbd9de0	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30511 74621374229a21b69105138ec630b367b58ea241	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	64261		

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

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

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/490,294	06/06/2012	Matthew L. Boney	WEBR-044/01US 303666-2126

CONFIRMATION NO. 1064

POA ACCEPTANCE LETTER

OC000000060255662

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

Date Mailed: 04/08/2013

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 03/28/2013.

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.

/fstephanos/

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

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.

Under the Paperwork Reduction Act of1995, no persons arerequired to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: Webroot Inc.

Application No./Patent No.: 13/490,294 Filed/Issue Date: 2012-06-06

Titled: BACKWARDS RESEARCHING ACTIVITY INDICATIVE 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 028385, Frame 0242, 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 029066, Frame 0457, 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.

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/	2013-03-28
Signature	Date
Bradley M. Knepper	Attorney
Printed or Typed Name	Title or Registration Number

Privacy Act Statement

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

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

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

Electronic Acknowledgement Receipt

EFS ID:	15378149
Application Number:	13490294
International Application Number:	
Confirmation Number:	1064
Title of Invention:	BACKWARDS RESEARCHING ACTIVITY INDICATIVE OF PESTWARE
First Named Inventor/Applicant Name:	Matthew L. Boney
Customer Number:	58249
Filer:	Bradley M. Knepper/Leslie Roberts
Filer Authorized By:	Bradley M. Knepper
Attorney Docket Number:	WEBR-044/01US 303666-2126
Receipt Date:	28-MAR-2013
Filing Date:	06-JUN-2012
Time Stamp:	14:20:05
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	POA_Executed_Webroot_AIA.pdf	58673 b6ad010c1b704f220368f04f22c78a2072084c20	no	1

Warnings:

Information:

2	Assignee showing of ownership per 37 CFR 3.73.	STATEMENT.pdf	119674 f311234a3f78f3c056a6743e817b1b8747194b20	no	3

Warnings:

Information:

Total Files Size (in bytes):	178347

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

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

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

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

MAILED
NOV 26 2012
OFFICE OF PETITIONS

In re Application of	:	
Matthew L. Boney	:	
Application No. 13/490,294	:	DECISION ON PETITION
Filed: June 6, 2012	:	TO WITHDRAW
Attorney Docket No. WEBR-044/01US 303666-2126	:	FROM RECORD
	:	

This is a decision on the Request to Withdraw as attorney or agent under 37 CFR § 1.36(b) or 37 CFR § 10.40 filed September 20, 2012.

The request is **NOT APPROVED**.

The Office will no longer approve requests from practitioners to withdraw from application where the requesting practitioners is acting, or has acted, in a representative capacity pursuant to 37 CFR 1.34. In these situations, the practitioner is responsible for the correspondence the practitioner files in the application while acting in a representative capacity. As such, there is no need for the practitioner to obtain the Office's permission to withdraw from representation. However, practitioners acting in a representative capacity, like practitioners, who have power of attorney in the application, remain responsible for noncompliance with 37 CFR 1.56, as well as 37 CFR 10.18, with respect to the documents they file.

A review of the record shows that Mark R. Schafer was never appointed power of attorney in this patent application, but they may have been employed or otherwise engaged in the proceedings in this patent application. Unfortunately, the request to withdraw under 37 CFR 1.36 is not applicable.

In view of the above, all future communications from the Office will continue to be directed to the above-listed address unless properly notified by the applicant.

Telephone inquiries concerning this decision should be directed to the undersigned at (571) 272-3226.

/Andrea Smith/
Andrea Smith
Petitions Examiner
Office of Petitions

cc: Webroot, Inc. c/o Sheridan Ross
1560 Broadway, Suite 1200
Denver, CO 80202

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/490,294	06/06/2012	Matthew L. Boney	WEBR-044/01US 303666-2126

CONFIRMATION NO. 1064

58249
COOLEY LLP
ATTN: Patent Group
Suite 1100
777 - 6th Street, NW
WASHINGTON, DC 20001

PUBLICATION NOTICE

OC000000056791051

Title:BACKWARDS RESEARCHING ACTIVITY INDICATIVE OF PESTWARE

Publication No.US-2012-0246722-A1
Publication Date:09/27/2012

NOTICE OF PUBLICATION OF APPLICATION

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

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

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

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

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

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

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

- [x] 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)	[x] 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. [x] 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. [x] 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. [x] 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.

AmericanLegalNet, Inc.
www.FormsWorkflow.com

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

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:	13800882
Application Number:	13490294
International Application Number:	
Confirmation Number:	1064
Title of Invention:	BACKWARDS RESEARCHING ACTIVITY INDICATIVE OF PESTWARE
First Named Inventor/Applicant Name:	Matthew L. Boney
Customer Number:	58249
Filer:	Mark Randolph Schafer/Sherry Bitler
Filer Authorized By:	Mark Randolph Schafer
Attorney Docket Number:	WEBR-044/01US 303666-2126
Receipt Date:	20-SEP-2012
Filing Date:	06-JUN-2012
Time Stamp:	18:30:34
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.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number
13/490,294

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	380
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	620
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	250
TOTAL CLAIMS (37 CFR 1.16(i))	18 minus 20 =	*			OR	x 60 =	0.00
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*				x 250 =	0.00
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	1250

APPLICATION AS AMENDED - PART II

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

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/490,294	06/06/2012	2431	1250	WEBR-044/01US 303666-2126	18	3

CONFIRMATION NO. 1064

58249
COOLEY LLP
ATTN: Patent Group
Suite 1100
777 - 6th Street, NW
WASHINGTON, DC 20001

FILING RECEIPT

OC000000054862335

Date Mailed: 06/19/2012

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

Applicant(s)
Matthew L. Boney, Longmont, CO;

Assignment For Published Patent Application
Webroot, Inc., Broomfield, CO

Power of Attorney: None

Domestic Priority data as claimed by applicant
This application is a CON of 11/408,146 04/20/2006 PAT 8201243 *
(*)Data provided by applicant is not consistent with PTO records.

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

If Required, Foreign Filing License Granted: 06/14/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/490,294**

Projected Publication Date: 09/27/2012

Non-Publication Request: No

Early Publication Request: No

Title

BACKWARDS RESEARCHING ACTIVITY INDICATIVE OF PESTWARE

Preliminary Class

726

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

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

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

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

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

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

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

NOT GRANTED

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

SelectUSA

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

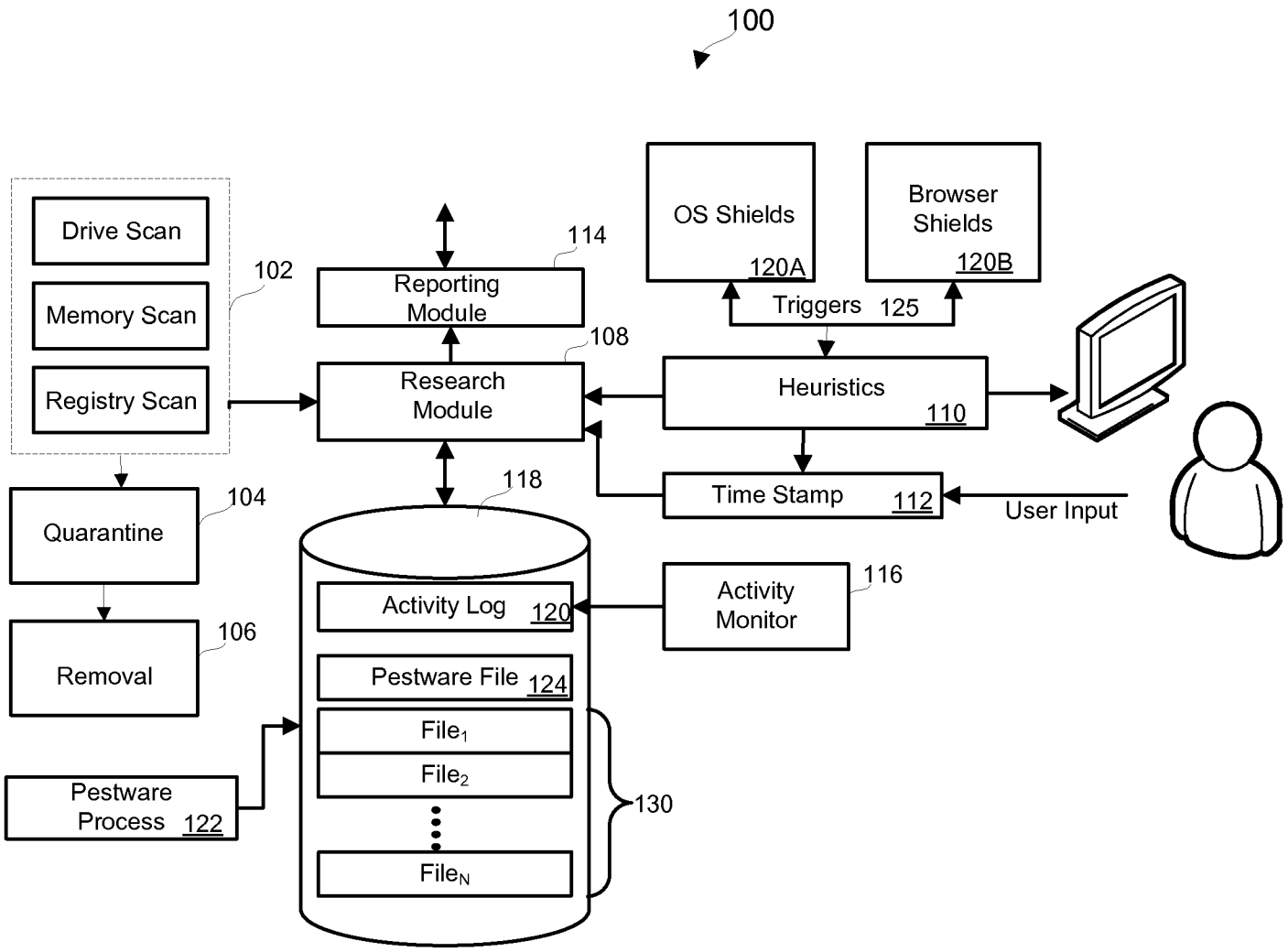
100
Drive Scan
Memory Scan
Registry Scan
102
Quarantine
104
Removal
106
Pestware Process 122
Reporting Module
114
Research Module
108
118
Activity Log 120
Pestware File 124
File1
File2
FileN
130
OS Shields 120A
Browser Shields 120B
Triggers 125
Heuristics 110
Time Stamp 112
User Input
Activity Monitor
116

FIGURE 1

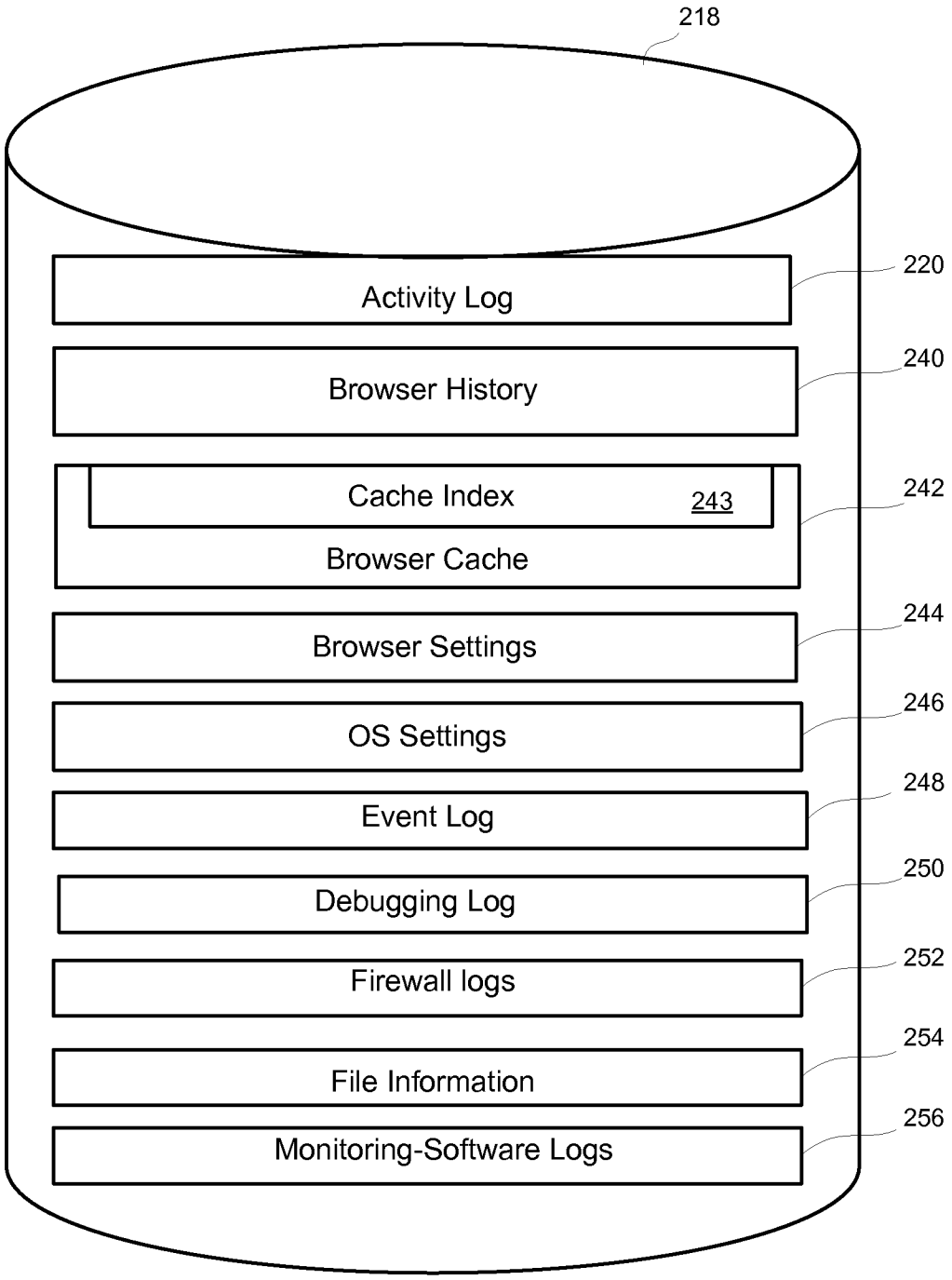
218
Activity Log
220
Browser History
240
Cache Index
243
Browser Cache
242
Browser Settings
244
OS Settings
246
Event Log
248
Debugging Log
250
Firewall logs
252
File Information
254
Monitoring-Software Logs
256

FIGURE 2

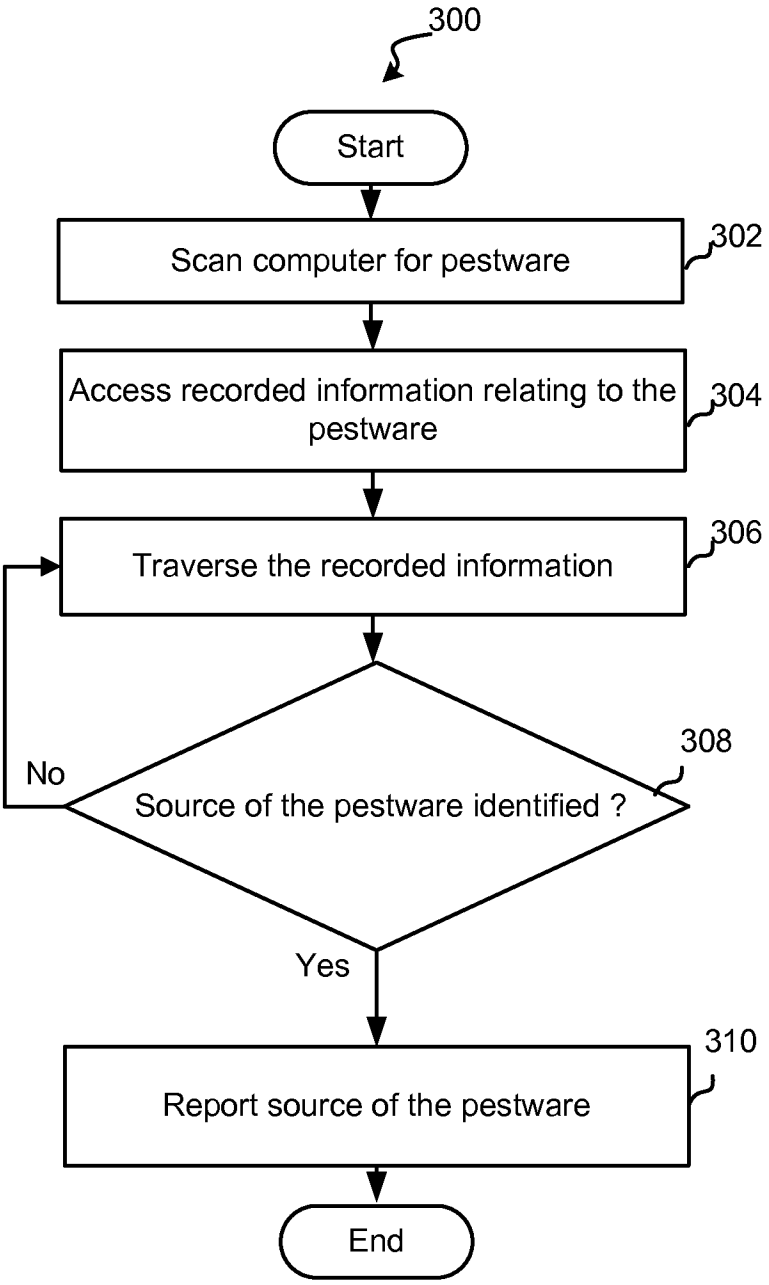
300
Start
Scan computer for pestware
302
Access recorded information relating to the pestware
304
Traverse the recorded information
306
Source of the pestware identified ?
308
No
Yes
Report source of the pestware
310
End

FIGURE 3

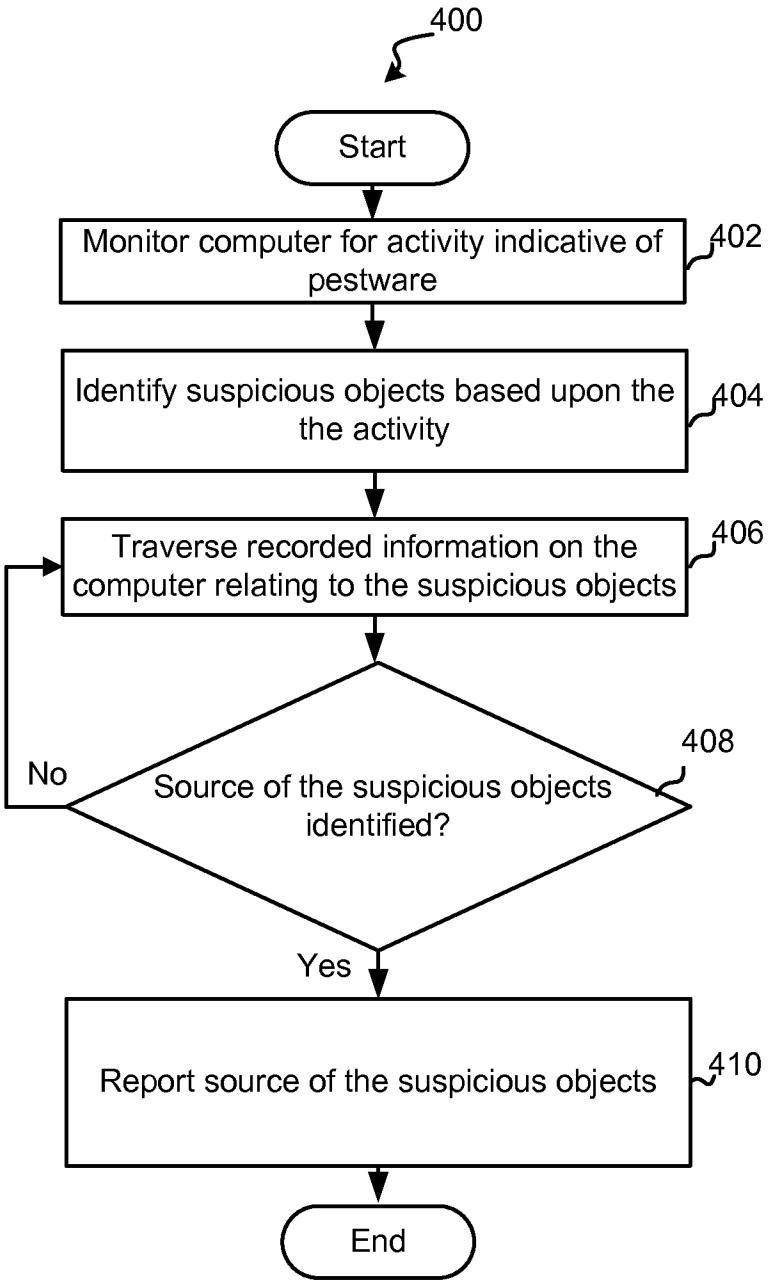
400
Start
Monitor computer for activity indicative of pestware
402
Identify suspicious objects based upon the the activity
404
Traverse recorded information on the computer relating to the suspicious objects
406
Source of the suspicious objects identified?
408
No
Yes
Report source of the suspicious objects
410
End

FIGURE 4

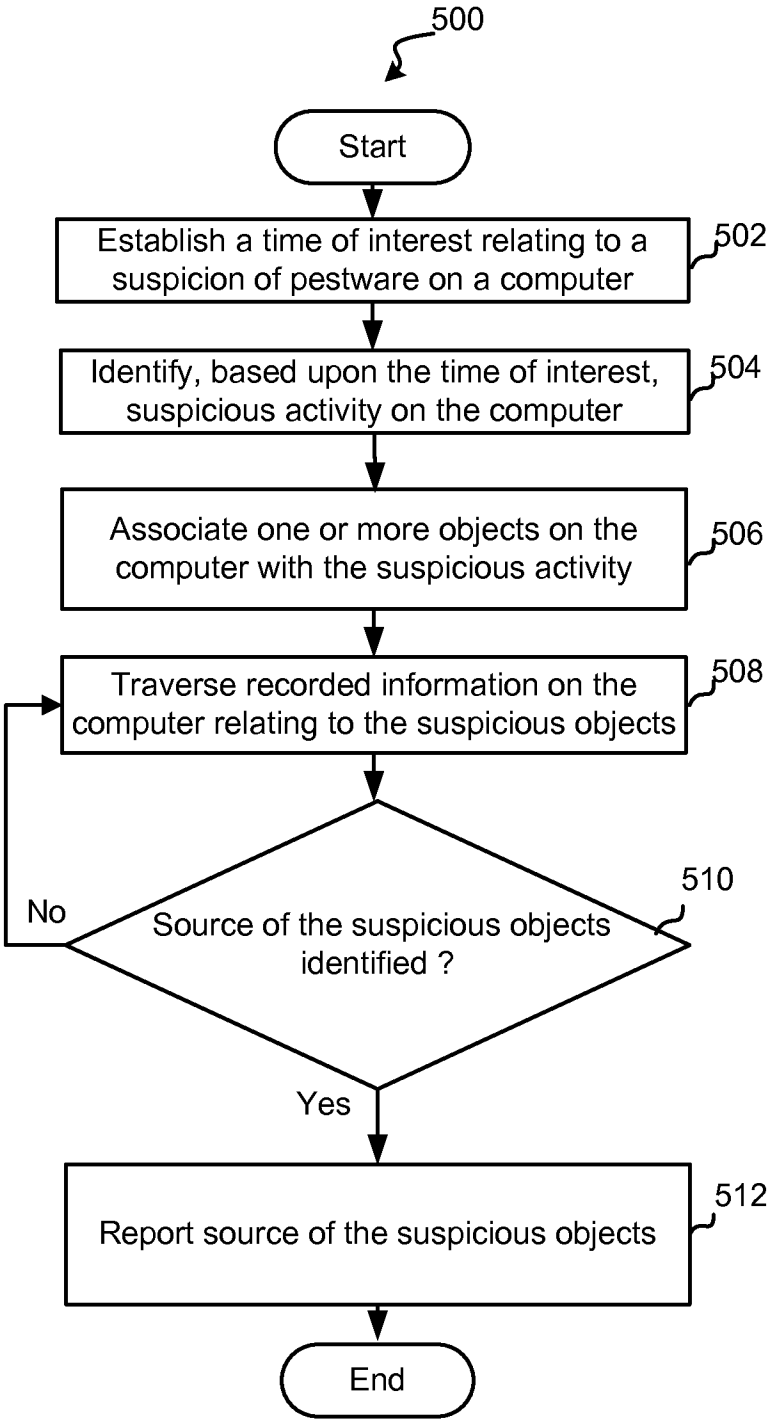
500
Start
Establish a time of interest relating to a suspicion of pestware on a computer
502
Identify, based upon the time of interest, suspicious activity on the computer
504
Associate one or more objects on the computer with the suspicious activity
506
Traverse recorded information on the computer relating to the suspicious objects
508
Source of the suspicious objects identified ?
510
No
Yes
Report source of the suspicious objects
512
End

FIGURE 5

OIPE IAP58
JUN 1 5 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 ACTIVITY INDICATIVE OF PESTWARE

the specification of which:

(check one)

[] is attached hereto;

[X] was filed as United States Application Serial No. 11/408,146 file 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

TITLE: BACKWARDS RESEARCHING ACTIVITY INDICATIVE OF PESTWARE

PRIORITY

[0001] The present application is a continuation of commonly-owned and assigned Application No. 11/408,146, entitled *Backwards Researching Activity Indicative of Pestware*, filed April 20, 2006, which is incorporated herein by reference in its entirety and for all purposes.

RELATED APPLICATIONS

[0002] The present application is related to commonly-owned and assigned Application No. 10/956,573, entitled *System and Method For Heuristic Analysis to Identify Pestware*, which issued as U.S. Patent No. 7,480,683; Application No. 10/956,574, entitled *System and Method for Pestware Detection and Removal* which issued as U.S. Patent No. 7,533,131; Application No. 11/237,291, entitled *System and Method for Locating Malware and Generating Malware Definitions*; Application No. 11/257,609, entitled *System and Method for Kernel-Level Pestware Management*; Application No. 11/237,291, entitled *Client Side Exploit Tracking*; Application No. 11/408,215, entitled *Backward Researching Existing Pestware*; and Application No. 11/408,145, entitled *Backward Researching Time Stamped Events to Find an Origin of Pestware*, which are incorporated herein by reference.

COPYRIGHT

[0003] 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

[0004] 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

[0005] 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.

[0006] 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.

[0007] 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

[0008] 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.

[0009] The present invention can provide a system and method for researching an identity of a source of activity that is indicative of pestware. In one embodiment the method comprises monitoring, using a kernel-mode driver, API call activity on the computer; storing information related to the API call activity in a log; analyzing, heuristically, the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold; identifying, based upon the API call activity, a suspected pestware object on the computer; identifying, in response to the identifying the suspected pestware object, a reference to an

identity of an externally networked source of the suspected pestware object; and reporting the identity of the externally networked source to an externally networked pestware research entity.

[0010] 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

[0011] 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.

DETAILED DESCRIPTION

[0012] 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.

[0013] 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.

[0014] 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 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.

[0015] 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.

[0016] 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.

[0017] 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.

[0018] 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.

[0019] 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 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.

[0020] 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.*

[0021] 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.

[0022] 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 110 about the activities and the heuristics engine 110 determines whether the research module 108 should be informed and/or whether the activity should be blocked.

[0023] 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.*

[0024] 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 110. In some embodiments for example, the heuristics module 110 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.

[0025] 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 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.

[0026] 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.

[0027] 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.

[0028] 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.

[0029] 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*.

[0030] 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.

[0031] 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 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.

[0032] 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.

[0033] 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.

[0034] 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.

[0035] 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.

[0036] 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.

[0037] 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.

[0038] 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.

[0039] 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.

[0040] 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.

[0041] 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 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).

[0042] 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.

[0043] 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.

[0044] 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.

[0045] 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 and/or one or more of the *N* files for information relating to the pestware-related activity.

[0046] 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.

[0047] 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.

[0048] 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.

[0049] 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.

[0050] 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.

[0051] 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).

[0052] 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.

[0053] 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.

[0054] 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.

[0055] 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).

[0056] 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.

[0057] 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 activity on a computer that is indicative of pestware comprising:

monitoring, using a kernel-mode driver, API call activity on the computer;

storing information related to the API call activity in a log;

analyzing, heuristically, the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold;

identifying, based upon the API call activity, a suspected pestware object on the computer;

identifying, in response to the identifying the suspected pestware object, a reference to an identity of an externally networked source of the suspected pestware object; and

reporting the identity of the externally networked source to an externally networked pestware research entity.

2. The method of claim 1, wherein the identity of the externally networked source is selected from the group consisting of an I.P. address, a URL, an email client and a program.

3. The method of claim 1, wherein the identifying the suspected pestware object includes accessing an activity log that includes information that relates the activity to the suspected pestware object.

4. The method of claim 1, wherein the identifying a reference includes accessing at least a portion of a recorded history of externally networked sources.

5. The method of claim 4, wherein the recorded history resides in 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.

6. A system for identifying a source of activity on a computer that is indicative of pestware including:

a kernel-level monitor configured to monitor API call activity on the computer and to store information related to the API call activity in a log;

a heuristics module configured to analyze the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold;

a research portion configured to identify, in response to a prompt from the heuristics module, a suspected pestware object on the computer; and

a reporting portion configured to generate a report including a reference to an identity of an externally networked source of the suspected pestware object and to report the identity of the externally networked source to an externally networked pestware research entity.

7. The system of claim 6, wherein the kernel-level monitor is configured to store information about a relationship between at least one API call of the API call activity and a file.

8. The system of claim 7, wherein the information comprises an identity of at least one process that made at least one API call in the log.

9. The system of claim 6, wherein the heuristics module is configured to receive information about the API call activity from the kernel-level monitor and to determine whether the API call activity is indicative of pestware.

10. The system of claim 6, wherein the kernel-level monitor is configured to intercept at least one API call.

11. The system of claim 6, wherein the identity of the externally networked source is selected from the group consisting of an I.P. address, a URL, an email client and a program name.

12. The system of claim 6, wherein the research portion is configured to access at least a portion of a recorded history of externally networked sources.

13. The system of claim 12, wherein the recorded history resides in 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.

14. A computer-readable medium including processor-executable instructions for identifying an origin of activity on a computer that is indicative of pestware, the instructions including instructions for:

monitoring, using a kernel-mode driver, API call activity on the computer;

storing information related to the API call activity in a log;

analyzing, heuristically, the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold;

identifying, based upon the API call activity, a suspected pestware object on the computer;

identifying, in response to the identifying the suspected pestware object, a reference to an identity of an externally networked source of the suspected pestware object; and

reporting the identity of the externally networked source to an externally networked pestware research entity.

15. The computer-readable medium of claim 14, wherein the identity of the externally networked source is selected by an identifier selected from the group consisting of an I.P. address, a URL, an email client and a program.

16. The method of claim 14, wherein the instructions for identifying the suspected pestware object include instructions for accessing an activity log that includes information that relates the activity to the suspected pestware object.

17. The computer-readable medium of claim 14, wherein the instructions for identifying a reference include instructions for accessing at least a portion of a recorded history of externally networked sources.

18. The computer-readable medium of claim 17, wherein the recorded history resides in 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 researching an identity of a source of activity that is indicative of pestware is described. In one embodiment the method comprises monitoring, using a kernel-mode driver, API call activity on the computer; storing information related to the API call activity in a log; analyzing, heuristically, the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold; identifying, based upon the API call activity, a suspected pestware object on the computer; identifying, in response to the identifying the suspected pestware object, a reference to an identity of an externally networked source of the suspected pestware object; and reporting the identity of the externally networked source to an externally networked pestware research entity.

Sophos Ex. 1002
Page 108 of 120

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

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	WEBR-044/01US 303666-2126
	Application Number	

Title of Invention	BACKWARDS RESEARCHING ACTIVITY INDICATIVE OF PESTWARE

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

Secrecy Order 37 CFR 5.2

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

Applicant Information:

Applicant 1

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

Prefix	Given Name	Middle Name	Family Name	Suffix
	Matthew	L.	Boney	

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

City	Longmont	State/Province	CO	Country of Residence	US

Citizenship under 37 CFR 1.41(b)	US

Mailing Address of Applicant:

Address 1	1100 East 17th Avenue, E303
Address 2	

City	Longmont	State/Province	CO
Postal Code	80501	Country	US

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

Correspondence Information:

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

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

Customer Number	58249		
Email Address	zpatdcdocketing@cooley.com	Add Email	Remove Email

Application Information:

Title of the Invention	BACKWARDS RESEARCHING ACTIVITY INDICATIVE OF PESTWARE		
Attorney Docket Number	WEBR-044/01US 303666-2126	Small Entity Status Claimed	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		Sub Class (if any)	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)	5	Suggested Figure for Publication (if any)	1

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

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	WEBR-044/01US 303666-2126
	Application Number	
Title of Invention	BACKWARDS RESEARCHING ACTIVITY INDICATIVE OF PESTWARE	

Publication Information:

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

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

Representative Information:

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

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	58249		

Domestic Benefit/National Stage Information:

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

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	11408146	2006-04-20

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

Foreign Priority Information:

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

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

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

Assignee Information:

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

Assignee 1

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

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	WEBR-044/01US 303666-2126
	Application Number	
Title of Invention	BACKWARDS RESEARCHING ACTIVITY INDICATIVE OF PESTWARE	

If the Assignee is an Organization check here. ☒			
Organization Name	Webroot, Inc.		
Mailing Address Information:			
Address 1	385 Interlocken Crescent, Suite 800		
Address 2			
City	Broomfield	**State/Province**	CO
Country	US	Postal Code	80021
Phone Number		Fax Number	
Email Address			
Additional Assignee Data may be generated within this form by selecting the **Add** button.			

Signature:

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

Signature	/Mark R. Schafer/			Date (YYYY-MM-DD)	2012-06-06
First Name	Mark	Last Name	Schafer	Registration Number	65336

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	BACKWARDS RESEARCHING ACTIVITY INDICATIVE OF PESTWARE
First Named Inventor/Applicant Name:	Matthew L. Boney
Filer:	Mark Randolph Schafer/Sherry Bitler
Attorney Docket Number:	WEBR-044/01US 303666-2126

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility application filing	1011	1	380	380
Utility Search Fee	1111	1	620	620
Utility Examination Fee	1311	1	250	250
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**1250**

Electronic Acknowledgement Receipt

EFS ID:	12952389
Application Number:	13490294
International Application Number:	
Confirmation Number:	1064
Title of Invention:	BACKWARDS RESEARCHING ACTIVITY INDICATIVE OF PESTWARE
First Named Inventor/Applicant Name:	Matthew L. Boney
Customer Number:	58249
Filer:	Mark Randolph Schafer/Sherry Bitler
Filer Authorized By:	Mark Randolph Schafer
Attorney Docket Number:	WEBR-044/01US 303666-2126
Receipt Date:	06-JUN-2012
Filing Date:	
Time Stamp:	18:36:50
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1250
RAM confirmation Number	8389
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	Drawings-only black and white line drawings	WEBR04401US_Drawings.pdf	51500 de2793ba9c5c523ba1098c140f66edb3eba638d4	no	5
Warnings:					
Information:					
2	Oath or Declaration filed	WEBR04401US-declaration.pdf	53000 916dd6cf493fa09acdc6b6506916dfee6ecfd30d	no	2
Warnings:					
Information:					
3		WEBR04401US_Continuation_Application.pdf	162566 20d50656c953adfcf22616a964479927dad25608	yes	26

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	20
Claims	21	25
Abstract	26	26

Warnings:					
Information:					
4	Application Data Sheet	WEBR04401US-ads.pdf	87419 6a899f8297488fb1d1bce1e444db97b101d43839	no	4
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
5	Fee Worksheet (SB06)	fee-info.pdf	33311 47cad0294b07865ae2e2f2c4e64508f06e5aa6f1	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	387796		

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

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

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

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

Electronic Acknowledgement Receipt

EFS ID:	12952389
Application Number:	13490294
International Application Number:	
Confirmation Number:	1064
Title of Invention:	BACKWARDS RESEARCHING ACTIVITY INDICATIVE OF PESTWARE
First Named Inventor/Applicant Name:	Matthew L. Boney
Customer Number:	58249
Filer:	Mark Randolph Schafer/Sherry Bitler
Filer Authorized By:	Mark Randolph Schafer
Attorney Docket Number:	WEBR-044/01US 303666-2126
Receipt Date:	06-JUN-2012
Filing Date:	
Time Stamp:	18:36:50
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1250
RAM confirmation Number	8389
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	Drawings-only black and white line drawings	WEBR04401US_Drawings.pdf	51500 de2793ba9c5c523ba1098c140f66edb3eba638d4	no	5
Warnings:					
Information:					
2	Oath or Declaration filed	WEBR04401US-declaration.pdf	53000 916dd6cf493fa09acdc6b6506916dfee6ecfd30d	no	2
Warnings:					
Information:					
3		WEBR04401US_Continuation_Application.pdf	162566 20d50656c953adfcf22616a964479927dad25608	yes	26

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	20
Claims	21	25
Abstract	26	26

Warnings:					
Information:					
4	Application Data Sheet	WEBR04401US-ads.pdf	87419 6a899f8297488fb1d1bce1e444db97b101d43839	no	4
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
5	Fee Worksheet (SB06)	fee-info.pdf	33311 47cad0294b07865ae2e2f2c4e64508f06e5aa6f1	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	387796		

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.