PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	
Filing Date	
First Named Inventor	Mauritius Schmidtler
Art Unit	
Examiner Name	Not Assigned
Attorney Docket Number	04584.0168US01

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

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

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Mauritius Schmidtler
	Art Unit	
	Examiner Name	Not Assigned
	Attorney Docket Number	04584.0168US01

	1	KHAN, Hassan et al., "Determining Malicious Executable Distinguishing Attributes and Low-Complexity Detection", J. Comput Virol, 7.2 (2011), pgs. 95-105.	☐
	2	KOLTER, J. Zico et al., "Learning to Detect and Classift Malicious Executables in the Wild", Journal of Machine Learning Research 7 (2006), pgs. 2721-2744.	☐

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Mauritius Schmidtler
	Art Unit	
	Examiner Name	Not Assigned
	Attorney Docket Number	04584.0168US01

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☒ None

SIGNATURE

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

Signature	/Jason E. Becker/	Date (YYYY-MM-DD)	2015-05-12
Name/Print	Jason E. Becker	Registration Number	66632

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

PTO/AIA/82A (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	Filed herewith
Filing Date	Filed herewith
First Named Inventor	Mauritius Schmidtler
Title	AUTOMATIC THREAT DETECTON OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS
Art Unit	Not assigned
Examiner Name	Not assigned
Attorney Docket Number	04584.0168US01

SIGNATURE of Applicant or Patent Practitioner

Signature	/Jason E. Becker/	Date (Optional)	May 12, 2015
Name	Jason E. Becker	Registration Number	66632
Title (if Applicant is a juristic entity)	Attorney		
Applicant Name (if Applicant is a juristic entity)	Webroot Inc.		

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ *Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 11/30/2014. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 23552

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

WEBROOT INC.

☐ Inventor or Joint Inventor (title not required below)
☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)
☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)
☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature	/RH/	Date (Optional)	May 12, 2014
Name	Ryan Howe		
Title	Associate General Counsel		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ Total of forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

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

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	AUTOMATIC THREAT DETECTON OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS
First Named Inventor/Applicant Name:	Mauritius Schmidtler
Filer:	Jason Evan Becker/Jacquelyn Slate
Attorney Docket Number:	04584.0168US01

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	70	70
Utility Search Fee	2111	1	300	300
Utility Examination Fee	2311	1	360	360
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**730**

Electronic Acknowledgement Receipt

EFS ID:	22322426
Application Number:	14709875
International Application Number:	
Confirmation Number:	1593
Title of Invention:	AUTOMATIC THREAT DETECTON OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS
First Named Inventor/Applicant Name:	Mauritius Schmidtler
Customer Number:	23552
Filer:	Jason Evan Becker/Jacquelyn Slate
Filer Authorized By:	Jason Evan Becker
Attorney Docket Number:	04584.0168US01
Receipt Date:	12-MAY-2015
Filing Date:	
Time Stamp:	14:45:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$730
RAM confirmation Number	1057
Deposit Account	
Authorized User	

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	2015_05_12_ADS_04584_0168US01.PDF	1561132 b19bb9e7ec8b6593ed865b3915d389066cc97677	no	7
Warnings:					
Information:					
2	Oath or Declaration filed	2015_05_12_Declaration_Executed_04584_0168US01.PDF	340074 ae1273fc4b71ee40159d2acc05786e5379ffcb13	no	6
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
3		2015_05_12_SpecificationAsFiled_04584_0168US01.PDF	181213 7d839a3a92fbaca1cabda1e7d17f73b3208bedc1	yes	28

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Specification	1	23
Claims	24	27
Abstract	28	28

Warnings:					
Information:					
4	Drawings-only black and white line drawings	2015_05_12_FiguresAsFiled_04584_0168US01.PDF	148489 af79014775b8f4526957867ddc7b23980e5d2572	no	4
Warnings:					
Information:					
5	Transmittal Letter	2015_05_12_IDS_TransLtr_04584_0168US01.PDF	74414 63836f1230f18d3056637be2e8847901fb5d2474	no	2
Warnings:					
Information:					

6	Information Disclosure Statement (IDS) Form (SB08)	2015_05_12_IDS_SB08_04584_0168US01.PDF	612119 0843301ee59c8a8a4b18191dc2467847faf6c0bf	no	4
Warnings:					
Information:					
A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
7	Non Patent Literature	KHAN_determining_malicious.PDF	360303 0c92e5c380ab034b45d8ce348c867a03cfe3881b	no	11
Warnings:					
Information:					
8	Non Patent Literature	KOLTER_learning_to_detect.PDF	183157 b0544fc94d8bc745cad0d67b9e333358cf9c9dd8	no	24
Warnings:					
Information:					
9	Power of Attorney	2015_05_12_POA_04584_0168US01.PDF	393963 756e9444c7db239e50f3c6ac3d53c1e2d246a36c	no	2
Warnings:					
Information:					
10	Fee Worksheet (SB06)	fee-info.pdf	35288 f1f4d93a39c2ea3bd384c2df4b987f5473305ba2	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	3890152	

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0168US01
	Application Number	
Title of Invention	AUTOMATIC THREAT DETECTON OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS	

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.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Mauritius		Schmidtler	

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

City	Escondido	State/Province	CA	Country of Residence i	US

Mailing Address of Inventor:

Address 1	c/o Webroot Inc.
Address 2	385 Interlocken Crescent

City	Broomfield	State/Province	CO
Postal Code	80021	Country i	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Gaurav		Dalal	

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

City	San Jose	State/Province	CA	Country of Residence i	US

Mailing Address of Inventor:

Address 1	c/o Webroot Inc.
Address 2	385 Interlocken Crescent

City	Broomfield	State/Province	CO
Postal Code	80021	Country i	US

Inventor 3 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Reza		Yoosoofmiya	

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

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0168US01
	Application Number	
Title of Invention	AUTOMATIC THREAT DETECTON OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS	

City	San Diego	State/Province	CA	Country of Residence i	US

Mailing Address of Inventor:

Address 1	c/o Webroot Inc.		
Address 2	385 Interlocken Crescent		
City	Broomfield	State/Province	CO
Postal Code	80021	Country i	US

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

Correspondence Information:

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

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

Customer Number	23552		
Email Address	DOCKMPLS@merchantgould.com	Add Email	Remove Email

Application Information:

Title of the Invention	AUTOMATIC THREAT DETECTON OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS		
Attorney Docket Number	04584.0168US01	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	4	Suggested Figure for Publication (if any)	

Filing By Reference :

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country i

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.

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0168US01
	Application Number	
Title of Invention	AUTOMATIC THREAT DETECTON OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS	

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).
Either enter 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	23552		

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.
When referring to the current application, please leave the application number blank.

Prior Application Status			Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)

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

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. 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(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) [i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

			Remove
Application Number	Country [i]	Filing Date (YYYY-MM-DD)	Access Code [i] (if applicable)

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

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0168US01
	Application Number	
Title of Invention	AUTOMATIC THREAT DETECTON OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS	

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☒ Authorization to Permit Access to the Instant Application by the Participating Offices

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

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

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0168US01
	Application Number	
Title of Invention	AUTOMATIC THREAT DETECTON OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS	

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

(•) Assignee	( ) Legal Representative under 35 U.S.C. 117	( ) Joint Inventor
( ) Person to whom the inventor is obligated to assign.	( ) Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

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

Organization Name	Webroot Inc.

Mailing Address Information:

Address 1	385 Interlocken Crescent		
Address 2			
City	Broomfield	**State/Province**	CO
Country [i]	US	Postal Code	80021
Phone Number		Fax Number	
Email Address			

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

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. [ ]

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0168US01
	Application Number	
Title of Invention	AUTOMATIC THREAT DETECTON OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS	

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

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

Signature	/Jason E. Becker/			Date (YYYY-MM-DD)	2015-05-12
First Name	Jason E.	Last Name	Becker	Registration Number	66632

Additional Signature may be generated within this form by selecting the Add button. Add

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.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

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

Title of Invention	AUTOMATIC THREAT DETECTON OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____

filed on _____

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

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

LEGAL NAME OF INVENTOR

Inventor: Mauritius Schmidtler Date (Optional): May 11th 2015

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

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

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

Privacy Act Statement

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

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

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

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

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

Title of Invention	AUTOMATIC THREAT DETECTON OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____

filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

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

LEGAL NAME OF INVENTOR

Inventor: Gaurav Dalal Date (Optional): 05/11/15

Signature: Gaurav Dalal

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

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

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

Privacy Act Statement

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

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

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

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

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

Title of Invention	AUTOMATIC THREAT DETECTON OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [■] The attached application, or
- [ ] United States application or PCT international application number _____

filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

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

LEGAL NAME OF INVENTOR

Inventor: Reza Yoosoofmiya Date (Optional): 05/11/2015

Signature: 

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

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

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

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.

AUTOMATIC THREAT DETECTON OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS

Background

[0001] Everyday new executable files are created and distributed across networks. A large portion of these distributed executable files are unknown. For instance, it is not known if such distributed executable files are malicious or not. Given the high volume of new unknown files distributed on a daily basis, it is important to determine threats contained in the set of new unknown files instantaneously and accurately. It is with respect to this general environment that aspects of the present technology disclosed herein have been contemplated.

Summary

[0002] Aspects of the present disclosure relate to threat detection of executable files. A plurality of static data points are extracted from an executable file without decrypting or unpacking the executable file. The executable file may then be analyzed without decrypting or unpacking the executable file. Analyzing of the executable file comprises applying a classifier to the plurality of static data points extracted from the executable file. The classifier is trained from data comprising known malicious executable files, known benign executable files and potentially unwanted executable files. Based upon the analysis of the executable file, a determination is made as to whether the executable file is harmful. In some examples, execution of the executable file is prevented when a determined probability value that the executable file is harmful exceeds a threshold value.

[0003] This summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used to limit the scope of the claimed subject matter.

Brief Description of the Drawings

[0004] Non-limiting and non-exhaustive examples are described with reference to the following figures. As a note, the same number represents the same element or same type of element in all drawings.

[0005] Figure 1 illustrates an exemplary system 100 showing interaction of components for implementation threat detection as described herein.

[0006] Figure 2 illustrates an exemplary distributed system 200 showing interaction of components for implementation of exemplary threat detection as described herein.

[0007] Figure 3 illustrates an exemplary method 300 for implementation of threat detection systems and methods described herein.

[0008] Figure 4 illustrates one example of a suitable operating environment 400 in which one or more of the present examples may be implemented.

Detailed Description

[0009] Non-limiting examples of the present disclosure relate to the threat detection of executable files. The examples disclosed herein may also be employed to detect zero day threats from unknown executable files. However, one skilled in the art will recognize that the present disclosure is not limited to detection of executable files that may present zero day threats and can be applicable to any unknown file that is attempting to execute on a system (e.g., processing device). The present disclosure is able to detect whether an executable file is harmful or benign before the executable file is actually executed on a processing device. In examples, machine learning processing applies a classifier to evaluate an executable file based on static points data collected from the executable file. The classifier is trained from a collection of data comprising known malicious files, potentially unwanted files and benign files. The classifier is designed and trained such that it can handle encrypted and/or compressed files without decrypting and/or decompressing the files.

Sophos Ex. 1003
Page 27 of 456

[0010] Approaches to detecting threats typically focus on finding malicious code blocks within a file and analyzing the behavior of the file. Such approaches are expensive and time-consuming operations that require decrypting encrypted files, dissembling code, analyzing behavior of malware, among other things. Additionally, behavioral detection requires the execution of the potentially malicious code, thereby presenting an opportunity for the malicious code to harm the computing system is executing on. The present disclosure achieves high and accurate classification rates for potentially malicious executables without the need to employ time consuming processing steps like decryption, unpacking or executing unknown files while maintaining a controlled and safe environment. The determination of unknown files is achieved by evaluating static data points extracted from an executable file using a trained classification system that is able to identify potential threats without analyzing executable behavior of a file. The present disclosure also provides for the creation of a training set that adaptively learns what static data points may indicate the existence of malicious code using training data that contains a statistically significant number of both encrypted and non-encrypted examples of malicious or unwanted executable files, among other information. By collecting a large set of training examples as they appear as publicly available and distributed over network connection (e.g., "in the wild"), the present disclosure ensures that its adaptive learning processing is robust enough to comprise sufficient representation of features (and distributions) from files that may be encrypted, not-encrypted, compressed, and uncompressed, among other examples.

[0011] A number of technical advantages are achieved based on the present disclosure including, but not limited to: enhanced security protection including automatic detection of threats, reduction or minimization of error rates in identification and marking of suspicious behavior or files (e.g., cut down on the number of false positives), ability to adapt over time to continuously and quickly detect new threats or potentially unwanted files/applications, improved efficiency in detection of malicious files, and improved usability and interaction for users by eliminating the need to continuously check for security threats, among other benefits that will be apparent to one of skill in the art.

[0012] Figure 1 illustrates an exemplary system 100 showing an interaction of components for implementation threat detection as described herein. Exemplary system 100 may be a combination of interdependent components that interact to form an integrated whole for execution of threat detection and/or prevention operations. Components of the systems may be hardware components or software implemented on and/or executed by hardware components of the systems. In examples, system 100 may include any of hardware components (e.g., used to execute/run operating system (OS)), and software components (e.g., applications, application programming interfaces, modules, virtual machines, runtime libraries, etc.) running on hardware. In one example, an exemplary system 100 may provide an environment for software components to run, obey constraints set for operating, and/or makes use of resources or facilities of the system 100, where components may be software (e.g., application, program, module, etc.) running on one or more processing devices. For instance, threat detection operations (e.g., application, instructions, modules, etc.) may be run on a processing device such as a computer, a client device (e.g., mobile processing device, laptop, smartphone/phone, tablet, etc.) and/or any other electronic devices, where the components of the system may be executed on the processing device. In other examples, the components of systems disclosed herein may be spread across multiple devices. For instance, files to be evaluated may be present on a client device and information may be processed or accessed from other devices in a network such as, for example, one or more server devices that may be used to perform threat detection processing and/or evaluation a file before execution of the file by the client device.

[0013] As one example, system 100 comprises a knowledge component 102, a learning classifier component 104, and a threat determination component 106, each having one or more additional components. The scale of systems such as system 100 may vary and include more or less components than those described in Figure 1. In alternative examples of system 100, interfacing between components of the system 100 may occur remotely, for example where threat detection processing is implemented on a first device (e.g., server) that remotely monitors and controls process flow for threat detection and prevention of a second processing device (e.g., client).

[0014] As an example, threat detection may detection exploits that are executable files. However, one skilled in the art will recognize that the descriptions herein referring to executable files are just an example. Threat detection examples described herein can relate to any computer file. In one example, an executable file may be a portable executable (PE) file that is a file format for executables, object code, dynamic link library files (DLLs), and font library files, among other examples. However, one skilled in the art will recognize that executable files are not limited to PE files and can be any file or program that executes a task according to an encoded instruction. Knowledge component 102 described herein may collect data for use in building, training and/or re-training a learning classifier to evaluate executable files. The knowledge component 102 is one or more storages, memories, and/or modules that continuously collects and manages data that may be used to detect threats in files such as executable files. In one example, the knowledge component 102 maintains a robust collection of data comprising known malicious executable files, known benign executable files, and potentially unwanted executable files. As an example, Malicious executable files may be any type of code, data, objects, instructions, etc., that may cause harm or alter an intended function of a system and/or any system resources (e.g., memory, processes, peripherals, etc.) and/or applications running on a device such as an operating system (OS). A benign executable file is a file that upon execution, will not cause harm/damage or alter an intended system function. In other examples, a benign executable may cause harm/damage or alter an intended system; however, the potential harm/damage or alteration may be acceptable to the owner of the system or device. In examples, potentially unwanted executable files are files that may be installed on system 100 that may not be malicious, but a user of the device may not want such a file to execute and/or a file that is executed/installed unknowingly to a user. In one example, classification of executable files as malicious, benign or potentially unwanted are done by research and development support associated with developments and programming of a threat detection application/module. However, one skilled in the art will recognize that identification and classification of files into the above identified categories may be done by monitoring or evaluating a plurality of resources including but not limited to: network data, executable file libraries and information on previously known malicious executable files as well as benign executable

files and potentially unwanted executable files, users/customers of threat detection/computer security software, network flow observed from use of threat detection processing and products, business associations (e.g., other existing threat detection services or partners), third-party feeds, and updates from threat detection performed using learning classifier of present disclosure, among other examples.

[0015] To classify executable files into one of the above identified categories, the knowledge component 102 collects static data on a large variety of executable files (e.g., PE files). Examples of different types of executable files collected and evaluated include but are not limited to: bit files (e.g., 32/64 bit files), operating system files (e.g., Windows, Apple, Linux, Unix, etc.), custom built files (e.g., internal tool files), corrupted files, partial downloaded files, packed files, encrypted files, obfuscated files, third party driver files, manually manipulated binary files, unicode files, infected files, and/or memory snapshots, among other examples. The data collected and maintained by the knowledge component 102 yields a knowledgebase that may be used to periodically train a classifier, e.g. learning classifier component 104 utilized by system 100. The learning classifier component may be used to classify an executable file as one of the following classifications: malicious, benign or potentially unwanted. In some examples, classification may span two or more two or more of those classification categories. For example, an executable file may be benign in the sense that it is not harmful to system 100 but may also be classified as potentially unwanted as it might be installed without explicit user consent, for example. Data maintained by the knowledge component 102 may be continuously updated system 100 or a service that updates system 100 with new exploits to add to the training sample. For example, a research team may be employed to continuously collect new examples of harmful executables, benign executables, and potentially unwanted executables, as many unknown executable files are generated on a daily basis over the Internet. Executable files may be evaluated by the research team such as by applying applications or processing to evaluate executable files including data associated with the file and/or actions associated with the file (e.g., how it is installed and what a file does upon execution). Continuous update of the data maintained by the knowledge component 102 in conjunction with on-going re-learning/re-training of the learning classifier component 104 ensures that system 100 is up-to-date on current

threats. Knowledge of the most current threats improves the generalization capability of system 100 to new unknown threats. By incorporating malicious files, benign files and potentially unwanted files, the present disclosure greatly improves a knowledge base that may be used to in training a learning classifier thereby resulting in more accurate classifications as compared with other knowledge bases that are based on only malicious and/or benign files.

[0016] In examples, the collected data on the executable files is analyzed to identify static data points that may indicate one of a malicious file, a benign file or a potentially unwanted file. For instance, the knowledge component 102 may employ one or more programming operations to identify static data points for collection, and to associate the static data points with one of the categories of files (e.g., malicious, benign or potentially unwanted). Programming operations utilized by the knowledge component 102 include operations to collect file data (e.g., executable files or data points from executable files), parse the file data, and store extracted data points. In at least one example, the knowledge component 102 comprises one or more components to manage file data. For example, the knowledge component 102 may comprise one or more storages such as databases, and one or more additional components (e.g., processors executing programs, applications, application programming interfaces (APIs), etc.).

[0017] Further, the knowledge component 102 may be configured to continuously collect data, generate a more robust collection of file data to improve classification of file data and train a classifier used to detect whether an executable file is harmful, benign, or potentially unwanted. The identification of static data points to be collected and analyzed for executable files may be continuously updated as more information becomes available to the knowledge component 102. A static data point may be a point of reference used to evaluate an executable file. As examples, static data points include, but are not limited to: header information, section information, import and export information, certificate information, resource information, string and flag information, legal information, comments, and/or program information (e.g., APIs and DLLs), among other examples. Static data points may be organized into categories that identify a type of static data point. Categories of static data points comprise, but are not limited to: numeric values,

nominal values string sequences, byte sequences, and/or Boolean values, among other examples. Any number of static data points may be collected and analyzed for an executable file. In general, collecting and analyzing a greater number of static data points results in more accurate classification of an executable file. For example, eighty static data points may be identified and collected (or attempted to be collected) from an executable file during analysis of an executable file. While a specific number is static data points are provided herein, one of skill in the art will appreciate the more or fewer static data points may be collected without departing from the scope of this disclosure. As an example, the following table, Table 1.1, identifies some of the static data points identified for analysis of an executable file, where the static data points are organized by category:

Table 1.1

Numeric values	**Nominal values**	**Strings/Byte sequences**	**Boolean values**
File size	initialize	Comments	Address Of Entry Point Anomaly
linker version	Un-initialize	company name	Image Base Anomaly
code size	entry point	file description	Section Alignment Anomaly
OS version	subsystem	internal name	Size Of Code Mismatch Anomaly
image version	file subtype	legal copyright	Low Import Count Anomaly
subsystem version	language	original file	Entry Point Anomaly
file version number	file flags masks	private build	certificate Validity
product version number	file flags	product name	Certificate Exception
size of heapr	file OS	special build	Code Characteristics Anomaly

size of stackr	file type	product version	Code Name Anomaly
size of image	machine type	file version	Count Anomaly
PE header time	PE type	package code	Data Characteristics Anomaly
Section Entropy	section counts	product code	Data Name Anomaly
Sections count	DLL count	export DLL name	Export Exception
	DLL functions	assembly version	Large Number of DLLs Anomaly
	data directory	Certificate Issuer	flag DLL Name Anomaly
	export count	Certificate Subject	Number of Functions Anomaly
	Earliest Data Byte	Imports	Function Name Anomaly
	resources	Exports	PE Header Anomaly
	resources language	Section Names	High Section Count Anomaly
	resource Encoding	Non-resource section strings	PE Magic Validity
	resource code page		Resource Exception
	resource size		VR Code Ratio Anomaly
	DLL characteristics		Import Exception

[0018] Examples of the present disclosure need not distinguish between encrypted files and non-encrypted files. The static data points may be extracted from files regardless of whether or not they are encrypted and/or compressed. Given that the training set contains a statistically significant number of encrypted and non-encrypted examples, as well as compressed and decompressed files, a learning classifier (e.g., learning classifier component 104) may be trained to identify features in the extracted data to identify malicious files. Since a very large majority of the files "in the wild" use few tools to

encrypt the files (e.g., encryption algorithm, packers, etc.), the distribution of the data found across large number of files is preserved after encryption, although the actual content of the data is transformed into something different. By collecting a large set of training examples as they appear "in the wild", a sufficient representation of features and distributions associated with the represented features exist in a training set that are both encrypted and not-encrypted. The present disclosure provides at least one benefit over other threat detection applications/programs by utilizing a very large and diverse training sample, thereby enabling a more intelligent and adaptive learning classifier that is able to achieve high detection rates for threats and low false positive rates, among other benefits.

[0019] In addition to collecting and managing information to train a learning classifier, the knowledge component 102 is used to evaluate an executable file and extract/collect static data points for evaluation of the file by the learning classifier before the file is executed. In one example, the system automatically identifies a new file (e.g., unknown file) for evaluation. As examples, identification of an executable file for evaluation may occur in examples such as: when a download of a file is requested, while a download is being performed, evaluation of streaming data, when a new file is detected as attempting to execute (e.g., potentially unwanted file), and before an unknown file or file containing executable code that was not previously checked attempts to execute, among other examples. In another example, a user of a device with which components of system 100 are operating may identify a file to be evaluated. The knowledge component 102 collects as many static data points as it can to evaluate the executable file using a learning classifier built by the learning classifier component 102. In an exemplary extraction, the knowledge component 102 extracts each of the static data points identified in Table 1.1. The learning classifier component 102 intelligently builds a learning classifier to evaluate a file based on the extracted static data points of the file and the data managed by the knowledge component 102.

[0020] The learning classifier component 104 is a component used to evaluate an executable file using the information provided by the knowledge component 102. The learning classifier component 104 interfaces with the knowledge component 102 and a threat detection component 106 for the system 100 to evaluate an executable file as a

possible threat. As an example, the learning classifier 104 applies programming operations or machine learning processing to evaluate static data points extracted from a file to be analyzed. In doing so, the learning classifier component 104 builds a learning classifier based on information from the knowledge component 102 including the extracted static data points of a file and the information used to train/re-train the learning classifier (e.g., static data on the robust collection of executable files including variety of file types of malicious executable files, benign executable files, and potentially unwanted executable files).

[0021] As an example, the learning classifier can adaptively set features of a learning classifier based on the static data points extracted for a file. For example, ranges of data can be identified for static data points that may enable the learning classifier to controllably select (e.g., turn on/off) features for evaluation by learning classifier. In one instance where a static data point extracted for evaluation is a file size (e.g., numeric value), the learning classifier may turn on/off features for evaluation based on whether a the file size of the file is within a certain range. In another example, the learning classifier may detect that the file does not contain "legal information" in the file. Legal information may be any identifying information indicating data that conveys rights to one or more parties including: timestamp data, licensing information, copyright information, indication of intellectual property protection, etc. In an example where the learning classifier detects the presence of legal information does not exist in the executable file, this may trigger the learning classifier to adaptively check for additional features that might be indicative of a threat or malicious file as well as turn off other features related to an evaluation of the "legal information." The learning classifier component 104 utilizes programming operations or machine-learning processing to train/re-train the learning classifier to uniquely evaluate any file/file type. One of skill in the art will appreciate different types of processing operations may be employed without departing from the spirit of this disclosure. For example, the learning classifier component 104 may utilize an artificial neural network (ANN), a decision tree, association rules, inductive logic, a support vector machine, clustering analysis, and Bayesian networks, among other examples.

[0022] The learning classifier component 104 processes and encodes collected/extracted data from a file to make the static data points suitable for processing operations. The processing and encoding executed by the learning classifier component 104 may vary depending on the identified categories and/or type (e.g., numeric values, nominal values, string/byte sequences, Boolean values, etc.) of static data points collected by the knowledge component 102. As an example, string sequence data as well as byte sequence data may be parsed and processed as n-grams and/or n-gram word prediction (e.g., word-grams). For instance, for a given string all unigrams, bigrams and so forth up to a given length n are generated and the counts of the individual n-grams are determined. The resulting counts of the unique n-grams string and/or byte sequences are then used as input to a generated feature vector. In one example, strings are processed directly according to a bag of word model. A bag of word model is a simplifying representation used in natural language processing and information retrieval. In another example, numeric value static data points may be binned appropriately ensuring a good balance between information loss through data binning and available statistics. Nominal values as well Boolean values may be encoded using true/false flags. All of the different encoded data may be combined into one or more final feature vectors, for example after a complex vector coding/processing is performed (e.g., L2 norm).

[0023] As an application example of processing performed by the learning classifier component 104, suppose extraction of static data points from a file identifies the following four (4) data points:

File size: 4982784
PEHeader Anomaly: False
Section name: .TEXT
Legal copyright: Copyright (C) Webroot Inc. 1997

Processing these 4 data points into a feature vector may require binning the file size, labeling the PE Header Anomaly, build n-grams for the section name and building word-gram for legal copyright. Encapsulation of special characters that sometimes appear in text (e.g., section names) may be desirable. In an example, strings of data may be transformed first into hex code representation and then build n-grams or word-grams. In

this particular example, the section name is transformed into n-grams while the legal copyright text is transformed into word-grams. In evaluation using the classifier, the features related to the extracted data points may be weighted by the particular data point being evaluated or by category, for example. For instance, the training of the learning classifier may indicate that legal information (e.g., "legal copyright") provides a better indication that a file may be malicious than that of a section name. Features being evaluated (and their distributions) differ for benign files as compared to malicious files (e.g., harmful executables such as malware). For example, the data field "Legal Copyright" for benign files tends to have meaningful words, whereas in a malicious file, this data field is often left empty or it is filled with random characters. Commercial software files tend to have a valid certificate, whereas malware in general do not have valid certificates. Similarly, each data field for a static data point evaluated provides further indication about the maliciousness of the file. The combined information from all these data fields coupled with machine learning enables accurate prediction determination as to whether a file is malicious, benign or potentially unwanted. As an example, the resulting feature vector in sparse form is shown below:

secname_002e00740065:0.204124145232
secname_0065:0.0944911182523
secname_0074006500780074:0.353553390593
secname_006500780074:0.408248290464
secname_00740065:0.144337567297
secname_002e007400650078:0.353553390593
secname_00650078:0.144337567297
secname_002e0074:0.144337567297
secname_002e:0.0944911182523
secname_00780074:0.433012701892
secname_0078:0.0944911182523
secname_007400650078:0.204124145232
secname_0074:0.472455591262
legalcopyright_0043006f00700079007200690067006800740:0.4472135955
legalcopyright_002800430029:0.4472135955
legalcopyright_0043006f00720070002e:0.4472135955
legalcopyright_0031003900390035:0.4472135955
legalcopyright_004d006900630072006f0073006f00660074:0.4472135955
filesize_9965:1.0

PEHeaderAnomaly_False:1.0

[0024] In examples, the learning classifier component 104 provides the one or more feature vectors as input to a support vector machine (SVM). The SVM may then perform data analysis and pattern recognition on the one or more feature vectors. In one example the SVM, may be a linear SVM. Given a set of training examples provided by the knowledge component 102, an SVM may build a probabilistic model that indicates whether or not a file may be malicious. In another example, a hybrid approach may be elected that combines two or more individual linear SVM classifiers into a final classifier using ensemble methods. Specifically, the evaluated static data points may be subdivided into a set of families (e.g., sections, certificate, header data, and bytes sequences are used as different families). For each family, a linear SVM may be trained. The resulting classification scores generated by each linear SVM may then be combined into a final classification score using a decision tree. As an example, the decision tree may be trained using two-class logistic gradient boosting. In yet another example of feature classification evaluation, a classification may be subdivided into a three class classification problem defined by malicious files, potentially unwanted files/applications and benign files. The resulting three class problem is solved using multi-class classification (e.g., Directed Acyclic Graph (DAG) SVM) or, in case of the hybrid approach based on feature families, using a decision tree based on three-class logistic gradient boosting.

[0025] The threat detection component 106 is a component of system 100 that evaluates results of the processing performed by the learning classifier component 104 to make a determination as to whether the executable file is malicious, benign or a potentially unwanted file/application. As an example, a probabilistic value may be a final score determined from evaluating all static data points (or feature distributions) individually and determining an aggregate score that may be used for the evaluation of an executable file. In another example, correlation between static data points may be determined by the learning classification component 104 and a final score may be generated based on the correlation between static data points evaluated.

[0026] In one example, a classification as to whether a file is malicious or not may be based on comparison with a predetermined threshold value. For instance, a final score (e.g., probability value/evaluation) is determined based on feature vector processing performed by the learning classifier component 104 and compared with a probability threshold value for determining whether an executable file is malicious. As an example, a threshold value(s) may be set based on predetermined false positive range data where ranges may be set for one or more of the malicious executable files, the benign executable files and the potentially unwanted executable files. The threshold values for each of the different types may be the same or different. For instance, a threshold value may be set that indicates a confidence score in classifying an executable file as a malicious executable file. Ranges may be determined indicating how confident the system 100 is in predicting that a file is malicious. That may provide an indication of whether further evaluation of an executable file should occur. However, one skilled in the art will recognize that threshold determinations can be set in any way that be used to determine whether an executable file is malicious or not. Examples of further evaluation include but are not limited to: additional processing using a learning classifier, identification of an executable file as potentially malicious where services associated with the system 100 may follow-up, quarantining a file, and moving the file to a secure environment for execution (e.g., sandbox) among other examples. In other examples, retraining of the classifier may occur based on confidence scores. In examples, when a probability value exceeds or threshold value (or alternatively is less than a threshold value), it may be determined that an executable file may be identified as malicious. One skilled in the art will recognize that determination for predictive classification of executable files is not limited to threshold determinations. For example, any type of analytical, statistical or graphical analysis may be performed on data to classify an executable file/unknown executable file. As identified above, the threat detection component 106 may interface with the learning classifier component 104 to make a final determination as to how to classify an executable file as well as interface with the knowledge component 102 for training/retraining associated with the learning classifier.

[0027] Figure 2 illustrates an exemplary distributed system 200 showing interaction of components for implementation of exemplary threat detection system as described herein.

Where Figure 1 illustrates an example system 100 having components (hardware or software) operating on a client, Figure 2 illustrates an exemplary distributed system 200 comprising a client component 202 connected with at least one server component 204 via communication line 203. Communication line 203 represents the ability of the client component 202 to communicate with the server component 204, for example, to send or receive information over a network connection. That is, client component 202 and server component 204 are connectable over a network connection (e.g., a connection Internet via, for example, a wireless connection, a mobile connection, a hotspot, a broadband connection, a dial-up, a digital subscriber line, a satellite connection, an integrated services digital network, etc.).

[0028] The client component 202 may be any hardware (e.g., processing device) or software (e.g., application/service or remote connection running on a processing device) that accesses a service made available by the server component 204. The server component 204 may be any hardware or software (e.g., application or service running on a processing device) capable of communicating with the client component 202 for execution of threat detection processing (e.g., threat detection application/service). Threat detection processing may be used to evaluate a file before execution of the file as described in Figure 1. Threat detection application or services may be present on at least one of the client component 202 and the server component 204. In other examples, applications or components (e.g., hardware or software) may be present on both the client component 202 and the server component 204 to enable processing by threat detection application/services when a network connection to the server cannot be established. In one example of system 200, client component 202 (or server component 204) may comprise one or more components for threat detection as described in system 100 including a knowledge component 102, a learning classifier component 104 and/or a threat detection component 106, as described in the description of Figure 1. In other examples, the client component 202 may transmit data to/from the server component 204 to enable threat detections services over distributed network 200, for example as represented by communication line 203. In one example, threat detection applications/services operating on the client component 202 may receive updates from the server component 204. For instance, updates may be received by the client

component 202 for re-training of a learning classifier used to evaluate an executable file on the client component 202.

[0029] Figure 3 illustrates an exemplary method 300 for performing threat detection. As an example, method 300 may be executed by an exemplary system such as system 100 of Figure 1 and system 200 of Figure 2. In other examples, method 300 may be executed on a device comprising at least one processor configured to store and execute operations, programs or instructions. However, method 300 is not limited to such examples. Method 300 may be performed by any application or service that may include implementation of threat detection processing as described herein. The method 300 may be implemented using software, hardware or a combination of software and hardware.

[0030] Method 300 begins at operation 302 where a knowledge base is built for training/retraining of a learning classifier used to detect threats in executable files. Operation 302 builds the knowledge base from data collected and evaluated related to known malicious executable files, known benign executable files and potentially unwanted executable files as described in the description of Figure 1 (e.g., knowledge component 102). The knowledge base may be used to automatically train/re-train one or more learning classifiers used to evaluate threats in executable files based on the known malicious executable files, known benign executable files and the potentially unwanted executable files. In examples, the knowledge base may be maintained on at least one of a client component and a server component, and the knowledge base may be continuously updated with information from the resources described in Figure 1 including update information based on threat detection processing evaluation performed on unknown executable files.

[0031] When an executable file is identified for evaluation, flow proceeds to operation 304 where a one or more static data points are extracted from an executable file. In operation 304, an executable file is analyzed using machine learning processing as described with respect to the knowledge component 102 of Figure 1 to collect/extract static data points from an executable file for evaluation. In examples, operation 304 occurs without decrypting or unpacking the executable file. However, in other examples,

machine learning processing performed has the capability to evaluate static data points from extracted/unpacked content. In one example, machine learning processing is used to extract static data points from encrypted and/or compress versions of one or more files. In another example, machine learning processing is used to extract static data points from decrypted and/or unpacked versions of one or more files. In any example, extraction of static data points from different files (e.g. executable files) can be used to enhance training of a learning classifier, providing better results for extraction of static data points and classification of files.

[0032] In examples, operation 304 further comprises classifying extracted data according to a type of data extracted. For instance, the actions performed at operation 304 may be used to classify the plurality of static data points extracted into categories (categorical values) comprising numeric values, nominal values, string or byte sequences, and Boolean values, for example, as described with respect to Figure 1. In examples, data of an executable file (e.g., binary file data) may be parsed and compared against data maintained by a threat detection application/service as described in the present disclosure to determine static data points for extraction/collection.

[0033] In operation 306, the executable file is analyzed for threats. As an example, operation 306 analyzes an executable without decrypting or unpacking the executable file. However, in other examples, the machine learning processing being performed has the capability to evaluate static data points from extracted/unpacked content. Operation 306 comprises applying a learning classifier (e.g., the learning classifier generated during performance of operation 302) to the plurality of static data points extracted from the file. As discussed, the learning classifier may be built from data comprising known malicious executable files, known benign executable files and known unwanted executable files, for example. In one example, operation 306 comprises generating at least one feature vector from the plurality of static data points extracted using the learning classifier trained by the knowledge base. In order to generate the feature vector for the learning classifier, data may be parsed and encoded for machine learning processing.

Sophos Ex. 1003
Page 43 of 456

[0034] In one example, generation of the feature vector may comprise selectively setting features of the learning classifier based on the one or more of static data points extracted. Features of the generated feature vector may be weighted based on classified categories identified by the knowledge base (as described above) and the plurality of static data points extracted from the file. As an example, one or more features of the feature vector may be selectively turned on or off based on evaluation of whether a value of a static data point is within a predetermined range. However, one skilled in the art will recognize that the learning classifier can uniquely generate a feature vector for analysis of the executable file based on any data used to train/ re-train the learning classifier. In examples, operation 306 further comprises evaluating the feature vector using linear or nonlinear support vector processing to determine a classification for the executable file, for example whether the executable file is harmful, benign, or unwanted.

[0035] Flow proceeds to operation 308, where a determination is made as to a classification of the executable file. For example, operation 308 makes a final determination as to whether the executable file is harmful (e.g., malicious, malware) or not based on results of the analysis of the executable file (e.g., using machine learning processing by a learning classifier). In one example, results of the analysis of an executable file may be data obtained from learning classifier, such as, for example an SVM, processing data. In one example, operation 308 further comprises preventing execution of the executable file when a probability value that the executable file is harmful exceeds a threshold value. The probability value for the executable file may be determined based on applying the learning classifier to the executable file. As an example, the threshold value may be set based on predetermined false positive range data for identifying a malicious or harmful executable file. False positive range data may be determined from the analysis/evaluation of the known malicious executable files, known benign files and potentially unwanted executable files/applications, of the knowledge base. However, as acknowledged above, determining a classification of an executable file may be based on any type of analytical, statistical or graphical analysis, or machine learning processing. In one example, ranges can be based on evaluation of data during operation of the threat detection service as well as analysis related to unknown files, for example analytics performed to evaluate unknown files.

[0036] At any point in time, operation 310 may occur where a learning classifier used for threat detection processing is re-trained. Continuously re-training of the learning classifier may ensure that the threat detection application/service is up to date and able to accurately detect new threats. As identified above, re-training may occur through results of threat detection processing including updated information added to the knowledge base. In one example, training of a learning classifier can be based on evaluation of data during operation of the threat detection service as well as analysis related to unknown files, for example analytics performed to evaluate unknown files.

[0037] Figure 4 and the additional discussion in the present specification are intended to provide a brief general description of a suitable computing environment in which the present invention and/or portions thereof may be implemented. Although not required, the embodiments described herein may be implemented as computer-executable instructions, such as by program modules, being executed by a computer, such as a client workstation or a server. Generally, program modules include routines, programs, objects, components, data structures and the like that perform particular tasks or implement particular abstract data types. Moreover, it should be appreciated that the invention and/or portions thereof may be practiced with other computer system configurations, including hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers and the like. The invention may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

[0038] Figure 4 illustrates one example of a suitable operating environment 400 in which one or more of the present embodiments may be implemented. This is only one example of a suitable operating environment and is not intended to suggest any limitation as to the scope of use or functionality. Other well-known computing systems, environments, and/or configurations that may be suitable for use include, but are not limited to, personal computers, server computers, hand-held or laptop devices, multiprocessor systems, microprocessor-based systems, programmable consumer electronics such as smart

phones, network PCs, minicomputers, mainframe computers, distributed computing environments that include any of the above systems or devices, and the like.

[0039] In its most basic configuration, operating environment 400 typically includes at least one processing unit 402 and memory 404. Depending on the exact configuration and type of computing device, memory 404 (storing, among other things, executable evaluation module(s), e.g., malware detection applications, APIs, programs etc. and/or other components or instructions to implement or perform the system and methods disclosed herein, etc.) may be volatile (such as RAM), non-volatile (such as ROM, flash memory, etc.), or some combination of the two. This most basic configuration is illustrated in FIG. 4 by dashed line 406. Further, environment 400 may also include storage devices (removable, 408, and/or non-removable, 410) including, but not limited to, magnetic or optical disks or tape. Similarly, environment 400 may also have input device(s) 414 such as keyboard, mouse, pen, voice input, etc. and/or output device(s) 416 such as a display, speakers, printer, etc. Also included in the environment may be one or more communication connections, 412, such as LAN, WAN, point to point, etc.

[0040] Operating environment 400 typically includes at least some form of computer readable media. Computer readable media can be any available media that can be accessed by processing unit 402 or other devices comprising the operating environment. By way of example, and not limitation, computer readable media may comprise computer storage media and communication media. Computer storage media includes volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information such as computer readable instructions, data structures, program modules or other data. Computer storage media includes, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other non-transitory medium which can be used to store the desired information. Computer storage media does not include communication media.

[0041] Communication media embodies computer readable instructions, data structures, program modules, or other data in a modulated data signal such as a carrier wave or other transport mechanism and includes any information delivery media. The term "modulated data signal" means a signal that has one or more of its characteristics set or changed in such a manner as to encode information in the signal. By way of example, and not limitation, communication media includes wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, RF, infrared and other wireless media. Combinations of the any of the above should also be included within the scope of computer readable media.

[0042] The operating environment 400 may be a single computer operating in a networked environment using logical connections to one or more remote computers. The remote computer may be a personal computer, a server, a router, a network PC, a peer device or other common network node, and typically includes many or all of the elements described above as well as others not so mentioned. The logical connections may include any method supported by available communications media. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets and the Internet.

[0043] The different aspects described herein may be employed using software, hardware, or a combination of software and hardware to implement and perform the systems and methods disclosed herein. Although specific devices have been recited throughout the disclosure as performing specific functions, one of skill in the art will appreciate that these devices are provided for illustrative purposes, and other devices may be employed to perform the functionality disclosed herein without departing from the scope of the disclosure.

[0044] As stated above, a number of program modules and data files may be stored in the system memory 404. While executing on the processing unit 402, program modules 408 (e.g., applications, Input/Output (I/O) management, and other utilities) may perform processes including, but not limited to, one or more of the stages of the operational methods described herein such as method 300 illustrated in Figure 3, for example.

[0045] Furthermore, examples of the invention may be practiced in an electrical circuit comprising discrete electronic elements, packaged or integrated electronic chips containing logic gates, a circuit utilizing a microprocessor, or on a single chip containing electronic elements or microprocessors. For example, examples of the invention may be practiced via a system-on-a-chip (SOC) where each or many of the components illustrated in FIG. 4 may be integrated onto a single integrated circuit. Such an SOC device may include one or more processing units, graphics units, communications units, system virtualization units and various application functionality all of which are integrated (or "burned") onto the chip substrate as a single integrated circuit. When operating via an SOC, the functionality described herein may be operated via application-specific logic integrated with other components of the operating environment 400 on the single integrated circuit (chip). Examples of the present disclosure may also be practiced using other technologies capable of performing logical operations such as, for example, AND, OR, and NOT, including but not limited to mechanical, optical, fluidic, and quantum technologies. In addition, examples of the invention may be practiced within a general purpose computer or in any other circuits or systems.

[0046] This disclosure described some aspects of the present technology with reference to the accompanying drawings, in which only some of the possible embodiments were shown. Other aspects may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. Rather, these aspects were provided so that this disclosure was thorough and complete and fully conveyed the scope of the possible embodiments to those skilled in the art.

[0047] Although specific aspects were described herein, the scope of the technology is not limited to those specific embodiments. One skilled in the art will recognize other embodiments or improvements that are within the scope and spirit of the present technology. Therefore, the specific structure, acts, or media are disclosed only as illustrative embodiments. The scope of the technology is defined by the following claims and any equivalents therein.

CLAIMS

What is claimed is:

1. A computer-implemented method comprising:

extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file;

analyzing the executable file without decrypting or unpacking the executable file, wherein analyzing the executable file comprises applying a classifier to the plurality of static data points, wherein the classifier is trained from data that comprises known malicious executable files, known benign executable files and known unwanted executable files; and

determining whether the executable file is harmful based on the analysis.

2. The computer-implemented method according to claim 1, wherein the extracting the plurality of static data points further comprises classifying the extracted static data points according to a type of data extracted from the executable file, and encoding the extracted static data points for the classifier based on the classification.

3. The computer-implemented method according to claim 2, wherein analyzing the executable file further comprises generating a feature vector from the plurality of extracted static data points and evaluating the feature vector using support vector processing to determine whether the executable file is at least one of harmful, benign, and potentially unwanted.

4. The computer-implemented method according to claim 3, wherein generating the at least one feature vector comprises selectively setting features of the classifier based on the plurality of extracted static data points.

5. The computer-implemented method according to claim 4, wherein features of the feature vector are selectively turned on or off based on evaluation of whether a value of a static data point from the plurality of extracted static data points is within a predetermined range.

6. The computer-implemented method according to claim 2, wherein the classifying the at least one static data point comprises classifying the plurality of extracted static data points into categories comprising numeric values, nominal values, string or byte sequences, and Boolean values.

7. The computer-implemented method according to claim 6, wherein analyzing the executable file further comprises generating at least one feature vector from the plurality of extracted static data points, wherein features of the generated feature vector are weighted based at least upon the classified categories and the plurality of extracted static data points.

8. The computer-implemented method according to claim 1, wherein determining whether the executable file is harmful further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value.

9. The computer-implemented method according to claim 8, wherein the threshold value is set based on predetermined false positive range data.

10. A computer-readable storage device containing instructions, that when executed on at least one processor, causing the processor to execute a process comprising:

extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file;

analyzing the executable file without decrypting or unpacking the executable file, wherein the analyzing the executable file comprises applying a classifier to the plurality of static data points extracted, wherein the classifier is trained from data comprising known malicious executable files, known benign executable files and known unwanted executable files; and

determining whether the executable file is harmful based on the analyzing of the executable file.

11. The computer-readable storage device according to claim 10, wherein the extracting of the plurality of static data points executed by the processor further comprises classifying the extracted static data points according to a type of data extracted from the executable file, and encoding the extracted static data points for the classifier based on the classifying.

12. The computer-readable storage device according to claim 11, wherein analyzing the executable file further comprises generating at least one feature vector from the plurality of extracted static data points and evaluating the feature vector using linear or nonlinear support vector processing to determine whether the executable file is at least one of harmful, benign, and potentially unwanted.

13. The computer-readable storage device according to claim 12, wherein generating the at least one feature vector comprises selectively setting features of the classifier based on the plurality of extracted static data points.

14. The computer-readable storage device according to claim 13, wherein features of the feature vector are selectively turned on or off based on evaluation of whether a value of a static data point from the plurality of extracted static data points is within a predetermined range.

15. The computer-readable storage device according to claim 11, wherein the classifying the at least one static data point comprises classifying the plurality of extracted static data points into categories comprising numeric values, nominal values, string or byte sequences, and Boolean values.

16. The computer-readable storage device according to claim 15, wherein analyzing the executable file further comprises generating a feature vector from the plurality of extracted static data points, wherein features of the generated feature vector are weighted based at least upon the classified categories and the plurality of extracted static data points.

17. The computer-readable storage device according to claim 10, wherein determining whether the executable file is harmful further comprises preventing execution of the

executable file when a determined probability value that the executable file is harmful exceeds a threshold value.

18. The computer-readable storage device according to claim 17, wherein the threshold value is set based on predetermined false positive range data.

19. A system comprising:

at least one memory; and

at least one processor operatively connected with the memory and configured to perform operation of:

extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file,

analyzing the executable file without decrypting or unpacking the executable file, wherein the analyzing the executable file comprises applying a classifier to the plurality of static data points extracted, wherein the classifier is trained from data comprising known malicious executable files, known benign executable files and known unwanted executable files, and

determining whether the executable file is harmful based on the analyzing of the executable file.

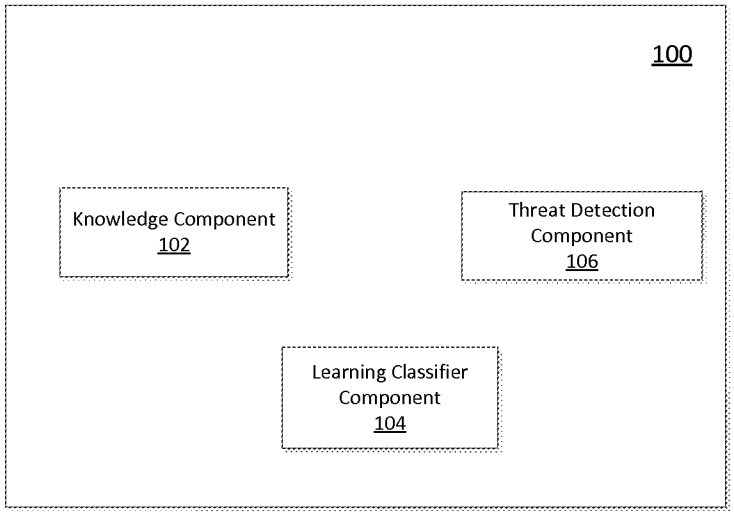
20. The system according to claim 19, wherein the determining further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value, and wherein the threshold value is set based on predetermined false positive range data.

Abstract

Aspects of the present disclosure relate to threat detection of executable files. A plurality of static data points may be extracted from an executable file without decrypting or unpacking the executable file. The executable file may then be analyzed without decrypting or unpacking the executable file. Analysis of the executable file may comprise applying a classifier to the plurality of extracted static data points. The classifier may be trained from data comprising known malicious executable files, known benign executable files and known unwanted executable files. Based upon analysis of the executable file, a determination can be made as to whether the executable file is harmful.

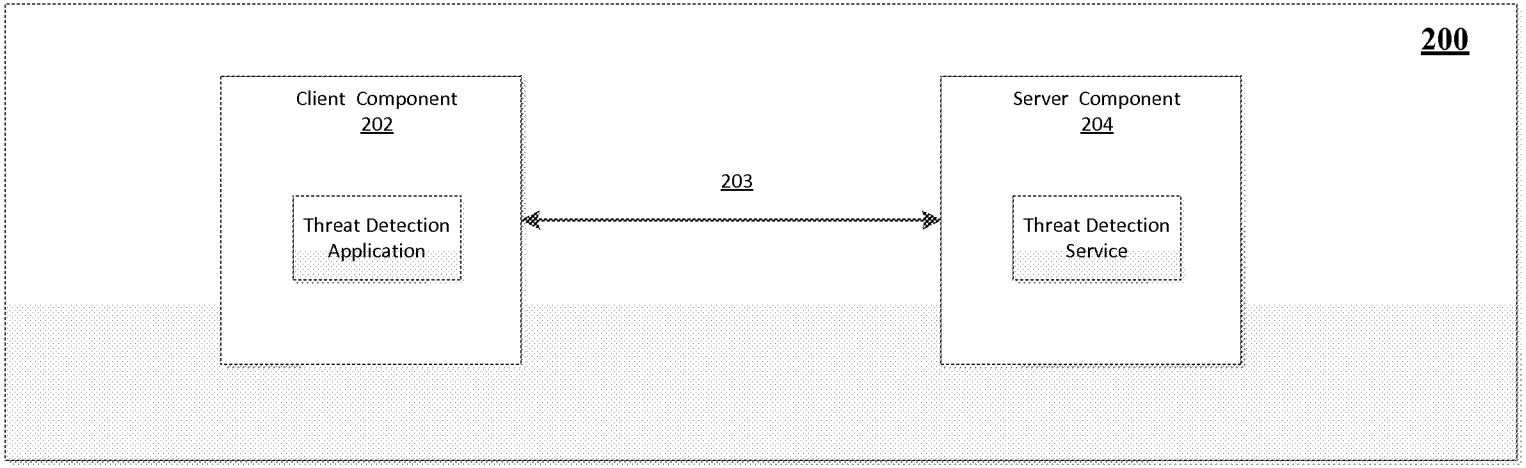
Sophos Ex. 1003
Page 53 of 456

FIG. 1



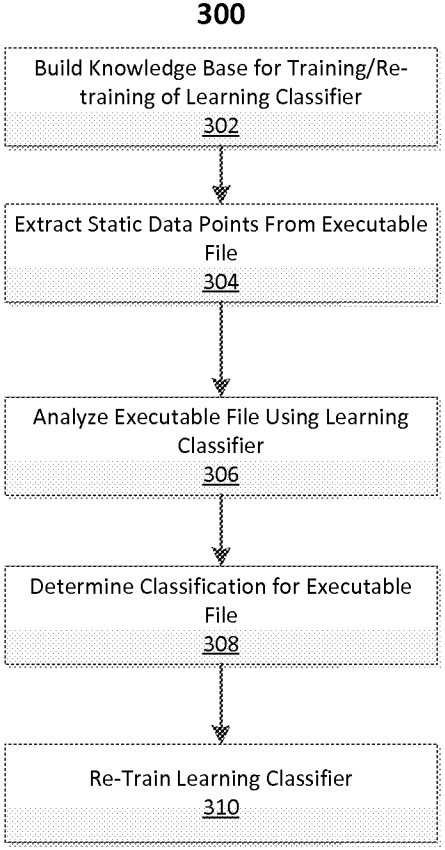
Sophos Ex. 1003
Page 54 of 456

FIG. 2



Sophos Ex. 1003
Page 55 of 456

FIG. 3



Sophos Ex. 1003
Page 56 of 456

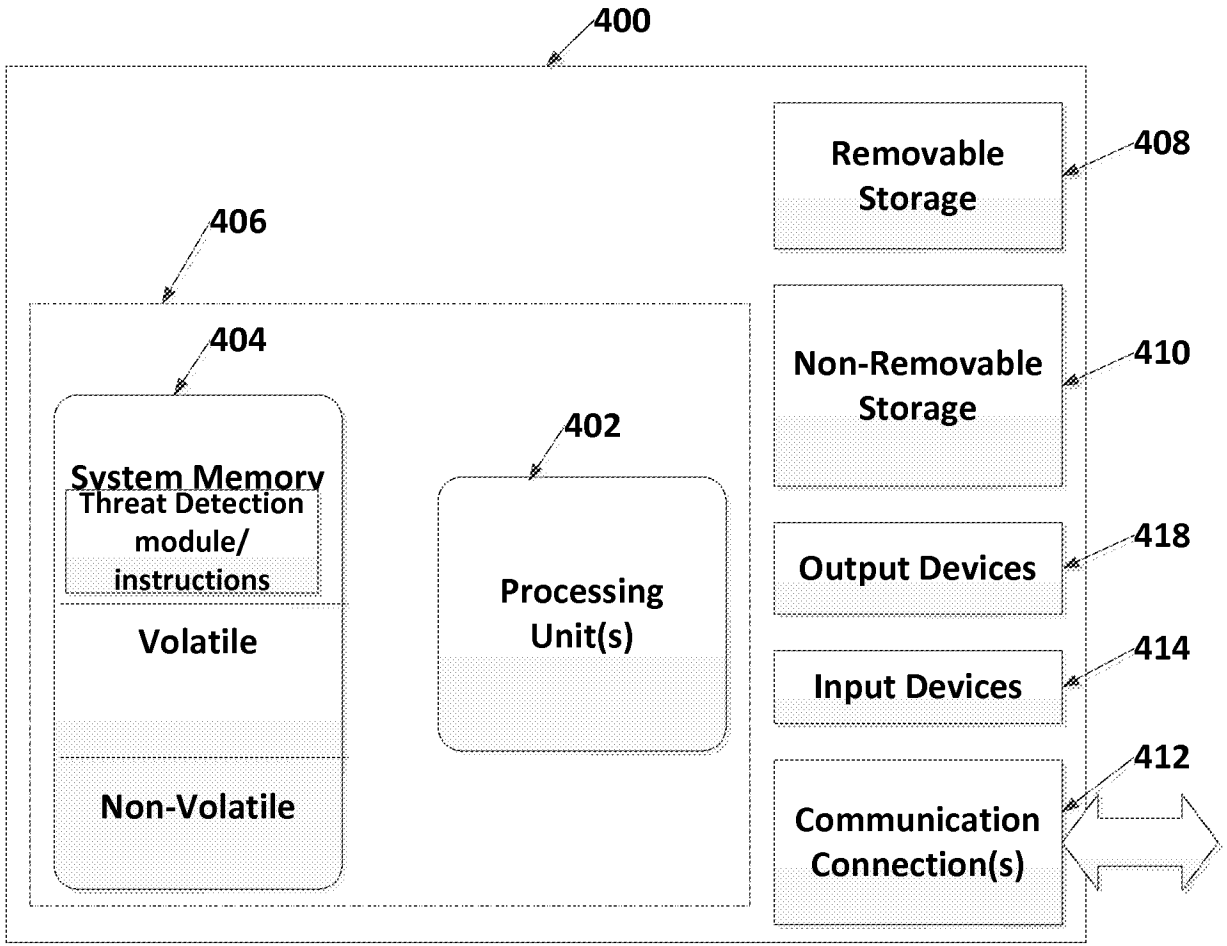


FIG. 4

Sophos Ex. 1003
Page 57 of 456

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Schmidtler, et al.	Examiner:	Not Assigned
Serial No.:	Filed herewith	Group Art Unit:	Not Assigned
Filed:	Filed herewith	Docket No.:	04584.0168US01
Title:	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS		

Filed via EFS-Web

INFORMATION DISCLOSURE STATEMENT (37 C.F.R. § 1.97(b))

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

Attention: Commissioner for Patents

With regard to the above-identified application, the items of information listed on the enclosed Form PTO/SB/08a are brought to the attention of the Examiner.

This statement should be considered because it is submitted within three months of the filing date of the above-identified application, which is not an application under 37 C.F.R. § 1.53(d). Accordingly, no fee is due for consideration of the items listed on the enclosed Form PTO/SB/08a.

In accordance with 37 C.F.R. § 1.98(a)(2), a copy of each foreign patent and/or a copy of each publication, other than U.S. patents and U.S. patent application publications, listed on the accompanying Form PTO/SB/08a is enclosed.

No representation is made that a reference is "prior art" within the meaning of 35 U.S.C. §§ 102 and 103 and Applicants reserve the right, pursuant to 37 C.F.R. § 1.131 or otherwise, to establish that the reference(s) are not "prior art." Moreover, Applicants do not represent that a reference has been thoroughly reviewed or that any relevance of any portion of a reference is intended.

Consideration of the items listed is respectfully requested. Pursuant to the provisions of M.P.E.P. 609, it is requested that the Examiner return a copy of the attached Form PTO/SB/08a,

marked as being considered and initialed by the Examiner, to the undersigned with the next official communication.

Please charge any additional fees or credit any overpayment to Deposit Account No. 13-2725.

Respectfully submitted,

Date: May 12, 2015

/Jason E. Becker/

Jason E. Becker, Reg. No. 66,632
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1637

23552
PATENT TRADEMARK OFFICE

SCORE Placeholder Sheet for IFW Content

Application Number: 14709875 Document Date: 05/12/2015

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

- Drawings – Other than Black and White Line Drawings

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

To access the documents in the SCORE database, refer to instructions below.

At the time of document entry (noted above):

- Examiners may access SCORE content via the eDAN interface.
- Other USPTO employees can bookmark the current SCORE URL (http://Score.uspto.gov/ScoreAccessWeb/).
- External customers may access SCORE content via the Public and Private PAIR interfaces.

Form Revision Date: September 30, 2013

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 14/709,875

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	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	*	x 40 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 210 =	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	730		TOTAL	

APPLICATION AS AMENDED - PART II

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

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/709,875	05/12/2015	2431	730	04584.0168US01	20	3

CONFIRMATION NO. 1593

FILING RECEIPT

23552
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

OC000000075407547

Date Mailed: 05/29/2015

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**

Inventor(s)

Mauritius Schmidtler, Escondido, CA;
Gaurav Dalal, San Jose, CA;
Reza Yoosoofmiya, San Diego, CA;

Applicant(s)

Webroot Inc., Broomfield, CO;

Power of Attorney: The patent practitioners associated with Customer Number 23552

Domestic Applications for which benefit is claimed - None.
A proper domestic benefit claim must be provided in an Application Data Sheet in order to constitute a claim for domestic benefit. See 37 CFR 1.76 and 1.78.

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access - A proper **Authorization to Permit Access to Application by Participating Offices** (PTO/SB/39 or its equivalent) has been received by the USPTO.

If Required, Foreign Filing License Granted: 05/27/2015
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/709,875**
Projected Publication Date: 11/17/2016
Non-Publication Request: No

Early Publication Request: No
** **SMALL ENTITY** **
Title

AUTOMATIC THREAT DETECTON OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS

Preliminary Class

726

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

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 (1-866-999-4258).

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 U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY.DOCKET NO./TITLE	REQUEST ID
14/709,875	05/12/2015	Webroot Inc.	04584.0168US01	18147

Acknowledgement of Loss of Entitlement to Entity Status Discount

The entity status change request below filed through Private PAIR on 05/18/2016 has been accepted.

CERTIFICATIONS:

Change of Entity Status:

X Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be notification of loss of entitlement to small or micro entity status, as applicable.

This portion must be completed by the signatory or signatories making the entity status change in accordance with 37 CFR 1.4(d)(4).

Signature:	/Andrew T. Pouzeshi/
Name:	Andrew T. Pouzeshi
Registration Number:	67672

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Mauritius Schmidtler et al.	Examiner:	Lavelle, Gary E.
Serial No.:	14/709,875	Group Art Unit:	2493
Filed:	May 12, 2015	Docket No.:	04584.0168US01
Title:	**AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS (as amended)**		

PRELIMINARY AMENDMENT

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

Dear Commissioner:

Please find this Preliminary Amendment and amend the above-identified application as follows:

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

Remarks begin on page 3 of this paper.

Amendments to the Specification:

Please amend the Title of the Specification, at page 1, as follows:

AUTOMATIC THREAT ~~DETECTON~~ DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS

REMARKS

This Preliminary Amendment is filed in reference to the above-identified application filed on May 12, 2015. Specifically, the Title of the Specification has been amended to correct a typographical error. As such, the amendment to the Specification does not add new matter. Thus, Applicants respectfully request that the Examiner enter the amendments at the Examiner's earliest convenience.

CONCLUSION

This Preliminary Amendment is submitted with reference to U.S. Application Serial No. 14/709,875 filed on May 12, 2015. It is believed that no further fees are due with this Amendment. However, the Commissioner is hereby authorized to charge any deficiencies or credit any overpayment with respect to this patent application to deposit account number 13-2725.

If the Examiner believes a telephone conference would advance the prosecution of this application, the Examiner is invited to telephone the undersigned at the below-listed telephone number.

Respectfully submitted,

Date: June 14, 2016

/Jason E. Becker/

Jason E. Becker, Reg. No. 66,632
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1221

23552
PATENT TRADEMARK OFFICE

Electronic Acknowledgement Receipt

EFS ID:	26061882
Application Number:	14709875
International Application Number:	
Confirmation Number:	1593
Title of Invention:	AUTOMATIC THREAT DETECTON OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS
First Named Inventor/Applicant Name:	Mauritius Schmidtler
Customer Number:	23552
Filer:	Jason Evan Becker/Julie Borrego
Filer Authorized By:	Jason Evan Becker
Attorney Docket Number:	04584.0168US01
Receipt Date:	14-JUN-2016
Filing Date:	12-MAY-2015
Time Stamp:	15:52:19
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		2016_06_14_PRELIM_AMD_04584_0168US01.pdf	77229 2011f22d28f12baa38f29e73a3103409e2f7f3a9	yes	3

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Preliminary Amendment	1	1
	Specification	2	2
	Applicant Arguments/Remarks Made in an Amendment	3	3
Warnings:			
Information:			
	Total Files Size (in bytes):	77229	

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

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

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

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

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/709,875	Filing Date 05/12/2015	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

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

APPLICATION AS AMENDED – PART II

AMENDMENT **06/14/2016**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	X $80 =	0
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $420 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

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

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

LIE
/TRINA STEPTOE/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14709875
Filing Date	2015-05-12
First Named Inventor	Mauritius Schmidtler
Art Unit	2493
Examiner Name	LAVELLE, GARY E.
Attorney Docket Number	04584.0168US01

U.S.PATENTS

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

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

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20100192222		2010-07-29	Stokes et al.	

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

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

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

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14709875
	Filing Date	2015-05-12
	First Named Inventor	Mauritius Schmidtler
	Art Unit	2493
	Examiner Name	LAVELLE, GARY E.
	Attorney Docket Number	04584.0168US01

	1	International Patent Application No. PCT/US2016/032090, International Search Report and Written Opinion mailed July 29, 2016, 13 pages.	☐
	2	Perdisci et al. (2008) Pattern Recognition Letters 29:1941-1946 "Classification of packed executables for accurate computer virus detection"	☐
	3	Perdisci et al. (2008) IEEE: Annual Computer Security Applications Conference 301-310 "McBoost: Boosting Scalability in Malware Collection and Analysis Using Statistical Classification of Executables"	☐

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14709875
	Filing Date	2015-05-12
	First Named Inventor	Mauritius Schmidtler
	Art Unit	2493
	Examiner Name	LAVELLE, GARY E.
	Attorney Docket Number	04584.0168US01

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/David D. Harrell/	Date (YYYY-MM-DD)	2016-10-17
Name/Print	David D. Harrell	Registration Number	71855

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

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
Bruesss, Steven C.
MERCHANT & GOULD P.C.
P.O. Box 2903
Minneapolis, Minnesota 55402-0903
ETATS-UNIS D'AMERIQUE

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

	Date of mailing *(day/month/year)* 29 July 2016 (29-07-2016)
Applicant's or agent's file reference 4584-168WO01	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US2016/032090	International filing date *(day/month/year)* 12 May 2016 (12-05-2016)
Applicant WEBROOT INC.	

1. [X] The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the International Search Report.

   How? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Fasoimile No.: (41-22) 338.82.70

   For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 - 9.011.

2. [ ] The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. [ ] **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   [ ] the protest together with the decision thereon has been transmitted to the International Bureau together with any applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

   [ ] no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   The applicant may **submit comments on an informal basis on the written opinion of the International Searching Authority** to the International Bureau. These comments will be made available to the public after international publication. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established.

   Shortly after the expiration of **18 months from the priority date, the international application will be published** by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before the completion of the technical preparations for international publication (Rules 90*bis*.1 and 90*bis*.3).

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for **entry into the national phase** before those designated Offices. In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months. For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the *PCT Applicant's Guide*, National Chapters.

   Within **19 months from the priority date, the applicant may request that a supplementary international search be carried out** by a different International Searching Authority that offers this service (Rule 45*bis*.1). The procedure for requesting supplementary international search is described in the *PCT Applicant's Guide*, International Phase, paragraphs 8.006-8.032.

Name and mailing address of the International Searching Authority	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040 Fax: (+31-70) 340-3016	FILIP, Hannelore Tel: +49 (0)89 2399-2861

Form PCT/ISA/220 (July 2014)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
4584-168WO01		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2016/032090	12 May 2016 (12-05-2016)	12 May 2015 (12-05-2015)
Applicant		
WEBROOT INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 4 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language,** the international search was carried out on the basis of:
      [X] the international application in the language in which it was filed
      [ ] a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. [ ] This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. [ ] **Certain claims were found unsearchable** (See Box No. II)

3. [ ] **Unity of invention is lacking** (see Box No III)

4. With regard to the **title,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings,**
   a. the figure of the **drawings** to be published with the abstract is Figure No. 3
      [X] as suggested by the applicant
      [ ] as selected by this Authority, because the applicant failed to suggest a figure
      [ ] as selected by this Authority, because this figure better characterizes the invention
   b. [ ] none of the figures is to be published with the abstract

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/032090

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/56 G06F11/36 G06F9/44
ADD. G06F21/64 G06F21/62

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	PERDISCI R ET AL: "Classification of packed executables for accurate computer virus detection", PATTERN RECOGNITION LETTERS, ELSEVIER, AMSTERDAM, NL, vol. 29, no. 14, 15 October 2008 (2008-10-15), pages 1941-1946, XP024520140, ISSN: 0167-8655, DOI: 10.1016/J.PATREC.2008.06.016 [retrieved on 2008-07-03] page 1942, left-hand column, lines 10-14, 41-42, 51-53; figure 1 page 1943, left-hand column, lines 9-14 section 4 "Experiments"; page 1944, right-hand column, lines 6-9, 24, 25, 28 page 1945; table 1 ----- -/--	1-20

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 July 2016	29/07/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Madzharova, Violeta

2

Form PCT/ISA/210 (second sheet) (April 2005)

Sophos Ex. 1003
Page 77 of 456

International application No
PCT/US2016/032090

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	ROBERTO PERDISCI ET AL: "McBoost: Boosting Scalability in Malware Collection and Analysis Using Statistical Classification of Executables", COMPUTER SECURITY APPLICATIONS CONFERENCE, 2008. ACSAC 2008. ANNUAL, IEEE, PISCATAWAY, NJ, USA, 8 December 2008 (2008-12-08), pages 301-310, XP031376785, ISBN: 978-0-7695-3447-3 page 304, left-hand column	1-20
A	US 2010/192222 A1 (STOKES JACK W [US] ET AL) 29 July 2010 (2010-07-29) sentences 3-6, paragraph [0019] sentences 9-11, paragraph [0032]	1-20

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

Sophos Ex. 1003
Page 78 of 456

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2016/032090

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010192222 A1	29-07-2010	NONE	

Information on Search Strategy - Pilot phase (see OJ 2015, A86)
The type of information contained in this sheet may change during the pilot for improving the usefulness of this new service.

Application Number
PCT/US2016/032090

TITLE: AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS

APPLICANT: WEBROOT INC.

IPC CLASSIFICATION: G06F21/56, G06F11/36, G06F9/44, G06F21/64, G06F21/62

EXAMINER: Madzharova, Violeta

CONSULTED DATABASES: NPL

CLASSIFICATION SYMBOLS DEFINING EXTENT OF THE SEARCH:

IPC:

CPC: G06F21/562, G06F11/3604, G06F8/74

FI/F-TERMS:

KEYWORDS OR OTHER ELEMENTS FEATURING THE INVENTION:
Keywords: Portable Executable (PE), static analysis, section entropy, False Positive (FP) rate, packed executable, malware detection.

EPO FORM P04A42

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2016/032090	12.05.2016	12.05.2015

International Patent Classification (IPC) or both national classification and IPC
INV. G06F21/56 G06F11/36 G06F9/44 ADD. G06F21/64 G06F21/62

Applicant
WEBROOT INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☒ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Fax: +49 89 2399 - 4465	see form PCT/ISA/210	Madzharova, Violeta Telephone No. +49 89 2399-0

Form PCT/ISA/237 (Cover Sheet) (January 2015)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing:

   a. ☐ forming part of the international application as filed:

      ☐ in the form of an Annex C/ST.25 text file.

      ☐ on paper or in the form of an image file.

   b. ☐ furnished together with the international application under PCT Rule 13*ter*.1(a) for the purposes of international search only in the form of an Annex C/ST.25 text file.

   c. ☐ furnished subsequent to the international filing date for the purposes of international search only:

      ☐ in the form of an Annex C/ST.25 text file (Rule 13*ter*.1(a)).

      ☐ on paper or in the form of an image file (Rule 13*ter*.1(b) and Administrative Instructions, Section 713).

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that forming part of the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	4, 5, 7-9, 13, 14
	No:	Claims	1-3, 6, 10-12, 15-20
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-20
Industrial applicability (IA)	Yes:	Claims	1-20
	No:	Claims	

2. Citations and explanations

see separate sheet

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 Reference is made to the following documents:

D1 PERDISCI R ET AL: "Classification of packed executables for accurate computer virus detection", PATTERN RECOGNITION LETTERS, ELSEVIER, AMSTERDAM, NL, vol. 29, no. 14, 15 October 2008 (2008-10-15), pages 1941-1946, XP024520140, ISSN: 0167-8655, DOI: 10.1016/J.PATREC.2008.06.016 [retrieved on 2008-07-03]

D2 ROBERTO PERDISCI ET AL: "McBoost: Boosting Scalability in Malware Collection and Analysis Using Statistical Classification of Executables", COMPUTER SECURITY APPLICATIONS CONFERENCE, 2008. ACSAC 2008. ANNUAL, IEEE, PISCATAWAY, NJ, USA, 8 December 2008 (2008-12-08), pages 301-310, XP031376785, ISBN: 978-0-7695-3447-3

D3 US 2010/192222 A1 (STOKES JACK W [US] ET AL) 29 July 2010 (2010-07-29)

2 The present application does not meet the criteria of Article 33(2) PCT, because the subject-matter of **claim 1** is not new.

D1 discloses (references in parentheses referring to **D1**):

A computer-implemented method comprising:

extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file;	p. 1942, Fig. 1, Static PE Analysis of Executable, where determination is made whether the executable is packed or not packed; p. 1942, left col., l. 10-14: "*The objective is to accurately distinguish between*

	packed and non-packed executables, so that only the executables detected as packed will be sent to a ... universal unpacker for hidden code extraction, before being sent to the anti-virus software."; p. 1943, left col., l. 9-11: "*... approach ... do not need to to execute an application to detect if it contains packed executable code.*"; p. 1945, Table 1, "*Summary of features extracted from PE files*", including number of standard vs. non-standard sections, entropy of header, code and data sections. It is well known to the skilled person in the field of malware analysis that PE file entropy is commonly used to asses whether a file is encrypted or not (see also p. 1944, right col., l. 6-9: "*... measure the byte entropy of the code and data sections in the PE file. If the entropy of a sections is close to 8 bits, which is the maximum byte entropy, the section likely contains encrypted code.*";
analyzing the executable file without decrypting or unpacking the executable file, wherein analyzing the executable file comprises applying a classifier to the plurality of static data points,	p. 1942, Fig. 1, PE file Classifier; p. 1943, left col., l. 11-14: "*... classification system extracts a number of features from executable files in PE format through static analysis ... used to classify packed executables without need to actually execute them.*"; p. 1945, Table 1, "*Summary of features extracted from PE files*";

wherein the classifier is trained from data that comprises known malicious executable files, known benign executable files and known unwanted executable files; and	p. 1944, right col., section 4. "Experiments", wherein the training dataset comprises "*packed viruses*" (l. 24), "*non-packed benign executables*" (l. 25), and "*packed benign executables*" (l. 28);
determining whether the executable file is harmful based on the analysis.	p. 1942, Fig. 1, determination of packed vs. unpacked executable and subsequent determination whether it is a "*virus*" or "*benign*".

3 Referring to the objection raised above, independent **claims 10 and 19** are also not allowable for lack of novelty (Article 33(2) PCT) since their subject-matter corresponds to that of **claim 1**.

4 Furthermore, the **dependent claims 2-9, 11-18 and 20** do not appear to contain any additional technical features which, either alone or in combination with the features of any claim to which they refer, render the present subject-matter novel (Article 33(2) PCT) or inventive (Article 33(3) PCT) since their features are either known from the prior art or merely represent minor implementation details to the person skilled in the art (see cited passages in the ISR, and in particular, for **claims 2 and 11** (classifying according to a type of extracted data), document **D1** (p. 1945, Table 1); for **claims 3 and 12** (generating a feature vector and using support vector processing), documents **D1** (p. 1942, left col., l. 41-42 and 51-53) and **D2** (p. 304, left col.); for **claims 7 and 16** (features of the feature vector being weighted), document **D3** (par. [0019], l. 3-6); for **claims 8 and 17** (preventing execution of the executable file when probability that file might be harmful exceeds a predetermined threshold value), document **D3** (par. [0032], l. 9-11).

Re Item VIII

Certain observations on the international application

5 It should be noted by the applicant that in certain jurisdictions, the expression "*without*" used in the wording of claim 1 might be regarded as being unclear, since it appears to comprise a negative limitation.

Bitte beachten Sie, dass angeführte Nichtpatentliteratur (wie z. B. wissenschaftliche oder technische Dokumente) je nach geltendem Recht dem Urheberrechtsschutz und/oder anderen Schutzarten für schriftliche Werke unterliegen könnte. Die Vervielfältigung urheberrechtlich geschützter Texte, ihre Verwendung in anderen elektronischen oder gedruckten Publikationen und ihre Weitergabe an Dritte ist ohne ausdrückliche Zustimmung des Rechtsinhabers nicht gestattet.

Veuillez noter que les ouvrages de la littérature non-brevets qui sont cités, par exemple les documents scientifiques ou techniques, etc., peuvent être protégés par des droits d'auteur et/ou toute autre protection des écrits prévue par les législations applicables. Les textes ainsi protégés ne peuvent être reproduits ni utilisés dans d'autres publications électroniques ou imprimées, ni rediffusés sans l'autorisation expresse du titulaire du droit d'auteur.

Please be aware that cited works of non-patent literature such as scientific or technical documents or the like may be subject to copyright protection and/or any other protection of written works as appropriate based on applicable laws. Copyrighted texts may not be copied or used in other electronic or printed publications or re-distributed without the express permission of the copyright holder.

XS CPRTENFRDE

Electronic Acknowledgement Receipt

EFS ID:	27229208
Application Number:	14709875
International Application Number:	
Confirmation Number:	1593
Title of Invention:	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS
First Named Inventor/Applicant Name:	Mauritius Schmidtler
Customer Number:	23552
Filer:	David Dwayne Harrell/Elizabeth Pallardy
Filer Authorized By:	David Dwayne Harrell
Attorney Docket Number:	04584.0168US01
Receipt Date:	17-OCT-2016
Filing Date:	12-MAY-2015
Time Stamp:	11:33:34
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	Information Disclosure Statement (IDS) Form (SB08)	04584_0168US01_IDS.pdf	484288 da347c4a2005dd8302f87d8d8ccf45c5571ca96d	no	3

Warnings:

Information:					
This is not an USPTO supplied IDS fillable form					
2	Non Patent Literature	ISR-WO_PCTUS2016032090_072916_13pgs.PDF	12820719 f65e99a7867c4ffd6b73f7100d17562017305a9c	no	13
Warnings:					
Information:					
3	Non Patent Literature	Perdisci_2008_Pattern_Recognition_Letters.PDF	4583829 7eb1fcf017740795735fb0fca47d47ec20e2ac27	no	6
Warnings:					
Information:					
4	Non Patent Literature	Perdisci_2008_IEEE.PDF	12496921 b9277e59790334823c090fed8badf27f2b131fff	no	10
Warnings:					
Information:					
			Total Files Size (in bytes):	30385757	

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
14/709,875	05/12/2015	Mauritius Schmidtler	04584.0168US01

CONFIRMATION NO. 1593

23552
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

PUBLICATION NOTICE

OC00000087287924

Title:AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS

Publication No.US-2016-0335435-A1
Publication Date:11/17/2016

NOTICE OF PUBLICATION OF APPLICATION

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

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

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

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

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/709,875	05/12/2015	Mauritius Schmidtler	04584.0168US01	1593

23552 7590 12/08/2016

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
LAVELLE, GARY E	

ART UNIT	PAPER NUMBER
2493	

NOTIFICATION DATE	DELIVERY MODE
12/08/2016	ELECTRONIC

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

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

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

USPTO23552@merchantgould.com

Office Action Summary	Application No. 14/709,875	Applicant(s) SCHMIDTLER ET AL.	
	Examiner GARY LAVELLE	Art Unit 2493	AIA (First Inventor to File) Status Yes

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

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

Status

1)☒ Responsive to communication(s) filed on *5/12/2015*.

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

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

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

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

Disposition of Claims*

5)☒ Claim(s) *1-20* is/are pending in the application.

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

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-20* is/are rejected.

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

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

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

Application Papers

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

11)☒ The drawing(s) filed on *5/12/2015* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

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

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

Priority under 35 U.S.C. § 119

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

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

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

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

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

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

Attachment(s)

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

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

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

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Status of Claims

2. Claims 1-20 are pending.

Information Disclosure Statement

3. The information disclosure statements (IDS) submitted on 5/13/2015 and 10/17/2016 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statements are being considered by the examiner.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a)(2) the claimed invention was described in a patent issued under section 151, or in an application for patent published or deemed published under section 122(b), in which the patent or application, as the case may be, names another inventor and was effectively filed before the effective filing date of the claimed invention.

5. **Claims 1, 2, 10, 11 and 19** are rejected under 35 U.S.C. 102(a)(2) as being anticipated by Wojnowicz et al. (U.S. Patent No. 8,709,924) hereinafter Wojnowicz.

With respect to **claim 1**, Wojnowicz teach "a computer-implemented method" (computer systems include one or more data processors and memory storing instructions that cause at least one processor to perform one or more of operations [column 1, lines 57-67]) "comprising:

extracting a plurality of static data points (chunks of code) from an executable file without decrypting or unpacking the executable file;" (The current subject matter addresses the issue of detecting malicious commands within portable executable files that are encrypted or compressed [column 2, lines 37-40]. The current subject matter is particularly useful for malware files that contain encrypted or compressed ("packed") segments which conceal malicious commands. Entropy analysis can be used in this regard [column 3, lines 1-6] and [abstract]. An entropy time series (ETS) is constructed for each file. To compute the entropy of an executable file, the original file, represented in hexadecimal (00hFFh), can be split into non-overlapping chunks of fixed length, typically 256 bytes (*i.e. data points*). For each chunk of code, the entropy can then be computed. [column 6, lines 4-26 and Fig. 1 and associated text] *Thus, it is apparent that static data points are used without decrypting or unpacking*).

"analyzing the executable file without decrypting or unpacking the executable file," (The current subject matter provides enhanced techniques for identifying malicious commands within code that are compressed and/or encrypted [column 2, lines 37-40]

and [column 3, lines 1-3]. Entropy analysis can be used in this regard [column 3, lines 3-6] and [abstract]. See also [column 3, lines 45-59].

"wherein analyzing the executable file comprises applying a classifier to the plurality of static data points," (Based on entropic energy spectrum, a suspiciously structured entropy score (SSES) was derived. SSES can be combined with any number of additional features in a malware classifier. An entropy time series can characterize the amount of entropy over a chunk of code in a certain location of the file. The amount of entropic structure can then be quantified [column 2, line 50 through column 3, line 23] and [column 3, lines 32-38]. Wavelet-based classifiers may be used [column 5, lines 7-65]).

"wherein the classifier is trained from data that comprises known malicious executable files, known benign executable files and known unwanted executable files;" (The determination of whether nor not a file is likely to be malicious can be accomplished by generating, using at least one predictive model trained using data sets comprising files known to contain malware. Files having a score above a pre-defined threshold are determined to be likely malicious and files having a score below the pre-defined threshold are determined to be not likely malicious [column 1, lines 32-39]. The data set comprised n=39,968 portable executable files from a data repository. 19,988 (50.01%) of these files were known to be malicious, and the remaining files were benign [column 5, line 66 through column 6, line 3]. *It is apparent that malicious executable malware is "unwanted"* [column 1, lines 23-31] and [column 1, lines 13-19].

"and

determining whether the executable file is harmful based on the analysis." (The determination of whether nor not a file is likely to be malicious can be accomplished by generating, using at least one predictive model trained using data sets comprising files known to contain malware. A suspiciously structured entropy score for each file such that files having a score above a pre-defined threshold are determined to be likely malicious [column 1, lines 32-39]).

With respect to **claim 2**, Wojnowicz teach "the computer-implemented method according to claim 1, wherein the extracting the plurality of static data points further comprises classifying the extracted static data points according to a type of data (file size) extracted from the executable file," (A wavelet based classifier strategy may use wavelet coefficients as features in a classifier. Such wavelet coefficients can be used as features within any machine learning or statistical classifier, for example, logistic regression or lasso logistic regression, decision trees, support vector machines, etc. [column 5, lines 8-16]. Two files A & B belonging to the same file size category [column 8, lines 11-17 and 25-28] and Fig. 2). "and

encoding the extracted static data points for the classifier based on the classification." (Data points may be pooled together into a "bin" and indexed *j* and *k* [column 6, lines 63-66] (*i.e. encoding*) Files A and B are placed in file size group J=5 [column 8, lines 48-50] and see Fig.2 and related text).

Claims 10 and 11 are computer-readable storage device versions of the method of Wojnowicz as discussed the analysis of claims 1 and 2 above and the claims are rejected on that basis.

Claim 19 is a system version of the method of Wojnowicz as discussed the analysis of claim 1 above and the claim is rejected on that basis.

Claim Rejections - 35 USC § 103

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

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102 of this title, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

7. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103 are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.

3. Resolving the level of ordinary skill in the pertinent art.

4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

8. **Claims 3, 4, 12 and 13** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wojnowicz in view of Tuvell et al. (U.S. Publication No. 2007/0240220).

With respect to **claim 3**, Wojnowicz teach the claimed subject matter as discussed in the analysis of claim 2 above the rejection of which is incorporated herein. In addition, Wojnowicz describes the use of wavelet-based classifiers and indicates that wavelet coefficients can be used as features within any machine learning or statistical classifier (logistic regression or lasso logistic regression, decision trees, support vector machines, etc.) [column 5, lines 9-15] and also discussed with regard to claim 1 above. Therefore, Wojnowicz teach "using support vector processing to determine whether the executable file is at least one of harmful, benign, and potentially unwanted." but may not specifically disclose "wherein analyzing the executable file further comprises generating a feature vector from the plurality of extracted static data points and evaluating the feature vector".

Tuvell, from the same or similar field of endeavor, teach "wherein analyzing the executable file further comprises generating a feature vector from the plurality of extracted static data points" (The information used to detect malware comprises a feature set selected from the list comprising program information or features such as file name, file size, vendor of the program and version of the program (*e.g. static data points*) [0104]. A feature set of the following three feature elements DLL1, DLL2, DLL3 and an input executable that contained only DLL1 and DLL3, the feature vector is 1 0 1.

Then, the probability of that specific executable being a virus with the feature vector 1 0 1 is then computed [0161]. See also [0336] and Fig. 9) “and

evaluating the feature vector using support vector processing to determine whether the executable file is at least one of harmful, benign, and potentially unwanted.” (For example, with a feature set of the following three feature elements DLL1, DLL2, DLL3 and an input executable that contained only DLL1 and DLL3, the feature vector is 1 0 1. Then, the probability of that specific executable being a virus with the feature vector 1 0 1 is then computed [0161]. Probabilities are computed from the training data. Once the probabilities are calculated, a target executable is classified as a virus according to the probability model [0162]. A data structure is created 716 which nominally is one or more feature vectors describing the presence or absence of each feature element associated with each of the malware profiles. The feature vectors are compared to the malware profiles to determine if malware is present in a target application [0163] and Fig. 7. See also [0323], [0336] and Fig. 9. Once a malware feature set is sufficiently complete, two probability models are created 910 based on the feature sets: one for malware and the other for benign or malware-free programs. With these probability models, it is possible to compare 918 a target application with the probability models and distinguish malware-infected from malware-free programs [0323].)

Tuvell is analogous art directed to a system and method for detecting malware [abstract]. Based upon Wojnowicz in view of Tuvell it would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to

utilize the teachings of Tuvell within the method of Wojnowicz with the motivation of improving malware detection of polymorphic viruses that change their signatures every time they replicate (see Tuvell, [0009]) and also to improve operation on systems with limited storage and processing capacity (see Tuvell, [0011]) and also because all of the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination would have yielded predictable results to one of ordinary skill in the art at the time of the invention.

With respect to **claim 4**, Wojnowicz in view of Tuvell teach the claimed subject matter as discussed in the analysis of claim 3 above the rejection of which is incorporated herein. In addition, Tuvell teach “wherein generating the at least one feature vector comprises selectively setting features of the classifier based on the plurality of extracted static data points.” (The information used to detect malware comprises a feature set selected from the list comprising program information or features such as file name, file size, vendor of the program and version of the program (*e.g. static data points*) [0104]. Each of the feature elements in a pre-defined feature set are derived 916 from the target application. The result is represented in a binary feature set vector, or feature vector, with a "1" indicating that the procedure is present in the searched executable, and a "0" otherwise [0336] and Fig. 9. For example, feature set of the following three feature elements DLL1, DLL2, DLL3 and an input executable that contained only DLL1 and DLL3, the feature vector is 1 0 1 [0161]) with the same motivation as discussed in the analysis of claim 3 above.

Claims 12 and 13 are computer-readable storage device versions of the method of Wojnowicz and Tuvell as discussed the analysis of claims 3 and 4, respectively above, and the claims are rejected on that basis.

9. **Claims 5 and 14** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wojnowicz in view of Tuvell and further in view of Gilbert et al. (U.S. Patent No. 9,197,663) hereinafter Gilbert.

With respect to **claim 5**, Wojnowicz in view of Tuvell teach the claimed subject matter including "wherein features of the feature vector are selectively turned on or off based on evaluation of"…"a value of a static data point" as discussed in the analysis of claim 4 above the rejection of which is incorporated herein but may not specifically disclose "based on evaluation of whether a value of a static data point from the plurality of extracted static data points is within a predetermined range."

Gilbert, from the same or similar field of endeavor, teach "evaluation of whether a value of a static data point from the plurality of extracted static data points is within a predetermined range." (Gilbert identifies malware by combining an analysis of visual and non-visual information associated with the software packages. The non-visual elements can include data identifying a publisher, filenames, external function calls, registered operating system functions, operating system filenames, registry key, system file value, application filenames, library filenames, file size, provider, vendor tags and path names. The visual elements can include an icon (*i.e. static data points*) [column 2, lines 17-20 and 47-52]. Performing the comparison of the icon image and the reference

image may involve determining whether the difference between the quantitative identity of the icon image and the quantitative identity of the reference image is less than a threshold difference (*i.e. a range*) [column 3, lines 26-30]. See also [column 20, lines 44-61].

Gilbert is analogous art directed to candidate files which are analyzed to determine whether the candidate files are malware [abstract]. Based upon Wojnowicz in view of Tuvell in view of Gilbert it would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to utilize the teachings of Gilbert within the method of Wojnowicz and Tuvell with the motivation of improving the issues of privacy and data security and also to avoid detrimental effects on the operation of the computer and/or network on which it resides and also because the transmission and operation of the spyware consume bandwidth and memory and also because users often experience a degradation in system performance, instability, and even total system failure (See Gilbert [column 4, line 64 through column 5, line 3]) and also because all of the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination would have yielded predictable results to one of ordinary skill in the art at the time of the invention.

Claim 14 is a computer-readable storage device version of the method of Wojnowicz and Tuvell as discussed the analysis of claim 5 above and the claim is rejected on that basis.

10. **Claims 6 and 15** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wojnowicz in view of Thomas et al. (U.S. Publication No. 2012/0079596) hereinafter Thomas.

With respect to **claim 6**, Wojnowicz teach the claimed subject matter as discussed in the analysis of claim 2 above the rejection of which is incorporated herein but may not specifically disclose “wherein the classifying the at least one static data point comprises classifying the plurality of extracted static data points into categories comprising numeric values, nominal values, string or byte sequences, and Boolean values.”

Thomas, from the same or similar field of view, teach “wherein the classifying the at least one static data point comprises classifying the plurality of extracted static data points into categories" (The malware detection and analysis system can identify and classify malware families. [0239]) “comprising numeric values” (file size [0175], [0225] and [0272]), “nominal values” (file type [0038], [0175], [0225] and [0272], and resource, [0191, table 4] and [0257]), “string or byte sequences” (original file [0250] and section name [0191, table 4], imports, exports [0195 and Fig. 8], original file name and comments [0250], [0251] and [0267]), “and Boolean values” (Boolean values [0062] and [0078], entry point [0095], resource and section name [0191, table 4] and [0269]).

Thomas is analogous art directed to detecting malicious software/malware [abstract]. Based upon Wojnowicz in view of Thomas it would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to utilize the classification of Thomas within the method of Wojnowicz with the same

motivation as discussed in the analysis of claim 3 above and also with the motivation of providing the improvement of allowing the analysis to go much deeper into the heart of the operating system while not being disruptive since operation occurs on a memory dump once the system is frozen or powered down to detect attempts for malware to hide in the stealthiest ways (see Thomas, [0023]) and also because Wojnowicz indicates that SSES can be combined with any number of additional features in a malware classifier of choice [column 2, lines 63-64].

Claim 15 is a computer-readable storage device version of the method of Wojnowicz and Thomas as discussed the analysis of claim 6 above and the claim is rejected on that basis.

11. **Claims 7 and 16** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wojnowicz in view of Tuvell and further in view of Thomas.

With respect to **claim 7**, Wojnowicz in view of Tuvell in view of Thomas teach the claimed subject matter including the classification of the plurality of extracted static data points as discussed in the analysis of claim 6 above the rejection of which is incorporated herein. In addition, Tuvell teach "wherein analyzing the executable file further comprises generating at least one feature vector from the plurality of extracted static data points," (The information used to detect malware comprises a feature set selected from the list comprising program information or features such as file name, file size, vendor of the program and version of the program (*e.g. static data points*) [0104]. Each of the feature elements in a pre-defined feature set are derived 916 from the

target application. The result is represented in a binary feature set vector, or feature vector, with a "1" indicating that the procedure is present in the searched executable, and a "0" otherwise [0336] and Fig. 9. For example, feature set of the following three feature elements DLL1, DLL2, DLL3 and an input executable that contained only DLL1 and DLL3, the feature vector is 1 0 1 [0161]).

"wherein features of the generated feature vector are weighted based at least upon the classified categories and the plurality of extracted static data points." (The heuristic rules are derived from a classification [0020]. Wherein said rule comprises one or more weights, each said weight assigned to a feature element [claim 6]) with the same motivation as discussed in the analysis of claims 3 and 6 above.

Claim 16 is a computer-readable storage device version of the method of Wojnowicz, Tuvell and Thomas as discussed the analysis of claim 7 above and the claim is rejected on that basis.

12. **Claims 8, 9, 17, 18 and 20** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wojnowicz in view of Gilbert.

With respect to **claim 8**, Wojnowicz teach the claimed subject matter as discussed in the analysis of claim 1 above the rejection of which is incorporated herein. In addition, Wojnowicz teach "wherein determining whether the executable file is harmful further comprises…when a determined probability value that the executable file is harmful exceeds a threshold value." (Files having a score above a pre-defined

threshold are determined to be likely malicious [column 1, lines 32-39]) but does not specifically disclose “preventing execution of the executable file”.

Gilbert, from the same or similar field of endeavor, teach “preventing execution of the executable file” (Anti-virus and anti-spyware software detects, quarantines, and in some cases removes software, such as malware, that is malicious in nature and generally unwanted from a computer or computer [column 2, lines 17-28]).

Gilbert is analogous art directed to candidate files which are analyzed to determine whether the candidate files are malware [abstract]. Based upon Wojnowicz in view of Gilbert it would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to quarantine or eliminate the files of Gilbert within the method of Wojnowicz with the motivation of improving the issues of privacy and data security and also to avoid detrimental effects on the operation of the computer and/or network on which it resides and also because the transmission and operation of the spyware consume bandwidth and memory and also because users often experience a degradation in system performance, instability, and even total system failure (See Gilbert [column 4, line 64 through column 5, line 3]).

With respect to **claim 9**, Wojnowicz in view of Gilbert teach the claimed subject matter as discussed in the analysis of claim 8 above the rejection of which is incorporated herein. In addition, Gilbert teach “wherein the threshold value is set based on predetermined false positive range data.” (The threshold value may be tuned, automatically or manually, based on the performance of malware identification system 100, for example, malware detection rate, false positive rate, etc. The threshold value

may be set such that two images are determined to match when the difference between the images is less than approximately 40%, (i.e. *a range*) for example, the threshold value may be set to 0.4 [column 9, lines 21-34]) with the same motivation as discussed in the analysis of claim 8 above and also because all of the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination would have yielded predictable results to one of ordinary skill in the art at the time of the invention.

The limitations of **claims 17, 18 and 20** are rejected in the analysis of claims 8 and 9 above and the claims are rejected on that basis.

Conclusion

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

Williamson et al. (U.S. Patent No. 8,719,924) teach detecting harmful software by collecting data points and training classifiers.

Friedrichs et al. (U.S. Publication No. 2014/0165203) teach the detection of malicious software based upon categories and feature vectors.

Stokes et al. (U.S. Publication No. 2010/0192222) teach identifying a malware file which includes static metadata by using multiple classifiers.

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to GARY LAVELLE whose telephone number is 571 270-7575 and whose direct facsimile number is 571 270-8575. The examiner can normally be reached on Mon-Fri 9-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Carl Colin can be reached on 571 272-3862. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

15. 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.

Gary Lavelle
Examiner, Art Unit 2493
/gl/

/CARL COLIN/

Supervisory Patent Examiner, Art Unit 2493

Notice of References Cited	Application/Control No. 14/709,875	Applicant(s)/Patent Under Reexamination SCHMIDTLER ET AL.	
	Examiner GARY LAVELLE	Art Unit 2493	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-9,465,940 B1	10-2016	Wojnowicz; Michael	G06F21/565	1/1
*	B	US-2007/0240220 A1	10-2007	Tuvell; George	G06F21/56	726/24
*	C	US-2012/0079596 A1	03-2012	Thomas; Ralph	G06F21/55	726/24
*	D	US-9,197,663 B1	11-2015	Gilbert; Mark	G06F3/04817	1/1
*	E	US-8,719,924 B1	05-2014	Williamson; Matthew	G06F21/568	713/188
*	F	US-2014/0165203 A1	06-2014	FRIEDRICHS; Oliver	G06F21/56	726/24
*	G	US-2010/0192222 A1	07-2010	Stokes; Jack W.	G06F21/563	726/22
	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	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Shabtai, A et al. "Detection of malicious code by applying machine learning classifiers on static features: A state-of-the-art survey". Information Security Technical Report, Elsevier Advanced Technology. Amsterdam, NL, vol. 14, No. 1, Feb. 1, 2009, pp. 16-29, XP026144093, ISSN: 1363-4127.
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L6	53	((Mauritius) near2 (Schmidtler)).INV.	US-PGPUB; USPAT	NEAR	ON	2016/11/27 23:05
L7	4	((Mauritius) near2 (Schmidtler)).INV. and (classif$5 or categor$5) and (malware or malicious or virus)	US-PGPUB; USPAT	NEAR	ON	2016/11/27 23:07
L8	2	((Gaurav) near2 (Dalal)).INV.	US-PGPUB; USPAT	NEAR	ON	2016/11/27 23:16
L9	1	((Reza) near2 (Yoosoofmiya)).INV.	US-PGPUB; USPAT	NEAR	ON	2016/11/27 23:18
S4	5	(G06F21/565 or G06F99/005 or G06F221/033).cpc. static data adj point and (@pd or @ptad or @prad or @ad or @rlad)<"20151205"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2016/11/10 22:45
S5	2	(G06F21/565 or G06F99/005 or G06F221/033).cpc. static data adj point classif$5 train$3 and (@pd or @ptad or @prad or @ad or @rlad)<"20151205"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2016/11/10 22:53
S6	1	"9465940".pn. (classif$5 or categor$5) with chunk	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2016/11/12 20:16
S7	1	"9465940".pn. (classif$5 or categor$5) chunk	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2016/11/12 20:17
S8	1	"9465940".pn. (classif$5 or categor$5) chunk vector	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2016/11/12 22:29
S9	3	("9465940").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	AND	ON	2016/11/12 23:13

			IBM_TDB			
S10	2	("20100192222").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2016/11/12 23:18
S12	6541452	(Numeric adj values file adj size linker adj version code adj size OS adj version image adj version subsystem adj version file adj version adj number size adj of adj stackr size adj of adj image "PE header time" Section adj Entropy section adj count) and (Nominal adj values) and (Strings/Byte adj sequences) and (Boolean adj values) File adj size initialize Comments "Address Of Entry Point Anomaly" Un-initialize company adj name Image adj Base adj Anomaly entry adj point file adj description "Section Alignment Anomaly" internal adj name "Size Of Code Mismatch Anomaly" file adj subtype legal adj copyright "Low Import Count Anomaly" language original adj file "Entry Point Anomaly" file adj flags adj masks private adj build certificate adj Validity product adj version adj number file adj flags product adj name Certificate adj Exception size adj of adj heapr adj file file adj OS special adj build "Code Characteristics Anomaly" file adj type product adj version "Code Name Anomaly" machine adj type file adj version Count adj Anomaly PE adj type package adj code "Data Characteristics Anomaly" product adj code Data adj Name adj Anomaly Sections adj count DLL adj count export adj DLL adj name Export adj Exception DLL adj functions assembly adj version "Large Number of DLLs Anomaly" data adj directory "Certificate Issuer" "flag DLL Name Anomaly" export adj count Certificate adj Subject "Number of Functions Anomaly" "Earliest Data Byte" Imports "Function Name Anomaly" resources Exports "PE Header Anomaly" resources adj language Section adj Names "High Section Count Anomaly" non-resource adj section adj strings resource adj Encoding Non-resource adj section adj strings "PE Magic Validity" resource adj code adj page Resource adj Exception resource adj size "VR Code Ratio Anomaly" DLL adj characteristics Import adj Exception	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/11/15 15:19
S13	2297554	(Numeric adj values file adj size linker adj version code adj size OS adj version image adj version subsystem adj version file adj version adj number size adj of adj stackr size adj of file adj OS	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2016/11/15 16:28

		adj image "PE header time" Section adj Entropy section adj count) and (Nominal adj values initialize Un-initialize entry adj point subsystem file adj subtype language file adj flags adj masks file adj flags product adj name size adj of adj heapr) and (Strings/Byte adj sequences Comments company adj name file adj descriptioninternal adj name legal adj copyright original adj file private adj build special adj build) and (Boolean adj values "Address Of Entry Point Anomaly" Image adj Base adj Anomaly "Section Alignment Anomaly" "Size Of Code Mismatch Anomaly" "Low Import Count Anomaly" "Entry Point Anomaly" certificate adj Validity Certificate adj Exception "Code Characteristics Anomaly") file adj type product adj version "Code Name Anomaly" machine adj type file adj version Count adj Anomaly PE adj type package adj code "Data Characteristics Anomaly" product adj code Data adj Name adj Anomaly Sections adj count DLL adj count export adj DLL adj name Export adj Exception DLL adj functions assembly adj version "Large Number of DLLs Anomaly" data adj directory "Certificate Issuer" "flag DLL Name Anomaly" export adj count Certificate adj Subject "Number of Functions Anomaly" "Earliest Data Byte" Imports "Function Name Anomaly" resources Exports "PE Header Anomaly" resources adj language Section adj Names "High Section Count Anomaly" non-resource adj section adj strings resource adj Encoding Non-resource adj section adj strings "PE Magic Validity" resource adj code adj page Resource adj Exception resource adj size "VR Code Ratio Anomaly" DLL adj characteristics Import adj Exception	DERWENT; IBM_TDB			
S14	2181680	(Numeric adj values file adj size linker adj version code adj size OS adj version image adj version subsystem adj version file adj version adj number size adj of adj stackr size adj of file adj OS adj image "PE header time" Section adj Entropy section adj count) and (Nominal adj values initialize Un-initialize entry adj point subsystem file adj subtype language file adj flags adj masks file adj flags product adj name size adj of adj heapr file adj type machine adj type PE adj type) and (Strings/Byte adj sequences Comments company adj name file adj descriptioninternal adj name legal adj copyright original adj file private adj build special adj build product adj version file adj version package adj code) and (Boolean adj values	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/11/15 16:39

		"Address Of Entry Point Anomaly" Image adj Base adj Anomaly "Section Alignment Anomaly" "Size Of Code Mismatch Anomaly" "Low Import Count Anomaly" "Entry Point Anomaly" certificate adj Validity Certificate adj Exception "Code Characteristics Anomaly" "Code Name Anomaly" Count adj Anomaly "Data Characteristics Anomaly") product adj code Data adj Name adj Anomaly Sections adj count DLL adj count export adj DLL adj name Export adj Exception DLL adj functions assembly adj version "Large Number of DLLs Anomaly" data adj directory "Certificate Issuer" "flag DLL Name Anomaly" export adj count Certificate adj Subject "Number of Functions Anomaly" "Earliest Data Byte" Imports "Function Name Anomaly" resources Exports "PE Header Anomaly" resources adj language Section adj Names "High Section Count Anomaly" non-resource adj section adj strings resource adj Encoding Non-resource adj section adj strings "PE Magic Validity" resource adj code adj page Resource adj Exception resource adj size "VR Code Ratio Anomaly" DLL adj characteristics Import adj Exception				
S15	1301	(Numeric adj values file adj size linker adj version code adj size OS adj version image adj version subsystem adj version file adj version adj number size adj of adj stackr size adj of file adj OS adj image "PE header time" Section adj Entropy section adj count)and (Nominal adj values initialize Un-initialize entry adj point subsystem file adj subtype language file adj flags adj masks file adj flags product adj name size adj of adj heapr file adj type machine adj type PE adj type Sections adj count DLL adj count DLL adj functions data adj directory export adj count "Earliest Data Byte" resources resources adj language resource adj Encoding resource adj code adj page resource adj size DLL adj characteristics resource adj size DLL adj characteristics) and (Strings/Byte adj sequences Comments company adj name file adj descriptioninternal adj name legal adj copyright original adj file private adj build special adj build product adj version file adj version package adj code product adj code export adj DLL adj name assembly adj version "Certificate Issuer" Certificate adj Subject Imports Exports Section adj Names non-resource adj section adj strings non-resource adj section adj strings) and (Boolean adj values "Address Of Entry Point Anomaly" Image adj Base adj Anomaly "Section	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/11/15 19:51

		Alignment Anomaly" "Size Of Code Mismatch Anomaly" "Low Import Count Anomaly" "Entry Point Anomaly" certificate adj Validity Certificate adj Exception "Code Characteristics Anomaly" "Code Name Anomaly" Count adj Anomaly "Data Characteristics Anomaly" Data adj Name adj Anomaly Export adj Exception "Large Number of DLLs Anomaly" "flag DLL Name Anomaly" "Number of Functions Anomaly" "Function Name Anomaly" "PE Header Anomaly" "High Section Count Anomaly" "PE Magic Validity" Resource adj Exception "VR Code Ratio Anomaly" Import adj Exception)				
S16	3	(G06F21/565 or G06F99/005 or G06F221/033).cpc. and (Numeric adj values file adj size linker adj version code adj size OS adj version image adj version subsystem adj version file adj version adj number size adj of adj stackr size adj of file adj OS adj image "PE header time" Section adj Entropy section adj count)and (Nominal adj values initialize Un-initialize entry adj point subsystem file adj subtype language file adj flags adj masks file adj flags product adj name size adj of adj heapr file adj type machine adj type PE adj type Sections adj count DLL adj count DLL adj functions data adj directory export adj count "Earliest Data Byte" resources resources adj language resource adj Encoding resource adj code adj page resource adj size DLL adj characteristics resource adj size DLL adj characteristics) and (Strings/Byte adj sequences Comments company adj name file adj descriptioninternal adj name legal adj copyright original adj file private adj build special adj build product adj version file adj version package adj code product adj code export adj DLL adj name assembly adj version "Certificate Issuer" Certificate adj Subject Imports Exports Section adj Names non-resource adj section adj strings non-resource adj section adj strings) and (Boolean adj values "Address Of Entry Point Anomaly" Image adj Base adj Anomaly "Section Alignment Anomaly" "Size Of Code Mismatch Anomaly" "Low Import Count Anomaly" "Entry Point Anomaly" certificate adj Validity Certificate adj Exception "Code Characteristics Anomaly" "Code Name Anomaly" Count adj Anomaly "Data Characteristics Anomaly" Data adj Name adj Anomaly Export adj Exception "Large Number of DLLs Anomaly" "flag DLL Name Anomaly" "Number of Functions Anomaly" "Function Name Anomaly"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/11/15 19:53

		"PE Header Anomaly" "High Section Count Anomaly" "PE Magic Validity" Resource adj Exception "VR Code Ratio Anomaly" Import adj Exception)				
S17	3	(G06F21/565 or G06F99/005 or G06F221/033).cpc. and (Numeric adj values file adj size linker adj version code adj size OS adj version image adj version subsystem adj version file adj version adj number size adj of adj stackr size adj of file adj OS adj image "PE header time" Section adj Entropy section adj count)and (Nominal adj values initialize Un-initialize entry adj point subsystem file adj subtype language file adj flags adj masks file adj flags product adj name size adj of adj heapr file adj type machine adj type PE adj type Sections adj count DLL adj count DLL adj functions data adj directory export adj count "Earliest Data Byte" resources resources adj language resource adj Encoding resource adj code adj page resource adj size DLL adj characteristics resource adj size DLL adj characteristics) and (Strings/Byte adj sequences Comments company adj name file adj descriptioninternal adj name legal adj copyright original adj file private adj build special adj build product adj version file adj version package adj code product adj code export adj DLL adj name assembly adj version "Certificate Issuer" Certificate adj Subject Imports Exports Section adj Names non-resource adj section adj strings non-resource adj section adj strings) and (Boolean adj values "Address Of Entry Point Anomaly" Image adj Base adj Anomaly "Section Alignment Anomaly" "Size Of Code Mismatch Anomaly" "Low Import Count Anomaly" "Entry Point Anomaly" certificate adj Validity Certificate adj Exception "Code Characteristics Anomaly" "Code Name Anomaly" Count adj Anomaly "Data Characteristics Anomaly" Data adj Name adj Anomaly Export adj Exception "Large Number of DLLs Anomaly" "flag DLL Name Anomaly" "Number of Functions Anomaly" "Function Name Anomaly" "PE Header Anomaly" "High Section Count Anomaly" "PE Magic Validity" Resource adj Exception "VR Code Ratio Anomaly" Import adj Exception) and (@pd or @ptad or @prad or @ad or @rlad)<"20151205"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/11/16 12:17
S18	6	(G06F21/565 or G06F99/005 or G06F221/033).cpc. (malware or malicious or virus) and false adj positive same threshold and (@pd or @ptad or @prad or @ad or @rlad)<"20151205"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	AND	ON	2016/11/25 22:17

			IBM_TDB			
S19	1	("9465940").PN. bin (categor$5 or classif$5) type value	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2016/11/26 11:53
S21	1	("9465940").PN. bin (categor$5 or classif$5) type value file adj size	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2016/11/26 12:00
S22	1	("9465940").PN. vector	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2016/11/26 13:44
S23	1	("9465940").PN. vector feature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2016/11/26 13:44
S24	1	("9465940").PN. vector feature range	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2016/11/26 13:44
S25	1	("9465940").PN. vector same feature range vector	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2016/11/26 13:46
S26	1	("9465940").PN. vector same feature (range or threshold) vector	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2016/11/26 13:52
S27	1	("9465940").PN. vector same feature (range or threshold) vector chunk	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2016/11/26 14:57
S28	11	(G06F21/565 or G06F99/005 or G06F221/033).cpc. (malware or malicious or virus) and weight$5 and feature adj vector and (@pd or @ptad	US-PGPUB; USPAT; USOCR; FPRS;	AND	ON	2016/11/26 15:04

		or @prad or @ad or @rlad) <"20151205"	EPO; JPO; DERWENT; IBM_TDB			
S29	11	(G06F21/565 or G06F99/005 or G06F221/033).cpc. (malware or malicious or virus) and weight$5 and feature adj vector and(classif$5 or categor$5)and (@pd or @ptad or @prad or @ad or @rlad)<"20151205"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2016/11/26 15:05
S30	8	(G06F21/565 or G06F99/005 or G06F221/033).cpc. (malware or malicious or virus) and weight$5 and feature adj vector and(classif$5 or categor$5)and (static adj data adj points or header adj information or section adj information or import adj information or export adj information or certificate adj information or resource adj information or string adj information or flag adj information or legal adj information or comment or program adj information or API or DLL) and (@pd or @ptad or @prad or @ad or @rlad) <"20151205"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2016/11/26 17:17
S32	1	"20070240220".pn. rule feature adj vector	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2016/11/26 21:50
S33	1	"20070240220".pn. rule same feature adj vector	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2016/11/26 21:51

EAST Search History (Interference)

<This search history is empty>

11/28/2016 12:17:12 AM
C:\Users\glavelle\Documents\EAST\Workspaces\14709875.wsp

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14709875
Filing Date	2015-05-12
First Named Inventor	Mauritius Schmidtler
Art Unit	2493
Examiner Name	LAVELLE, GARY E.
Attorney Docket Number	04584.0168US01

U.S.PATENTS

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

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

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20100192222		2010-07-29	Stokes et al.	

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

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

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

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /G.L./

Receipt date: 10/17/2016	Application Number	14709875 14709875 - GAU: 2493
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	2015-05-12
(Not for submission under 37 CFR 1.99)	First Named Inventor	Mauritius Schmidtler
	Art Unit	2493
	Examiner Name	LAVELLE, GARY E.
	Attorney Docket Number	04584.0168US01

	1	International Patent Application No. PCT/US2016/032090, International Search Report and Written Opinion mailed July 29, 2016, 13 pages.	☐
	2	Perdisci et al. (2008) Pattern Recognition Letters 29:1941-1946 "Classification of packed executables for accurate computer virus detection"	☐
	3	Perdisci et al. (2008) IEEE: Annual Computer Security Applications Conference 301-310 "McBoost: Boosting Scalability in Malware Collection and Analysis Using Statistical Classification of Executables"	☐

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

EXAMINER SIGNATURE

Examiner Signature	/Gary Lavelle/	Date Considered	11/12/2016

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /G.L./

Receipt date: 10/17/2016	Application Number	14709875	14709875 - GAU: 2493
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2015-05-12	
	First Named Inventor	Mauritius Schmidtler	
	Art Unit	2493	
	Examiner Name	LAVELLE, GARY E.	
	Attorney Docket Number	04584.0168US01	

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/David D. Harrell/	Date (YYYY-MM-DD)	2016-10-17
Name/Print	David D. Harrell	Registration Number	71855

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /G.L./

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	
Filing Date	
First Named Inventor	Mauritius Schmidtler
Art Unit	
Examiner Name	Not Assigned
Attorney Docket Number	04584.0168US01

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

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

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /G.L./

Receipt date: 05/12/2015	Application Number	14709875 - GAU: 2493
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	
	First Named Inventor	Mauritius Schmidtler
	Art Unit	
	Examiner Name	Not Assigned
	Attorney Docket Number	04584.0168US01

	1	KHAN, Hassan et al., "Determining Malicious Executable Distinguishing Attributes and Low-Complexity Detection", J. Comput Virol, 7.2 (2011), pgs. 95-105.	☐
	2	KOLTER, J. Zico et al., "Learning to Detect and Classift Malicious Executables in the Wild", Journal of Machine Learning Research 7 (2006), pgs. 2721-2744.	☐

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

EXAMINER SIGNATURE

Examiner Signature	/Gary Lavelle/	Date Considered	11/12/2016

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /G.L./

Receipt date: 05/12/2015	Application Number	14709875 - GAU: 2493
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	
	First Named Inventor	Mauritius Schmidtler
	Art Unit	
	Examiner Name	Not Assigned
	Attorney Docket Number	04584.0168US01

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☒ None

SIGNATURE

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

Signature	/Jason E. Becker/	Date (YYYY-MM-DD)	2015-05-12
Name/Print	Jason E. Becker	Registration Number	66632

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /G.L./

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. 1593

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/709,875	05/12/2015	726	2493	04584.0168US01

APPLICANTS

Webroot Inc., Broomfield, CO;

INVENTORS

Mauritius Schmidtler, Escondido, CA;
Gaurav Dalal, San Jose, CA;
Reza Yoosoofmiya, San Diego, CA;

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

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

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

05/27/2015

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /GARY E LAVELLE/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CA	4	20	3

ADDRESS

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903
UNITED STATES

TITLE

AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS

FILING FEE RECEIVED		
730	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

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14709875	SCHMIDTLER ET AL.
	Examiner	**Art Unit**
	GARY LAVELLE	2493

✓	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	11/27/2016								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14709875	SCHMIDTLER ET AL.
	Examiner	Art Unit
	GARY LAVELLE	2493

CPC- SEARCHED		
Symbol	Date	Examiner
G06F21/565, G06F99/005 and G06F221/033	11/27/2016	Gary Lavelle

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor search	11/27/2016	Gary Lavelle
NPL search (Google, ACM and IEEE with seach terms including: malware | malicious | virus, classify, static data points, feature vector, packed, encrypted...)	11/25/2016	Gary Lavelle
East search (see attached search history listing)	11/27/2016	Gary Lavelle

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

/GARY LAVELLE/ Examiner.Art Unit 2493	

Sophos Ex. 1003
Page 126 of 456

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Mauritius Schmidtler et al.	Examiner:	Lavelle, Gary E.
Serial No.:	14/709,875	Group Art Unit:	2493
Filed:	May 12, 2015	Docket No.:	04584.0168US01
Title:	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS		

AMENDMENT & RESPONSE TO NON-FINAL OFFICE ACTION

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

Dear Commissioner:

In response to the Non-Final Office Action mailed December 8, 2016, please amend the above-identified application as follows:

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

Remarks/Arguments begin on page 7 of this paper.

Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (Currently Amended) A computer-implemented method comprising:

extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the static data points correspond to one or more points of reference used to evaluate the executable file;

analyzing the executable file without decrypting or unpacking the executable file, wherein analyzing the executable file comprises applying a classifier to the plurality of static data points, wherein the classifier is trained from data that comprises known malicious executable files, known benign executable files and known unwanted executable files; and

determining whether the executable file is harmful based on the analysis.

2. (Original) The computer-implemented method according to claim 1, wherein the extracting the plurality of static data points further comprises classifying the extracted static data points according to a type of data extracted from the executable file, and encoding the extracted static data points for the classifier based on the classification.

3. (Original) The computer-implemented method according to claim 2, wherein analyzing the executable file further comprises generating a feature vector from the plurality of extracted static data points and evaluating the feature vector using support vector processing to determine whether the executable file is at least one of harmful, benign, and potentially unwanted.

4. (Original) The computer-implemented method according to claim 3, wherein generating the at least one feature vector comprises selectively setting features of the classifier based on the plurality of extracted static data points.

5. (Original) The computer-implemented method according to claim 4, wherein features of the feature vector are selectively turned on or off based on evaluation of whether a value of a static data point from the plurality of extracted static data points is within a predetermined range.

6. (Original) The computer-implemented method according to claim 2, wherein the classifying the at least one static data point comprises classifying the plurality of extracted static data points into categories comprising numeric values, nominal values, string or byte sequences, and Boolean values.

7. (Original) The computer-implemented method according to claim 6, wherein analyzing the executable file further comprises generating at least one feature vector from the plurality of extracted static data points, wherein features of the generated feature vector are weighted based at least upon the classified categories and the plurality of extracted static data points.

8. (Original) The computer-implemented method according to claim 1, wherein determining whether the executable file is harmful further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value.

9. (Original) The computer-implemented method according to claim 8, wherein the threshold value is set based on predetermined false positive range data.

10. (Currently Amended) A computer-readable storage device containing instructions, that when executed on at least one processor, causing the processor to execute a process comprising:

extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the static data points correspond to one or more points of reference used to evaluate the executable file;

analyzing the executable file without decrypting or unpacking the executable file, wherein the analyzing the executable file comprises applying a classifier to the plurality of static

data points extracted, wherein the classifier is trained from data comprising known malicious executable files, known benign executable files and known unwanted executable files; and

determining whether the executable file is harmful based on the analyzing of the executable file.

11. (Original) The computer-readable storage device according to claim 10, wherein the extracting of the plurality of static data points executed by the processor further comprises classifying the extracted static data points according to a type of data extracted from the executable file, and encoding the extracted static data points for the classifier based on the classifying.

12. (Original) The computer-readable storage device according to claim 11, wherein analyzing the executable file further comprises generating at least one feature vector from the plurality of extracted static data points and evaluating the feature vector using linear or nonlinear support vector processing to determine whether the executable file is at least one of harmful, benign, and potentially unwanted.

13. (Original) The computer-readable storage device according to claim 12, wherein generating the at least one feature vector comprises selectively setting features of the classifier based on the plurality of extracted static data points.

14. (Original) The computer-readable storage device according to claim 13, wherein features of the feature vector are selectively turned on or off based on evaluation of whether a value of a static data point from the plurality of extracted static data points is within a predetermined range.

15. (Original) The computer-readable storage device according to claim 11, wherein the classifying the at least one static data point comprises classifying the plurality of extracted static data points into categories comprising numeric values, nominal values, string or byte sequences, and Boolean values.

16. (Original) The computer-readable storage device according to claim 15, wherein analyzing the executable file further comprises generating a feature vector from the plurality of extracted static data points, wherein features of the generated feature vector are weighted based at least upon the classified categories and the plurality of extracted static data points.

17. (Original) The computer-readable storage device according to claim 10, wherein determining whether the executable file is harmful further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value.

18. (Original) The computer-readable storage device according to claim 17, wherein the threshold value is set based on predetermined false positive range data.

19. (Currently Amended) A system comprising:

at least one memory; and

at least one processor operatively connected with the memory and configured to perform operation of:

extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the static data points correspond to one or more points of reference used to evaluate the executable file,

analyzing the executable file without decrypting or unpacking the executable file, wherein the analyzing the executable file comprises applying a classifier to the plurality of static data points extracted, wherein the classifier is trained from data comprising known malicious executable files, known benign executable files and known unwanted executable files, and

determining whether the executable file is harmful based on the analyzing of the executable file.

20. (Original) The system according to claim 19, wherein the determining further comprises preventing execution of the executable file when a determined probability value that the

executable file is harmful exceeds a threshold value, and wherein the threshold value is set based on predetermined false positive range data.

Sophos Ex. 1003
Page 132 of 456

REMARKS/ARGUMENTS

This Amendment and the following remarks are intended to fully respond to the Non-Final Office Action dated December 8, 2016, hereinafter "Office Action." In that Office Action, claims 1-20 were examined and all claims were rejected. Claims 1, 2, 10, 11 and 19 were rejected under 35 U.S.C. § 102(a)(2) as allegedly anticipated by Wojnowicz et al. (U.S. Pat. No. 9,465,940 hereinafter "Wojnowicz"). Claims 3, 4, 12 and 13 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Tuvell et al. (U.S. Pat. Publ. No. 2007/0240220; hereinafter "Tuvell"). Claims 5 and 14 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Tuvell, and further in view of Gilbert et al. (U.S. Pat. No. 9,197,663; hereinafter "Gilbert"). Claims 6 and 15 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz in view of Thomas et al. (U.S. Pat. Publ. No. 2012/0079596; hereinafter "Thomas"). Claims 7 and 16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Tuvell, and further in view of Thomas. Claims 8, 9, 17, 18 and 20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz in view of Gilbert.

Reconsideration of these rejections, as they might apply to the original and amended claims in view of these remarks, is respectfully requested. In this Amendment, claims 1, 10 and 19 have been amended, no claims have been canceled, and no claims have been added. Therefore, claims 1-20 remain present for examination.

Claim Rejections Under 35 U.S.C. § 102:

Claims 1, 2, 10, 11 and 19 were rejected under 35 U.S.C. § 102(a)(2) as allegedly anticipated by Wojnowicz. Applicants respectfully traverse this rejection because either the Examiner failed to state a *prima facie* case of anticipation or the current amendments to the claims now render the Examiner's arguments moot. "Anticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim." *Lindemann Mashinenfabrik GmbH v. Am. Hoist & Derrick Co.,* 730 F.2d 1452, 1458 (Fed. Cir. 1984); *see also,* MPEP § 2131. Applicants submit that the cited references do not disclose all of the elements of the rejected claims.

Non-limiting examples of the present application provide automatic threat detection of executable files based on static data analysis. In examples, a plurality of static data points may be extracted from an executable file without decrypting or unpacking the executable file. The executable file may then be analyzed without decrypting or unpacking the executable file. Analysis of the executable file may comprise applying a classifier to the plurality of extracted static data points. The classifier may be trained from data comprising known malicious executable files, known benign executable files and known unwanted executable files. Based upon analysis of the executable file, a determination can be made as to whether the executable file is harmful.

Wojnowicz relates to identifying malware using wavelet decomposition of software entropy. Specifically, Wojnowicz teaches receiving a set of data files. Each of the data files is split into non-overlapping file chunks of fixed length. The non-overlapping file chunks are represented as an entropy time series that reflects an amount of entropy across the file chunks for each file. A wavelet transform is applied to the corresponding entropy time series to generate an energy spectrum characterizing, for the file, an amount of entropic energy at multiple scales of code resolution. A determination is then made as to whether the file is likely to be malicious based on the energy spectrum. *Wojnowicz*, col. 1, ll. 23-31.

Turning specifically to the claims, without acquiescing to the propriety of the rejection and solely for the purpose of advancing prosecution, Applicants have amended the independent claims. The amended independent claims clarify that the static data points extracted from the received executable file correspond to points of reference (in the file content) that are used to evaluate the file. For instance, amended claim 1 recites, *inter alia*, "extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, *wherein the static data points correspond to one or more points of reference used to evaluate the executable file*" (emphasis added).

Wojnowicz does not teach, at least, "the static data points correspond to one or more points of reference used to evaluate the executable file," as recited in amended claim 1. Wojnowicz teaches the entropy of a received file can be calculated by splitting the file "into non-overlapping chunks of fixed length, typically 256 bytes," and applying an entropy time series to

the chunks. *Wojnowicz*, col. 6, ll. 7-8. According to Wojnowicz, splitting the file into chunks includes identifying an executable file can be represented as a string of hexadecimals, and bundling the hexadecimal characters along a fixed length boundary (e.g., 256 bytes). *Id.*, col. 3, ll. 9-18. These boundaries do not correspond to particular sections or portions of the file. As such, the content of each chunk is based on the size of the file, not the content of the file or the content of sections of the file. Wojnowicz acknowledged the shortcomings of the proffered teachings with respect to files of different lengths:

> One fundamental problem with applying wavelet-based classifiers to malware analysis is that executable files have different lengths. Controlled observational situations produce time series samples of fixed length that are held constant across the data set. In contrast, in uncontrolled observational contexts, time series lengths can differ wildly from sample to sample. Software samples, as one example, can exhibit huge variation in their length, from a handful of kilobytes to hundreds of megabytes.

Id., col. 5, ll. 26-34. Wojnowicz then goes on to describe a process for comparing entropy patterns for file having differing lengths, and, therefore different entropy time series and energy spectra. Notably, neither the described process nor the above file splitting process include evaluating a file based on a point of reference or file section corresponding to the file chunk. In contrast, the present application teaches static data points correspond to a point of reference in a received executable file:

> A static data point may be a point of reference used to evaluate an executable file. As examples, static data points include, but are not limited to: header information, section information, import and export information, certificate information, resource information, string and flag information, legal information, comments, and/or program information (e.g., APIs and DLLs), among other examples. Static data points may be organized into categories that identify a type of static data point. Categories of static data points comprise, but are not limited to: numeric values, nominal values string sequences, byte sequences, and/or Boolean values, among other examples.

Specification, para. [0017]. As described above, the static data points may correspond to one or more sections (or subsections) of an executable file. The static data points may also be organized in to categories that are used to evaluate the file. Wojnowicz provides no equivalent teachings for the file chunks. That is, Wojnowicz does not teach file chunks corresponding to

points of reference in a file or organizing file chunks in into categories to evaluate a file. As such, Wojnowicz does not anticipate amended claim 1.

The other independent claims recite similar limitations and are allowable over the recited reference for at least the same or similar reasons. For example, amended claim 10 recites, *inter alia*:

> extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the static data points correspond to one or more points of reference used to evaluate the executable file;

Amended claim 19 recites, *inter alia*:

> extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the static data points correspond to one or more points of reference used to evaluate the executable file;

The dependent claims, i.e. claims 2 and 11, incorporate all of the limitations of the above independent claims, respectively, and are allowable over Wojnowicz for at least the same reasons. As such, Applicants respectfully request that the Examiner withdraw the rejection and allow claims 1, 2, 10, 11 and 19 at the Examiner's earliest convenience.

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

Claims 3, 4, 12 and 13

Claims 3, 4, 12 and 13 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Tuvell. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

Tuvell relates to a malware detection system. Specifically, Tuvell teaches a system for detecting malware on a limited access mobile platform in a mobile network. The system uses one or more feature sets that describe various non-executable portions of malware-infected and malware-free applications, and compares an application on the limited access mobile platform to the features sets. A match of the features in a suspect application to one of the feature sets provides an indication as to whether the suspect application is malware-infected or malware-free.

Claims 3, 4, 12 and 13 depend from claims 1 and 10, respectively. As previously discussed, claims 1 and 10 are allowable over Wojnowicz. Tuvell does not cure the deficiencies of Wojnowicz, nor does the Office Action refer to it for such. Instead, the Office Action refers to Tuvell as disclosing the use of a feature set comprising program information or features used to detect malware. *Office Action*, pp. 7, 9, 10. Without conceding to the correctness of this characterization, Applicants submit that Tuvell does not teach the above-recited limitations. For example, Tuvell does not teach at least identifying static data points, data points that correspond to one or more points of reference or section in a file, or using data points to evaluate the file by, for example, grouping the data points into categories and generating feature vectors based thereon. Thus, Tuvell fails to teach at least "the static data points correspond to one or more points of reference used to evaluate the executable file," as recited in amended claims 1 and 10. As such, Applicants respectfully request withdrawal of the rejections and allowance of claims 3, 4, 12 and 13 at the Examiner's earliest convenience.

Claims 5 and 14

Claims 5 and 14 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Tuvell, and further in view of Gilbert. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

Gilbert relates to identifying potential software threats based on visual and non-visual data. Specifically, Gilbert teaches analyzing visual and non-visual elements associated with the candidate files to determine whether the candidate files are malware. A visual element (e.g., icon) is extracted from the candidate file, and the icon's image is compared to a group of reference images associated with trusted entities. If the icon's image matches a reference image, the candidate file may be malware masquerading as trusted software. The non-visual elements associated with the candidate file are used, in combination with the visual elements, to determine whether the candidate file is malware.

Claims 5 and 14 depend from claims 1 and 10, respectively. As previously discussed, claims 1 and 10 are allowable over the combination of Wojnowicz and Tuvell. Gilbert does not cure their deficiencies, nor does the Office Action refer to it for such. Instead, the Office Action refers to Gilbert as disclosing the determination of whether the difference between the quantitative identity of an icon image and the quantitative identity of a reference image is less than a threshold difference. *Office Action*, pp. 10-11. Without conceding to the correctness of this characterization, Applicants submit that Gilbert does not teach the above-recited limitations. For example, Gilbert does not teach at least identifying static data points, data points that correspond to one or more points of reference or section in a file, or using data points to evaluate the file by, for example, grouping the data points into categories and generating feature vectors based thereon. Thus, Gilbert fails to teach at least "the static data points correspond to one or more points of reference used to evaluate the executable file," as recited in amended claims 1 and 10. As such, Applicants respectfully request withdrawal of the rejections and allowance of claims 5 and 14 at the Examiner's earliest convenience.

Claims 6 and 15

Claims 6 and 15 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz in view of Thomas. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424

F.2d 1382, 1385 (C.C.P.A. 1970). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

Thomas relates to a method and system for the automatic detection and analysis of malware. Specifically, Thomas teaches a method of detecting malicious software (malware) includes receiving a file and storing a memory baseline for a system. The method also includes copying the file to the system, executing the file on the system, terminating operation of the system, and storing a post-execution memory map. The method further includes analyzing the memory baseline and the post-execution memory map and determining that the file includes malware.

Claims 6 and 15 depend from claims 1 and 10, respectively. As previously discussed, claims 1 and 10 are allowable over Wojnowicz. Thomas does not cure the deficiencies of Wojnowicz, nor does the Office Action refer to it for such. Instead, the Office Action refers to Thomas as disclosing the identification and classification of malware families. *Office Action*, pp. 12-13. Without conceding to the correctness of this characterization, Applicants submit that Thomas does not teach the above-recited limitations. For example, Thomas does not teach at least identifying static data points, data points that correspond to one or more points of reference or section in a file, or using data points to evaluate the file by, for example, grouping the data points into categories and generating feature vectors based thereon. Thus, Thomas fails to teach at least "the static data points correspond to one or more points of reference used to evaluate the executable file," as recited in amended claims 1 and 10. As such, Applicants respectfully request withdrawal of the rejections and allowance of claims 6 and 15 at the Examiner's earliest convenience.

Claims 7 and 16

Claims 7 and 16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Tuvell, and further in view of Thomas. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at

the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

Claims 7 and 16 depend from claims 1 and 10, respectively. As previously discussed, claims 1 and 10 are allowable over the combinations of Wojnowicz and Tuvell and Wojnowicz and Thomas. The further combination of Wojnowicz, Tuvell and Thomas does not cure their deficiencies of the individual combinations. For example, as discussed above, neither Tuvell nor Thomas teaches identifying static data points, data points that correspond to one or more points of reference or section in a file, or using data points to evaluate the file. Thus, the recited references fail to teach at least "the static data points correspond to one or more points of reference used to evaluate the executable file," as recited in amended claims 1 and 10. As such, Applicants respectfully request withdrawal of the rejections and allowance of claims 7 and 16 at the Examiner's earliest convenience.

Claims 8, 9, 17, 18 and 20

Claims 8, 9, 17, 18 and 20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz in view of Gilbert. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

Claims 8, 9, 17, 18 and 20 depend from claims 1, 10 and 19, respectively. As previously discussed, claims 1, 10 and 19 are allowable over the combinations of Wojnowicz, Tuvell and Gilbert. Removing Tuvell from the combination does not cure their deficiencies of Wojnowicz and Gilbert. For example, as discussed above, the combination of Wojnowicz nor Gilbert does not teach identifying static data points, data points that correspond to one or more points of

reference or section in a file, or using data points to evaluate the file. Thus, the recited references fail to teach at least "the static data points correspond to one or more points of reference used to evaluate the executable file," as recited in amended claims 1, 10 and 19. As such, Applicants respectfully request withdrawal of the rejections and allowance of claims 8, 9, 17, 18 and 20 at the Examiner's earliest convenience.

CONCLUSION

This Amendment fully responds to the Office Action mailed on December 8, 2016. Still, that Office Action may contain arguments and rejections that are not directly addressed by this Amendment due to the fact that they are rendered moot in light of the preceding arguments in favor of patentability. Hence, failure of this Amendment to directly address an argument raised in the Office Action should not be taken as an indication that the Applicant believes the argument has merit. Furthermore, the claims of the present application may include other elements, not discussed in this Amendment, which are not shown, taught, or otherwise suggested by the references of record. Accordingly, the preceding arguments in favor of patentability are advanced without prejudice to other bases of patentability.

It is believed that no further fees are due with this Response. However, the Commissioner is hereby authorized to charge any deficiencies or credit any overpayment with respect to this patent application to deposit account number 13-2725.

In light of the above remarks and amendments, it is believed that the application is now in condition for allowance and such action is respectfully requested. Should any additional issues need to be resolved, the Examiner is requested to telephone the undersigned to attempt to resolve those issues.

Respectfully submitted,

Dated: March 8, 2017

/David D. Harrell/

David D. Harrell, Reg. No. 71,855
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1242

27488
PATENT TRADEMARK OFFICE

Electronic Acknowledgement Receipt

EFS ID:	28567166
Application Number:	14709875
International Application Number:	
Confirmation Number:	1593
Title of Invention:	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS
First Named Inventor/Applicant Name:	Mauritius Schmidtler
Customer Number:	23552
Filer:	David Dwayne Harrell/Elizabeth Pallardy
Filer Authorized By:	David Dwayne Harrell
Attorney Docket Number:	04584.0168US01
Receipt Date:	08-MAR-2017
Filing Date:	12-MAY-2015
Time Stamp:	11:58:23
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		04584_0168US01_RespNFOA_12-08-16.PDF	149934 fafdddb495a005d328bf1fc6b0208ba35e2aa493	yes	16

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	6
	Applicant Arguments/Remarks Made in an Amendment	7	16
Warnings:			
Information:			
	Total Files Size (in bytes):	149934	

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

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

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

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

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/709,875	Filing Date 05/12/2015	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

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

APPLICATION AS AMENDED – PART II

AMENDMENT **03/08/2017**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	X $80 =	0
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $420 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

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

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

LIE
BRENDA HARRISON

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/709,875	05/12/2015	Mauritius Schmidtler	04584.0168US01	1593

23552 7590 03/24/2017

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
LAVELLE, GARY E	

ART UNIT	PAPER NUMBER
2493	

NOTIFICATION DATE	DELIVERY MODE
03/24/2017	ELECTRONIC

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

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

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

USPTO23552@merchantgould.com

Office Action Summary	Application No. 14/709,875	Applicant(s) SCHMIDTLER ET AL.	
	Examiner GARY LAVELLE	Art Unit 2493	AIA (First Inventor to File) Status Yes

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

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

Status

1)☒ Responsive to communication(s) filed on *3/8/2017*.

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

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

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

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

Disposition of Claims*

5)☒ Claim(s) *1-20* is/are pending in the application.

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

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-20* is/are rejected.

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

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

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

Application Papers

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

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

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

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

Priority under 35 U.S.C. § 119

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

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

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

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

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

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

Attachment(s)

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

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

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

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Status of Claims

2. In communications filed 3/8/2017 Applicants amend claims 1, 10, and 19. Claims 1-20 are pending.

Response to Arguments

3. With respect to claim 1, Applicants argue that Wojnowicz does not teach "extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the static data points correspond to one or more points of reference used to evaluate the executable file" as amended because Wojnowicz calculates entropy by splitting a file into chunks. Applicants explain that since the size of the file may vary, the content of each chunk is based on the size of the file, not the content of the file or the content of sections of the file. Applicants conclude that Wojnowicz does not teach file chunks corresponding to points of reference in a file. Furthermore, Applicants argue that Wojnowicz does not teach organizing file chunks in into categories to evaluate a file. (Remarks, page 8 through paragraph 1, page 10 with emphasis added by Applicants).

The Examiner respectfully disagrees. Applicants' specification indicates that a static data point may be a point of reference used to evaluate an executable file. An example of string information is provided (see instant specification, paragraph [0017]). Wojnowicz computes entropy of a string of hexadecimal characters. Applicants' arguments are moot in view of new grounds of rejection incorporating previously cited prior art. Furthermore, and in addition, the Examiner notes that the location of the string within the executable file is static. The division of the executable file into chunks as part of the evaluation process does not alter the position of the string within the executable file.

Regarding Applicants' argument that Wojnowicz does not teach organizing file chunks in into categories to evaluate a file, the Examiner respectfully disagrees because Wojnowicz calculates a suspiciously structured entropy score (SSES) which can be combined with any number of additional features in a malware classifier. The amount of entropic structure can then be quantified as taught by Wojnowicz and discussed in the claim analysis below. For these reasons, Applicants' arguments are not persuasive.

Applicants state that independent claims 10 and 19 have been amended to recite similar limitations and should be allowable for the same reasons. These arguments are not persuasive based upon the same rational.

Applicants argue with respect to dependent claims 3, 4, 12 and 13 that the reference of Tuvell does not overcome the alleged shortcomings of Wojnowicz for the same reasons. Applicants argue with respect to dependent claims 5 and 14 that the

references of Tuvell and Gilbert do not overcome the alleged shortcomings of Wojnowicz for the same reasons. Applicants argue with respect to dependent claims 6 and 15 that the reference of Thomas does not overcome the alleged shortcomings of Wojnowicz for the same reasons. Applicants argue with respect to dependent claims 7 and 16 that the references of Tuvell and Thomas do not overcome the alleged shortcomings of Wojnowicz for the same reasons. Applicants argue with respect to dependent claims 8, 9, 17, 18 and 20 that the reference of Gilbert does not overcome the alleged shortcomings of Wojnowicz for the same reasons. These arguments are not persuasive based upon the same rational as discussed above and in the claim analysis below.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a)(2) the claimed invention was described in a patent issued under section 151, or in an application for patent published or deemed published under section 122(b), in which the patent or application, as the case may be, names another inventor and was effectively filed before the effective filing date of the claimed invention.

5. **Claims 1, 2, 10, 11 and 19** are rejected under 35 U.S.C. 102(a)(2) as being anticipated by Wojnowicz et al. (U.S. Patent No. 8,709,924) hereinafter Wojnowicz.

With respect to **claim 1**, Wojnowicz teach “a computer-implemented method” (computer systems include one or more data processors and memory storing

instructions that cause at least one processor to perform one or more of operations [column 1, lines 57-67]) “comprising:

extracting a plurality of static data points (chunks of code) from an executable file without decrypting or unpacking the executable file, wherein the static data points correspond to one or more points of reference used to evaluate the executable file;” (The current subject matter addresses the issue of detecting malicious commands within portable executable files that are encrypted or compressed [column 2, lines 37-40]. The current subject matter is particularly useful for malware files that contain encrypted or compressed ("packed") segments which conceal malicious commands. Entropy analysis can be used in this regard [column 3, lines 1-6] and [abstract]. An entropy time series (ETS) is constructed for each file. To compute the entropy of an executable file, the original file, represented in hexadecimal (00hFFh), can be split into non-overlapping chunks of fixed length, typically 256 bytes (*i.e. data points*). For each chunk of code, the entropy can then be computed. [column 6, lines 4-26 and Fig. 1 and associated text] *Thus, it is apparent that static data points are used without decrypting or unpacking*). The current subject matter is particularly useful for malware files that contain encrypted or compressed ("packed") segments which conceal malicious commands. Entropy analysis can be used in this regard because files with high entropy are relatively likely to have encrypted or compressed sections inside them. In the context of software analysis, an executable file can be represented as a string of hexadecimals (00hFFh), where each observed hexadecimal character is considered to be an instantiation of a random variable (for example, with 256 possible values). A

string of these hexadecimal characters can be bundled up into a "chunk" of a file, and the statistical variation within that chunk can be estimated by computing the entropy within the chunk. Zero entropy means that the same character was repeated over and over (as might occur in a "padded" chunk of code) and maximum entropy means that a chunk consisted of entirely distinct values. Chunks of code that have been compressed or encrypted tend to have higher entropy than native code. [column 3, lines 1-23].

“analyzing the executable file without decrypting or unpacking the executable file,” (The current subject matter provides enhanced techniques for identifying malicious commands within code that are compressed and/or encrypted [column 2, lines 37-40] and [column 3, lines 1-3]. Entropy analysis can be used in this regard [column 3, lines 3-6] and [abstract]. See also [column 3, lines 45-59].

“wherein analyzing the executable file comprises applying a classifier to the plurality of static data points,” (Based on entropic energy spectrum, a suspiciously structured entropy score (SSES) was derived. SSES can be combined with any number of additional features in a malware classifier. An entropy time series can characterize the amount of entropy over a chunk of code in a certain location of the file. The amount of entropic structure can then be quantified [column 2, line 50 through column 3, line 23] and [column 3, lines 32-38]. Wavelet-based classifiers may be used [column 5, lines 7-65]).

“wherein the classifier is trained from data that comprises known malicious executable files, known benign executable files and known unwanted executable files;” (The determination of whether nor not a file is likely to be malicious can be

accomplished by generating, using at least one predictive model trained using data sets comprising files known to contain malware. Files having a score above a pre-defined threshold are determined to be likely malicious and files having a score below the pre-defined threshold are determined to be not likely malicious [column 1, lines 32-39]. The data set comprised n=39,968 portable executable files from a data repository. 19,988 (50.01%) of these files were known to be malicious, and the remaining files were benign [column 5, line 66 through column 6, line 3]. *It is apparent that malicious executable malware is "unwanted"* [column 1, lines 23-31] and [column 1, lines 13-19].

"and

determining whether the executable file is harmful based on the analysis." (The determination of whether nor not a file is likely to be malicious can be accomplished by generating, using at least one predictive model trained using data sets comprising files known to contain malware. A suspiciously structured entropy score for each file such that files having a score above a pre-defined threshold are determined to be likely malicious [column 1, lines 32-39]).

With respect to **claim 2**, Wojnowicz teach "the computer-implemented method according to claim 1, wherein the extracting the plurality of static data points further comprises classifying the extracted static data points according to a type of data (file size) extracted from the executable file," (A wavelet based classifier strategy may use wavelet coefficients as features in a classifier. Such wavelet coefficients can be used as features within any machine learning or statistical classifier, for example, logistic regression or lasso logistic regression, decision trees, support vector machines, etc.

[column 5, lines 8-16]. Two files A & B belonging to the same file size category [column 8, lines 11-17 and 25-28] and Fig. 2). “and

encoding the extracted static data points for the classifier based on the classification.” (Data points may be pooled together into a "bin" and indexed *j* and *k* [column 6, lines 63-66] (*i.e. encoding*) Files A and B are placed in file size group J=5 [column 8, lines 48-50] and see Fig.2 and related text).

Claims 10 and 11 are computer-readable storage device versions of the method of Wojnowicz as discussed the analysis of claims 1 and 2 above and the claims are rejected on that basis.

Claim 19 is a system version of the method of Wojnowicz as discussed the analysis of claim 1 above and the claim is rejected on that basis.

Claim Rejections - 35 USC § 103

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

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102 of this title, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

7. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103 are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.

3. Resolving the level of ordinary skill in the pertinent art.

4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

8. **Claims 3, 4, 12 and 13** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wojnowicz in view of Tuvell et al. (U.S. Publication No. 2007/0240220).

With respect to **claim 3**, Wojnowicz teach the claimed subject matter as discussed in the analysis of claim 2 above the rejection of which is incorporated herein. In addition, Wojnowicz describes the use of wavelet-based classifiers and indicates that wavelet coefficients can be used as features within any machine learning or statistical classifier (logistic regression or lasso logistic regression, decision trees, support vector machines, etc.) [column 5, lines 9-15] and also discussed with regard to claim 1 above. Therefore, Wojnowicz teach "using support vector processing to determine whether the executable file is at least one of harmful, benign, and potentially unwanted." but may not specifically disclose "wherein analyzing the executable file further comprises generating a feature vector from the plurality of extracted static data points and evaluating the feature vector".

Tuvell, from the same or similar field of endeavor, teach "wherein analyzing the executable file further comprises generating a feature vector from the plurality of extracted static data points" (The information used to detect malware comprises a

feature set selected from the list comprising program information or features such as file name, file size, vendor of the program and version of the program (*e.g. static data points*) [0104]. A feature set of the following three feature elements DLL1, DLL2, DLL3 and an input executable that contained only DLL1 and DLL3, the feature vector is 1 0 1. Then, the probability of that specific executable being a virus with the feature vector 1 0 1 is then computed [0161]. See also [0336] and Fig. 9) "and

evaluating the feature vector using support vector processing to determine whether the executable file is at least one of harmful, benign, and potentially unwanted." (For example, with a feature set of the following three feature elements DLL1, DLL2, DLL3 and an input executable that contained only DLL1 and DLL3, the feature vector is 1 0 1. Then, the probability of that specific executable being a virus with the feature vector 1 0 1 is then computed [0161]. Probabilities are computed from the training data. Once the probabilities are calculated, a target executable is classified as a virus according to the probability model [0162]. A data structure is created 716 which nominally is one or more feature vectors describing the presence or absence of each feature element associated with each of the malware profiles. The feature vectors are compared to the malware profiles to determine if malware is present in a target application [0163] and Fig. 7. See also [0323], [0336] and Fig. 9. Once a malware feature set is sufficiently complete, two probability models are created 910 based on the feature sets: one for malware and the other for benign or malware-free programs. With these probability models, it is possible to compare 918 a target application with the

probability models and distinguish malware-infected from malware-free programs [0323].)

Tuvell is analogous art directed to a system and method for detecting malware [abstract]. Based upon Wojnowicz in view of Tuvell it would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to utilize the teachings of Tuvell within the method of Wojnowicz with the motivation of improving malware detection of polymorphic viruses that change their signatures every time they replicate (see Tuvell, [0009]) and also to improve operation on systems with limited storage and processing capacity (see Tuvell, [0011]) and also because all of the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination would have yielded predictable results to one of ordinary skill in the art at the time of the invention.

With respect to **claim 4**, Wojnowicz in view of Tuvell teach the claimed subject matter as discussed in the analysis of claim 3 above the rejection of which is incorporated herein. In addition, Tuvell teach "wherein generating the at least one feature vector comprises selectively setting features of the classifier based on the plurality of extracted static data points." (The information used to detect malware comprises a feature set selected from the list comprising program information or features such as file name, file size, vendor of the program and version of the program (*e.g. static data points*) [0104]. Each of the feature elements in a pre-defined feature set are derived 916 from the target application. The result is represented in a binary feature

set vector, or feature vector, with a "1" indicating that the procedure is present in the searched executable, and a "0" otherwise [0336] and Fig. 9. For example, feature set of the following three feature elements DLL1, DLL2, DLL3 and an input executable that contained only DLL1 and DLL3, the feature vector is 1 0 1 [0161]) with the same motivation as discussed in the analysis of claim 3 above.

Claims 12 and 13 are computer-readable storage device versions of the method of Wojnowicz and Tuvell as discussed the analysis of claims 3 and 4, respectively above, and the claims are rejected on that basis.

9. **Claims 5 and 14** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wojnowicz in view of Tuvell and further in view of Gilbert et al. (U.S. Patent No. 9,197,663) hereinafter Gilbert.

With respect to **claim 5**, Wojnowicz in view of Tuvell teach the claimed subject matter including “wherein features of the feature vector are selectively turned on or off based on evaluation of”…”a value of a static data point” as discussed in the analysis of claim 4 above the rejection of which is incorporated herein but may not specifically disclose “based on evaluation of whether a value of a static data point from the plurality of extracted static data points is within a predetermined range.”

Gilbert, from the same or similar field of endeavor, teach “evaluation of whether a value of a static data point from the plurality of extracted static data points is within a predetermined range.” (Gilbert identifies malware by combining an analysis of visual and non-visual information associated with the software packages. The non-visual

elements can include data identifying a publisher, filenames, external function calls, registered operating system functions, operating system filenames, registry key, system file value, application filenames, library filenames, file size, provider, vendor tags and path names. The visual elements can include an icon (*i.e. static data points*) [column 2, lines 17-20 and 47-52]. Performing the comparison of the icon image and the reference image may involve determining whether the difference between the quantitative identity of the icon image and the quantitative identity of the reference image is less than a threshold difference (*i.e. a range*) [column 3, lines 26-30]. See also [column 20, lines 44-61].

Gilbert is analogous art directed to candidate files which are analyzed to determine whether the candidate files are malware [abstract]. Based upon Wojnowicz in view of Tuvell in view of Gilbert it would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to utilize the teachings of Gilbert within the method of Wojnowicz and Tuvell with the motivation of improving the issues of privacy and data security and also to avoid detrimental effects on the operation of the computer and/or network on which it resides and also because the transmission and operation of the spyware consume bandwidth and memory and also because users often experience a degradation in system performance, instability, and even total system failure (See Gilbert [column 4, line 64 through column 5, line 3]) and also because all of the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no

change in their respective functions, and the combination would have yielded predictable results to one of ordinary skill in the art at the time of the invention.

Claim 14 is a computer-readable storage device version of the method of Wojnowicz and Tuvell as discussed the analysis of claim 5 above and the claim is rejected on that basis.

10. **Claims 6 and 15** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wojnowicz in view of Thomas et al. (U.S. Publication No. 2012/0079596) hereinafter Thomas.

With respect to **claim 6**, Wojnowicz teach the claimed subject matter as discussed in the analysis of claim 2 above the rejection of which is incorporated herein but may not specifically disclose “wherein the classifying the at least one static data point comprises classifying the plurality of extracted static data points into categories comprising numeric values, nominal values, string or byte sequences, and Boolean values.”

Thomas, from the same or similar field of view, teach “wherein the classifying the at least one static data point comprises classifying the plurality of extracted static data points into categories" (The malware detection and analysis system can identify and classify malware families. [0239]) “comprising numeric values” (file size [0175], [0225] and [0272]), “nominal values” (file type [0038], [0175], [0225] and [0272], and resource, [0191, table 4] and [0257]), “string or byte sequences” (original file [0250] and section name [0191, table 4], imports, exports [0195 and Fig. 8], original file name and

comments [0250], [0251] and [0267]), “and Boolean values” (Boolean values [0062] and [0078], entry point [0095], resource and section name [0191, table 4] and [0269]).

Thomas is analogous art directed to detecting malicious software/malware [abstract]. Based upon Wojnowicz in view of Thomas it would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to utilize the classification of Thomas within the method of Wojnowicz with the same motivation as discussed in the analysis of claim 3 above and also with the motivation of providing the improvement of allowing the analysis to go much deeper into the heart of the operating system while not being disruptive since operation occurs on a memory dump once the system is frozen or powered down to detect attempts for malware to hide in the stealthiest ways (see Thomas, [0023]) and also because Wojnowicz indicates that SSES can be combined with any number of additional features in a malware classifier of choice [column 2, lines 63-64].

Claim 15 is a computer-readable storage device version of the method of Wojnowicz and Thomas as discussed the analysis of claim 6 above and the claim is rejected on that basis.

11. **Claims 7 and 16** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wojnowicz in view of Tuvell and further in view of Thomas.

With respect to **claim 7**, Wojnowicz in view of Tuvell in view of Thomas teach the claimed subject matter including the classification of the plurality of extracted static data points as discussed in the analysis of claim 6 above the rejection of which is

incorporated herein. In addition, Tuvell teach "wherein analyzing the executable file further comprises generating at least one feature vector from the plurality of extracted static data points," (The information used to detect malware comprises a feature set selected from the list comprising program information or features such as file name, file size, vendor of the program and version of the program (*e.g. static data points*) [0104]. Each of the feature elements in a pre-defined feature set are derived 916 from the target application. The result is represented in a binary feature set vector, or feature vector, with a "1" indicating that the procedure is present in the searched executable, and a "0" otherwise [0336] and Fig. 9. For example, feature set of the following three feature elements DLL1, DLL2, DLL3 and an input executable that contained only DLL1 and DLL3, the feature vector is 1 0 1 [0161]).

"wherein features of the generated feature vector are weighted based at least upon the classified categories and the plurality of extracted static data points." (The heuristic rules are derived from a classification [0020]. Wherein said rule comprises one or more weights, each said weight assigned to a feature element [claim 6]) with the same motivation as discussed in the analysis of claims 3 and 6 above.

Claim 16 is a computer-readable storage device version of the method of Wojnowicz, Tuvell and Thomas as discussed the analysis of claim 7 above and the claim is rejected on that basis.

12. **Claims 8, 9, 17, 18 and 20** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wojnowicz in view of Gilbert.

With respect to **claim 8**, Wojnowicz teach the claimed subject matter as discussed in the analysis of claim 1 above the rejection of which is incorporated herein. In addition, Wojnowicz teach "wherein determining whether the executable file is harmful further comprises…when a determined probability value that the executable file is harmful exceeds a threshold value." (Files having a score above a pre-defined threshold are determined to be likely malicious [column 1, lines 32-39]) but does not specifically disclose "preventing execution of the executable file".

Gilbert, from the same or similar field of endeavor, teach "preventing execution of the executable file" (Anti-virus and anti-spyware software detects, quarantines, and in some cases removes software, such as malware, that is malicious in nature and generally unwanted from a computer or computer [column 2, lines 17-28]).

Gilbert is analogous art directed to candidate files which are analyzed to determine whether the candidate files are malware [abstract]. Based upon Wojnowicz in view of Gilbert it would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to quarantine or eliminate the files of Gilbert within the method of Wojnowicz with the motivation of improving the issues of privacy and data security and also to avoid detrimental effects on the operation of the computer and/or network on which it resides and also because the transmission and operation of the spyware consume bandwidth and memory and also because users often experience a degradation in system performance, instability, and even total system failure (See Gilbert [column 4, line 64 through column 5, line 3]).

With respect to **claim 9**, Wojnowicz in view of Gilbert teach the claimed subject matter as discussed in the analysis of claim 8 above the rejection of which is incorporated herein. In addition, Gilbert teach "wherein the threshold value is set based on predetermined false positive range data." (The threshold value may be tuned, automatically or manually, based on the performance of malware identification system 100, for example, malware detection rate, false positive rate, etc. The threshold value may be set such that two images are determined to match when the difference between the images is less than approximately 40%, (i.e. *a range*) for example, the threshold value may be set to 0.4 [column 9, lines 21-34]) with the same motivation as discussed in the analysis of claim 8 above and also because all of the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination would have yielded predictable results to one of ordinary skill in the art at the time of the invention.

The limitations of **claims 17, 18 and 20** are rejected in the analysis of claims 8 and 9 above and the claims are rejected on that basis.

Conclusion

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to GARY LAVELLE whose telephone number is 571 270-7575 and whose direct facsimile number is 571 270-8575. The examiner can normally be reached on Mon-Fri 9-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Carl Colin can be reached on 571 272-3862. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

15. 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.

Gary Lavelle
Examiner, Art Unit 2493
/gl/

/CARL COLIN/
Supervisory Patent Examiner, Art Unit 2493

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14709875	SCHMIDTLER ET AL.
	Examiner	**Art Unit**
	GARY LAVELLE	2493

✓	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	11/27/2016	03/16/2017							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16	✓	✓							
	17	✓	✓							
	18	✓	✓							
	19	✓	✓							
	20	✓	✓							

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14709875	SCHMIDTLER ET AL.
	Examiner	Art Unit
	GARY LAVELLE	2493

CPC- SEARCHED		
Symbol	Date	Examiner
G06F21/565, G06F99/005 and G06F221/033	11/27/2016	Gary Lavelle

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor search	11/27/2016	Gary Lavelle
NPL search (Google, ACM and IEEE with seach terms including: malware | malicious | virus, classify, static data points, feature vector, packed, encrypted...)	11/25/2016	Gary Lavelle
East search (see attached search history listing)	11/27/2016	Gary Lavelle
Inventor search updated	3/19/2017	Gary Lavelle
NPL search updated (Google, ACM and IEEE with new search terms including: static reference points...)	3/19/2017	Gary Lavelle
East search (see attached search history listing)	3/20/2017	Gary Lavelle

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

/GARY LAVELLE/ Examiner.Art Unit 2493	

Sophos Ex. 1003
Page 168 of 456

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S38	1	"8709924".pn. and (header section import export certificate resource string flag legal comment program API DLL)	USPAT	OR	OFF	2017/03/16 15:28
S39	1	"9465940".pn. and (header section import export certificate resource string flag legal comment program API DLL)	USPAT	OR	OFF	2017/03/16 15:31
S41	4	((Mauritius) near2 (Schmidtler)).INV. and (classif$5 or categor$5) and (malware or malicious or virus)	US-PGPUB; USPAT	NEAR	ON	2017/03/19 21:57
S40	53	((Mauritius) near2 (Schmidtler)).INV.	US-PGPUB; USPAT	NEAR	ON	2017/03/19 21:57
S42	2	((Gaurav) near2 (Dalal)).INV.	US-PGPUB; USPAT	NEAR	ON	2017/03/19 22:04
S43	1	((Reza) near2 (Yoosoofmiya)).INV.	US-PGPUB; USPAT	NEAR	ON	2017/03/19 22:09
S44	15	(G06F21/565 or G06F99/005 or G06F221/033).cpc. and (malware or malicious or virus) and weight$5 and feature adj vector and(classif$5 or categor$5)and (header section import export certificate resource string flag legal comment program API DLL)and (@pd or @ptad or @prad or @ad or @rlad) <"20151205"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/03/20 08:49
L1	15	(G06F21/565 or G06F99/005 or G06F221/033).cpc. and (malware or malicious or virus) and weight$5 and feature adj vector and(classif$5 or categor$5)and (header section import export certificate resource string flag legal comment program API DLL)and (@pd or @ptad or @prad or @ad or @rlad) <"20151205" and referenc$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/03/20 10:08

EAST Search History (Interference)

<This search history is empty>

3/20/2017 10:10:30 AM
C:\Users\glavelle\Documents\EAST\Workspaces\14709875.wsp

PTO/SB/30EFS (07-14)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

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

Application Number	14709875	Filing Date	2015-05-12	Docket Number (if applicable)	04584.0168US01	Art Unit	2493
First Named Inventor	Mauritius Schmidtler			Examiner Name	LAVELLE, GARY E		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, to any international application that does not comply with the requirements of 35 U.S.C. 371, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV.

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☐ Other _____

☒ Enclosed

- ☒ Amendment/Reply
- ☐ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____ (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 132725

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

☐ Applicant Signature

PTO/SB/30EFS (07-14)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/David D. Harrell/	Date (YYYY-MM-DD)	2017-06-30
Name	David D. Harrell	Registration Number	71855

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

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

PTO/AIA/22 (03-13)
Approved for use through 7/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): 04584.0168US01

Application Number: 14/709,875

Filed: 2015-05-12

For: AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS

Art Unit: 2493

Examiner:

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

		Fee	Small Entity Fee	Micro Entity Fee	
☑	One month (37 CFR 1.17(a)(1))	$200	$100	$50	$ 200
☐	Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
☐	Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$
☐	Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐	Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

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

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 123735.

☑ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant.

☑ attorney or agent of record. Registration number 71855.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/David D. Harrell/ — Signature

06/30/2017 — Date

David D. Harrell — Typed or printed name

303-357-1242 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Electronic Patent Application Fee Transmittal

Application Number:	14709875
Filing Date:	12-May-2015
Title of Invention:	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS
First Named Inventor/Applicant Name:	Mauritius Schmidtler
Filer:	David Dwayne Harrell/Elizabeth Pallardy
Attorney Docket Number:	04584.0168US01

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

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

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 1 month with $0 paid	1251	1	200	200
Miscellaneous:				
RCE- 1st Request	1801	1	1200	1200
		Total in USD ($)		**1400**

Electronic Acknowledgement Receipt

EFS ID:	29666217
Application Number:	14709875
International Application Number:	
Confirmation Number:	1593
Title of Invention:	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS
First Named Inventor/Applicant Name:	Mauritius Schmidtler
Customer Number:	23552
Filer:	David Dwayne Harrell/Elizabeth Pallardy
Filer Authorized By:	David Dwayne Harrell
Attorney Docket Number:	04584.0168US01
Receipt Date:	30-JUN-2017
Filing Date:	12-MAY-2015
Time Stamp:	14:27:34
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$1400
RAM confirmation Number	070317INTEFSW14280800
Deposit Account	132725
Authorized User	Elizabeth Pallardy

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

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 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		04584_0168US01_RespFOA_03-24-17.PDF	149564 f6ba42da24cec6acd6c8cdf8b748624941586ff0	yes	16

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment Submitted/Entered with Filing of CPA/RCE	1	1
Claims	2	6
Applicant Arguments/Remarks Made in an Amendment	7	16

Warnings:

Information:

2	Request for Continued Examination (RCE)	04584_0168US01_RCE.PDF	256768 2bcd8f39a48edd0d327f3e1898f1d2a55084c44c	no	2

Warnings:

This is not a USPTO supplied RCE SB30 form.

Information:

3	Extension of Time	04584_0168US01_EOT.PDF	441860 78a0478965417776af6bc20bfca706f7ddf7a543	no	1

Warnings:

Information:

4	Fee Worksheet (SB06)	fee-info.pdf	32708 23497ee062899b386bb0a8a15bfac83a895b9cdf	no	2

Warnings:

Information:

Total Files Size (in bytes):	880900

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Mauritius Schmidtler et al.	Examiner:	Lavelle, Gary E.
Serial No.:	14/709,875	Group Art Unit:	2493
Filed:	May 12, 2015	Docket No.:	04584.0168US01
Title:	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS		

AMENDMENT & RESPONSE TO FINAL OFFICE ACTION

Mail Stop After Final
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Commissioner:

In response to the Final Office Action mailed March 24, 2017, please amend the above-identified application as follows:

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

Remarks/Arguments begin on page 7 of this paper.

Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (Currently Amended) A computer-implemented method comprising:

extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the static data points correspond to one or more points of reference used to evaluate the executable file, and wherein the one or more points of reference are defined by the executable file;

analyzing the executable file without decrypting or unpacking the executable file, wherein analyzing the executable file comprises applying a classifier to the plurality of static data points, wherein the classifier is trained from data that comprises known malicious executable files, known benign executable files and known unwanted executable files; and

determining whether the executable file is harmful based on the analysis.

2. (Original) The computer-implemented method according to claim 1, wherein the extracting the plurality of static data points further comprises classifying the extracted static data points according to a type of data extracted from the executable file, and encoding the extracted static data points for the classifier based on the classification.

3. (Original) The computer-implemented method according to claim 2, wherein analyzing the executable file further comprises generating a feature vector from the plurality of extracted static data points and evaluating the feature vector using support vector processing to determine whether the executable file is at least one of harmful, benign, and potentially unwanted.

4. (Original) The computer-implemented method according to claim 3, wherein generating the at least one feature vector comprises selectively setting features of the classifier based on the plurality of extracted static data points.

5. (Original) The computer-implemented method according to claim 4, wherein features of the feature vector are selectively turned on or off based on evaluation of whether a value of a static data point from the plurality of extracted static data points is within a predetermined range.

6. (Original) The computer-implemented method according to claim 2, wherein the classifying the at least one static data point comprises classifying the plurality of extracted static data points into categories comprising numeric values, nominal values, string or byte sequences, and Boolean values.

7. (Original) The computer-implemented method according to claim 6, wherein analyzing the executable file further comprises generating at least one feature vector from the plurality of extracted static data points, wherein features of the generated feature vector are weighted based at least upon the classified categories and the plurality of extracted static data points.

8. (Original) The computer-implemented method according to claim 1, wherein determining whether the executable file is harmful further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value.

9. (Original) The computer-implemented method according to claim 8, wherein the threshold value is set based on predetermined false positive range data.

10. (Currently Amended) A computer-readable storage device containing instructions, that when executed on at least one processor, causing the processor to execute a process comprising:

extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the static data points correspond to one or more points of reference used to evaluate the executable file, and wherein the one or more points of reference are defined by the executable file;

analyzing the executable file without decrypting or unpacking the executable file, wherein the analyzing the executable file comprises applying a classifier to the plurality of static

data points extracted, wherein the classifier is trained from data comprising known malicious executable files, known benign executable files and known unwanted executable files; and

determining whether the executable file is harmful based on the analyzing of the executable file.

11. (Original) The computer-readable storage device according to claim 10, wherein the extracting of the plurality of static data points executed by the processor further comprises classifying the extracted static data points according to a type of data extracted from the executable file, and encoding the extracted static data points for the classifier based on the classifying.

12. (Original) The computer-readable storage device according to claim 11, wherein analyzing the executable file further comprises generating at least one feature vector from the plurality of extracted static data points and evaluating the feature vector using linear or nonlinear support vector processing to determine whether the executable file is at least one of harmful, benign, and potentially unwanted.

13. (Original) The computer-readable storage device according to claim 12, wherein generating the at least one feature vector comprises selectively setting features of the classifier based on the plurality of extracted static data points.

14. (Original) The computer-readable storage device according to claim 13, wherein features of the feature vector are selectively turned on or off based on evaluation of whether a value of a static data point from the plurality of extracted static data points is within a predetermined range.

15. (Original) The computer-readable storage device according to claim 11, wherein the classifying the at least one static data point comprises classifying the plurality of extracted static data points into categories comprising numeric values, nominal values, string or byte sequences, and Boolean values.

16. (Original) The computer-readable storage device according to claim 15, wherein analyzing the executable file further comprises generating a feature vector from the plurality of extracted static data points, wherein features of the generated feature vector are weighted based at least upon the classified categories and the plurality of extracted static data points.

17. (Original) The computer-readable storage device according to claim 10, wherein determining whether the executable file is harmful further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value.

18. (Original) The computer-readable storage device according to claim 17, wherein the threshold value is set based on predetermined false positive range data.

19. (Currently Amended) A system comprising:

at least one memory; and

at least one processor operatively connected with the memory and configured to perform operation of:

extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the static data points correspond to one or more points of reference used to evaluate the executable file, and wherein the one or more points of reference are defined by the executable file;

analyzing the executable file without decrypting or unpacking the executable file, wherein the analyzing the executable file comprises applying a classifier to the plurality of static data points extracted, wherein the classifier is trained from data comprising known malicious executable files, known benign executable files and known unwanted executable files[[,]]; and

determining whether the executable file is harmful based on the analyzing of the executable file.

20. (Original) The system according to claim 19, wherein the determining further comprises preventing execution of the executable file when a determined probability value that the

executable file is harmful exceeds a threshold value, and wherein the threshold value is set based on predetermined false positive range data.

REMARKS/ARGUMENTS

This Amendment and the following remarks are intended to fully respond to the Final Office Action dated March 24, 2017, hereinafter "Office Action." In that Office Action, claims 1-20 were examined and all claims were rejected. Claims 1, 2, 10, 11 and 19 were rejected under 35 U.S.C. § 102(a)(2) as allegedly anticipated by Wojnowicz et al. (U.S. Pat. No. 9,465,940 hereinafter "Wojnowicz"). Claims 3, 4, 12 and 13 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Tuvell et al. (U.S. Pat. Publ. No. 2007/0240220; hereinafter "Tuvell"). Claims 5 and 14 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Tuvell, and further in view of Gilbert et al. (U.S. Pat. No. 9,197,663; hereinafter "Gilbert"). Claims 6 and 15 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Thomas et al. (U.S. Pat. Publ. No. 2012/0079596; hereinafter "Thomas"). Claims 7 and 16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Tuvell, and further in view of Thomas. Claims 8, 9, 17, 18 and 20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz in view of Gilbert.

Reconsideration of these rejections, as they might apply to the original and amended claims in view of these remarks, is respectfully requested. In this Amendment, claims 1, 10 and 19 have been amended, no claims have been canceled, and no claims have been added. Therefore, claims 1-20 remain present for examination.

Claim Rejections Under 35 U.S.C. § 102:

Claims 1, 2, 10, 11 and 19 were rejected under 35 U.S.C. § 102(a)(2) as allegedly anticipated by Wojnowicz. Applicants respectfully traverse this rejection because either the Examiner failed to state a *prima facie* case of anticipation or the current amendments to the claims now render the Examiner's arguments moot. "Anticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim." *Lindemann Mashinenfabrik GmbH v. Am. Hoist & Derrick Co.,* 730 F.2d 1452, 1458 (Fed. Cir. 1984); *see also,* MPEP § 2131. Applicants submit that the cited references do not disclose all of the elements of the rejected claims.

Non-limiting examples of the present application provide automatic threat detection of executable files based on static data analysis. In examples, a plurality of static data points may be extracted from an executable file without decrypting or unpacking the executable file. The executable file may then be analyzed without decrypting or unpacking the executable file. Analysis of the executable file may comprise applying a classifier to the plurality of extracted static data points. The classifier may be trained from data comprising known malicious executable files, known benign executable files and known unwanted executable files. Based upon analysis of the executable file, a determination can be made as to whether the executable file is harmful.

Wojnowicz relates to identifying malware using wavelet decomposition of software entropy. Specifically, Wojnowicz teaches receiving a set of data files. Each of the data files is to split into non-overlapping file chunks of fixed length. The non-overlapping file chunks are represented as an entropy time series that reflects an amount of entropy across the file chunks for each file. A wavelet transform is applied to the corresponding entropy time series to generate an energy spectrum characterizing, for the file, an amount of entropic energy at multiple scales of code resolution. A determination is then made as to whether the file is likely to be malicious based on the energy spectrum. *Wojnowicz*, col. 1, ll. 23-31.

Turning specifically to the claims, without acquiescing to the propriety of the rejection and solely for the purpose of advancing prosecution, Applicants have amended the independent claims. The amended independent claims clarify that the extracted data points correspond to points of reference (in the executable file) that are defined by the format of the executable file. For instance, amended claim 1 recites, *inter alia*, "extracting a plurality of static data points from an executable file … wherein the static data points correspond to one or more points of reference … *and wherein the one or more points of reference are defined by the executable file*" (emphasis added).

Wojnowicz does not teach, at least, "the one or more points of reference are defined by the executable file," as recited in amended claim 1. Wojnowicz teaches identifying whether executable files are malicious using entropy time series. The entropy time series represents the amount of entropy across locations in the file code and reflects the entropic energy at multiple

scales of code resolution. In operation, the entropy of a received executable file can be calculated by splitting the file "into non-overlapping chunks of fixed length, typically 256 bytes," and applying an entropy time series to the chunks. *Wojnowicz*, col. 6, ll. 7-8. Splitting the file into chunks includes identifying that an executable file can be represented as a string of hexadecimals (e.g., 00hFFh), and bundling the hexadecimal characters along a fixed length boundary (e.g., 256 bytes). *Id.*, col. 3, ll. 9-18. The statistical variation within a chunk can be estimated by computing the entropy in the chunk, such that zero entropy represents the same value repeatedly and maximum entropy represents entirely distinct values. Notably, the fixed length boundaries upon which the files are split do not correspond to particular sections, points of reference, or portions of the file. Nor are such boundaries representative of, or otherwise influenced by, the format/layout or content of the corresponding executable file. Instead, the boundaries simply occur randomly (with respect to the file content and format) throughout the file. In contrast, the present application teaches that static data points correspond to points of reference in a received executable file. The points of reference represent sections, subsections, or categories of an executable file:

> A static data point may be a point of reference used to evaluate an executable file. As examples, static data points include, but are not limited to: header information, section information, import and export information, certificate information, resource information, string and flag information, legal information, comments, and/or program information (e.g., APIs and DLLs), among other examples. Static data points may be organized into categories that identify a type of static data point. Categories of static data points comprise, but are not limited to: numeric values, nominal values string sequences, byte sequences, and/or Boolean values, among other examples.

Specification, para. [0017]. Although such points of reference may exist in the executable files processed in Wojnowicz, Wojnowicz does not teach or suggest the use of such points of reference in determining entropy. In fact, such points of reference are not taught or described in any meaning meaningful manner by Wojnowicz. Nor would Wojnowicz provide such a teaching, as the file chunks boundaries would ignore such points of reference; thereby, frustrating the techniques of the present application. As such, Wojnowicz provides no equivalent teachings of static data points or points of reference corresponding to the

format/layout of an executable file. Accordingly, Wojnowicz does not anticipate amended claim 1.

The other independent claims recite similar limitations and are allowable over the recited reference for at least the same or similar reasons. For example, amended claim 10 recites, *inter alia*:

> extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the static data points correspond to one or more points of reference used to evaluate the executable file, *and wherein the one or more points of reference are defined by the executable file*;

Amended claim 19 recites, *inter alia*:

> extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the static data points correspond to one or more points of reference used to evaluate the executable file, *and wherein the one or more points of reference are defined by the executable file*;

The dependent claims, i.e. claims 2 and 11, incorporate all of the limitations of the above independent claims, respectively, and are allowable over Wojnowicz for at least the same reasons. As such, Applicants respectfully request that the Examiner withdraw the rejection and allow claims 1, 2, 10, 11 and 19 at the Examiner's earliest convenience.

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

Claims 3, 4, 12 and 13

Claims 3, 4, 12 and 13 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Tuvell. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

Tuvell relates to a malware detection system. Specifically, Tuvell teaches a system for detecting malware on a limited access mobile platform in a mobile network. The system uses one or more feature sets that describe various non-executable portions of malware-infected and malware-free applications, and compares an application on the limited access mobile platform to the features sets. A match of the features in a suspect application to one of the feature sets provides an indication as to whether the suspect application is malware-infected or malware-free.

Claims 3, 4, 12 and 13 depend from claims 1 and 10, respectively. As previously discussed, claims 1 and 10 are allowable over Wojnowicz. Tuvell does not cure the deficiencies of Wojnowicz, nor does the Office Action refer to it for such. Instead, the Office Action refers to Tuvell as disclosing the use of a feature set comprising program information or features used to detect malware. *Office Action*, pp. 7, 9, 10. Without conceding to the correctness of this characterization, Applicants submit that Tuvell does not teach the above-recited limitations. For example, Tuvell does not teach at least identifying static data points, data points that correspond to one or more points of reference or section in a file, or using data points to evaluate the file by, for example, grouping the data points into categories and generating feature vectors based thereon. Thus, Tuvell fails to teach at least "the static data points correspond to one or more points of reference … defined by the executable file," as recited in amended claims 1 and 10. As such, Applicants respectfully request withdrawal of the rejections and allowance of claims 3, 4, 12 and 13 at the Examiner's earliest convenience.

Claims 5 and 14

Claims 5 and 14 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Tuvell, and further in view of Gilbert. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

Gilbert relates to identifying potential software threats based on visual and non-visual data. Specifically, Gilbert teaches analyzing visual and non-visual elements associated with the candidate files to determine whether the candidate files are malware. A visual element (e.g., icon) is extracted from the candidate file, and the icon's image is compared to a group of reference images associated with trusted entities. If the icon's image matches a reference image, the candidate file may be malware masquerading as trusted software. The non-visual elements associated with the candidate file are used, in combination with the visual elements, to determine whether the candidate file is malware.

Claims 5 and 14 depend from claims 1 and 10, respectively. As previously discussed, claims 1 and 10 are allowable over the combination of Wojnowicz and Tuvell. Gilbert does not cure their deficiencies, nor does the Office Action refer to it for such. Instead, the Office Action refers to Gilbert as disclosing the determination of whether the difference between the quantitative identity of an icon image and the quantitative identity of a reference image is less than a threshold difference. *Office Action*, pp. 10-11. Without conceding to the correctness of this characterization, Applicants submit that Gilbert does not teach the above-recited limitations. For example, Gilbert does not teach at least identifying static data points, data points that correspond to one or more points of reference or section in a file, or using data points to evaluate the file by, for example, grouping the data points into categories and generating feature vectors based thereon. Thus, Gilbert fails to teach at least "the static data points correspond to one or more points of reference … defined by the executable file," as recited in amended claims 1 and 10. As such, Applicants respectfully request withdrawal of the rejections and allowance of claims 5 and 14 at the Examiner's earliest convenience.

Claims 6 and 15

Claims 6 and 15 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz in view of Thomas. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424

F.2d 1382, 1385 (C.C.P.A. 1970). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

Thomas relates to a method and system for the automatic detection and analysis of malware. Specifically, Thomas teaches a method of detecting malicious software (malware) includes receiving a file and storing a memory baseline for a system. The method also includes copying the file to the system, executing the file on the system, terminating operation of the system, and storing a post-execution memory map. The method further includes analyzing the memory baseline and the post-execution memory map and determining that the file includes malware.

Claims 6 and 15 depend from claims 1 and 10, respectively. As previously discussed, claims 1 and 10 are allowable over Wojnowicz. Thomas does not cure the deficiencies of Wojnowicz, nor does the Office Action refer to it for such. Instead, the Office Action refers to Thomas as disclosing the identification and classification of malware families. *Office Action*, pp. 12-13. Without conceding to the correctness of this characterization, Applicants submit that Thomas does not teach the above-recited limitations. For example, Thomas does not teach at least identifying static data points, data points that correspond to one or more points of reference or section in a file, or using data points to evaluate the file by, for example, grouping the data points into categories and generating feature vectors based thereon. Thus, Thomas fails to teach at least "the static data points correspond to one or more points of reference … defined by the executable file," as recited in amended claims 1 and 10. As such, Applicants respectfully request withdrawal of the rejections and allowance of claims 6 and 15 at the Examiner's earliest convenience.

Claims 7 and 16

Claims 7 and 16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Tuvell, and further in view of Thomas. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at

the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

Claims 7 and 16 depend from claims 1 and 10, respectively. As previously discussed, claims 1 and 10 are allowable over the combinations of Wojnowicz and Tuvell and Wojnowicz and Thomas. The further combination of Wojnowicz, Tuvell and Thomas does not cure their deficiencies of the individual combinations. For example, as discussed above, neither Tuvell nor Thomas teaches identifying static data points, data points that correspond to one or more points of reference or section in a file, or using data points to evaluate the file. Thus, the recited references fail to teach at least "the static data points correspond to one or more points of reference … defined by the executable file," as recited in amended claims 1 and 10. As such, Applicants respectfully request withdrawal of the rejections and allowance of claims 7 and 16 at the Examiner's earliest convenience.

Claims 8, 9, 17, 18 and 20

Claims 8, 9, 17, 18 and 20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz in view of Gilbert. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

Claims 8, 9, 17, 18 and 20 depend from claims 1, 10 and 19, respectively. As previously discussed, claims 1, 10 and 19 are allowable over the combinations of Wojnowicz, Tuvell and Gilbert. Removing Tuvell from the combination does not cure their deficiencies of Wojnowicz and Gilbert. For example, as discussed above, the combination of Wojnowicz nor Gilbert does not teach identifying static data points, data points that correspond to one or more points of

reference or section in a file, or using data points to evaluate the file. Thus, the recited references fail to teach at least "the static data points correspond to one or more points of reference … defined by the executable file," as recited in amended claims 1, 10 and 19. As such, Applicants respectfully request withdrawal of the rejections and allowance of claims 8, 9, 17, 18 and 20 at the Examiner's earliest convenience.

CONCLUSION

This Amendment fully responds to the Office Action mailed on March 24, 2017. Still, that Office Action may contain arguments and rejections that are not directly addressed by this Amendment due to the fact that they are rendered moot in light of the preceding arguments in favor of patentability. Hence, failure of this Amendment to directly address an argument raised in the Office Action should not be taken as an indication that the Applicant believes the argument has merit. Furthermore, the claims of the present application may include other elements, not discussed in this Amendment, which are not shown, taught, or otherwise suggested by the references of record. Accordingly, the preceding arguments in favor of patentability are advanced without prejudice to other bases of patentability.

This Amendment is filed concurrently with a Petition for Extension of Time and Request for Continued Examination. It is believed that no further fees are due with this Response. However, the Commissioner is hereby authorized to charge any deficiencies or credit any overpayment with respect to this patent application to deposit account number 13-2725.

In light of the above remarks and amendments, it is believed that the application is now in condition for allowance and such action is respectfully requested. Should any additional issues need to be resolved, the Examiner is requested to telephone the undersigned to attempt to resolve those issues.

Respectfully submitted,

Dated: June 30, 2017

/David D. Harrell/

David D. Harrell, Reg. No. 71,855
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1242

23552
PATENT TRADEMARK OFFICE

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/709,875	Filing Date 05/12/2015	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

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

APPLICATION AS AMENDED – PART II

AMENDMENT 06/30/2017

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 20	Minus	** 20	=	X $ =	
Independent (37 CFR 1.16(h))	* 3	Minus	***3	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

AMENDMENT

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

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

LIE
PEGGY S. YARBOROUGH

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14709875
Filing Date	2015-05-12
First Named Inventor	Mauritius Schmidtler
Art Unit	2493
Examiner Name	LAVELLE, GARY E.
Attorney Docket Number	04584.0168US01

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

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

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14709875
	Filing Date	2015-05-12
	First Named Inventor	Mauritius Schmidtler
	Art Unit	2493
	Examiner Name	LAVELLE, GARY E.
	Attorney Docket Number	04584.0168US01

	1	International Patent Application No. PCT/US2016/032090, International Preliminary Report on Patentability mailed November 14, 2017, 7 pages.

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14709875
	Filing Date	2015-05-12
	First Named Inventor	Mauritius Schmidtler
	Art Unit	2493
	Examiner Name	LAVELLE, GARY E.
	Attorney Docket Number	04584.0168US01

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/David D. Harrell/	Date (YYYY-MM-DD)	2017-12-11
Name/Print	David D. Harrell	Registration Number	71855

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference 4584-168WO01	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/US2016/032090	International filing date *(day/month/year)* 12 May 2016 (12.05.2016)	Priority date *(day/month/year)* 12 May 2015 (12.05.2015)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant WEBROOT INC.		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 7 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☒	Box No. VIII	Certain observations on the international application

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 14 November 2017 (14.11.2017)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Authorized officer Athina Nickitas-Etienne e-mail: pct.team4@wipo.int

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2016/032090	12.05.2016	12.05.2015

International Patent Classification (IPC) or both national classification and IPC
INV. G06F21/56 G06F11/36 G06F9/44 ADD. G06F21/64 G06F21/62

Applicant
WEBROOT INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☒ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Fax: +49 89 2399 - 4465	see form PCT/ISA/210	Madzharova, Violeta Telephone No. +49 89 2399-0

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing:

   a. ☐ forming part of the international application as filed:

      ☐ in the form of an Annex C/ST.25 text file.

      ☐ on paper or in the form of an image file.

   b. ☐ furnished together with the international application under PCT Rule 13*ter*.1(a) for the purposes of international search only in the form of an Annex C/ST.25 text file.

   c. ☐ furnished subsequent to the international filing date for the purposes of international search only:

      ☐ in the form of an Annex C/ST.25 text file (Rule 13*ter*.1(a)).

      ☐ on paper or in the form of an image file (Rule 13*ter*.1(b) and Administrative Instructions, Section 713).

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that forming part of the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	4, 5, 7-9, 13, 14
	No:	Claims	1-3, 6, 10-12, 15-20
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-20
Industrial applicability (IA)	Yes:	Claims	1-20
	No:	Claims	

2. Citations and explanations

see separate sheet

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 Reference is made to the following documents:

D1 PERDISCI R ET AL: "Classification of packed executables for accurate computer virus detection", PATTERN RECOGNITION LETTERS, ELSEVIER, AMSTERDAM, NL, vol. 29, no. 14, 15 October 2008 (2008-10-15), pages 1941-1946, XP024520140, ISSN: 0167-8655, DOI: 10.1016/J.PATREC.2008.06.016 [retrieved on 2008-07-03]

D2 ROBERTO PERDISCI ET AL: "McBoost: Boosting Scalability in Malware Collection and Analysis Using Statistical Classification of Executables", COMPUTER SECURITY APPLICATIONS CONFERENCE, 2008. ACSAC 2008. ANNUAL, IEEE, PISCATAWAY, NJ, USA, 8 December 2008 (2008-12-08), pages 301-310, XP031376785, ISBN: 978-0-7695-3447-3

D3 US 2010/192222 A1 (STOKES JACK W [US] ET AL) 29 July 2010 (2010-07-29)

2 The present application does not meet the criteria of Article 33(2) PCT, because the subject-matter of **claim 1** is not new.

D1 discloses (references in parentheses referring to **D1**):

A computer-implemented method comprising:

extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file;	p. 1942, Fig. 1, Static PE Analysis of Executable, where determination is made whether the executable is packed or not packed; p. 1942, left col., l. 10-14: "*The objective is to accurately distinguish between*

	packed and non-packed executables, so that only the executables detected as packed will be sent to a ... universal unpacker for hidden code extraction, before being sent to the anti-virus software."; p. 1943, left col., l. 9-11: "... *approach ... do not need to to execute an application to detect if it contains packed executable code*."; p. 1945, Table 1, "*Summary of features extracted from PE files*", including number of standard vs. non-standard sections, entropy of header, code and data sections. It is well known to the skilled person in the field of malware analysis that PE file entropy is commonly used to asses whether a file is encrypted or not (see also p. 1944, right col., l. 6-9: "... *measure the byte entropy of the code and data sections in the PE file. If the entropy of a sections is close to 8 bits, which is the maximum byte entropy, the section likely contains encrypted code*.";
analyzing the executable file without decrypting or unpacking the executable file, wherein analyzing the executable file comprises applying a classifier to the plurality of static data points,	p. 1942, Fig. 1, PE file Classifier; p. 1943, left col., l. 11-14: "... *classification system extracts a number of features from executable files in PE format through static analysis ... used to classify packed executables without need to actually execute them*."; p. 1945, Table 1, "*Summary of features extracted from PE files*";

wherein the classifier is trained from data that comprises known malicious executable files, known benign executable files and known unwanted executable files; and	p. 1944, right col., section 4. "Experiments", wherein the training dataset comprises "*packed viruses*" (l. 24), "*non-packed benign executables*" (l. 25), and "*packed benign executables*" (l. 28);
determining whether the executable file is harmful based on the analysis.	p. 1942, Fig. 1, determination of packed vs. unpacked executable and subsequent determination whether it is a "*virus*" or "*benign*".

3 Referring to the objection raised above, independent **claims 10 and 19** are also not allowable for lack of novelty (Article 33(2) PCT) since their subject-matter corresponds to that of **claim 1**.

4 Furthermore, the **dependent claims 2-9**, **11-18 and 20** do not appear to contain any additional technical features which, either alone or in combination with the features of any claim to which they refer, render the present subject-matter novel (Article 33(2) PCT) or inventive (Article 33(3) PCT) since their features are either known from the prior art or merely represent minor implementation details to the person skilled in the art (see cited passages in the ISR, and in particular, for **claims 2 and 11** (classifying according to a type of extracted data), document **D1** (p. 1945, Table 1); for **claims 3 and 12** (generating a feature vector and using support vector processing), documents **D1** (p. 1942, left col., l. 41-42 and 51-53) and **D2** (p. 304, left col.); for **claims 7 and 16** (features of the feature vector being weighted), document **D3** (par. [0019], l. 3-6); for **claims 8 and 17** (preventing execution of the executable file when probability that file might be harmful exceeds a predetermined threshold value), document **D3** (par. [0032], l. 9-11).

Re Item VIII

Certain observations on the international application

5 It should be noted by the applicant that in certain jurisdictions, the expression "*without*" used in the wording of claim 1 might be regarded as being unclear, since it appears to comprise a negative limitation.

Electronic Acknowledgement Receipt

EFS ID:	31191884
Application Number:	14709875
International Application Number:	
Confirmation Number:	1593
Title of Invention:	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS
First Named Inventor/Applicant Name:	Mauritius Schmidtler
Customer Number:	23552
Filer:	David Dwayne Harrell/Elizabeth Pallardy
Filer Authorized By:	David Dwayne Harrell
Attorney Docket Number:	04584.0168US01
Receipt Date:	11-DEC-2017
Filing Date:	12-MAY-2015
Time Stamp:	17:42:06
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	04584_0168US01_2_SIDS.PDF	612025 96e9924195875bde7cd9c9823291d376dd99310b	no	4

Warnings:

Information:					
A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
2	Non Patent Literature	pct_iprp_pctus2016032090_Nov14-2017_7pgs.PDF	271463 f7fa004f6bba45e852d9f6500e397e39a8c06e7c	no	7
Warnings:					
Information:					
			Total Files Size (in bytes):	883488	

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/709,875	05/12/2015	Mauritius Schmidtler	04584.0168US01	1593

23552 7590 04/20/2018

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MINNESOTA 55402-0903
UNITED STATES OF AMERICA

EXAMINER
LAVELLE, GARY E

ART UNIT	PAPER NUMBER
2493	

NOTIFICATION DATE	DELIVERY MODE
04/20/2018	ELECTRONIC

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

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

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

USPTO23552@merchantgould.com

Office Action Summary	Application No. 14/709,875	Applicant(s) Schmidtler et al.	
	Examiner GARY E LAVELLE	Art Unit 2493	AIA Status Yes

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

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

Status

1)☑ Responsive to communication(s) filed on 6/30/2017.

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

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

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

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

Disposition of Claims*

5) ☑ Claim(s) 1-20 is/are pending in the application.

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

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-20 is/are rejected.

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

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

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

Application Papers

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

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

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

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

Priority under 35 U.S.C. § 119

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

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

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

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

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

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

Attachment(s)

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

2) ☑ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

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

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Continued Examination under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 6/30/2017 has been entered.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 12/11/2017 was filed after the mailing date of the application on 5/12/2015. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Status of Claims

4. In communications filed 6/30/2017 Applicants amend claims 1, 10, and 19. Claims 1-20 are pending.

Response to Arguments

5. With respect to claim 1, as amended, which recites in part "extracting a plurality of static data points from an executable … and wherein the static data points correspond to one or more points of reference … and wherein the one or more points of reference are defined by the executable file;" Applicants argue that Wojnowicz does not teach "and wherein the one or more points of reference are defined by the executable file;" as amended, because Wojnowicz calculates entropy by splitting a file into chunks. Applicant argues that the fixed length boundaries upon which the files are split do not correspond to particular sections, points of reference, or portions of the file. [Remarks/Arguments, page 7-9]

The Examiner respectfully disagrees because Wojnowicz splits the file into sections 256 byte apart, thus a point of reference is defined at each portion of the file located at each consecutive 256 byte location. Expressed differently, this point of reference is defined by the executable file because it is based upon the executable file and the number of sequential bytes counted in the executable file to define the each point. Therefor this argument is not persuasive.

Applicant continues this argument and states: Nor are such boundaries representative of, or otherwise influenced by, the format/layout or content of the corresponding executable file. [Remarks/Arguments, page 9, first paragraph]

The Examiner respectfully disagrees because the features upon which applicant relies (*i.e., boundaries and separately and additionally format/layout*) are not recited in the rejected claim(s).

Applicant continues this argument and states that in the present application, static data points correspond to points of reference in a received executable file. The points of reference represent sections, subsections, or categories of an executable file. Applicant cites specification paragraph [0017] for support. Applicant continues this argument and concludes that Wojnowicz does not teach static data points or points of reference corresponding to the format/layout of an executable file.

[Remarks/Arguments, page 9 continued on page 10]

The Examiner respectfully disagrees. Claim 1 recites in part "…the static data points correspond to one or more points of reference used to evaluate the executable file, and wherein the one or more points of reference are defined by the executable file;" (emphasis added). The recited "static data points" may correspond to the recited "one or more points of reference". Thus, it is apparent that the recited "static data points" are different entities than a claimed "point of reference". The specification further supports this interpretation. Specification paragraph [0017] indicates "A static data point may be a point of reference used to evaluate an executable file." While examples of "static data points" are provided by the specification, "point(s) of reference" appear to retain their ordinary meaning. The Applicant's disclosure does not appear to contain any disclosure of how the recited "one or more points of reference are defined by the executable file;" (emphasis added). Separately and in addition it is noted that the executable file may not be decrypted or unpacked thus hiding any encrypted or packed features of the executable file from evaluation. For these reasons the Examiner respectfully submits that Applicant's argument that points of reference represent sections, subsections, or

categories of an encrypted executable file and that points of reference corresponding to the format/layout of an executable file is not persuasive.

Applicant states that independent claims 10 and 19 have been amended to recite similar limitations and should be allowable for the same reasons. These arguments are not persuasive based upon the same rational.

Applicant argues with respect to dependent claims 3, 4, 12 and 13 that the reference of Tuvell does not overcome the alleged shortcomings of Wojnowicz for the same reasons. Applicants argue with respect to dependent claims 5 and 14 that the references of Tuvell and Gilbert do not overcome the alleged shortcomings of Wojnowicz for the same reasons. Applicants argue with respect to dependent claims 6 and 15 that the reference of Thomas does not overcome the alleged shortcomings of Wojnowicz for the same reasons. Applicants argue with respect to dependent claims 7 and 16 that the references of Tuvell and Thomas do not overcome the alleged shortcomings of Wojnowicz for the same reasons. Applicants argue with respect to dependent claims 8, 9, 17, 18 and 20 that the reference of Gilbert does not overcome the alleged shortcomings of Wojnowicz for the same reasons. These arguments are not persuasive based upon the same rational as discussed above with regard to the teachings of Wojnowicz and as discussed in the claim analysis below.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the first paragraph of 35 U.S.C. 112(a):

> (a) IN GENERAL.—The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

7. **Claims 1-20** are rejected under 35 U.S.C. 112(a) as failing to comply with the enablement requirement. The claims contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

Exemplary **claim 1** recites in part "...the static data points correspond to one or more points of reference used to evaluate the executable file, and wherein the one or more points of reference are defined by the executable file;" (emphasis added). The recited "static data points" may correspond to the recited "one or more points of reference". Thus, it is apparent that the recited "static data points" are different entities than a claimed "point of reference". The specification further supports this interpretation. Specification paragraph [0017] indicates "A static data point may be a point of reference used to evaluate an executable file." While examples of "static data points" are provided by the specification, "point(s) of reference" appear to retain their ordinary meaning. The Applicant's disclosure does not appear to contain any disclosure of how the recited "one or more points of reference are defined by the executable file;" (emphasis added). This claimed feature would not be expected to be apparent to one skilled in the art additionally because the executable file may be both encrypted and packed. Therefore, the claimed "one or more points of reference are defined by the executable file;" (emphasis added) fails to comply with the enablement requirement.

Independent **claims 10 and 19** recite substantially similar subject matter and are rejected based upon the same rational. Dependent **claims 2-9, 11-18 and 20** inherently

contain the features of the respective independent claims and are likewise rejected under 35 U.S.C. 112(a).

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a)(2) the claimed invention was described in a patent issued under section 151, or in an application for patent published or deemed published under section 122(b), in which the patent or application, as the case may be, names another inventor and was effectively filed before the effective filing date of the claimed invention.

9. **Claims 1, 2, 10, 11 and 19** are rejected under 35 U.S.C. 102(a)(2) as being anticipated by Wojnowicz et al. (U.S. Patent No. 8,709,924) hereinafter Wojnowicz.

With respect to **claim 1**, Wojnowicz teach "a computer-implemented method" (computer systems include one or more data processors and memory storing instructions that cause at least one processor to perform one or more of operations [column 1, lines 57-67]) "comprising:

extracting a plurality of static data points (chunks of code) from an executable file without decrypting or unpacking the executable file, wherein the static data points correspond to one or more points of reference used to evaluate the executable file, and wherein the one or more points of reference are defined by the executable file;" (The current subject matter addresses the issue of detecting malicious commands within portable executable files that are encrypted or compressed [column 2, lines 37-40]. The current subject matter is particularly useful for malware files that contain encrypted or compressed ("packed") segments which conceal malicious commands. Entropy

analysis can be used in this regard [column 3, lines 1-6] and [abstract]. An entropy time series (ETS) is constructed for each file. To compute the entropy of an executable file, the original file, represented in hexadecimal (00hFFh), can be split into non-overlapping chunks of fixed length, typically 256 bytes (*i.e. points defined by the original executable file*). For each chunk of code, the entropy can then be computed [column 6, lines 4-26] and Fig. 1 and associated text. The current subject matter is particularly useful for malware files that contain encrypted or compressed ("packed") segments which conceal malicious commands. Entropy analysis can be used in this regard because files with high entropy are relatively likely to have encrypted or compressed sections inside them. *Thus, it is apparent that static data points are used without decrypting or unpacking.* In the context of software analysis, an executable file can be represented as a string of hexadecimals (00hFFh), where each observed hexadecimal character is considered to be an instantiation of a random variable (for example, with 256 possible values). A string of these hexadecimal characters can be bundled up into a "chunk" of a file, and the statistical variation within that chunk can be estimated by computing the entropy within the chunk. Zero entropy means that the same character was repeated over and over (as might occur in a "padded" chunk of code) and maximum entropy means that a chunk consisted of entirely distinct values. Chunks of code that have been compressed or encrypted tend to have higher entropy than native code [column 3, lines 1-23].

"analyzing the executable file without decrypting or unpacking the executable file," (The current subject matter provides enhanced techniques for identifying malicious commands within code that are compressed and/or encrypted [column 2, lines 37-40]

and [column 3, lines 1-3]. Entropy analysis can be used in this regard [column 3, lines 3-6] and [abstract]. See also [column 3, lines 45-59].

"wherein analyzing the executable file comprises applying a classifier to the plurality of static data points," (Based on entropic energy spectrum, a suspiciously structured entropy score (SSES) was derived. SSES can be combined with any number of additional features in a malware classifier. An entropy time series can characterize the amount of entropy over a chunk of code in a certain location of the file. The amount of entropic structure can then be quantified [column 2, line 50 through column 3, line 23] and [column 3, lines 32-38]. Wavelet-based classifiers may be used [column 5, lines 7-65]).

"wherein the classifier is trained from data that comprises known malicious executable files, known benign executable files and known unwanted executable files;" (The determination of whether nor not a file is likely to be malicious can be accomplished by generating, using at least one predictive model trained using data sets comprising files known to contain malware. Files having a score above a pre-defined threshold are determined to be likely malicious and files having a score below the pre-defined threshold are determined to be not likely malicious [column 1, lines 32-39]. The data set comprised n=39,968 portable executable files from a data repository. 19,988 (50.01%) of these files were known to be malicious, and the remaining files were benign [column 5, line 66 through column 6, line 3]. *It is apparent that malicious executable malware is "unwanted"* [column 1, lines 23-31] and [column 1, lines 13-19].

"and

determining whether the executable file is harmful based on the analysis." (The determination of whether nor not a file is likely to be malicious can be accomplished by generating, using at least one predictive model trained using data sets comprising files known to contain malware. A suspiciously structured entropy score for each file such that files having a score above a pre-defined threshold are determined to be likely malicious [column 1, lines 32-39]).

With respect to **claim 2**, Wojnowicz teach "the computer-implemented method according to claim 1, wherein the extracting the plurality of static data points further comprises classifying the extracted static data points according to a type of data (file size) extracted from the executable file," (A wavelet based classifier strategy may use wavelet coefficients as features in a classifier. Such wavelet coefficients can be used as features within any machine learning or statistical classifier, for example, logistic regression or lasso logistic regression, decision trees, support vector machines, etc. [column 5, lines 8-16]. Two files A & B belonging to the same file size category [column 8, lines 11-17 and 25-28] and Fig. 2). "and

encoding the extracted static data points for the classifier based on the classification." (Data points may be pooled together into a "bin" and indexed *j* and *k* [column 6, lines 63-66] (*i.e. encoding*) Files A and B are placed in file size group J=5 [column 8, lines 48-50] and see Fig.2 and related text).

Claims 10 and 11 are computer-readable storage device versions of the method of Wojnowicz as discussed the analysis of claims 1 and 2 above and the claims are rejected on that basis.

Claim 19 is a system version of the method of Wojnowicz as discussed the analysis of claim 1 above and the claim is rejected on that basis.

Claim Rejections - 35 USC § 103

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

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102 of this title, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

11. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103 are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.

3. Resolving the level of ordinary skill in the pertinent art.

4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

12. **Claims 3, 4, 12 and 13** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wojnowicz in view of Tuvell et al. (U.S. Publication No. 2007/0240220).

With respect to **claim 3**, Wojnowicz teach the claimed subject matter as discussed in the analysis of claim 2 above the rejection of which is incorporated herein. In addition, Wojnowicz describes the use of wavelet-based classifiers and indicates that

wavelet coefficients can be used as features within any machine learning or statistical classifier (logistic regression or lasso logistic regression, decision trees, support vector machines, etc.) [column 5, lines 9-15] and also discussed with regard to claim 1 above. Therefore, Wojnowicz teach "using support vector processing to determine whether the executable file is at least one of harmful, benign, and potentially unwanted." but may not specifically disclose "wherein analyzing the executable file further comprises generating a feature vector from the plurality of extracted static data points and evaluating the feature vector".

Tuvell, from the same or similar field of endeavor, teach "wherein analyzing the executable file further comprises generating a feature vector from the plurality of extracted static data points" (The information used to detect malware comprises a feature set selected from the list comprising program information or features such as file name, file size, vendor of the program and version of the program (*e.g. static data points*) [0104]. A feature set of the following three feature elements DLL1, DLL2, DLL3 and an input executable that contained only DLL1 and DLL3, the feature vector is 1 0 1. Then, the probability of that specific executable being a virus with the feature vector 1 0 1 is then computed [0161]. See also [0336] and Fig. 9) "and

evaluating the feature vector using support vector processing to determine whether the executable file is at least one of harmful, benign, and potentially unwanted." (For example, with a feature set of the following three feature elements DLL1, DLL2, DLL3 and an input executable that contained only DLL1 and DLL3, the feature vector is 1 0 1. Then, the probability of that specific executable being a virus with the feature vector 1 0 1 is then computed [0161]. Probabilities are computed from the training data.

Once the probabilities are calculated, a target executable is classified as a virus according to the probability model [0162]. A data structure is created 716 which nominally is one or more feature vectors describing the presence or absence of each feature element associated with each of the malware profiles. The feature vectors are compared to the malware profiles to determine if malware is present in a target application [0163] and Fig. 7. See also [0323], [0336] and Fig. 9. Once a malware feature set is sufficiently complete, two probability models are created 910 based on the feature sets: one for malware and the other for benign or malware-free programs. With these probability models, it is possible to compare 918 a target application with the probability models and distinguish malware-infected from malware-free programs [0323].)

Tuvell is analogous art directed to a system and method for detecting malware [abstract]. Based upon Wojnowicz in view of Tuvell it would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to utilize the teachings of Tuvell within the method of Wojnowicz with the motivation of improving malware detection of polymorphic viruses that change their signatures every time they replicate (see Tuvell, [0009]) and also to improve operation on systems with limited storage and processing capacity (see Tuvell, [0011]) and also because all of the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination would have yielded predictable results to one of ordinary skill in the art at the time of the invention.

With respect to **claim 4**, Wojnowicz in view of Tuvell teach the claimed subject matter as discussed in the analysis of claim 3 above the rejection of which is incorporated herein. In addition, Tuvell teach "wherein generating the at least one feature vector comprises selectively setting features of the classifier based on the plurality of extracted static data points." (The information used to detect malware comprises a feature set selected from the list comprising program information or features such as file name, file size, vendor of the program and version of the program (*e.g. static data points*) [0104]. Each of the feature elements in a pre-defined feature set are derived 916 from the target application. The result is represented in a binary feature set vector, or feature vector, with a "1" indicating that the procedure is present in the searched executable, and a "0" otherwise [0336] and Fig. 9. For example, feature set of the following three feature elements DLL1, DLL2, DLL3 and an input executable that contained only DLL1 and DLL3, the feature vector is 1 0 1 [0161]) with the same motivation as discussed in the analysis of claim 3 above.

Claims 12 and 13 are computer-readable storage device versions of the method of Wojnowicz and Tuvell as discussed the analysis of claims 3 and 4, respectively above, and the claims are rejected on that basis.

13. **Claims 5 and 14** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wojnowicz in view of Tuvell and further in view of Gilbert et al. (U.S. Patent No. 9,197,663) hereinafter Gilbert.

With respect to **claim 5**, Wojnowicz in view of Tuvell teach the claimed subject matter including "wherein features of the feature vector are selectively turned on or off

based on evaluation of"…"a value of a static data point" as discussed in the analysis of claim 4 above the rejection of which is incorporated herein but may not specifically disclose "based on evaluation of whether a value of a static data point from the plurality of extracted static data points is within a predetermined range."

Gilbert, from the same or similar field of endeavor, teach "evaluation of whether a value of a static data point from the plurality of extracted static data points is within a predetermined range." (Gilbert identifies malware by combining an analysis of visual and non-visual information associated with the software packages. The non-visual elements can include data identifying a publisher, filenames, external function calls, registered operating system functions, operating system filenames, registry key, system file value, application filenames, library filenames, file size, provider, vendor tags and path names. The visual elements can include an icon (*i.e. static data points*) [column 2, lines 17-20 and 47-52]. Performing the comparison of the icon image and the reference image may involve determining whether the difference between the quantitative identity of the icon image and the quantitative identity of the reference image is less than a threshold difference (*i.e. a range*) [column 3, lines 26-30]. See also [column 20, lines 44-61].

Gilbert is analogous art directed to candidate files which are analyzed to determine whether the candidate files are malware [abstract]. Based upon Wojnowicz in view of Tuvell in view of Gilbert it would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to utilize the teachings of Gilbert within the method of Wojnowicz and Tuvell with the motivation of improving the issues of privacy and data security and also to avoid detrimental effects on the

operation of the computer and/or network on which it resides and also because the transmission and operation of the spyware consume bandwidth and memory and also because users often experience a degradation in system performance, instability, and even total system failure (See Gilbert [column 4, line 64 through column 5, line 3]) and also because all of the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination would have yielded predictable results to one of ordinary skill in the art at the time of the invention.

Claim 14 is a computer-readable storage device version of the method of Wojnowicz and Tuvell as discussed the analysis of claim 5 above and the claim is rejected on that basis.

14. **Claims 6 and 15** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wojnowicz in view of Thomas et al. (U.S. Publication No. 2012/0079596) hereinafter Thomas.

With respect to **claim 6**, Wojnowicz teach the claimed subject matter as discussed in the analysis of claim 2 above the rejection of which is incorporated herein but may not specifically disclose "wherein the classifying the at least one static data point comprises classifying the plurality of extracted static data points into categories comprising numeric values, nominal values, string or byte sequences, and Boolean values."

Thomas, from the same or similar field of view, teach "wherein the classifying the at least one static data point comprises classifying the plurality of extracted static

data points into categories" (The malware detection and analysis system can identify and classify malware families. [0239]) “comprising numeric values” (file size [0175], [0225] and [0272]), “nominal values” (file type [0038], [0175], [0225] and [0272], and resource, [0191, table 4] and [0257]), “string or byte sequences” (original file [0250] and section name [0191, table 4], imports, exports [0195 and Fig. 8], original file name and comments [0250], [0251] and [0267]), “and Boolean values” (Boolean values [0062] and [0078], entry point [0095], resource and section name [0191, table 4] and [0269]).

Thomas is analogous art directed to detecting malicious software/malware [abstract]. Based upon Wojnowicz in view of Thomas it would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to utilize the classification of Thomas within the method of Wojnowicz with the same motivation as discussed in the analysis of claim 3 above and also with the motivation of providing the improvement of allowing the analysis to go much deeper into the heart of the operating system while not being disruptive since operation occurs on a memory dump once the system is frozen or powered down to detect attempts for malware to hide in the stealthiest ways (see Thomas, [0023]) and also because Wojnowicz indicates that SSES can be combined with any number of additional features in a malware classifier of choice [column 2, lines 63-64].

Claim 15 is a computer-readable storage device version of the method of Wojnowicz and Thomas as discussed the analysis of claim 6 above and the claim is rejected on that basis.

15. **Claims 7 and 16** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wojnowicz in view of Tuvell and further in view of Thomas.

With respect to **claim 7**, Wojnowicz in view of Tuvell in view of Thomas teach the claimed subject matter including the classification of the plurality of extracted static data points as discussed in the analysis of claim 6 above the rejection of which is incorporated herein. In addition, Tuvell teach "wherein analyzing the executable file further comprises generating at least one feature vector from the plurality of extracted static data points," (The information used to detect malware comprises a feature set selected from the list comprising program information or features such as file name, file size, vendor of the program and version of the program (*e.g. static data points*) [0104]. Each of the feature elements in a pre-defined feature set are derived 916 from the target application. The result is represented in a binary feature set vector, or feature vector, with a "1" indicating that the procedure is present in the searched executable, and a "0" otherwise [0336] and Fig. 9. For example, feature set of the following three feature elements DLL1, DLL2, DLL3 and an input executable that contained only DLL1 and DLL3, the feature vector is 1 0 1 [0161]).

"wherein features of the generated feature vector are weighted based at least upon the classified categories and the plurality of extracted static data points." (The heuristic rules are derived from a classification [0020]. Wherein said rule comprises one or more weights, each said weight assigned to a feature element [claim 6]) with the same motivation as discussed in the analysis of claims 3 and 6 above.

Claim 16 is a computer-readable storage device version of the method of Wojnowicz, Tuvell and Thomas as discussed the analysis of claim 7 above and the claim is rejected on that basis.

16. **Claims 8, 9, 17, 18 and 20** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wojnowicz in view of Gilbert.

With respect to **claim 8**, Wojnowicz teach the claimed subject matter as discussed in the analysis of claim 1 above the rejection of which is incorporated herein. In addition, Wojnowicz teach "wherein determining whether the executable file is harmful further comprises…when a determined probability value that the executable file is harmful exceeds a threshold value." (Files having a score above a pre-defined threshold are determined to be likely malicious [column 1, lines 32-39]) but does not specifically disclose "preventing execution of the executable file".

Gilbert, from the same or similar field of endeavor, teach "preventing execution of the executable file" (Anti-virus and anti-spyware software detects, quarantines, and in some cases removes software, such as malware, that is malicious in nature and generally unwanted from a computer or computer [column 2, lines 17-28]).

Gilbert is analogous art directed to candidate files which are analyzed to determine whether the candidate files are malware [abstract]. Based upon Wojnowicz in view of Gilbert it would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to quarantine or eliminate the files of Gilbert within the method of Wojnowicz with the motivation of improving the issues of privacy and data security and also to avoid detrimental effects on the operation of the computer and/or network on which it resides and also because the transmission and operation of the spyware consume bandwidth and memory and also because users often experience a degradation in system performance, instability, and even total system failure (See Gilbert [column 4, line 64 through column 5, line 3]).

With respect to **claim 9**, Wojnowicz in view of Gilbert teach the claimed subject matter as discussed in the analysis of claim 8 above the rejection of which is incorporated herein. In addition, Gilbert teach "wherein the threshold value is set based on predetermined false positive range data." (The threshold value may be tuned, automatically or manually, based on the performance of malware identification system 100, for example, malware detection rate, false positive rate, etc. The threshold value may be set such that two images are determined to match when the difference between the images is less than approximately 40%, (i.e. *a range*) for example, the threshold value may be set to 0.4 [column 9, lines 21-34]) with the same motivation as discussed in the analysis of claim 8 above and also because all of the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination would have yielded predictable results to one of ordinary skill in the art at the time of the invention.

The limitations of **claims 17, 18 and 20** are rejected in the analysis of claims 8 and 9 above and the claims are rejected on that basis.

Conclusion

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to GARY E LAVELLE whose telephone number is (571)270-7575 and whose direct facsimile number is 571 270-8575. The examiner can normally be reached on M-Th 9-6 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Carl Colin can be reached on 571 272-3862. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

18. 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.

Gary Lavelle
Examiner, Art Unit 2493
/gl/
/CARL G COLIN/
Supervisory Patent Examiner, Art Unit 2493

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/709,875	Schmidtler et al.
	Examiner	**Art Unit**
	GARY E LAVELLE	2493

CPC - Searched*		
Symbol	**Date**	**Examiner**
G06F21/565, G06F99/005 and G06F221/033	11/27/2016	Gary Lavelle

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	**Date**	**Examiner**
Inventor search	11/27/2016	Gary Lavelle
NPL search (Google, ACM and IEEE with seach terms including: malware | malicious | virus, classify, static data points, feature vector, packed, encrypted...)	11/25/2016	Gary Lavelle
East search (see attached search history listing)	11/27/2016	Gary Lavelle
Inventor search updated	3/19/2017	Gary Lavelle
NPL search updated (Google, ACM and IEEE with new search terms including: static reference points...)	3/19/2017	Gary Lavelle
East search (see attached search history listing)	3/20/2017	Gary Lavelle
Inventor search updated	04/16/2018	Gary Lavelle
NPL search above updated (Google, ACM and IEEE with new search terms including: define file points of reference...)	04/10/2018	Gary Lavelle
G06F21/565, G06F99/005 and G06F221/033 EAST search updated (see attached search history listing included with this form to determine the scope of search)	04/16/2018	Gary Lavelle

	/GARY LAVELLE/ Examiner.Art Unit 2493

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/709,875	Schmidtler et al.
	Examiner	Art Unit
	GARY E LAVELLE	2493

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

	/GARY LAVELLE/ Examiner.Art Unit 2493

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/709,875	Schmidtler et al.
	Examiner	**Art Unit**
	GARY E LAVELLE	2493

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

CLAIMS

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

CLAIM		DATE								
Final	Original	11/27/2016	03/16/2017	04/16/2018						
	1	✓	✓	✓						
	2	✓	✓	✓						
	3	✓	✓	✓						
	4	✓	✓	✓						
	5	✓	✓	✓						
	6	✓	✓	✓						
	7	✓	✓	✓						
	8	✓	✓	✓						
	9	✓	✓	✓						
	10	✓	✓	✓						
	11	✓	✓	✓						
	12	✓	✓	✓						
	13	✓	✓	✓						
	14	✓	✓	✓						
	15	✓	✓	✓						
	16	✓	✓	✓						
	17	✓	✓	✓						
	18	✓	✓	✓						
	19	✓	✓	✓						
	20	✓	✓	✓						

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14709875
Filing Date	2015-05-12
First Named Inventor	Mauritius Schmidtler
Art Unit	2493
Examiner Name	LAVELLE, GARY E.
Attorney Docket Number	04584.0168US01

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

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

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14709875
	Filing Date	2015-05-12
	First Named Inventor	Mauritius Schmidtler
	Art Unit	2493
	Examiner Name	LAVELLE, GARY E.
	Attorney Docket Number	04584.0168US01

/G.E.L/	1	International Patent Application No. PCT/US2016/032090, International Preliminary Report on Patentability mailed November 14, 2017, 7 pages.

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

EXAMINER SIGNATURE

Examiner Signature	/GARY E LAVELLE/	Date Considered	04/16/2018

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14709875
Filing Date	2015-05-12
First Named Inventor	Mauritius Schmidtler
Art Unit	2493
Examiner Name	LAVELLE, GARY E.
Attorney Docket Number	04584.0168US01

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/David D. Harrell/	Date (YYYY-MM-DD)	2017-12-11
Name/Print	David D. Harrell	Registration Number	71855

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	59	((Mauritius) near2 (Schmidtler)).INV.	US-PGPUB; USPAT	NEAR	ON	2018/04/16 13:35
L2	5	((Mauritius) near2 (Schmidtler)).INV. and (classif$5 or categor$5) and (malware or malicious or virus)	US-PGPUB; USPAT	NEAR	ON	2018/04/16 13:36
L3	2	((Gaurav) near2 (Dalal)).INV.	US-PGPUB; USPAT	NEAR	ON	2018/04/16 13:38
L4	2	((Reza) near2 (Yoosoofmiya)).INV.	US-PGPUB; USPAT	NEAR	ON	2018/04/16 13:39
L5	3	(G06F21/565 or G06F99/005 or G06F221/033).cpc. (reference or(static with data)) adj point and (@pd or @ptad or @prad or @ad or @rlad)<"20151205"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2018/04/16 13:42
L6	5170	(decrypt$5 or unpack$5) (reference or(static with data))adj point and (@pd or @ptad or @prad or @ad or @rlad) <"20151205"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2018/04/16 13:44
L7	201	(decrypt$5 or unpack$5) (classif$6 or categor$6)same train$4 (reference or(static with data))adj point and (@pd or @ptad or @prad or @ad or @rlad)<"20151205"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2018/04/16 13:49
L8	54	(malware or virus or harmful or unsafe)same (file or program or application)(decrypt$5 or unpack$5) (classif$6 or categor$6)same train$4 (reference or(static with data))adj point and (@pd or @ptad or @prad or @ad or @rlad)<"20151205"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2018/04/16 13:54
L9	16	(G06F21/565 or G06F99/005 or G06F221/033).cpc. and (malware or malicious or virus) and weight$5 and feature adj vector and(classif$5 or categor$5)and (header section import export certificate resource string flag legal comment program API DLL)and (@pd or @ptad or @prad or @ad or @rlad) <"20151205"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/04/16 14:12
L10	12	(G06F21/565 or G06F99/005 or G06F221/033).cpc. and (malware or malicious or virus) and weight$5 and feature adj vector and(classif$5 or	US-PGPUB; USPAT; USOCR; FPRS;	OR	ON	2018/04/16 14:14

		categor$5)and (header section import export certificate resource string flag legal comment program API DLL)and (decrypt$5 or encrypt$5) and (@pd or @ptad or @prad or @ad or @rlad)<"20151205" and referenc$4	EPO; JPO; DERWENT; IBM_TDB			
L11	4	(G06F21/565 or G06F99/005 or G06F221/033).cpc. and (Numeric adj values file adj size linker adj version code adj size OS adj version image adj version subsystem adj version file adj version adj number size adj of adj stackr size adj of file adj OS adj image "PE header time" Section adj Entropy section adj count)and (Nominal adj values initialize Un-initialize entry adj point subsystem file adj subtype language file adj flags adj masks file adj flags product adj name size adj of adj heapr file adj type machine adj type PE adj type Sections adj count DLL adj count DLL adj functions data adj directory export adj count "Earliest Data Byte" resources resources adj language resource adj Encoding resource adj code adj page resource adj size DLL adj characteristics resource adj size DLL adj characteristics) and (Strings/Byte adj sequences Comments company adj name file adj descriptioninternal adj name legal adj copyright original adj file private adj build special adj build product adj version file adj version package adj code product adj code export adj DLL adj name assembly adj version "Certificate Issuer" Certificate adj Subject Imports Exports Section adj Names non-resource adj section adj strings non-resource adj section adj strings) and (Boolean adj values "Address Of Entry Point Anomaly" Image adj Base adj Anomaly "Section Alignment Anomaly" "Size Of Code Mismatch Anomaly" "Low Import Count Anomaly" "Entry Point Anomaly" certificate adj Validity Certificate adj Exception "Code Characteristics Anomaly" "Code Name Anomaly" Count adj Anomaly "Data Characteristics Anomaly" Data adj Name adj Anomaly Export adj Exception "Large Number of DLLs Anomaly" "flag DLL Name Anomaly" "Number of Functions Anomaly" "Function Name Anomaly" "PE Header Anomaly" "High Section Count Anomaly" "PE Magic Validity" Resource adj Exception "VR Code Ratio Anomaly" Import adj Exception) and (@pd or @ptad or @prad or @ad or @rlad)<"20151205"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/04/16 14:16

EAST Search History (Interference)

< This search history is empty>

4/ 16/ 2018 2:21:37 PM
C:\ Users\ glavelle\ Documents\ EAST\ Workspaces\ 14709875.wsp

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Mauritius Schmidtler et al.	Examiner:	Lavelle, Gary E.
Serial No.:	14/709,875	Group Art Unit:	2493
Filed:	May 12, 2015	Docket No.:	04584.0168US01
Title:	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS		

AMENDMENT & RESPONSE TO NON-FINAL OFFICE ACTION

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

Dear Commissioner:

In response to the Non-Final Office Action mailed April 20, 2018, please amend the above-identified application as follows:

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

Remarks/Arguments begin on page 7 of this paper.

Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (Currently Amended) A computer-implemented method comprising:

extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein one or more of the plurality of static data points ~~correspond to~~ are ~~one or more~~ points of reference representing sections of the executable file, ~~used to evaluate the executable file, and~~ wherein the ~~one or more~~ points of reference are used to evaluate ~~defined by~~ the executable file;

analyzing the executable file without decrypting or unpacking the executable file, wherein analyzing the executable file comprises applying a classifier to the plurality of static data points, wherein the classifier is trained from data that comprises known malicious executable files, known benign executable files and known unwanted executable files; and

determining whether the executable file is harmful based on the analysis.

2. (Original) The computer-implemented method according to claim 1, wherein the extracting the plurality of static data points further comprises classifying the extracted static data points according to a type of data extracted from the executable file, and encoding the extracted static data points for the classifier based on the classification.

3. (Original) The computer-implemented method according to claim 2, wherein analyzing the executable file further comprises generating a feature vector from the plurality of extracted static data points and evaluating the feature vector using support vector processing to determine whether the executable file is at least one of harmful, benign, and potentially unwanted.

4. (Original) The computer-implemented method according to claim 3, wherein generating the at least one feature vector comprises selectively setting features of the classifier based on the plurality of extracted static data points.

5. (Original) The computer-implemented method according to claim 4, wherein features of the feature vector are selectively turned on or off based on evaluation of whether a value of a static data point from the plurality of extracted static data points is within a predetermined range.

6. (Original) The computer-implemented method according to claim 2, wherein the classifying the at least one static data point comprises classifying the plurality of extracted static data points into categories comprising numeric values, nominal values, string or byte sequences, and Boolean values.

7. (Original) The computer-implemented method according to claim 6, wherein analyzing the executable file further comprises generating at least one feature vector from the plurality of extracted static data points, wherein features of the generated feature vector are weighted based at least upon the classified categories and the plurality of extracted static data points.

8. (Original) The computer-implemented method according to claim 1, wherein determining whether the executable file is harmful further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value.

9. (Original) The computer-implemented method according to claim 8, wherein the threshold value is set based on predetermined false positive range data.

10. (Currently Amended) A computer-readable storage device containing instructions, that when executed on at least one processor, causing the processor to execute a process comprising:

extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein one or more of the plurality of static data points ~~correspond to~~ are ~~one or more~~ points of reference representing sections of the executable file, ~~used to evaluate the executable file, and~~ wherein the ~~one or more~~ points of reference are used to evaluate ~~defined by~~ the executable file;

analyzing the executable file without decrypting or unpacking the executable file, wherein the analyzing the executable file comprises applying a classifier to the plurality of static data points extracted, wherein the classifier is trained from data comprising known malicious executable files, known benign executable files and known unwanted executable files; and

determining whether the executable file is harmful based on the analyzing of the executable file.

11. (Original) The computer-readable storage device according to claim 10, wherein the extracting of the plurality of static data points executed by the processor further comprises classifying the extracted static data points according to a type of data extracted from the executable file, and encoding the extracted static data points for the classifier based on the classifying.

12. (Original) The computer-readable storage device according to claim 11, wherein analyzing the executable file further comprises generating at least one feature vector from the plurality of extracted static data points and evaluating the feature vector using linear or nonlinear support vector processing to determine whether the executable file is at least one of harmful, benign, and potentially unwanted.

13. (Original) The computer-readable storage device according to claim 12, wherein generating the at least one feature vector comprises selectively setting features of the classifier based on the plurality of extracted static data points.

14. (Original) The computer-readable storage device according to claim 13, wherein features of the feature vector are selectively turned on or off based on evaluation of whether a value of a static data point from the plurality of extracted static data points is within a predetermined range.

15. (Original) The computer-readable storage device according to claim 11, wherein the classifying the at least one static data point comprises classifying the plurality of extracted static data points into categories comprising numeric values, nominal values, string or byte sequences, and Boolean values.

16. (Original) The computer-readable storage device according to claim 15, wherein analyzing the executable file further comprises generating a feature vector from the plurality of extracted static data points, wherein features of the generated feature vector are weighted based at least upon the classified categories and the plurality of extracted static data points.

17. (Original) The computer-readable storage device according to claim 10, wherein determining whether the executable file is harmful further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value.

18. (Original) The computer-readable storage device according to claim 17, wherein the threshold value is set based on predetermined false positive range data.

19. (Currently Amended) A system comprising:

at least one memory; and

at least one processor operatively connected with the memory and configured to perform operation of:

extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein one or more of the plurality of static data points ~~correspond to~~ are ~~one or more~~ points of reference representing sections of the executable file, ~~used to evaluate the executable file, and~~ wherein the ~~one or more~~ points of reference are used to evaluate ~~defined by~~ the executable file;

analyzing the executable file without decrypting or unpacking the executable file, wherein the analyzing the executable file comprises applying a classifier to the plurality of static data points extracted, wherein the classifier is trained from data comprising known malicious executable files, known benign executable files and known unwanted executable files; and

determining whether the executable file is harmful based on the analyzing of the executable file.

20. (Original) The system according to claim 19, wherein the determining further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value, and wherein the threshold value is set based on predetermined false positive range data.

REMARKS/ARGUMENTS

This Amendment and the following remarks are intended to fully respond to the Non-Final Office Action dated April 20, 2018, hereinafter "Office Action." In that Office Action, claims 1-20 were examined and all claims were rejected. Claims 1-20 were rejected under 35 U.S.C. § 112, first paragraph, for allegedly failing to comply with the enablement requirement. Claims 1, 2, 10, 11 and 19 were rejected under 35 U.S.C. § 102(a)(2) as allegedly anticipated by Wojnowicz et al. (U.S. Pat. No. 9,465,940 hereinafter "Wojnowicz"). Claims 3, 4, 12 and 13 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Tuvell et al. (U.S. Pat. Publ. No. 2007/0240220; hereinafter "Tuvell"). Claims 5 and 14 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Tuvell, and further in view of Gilbert et al. (U.S. Pat. No. 9,197,663; hereinafter "Gilbert"). Claims 6 and 15 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Thomas et al. (U.S. Pat. Publ. No. 2012/0079596; hereinafter "Thomas"). Claims 7 and 16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Tuvell, and further in view of Thomas. Claims 8, 9, 17, 18 and 20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz in view of Gilbert.

Reconsideration of these rejections, as they might apply to the original and amended claims in view of these remarks, is respectfully requested. In this Amendment, claims 1, 10 and 19 have been amended, and no claims have been canceled or added. Therefore, claims 1-20 remain present for examination.

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

Claims 1-20 were rejected under 35 U.S.C. § 112, first paragraph, for allegedly failing to comply with the enablement requirement. Specifically, the Office Action alleges that the present application does not appear to disclose how the points of reference are defined by the executable file. *Office Action*, pg. 6. The independent claims have been amended to recite "wherein one or more of the plurality of static data points are points of reference *representing sections* of the executable file" (emphasis added). Support for this amendment can be found at least in

paragraph [0017] of the specification. In light of this amendment, Applicants respectfully request that Examiner withdraw the rejection and allow claims 1-20.

Claim Rejections Under 35 U.S.C. § 102:

Claims 1, 2, 10, 11 and 19 were rejected under 35 U.S.C. § 102(a)(2) as allegedly anticipated by Wojnowicz. Applicants respectfully traverse this rejection because either the Examiner failed to state a *prima facie* case of anticipation or the current amendments to the claims now render the Examiner's arguments moot. "Anticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim." *Lindemann Mashinenfabrik GmbH v. Am. Hoist & Derrick Co.,* 730 F.2d 1452, 1458 (Fed. Cir. 1984); *see also,* MPEP § 2131. Applicants submit that the cited references do not disclose all of the elements of the rejected claims.

Non-limiting examples of the present application provide automatic threat detection of executable files based on static data analysis. In examples, a plurality of static data points may be extracted from an executable file without decrypting or unpacking the executable file. The executable file may then be analyzed without decrypting or unpacking the executable file. Analysis of the executable file may comprise applying a classifier to the plurality of extracted static data points. The classifier may be trained from data comprising known malicious executable files, known benign executable files and known unwanted executable files. Based upon analysis of the executable file, a determination can be made as to whether the executable file is harmful.

Turning specifically to the claims, without acquiescing to the propriety of the rejection and solely for the purpose of advancing prosecution, Applicants have amended the independent claims. The amended independent claims clarify that the data points extracted from the executable file are points of reference representing sections of the executable file, such as headers, section tables, etc. For instance, claim 1 as amended recites, *inter alia*, "extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein one or more of the plurality of static data points are points of reference

representing sections of the executable file, wherein the points of reference are used to evaluate the executable file."

Wojnowicz does not teach, at least, "wherein one or more of the plurality of static data points are points of reference representing sections of the executable file, wherein the points of reference are used to evaluate the executable file," as recited in claim 1 as amended. Wojnowicz a method for identifying malware using wavelet decomposition of software entropy. In the method, each of the data file in a set of received data files is split into non-overlapping file chunks of fixed length. The non-overlapping, fixed length file chunks are represented as an entropy time series that reflects an amount of entropy across the file chunks for each file. A wavelet transform is applied to the corresponding entropy time series to generate an energy spectrum characterizing, for the file, an amount of entropic energy at multiple scales of code resolution. A determination is then made as to whether the file is likely to be malicious based on the energy spectrum. *Wojnowicz*, col. 1, ll. 23-31. Notably, the fixed length boundaries upon which the files are split do not correspond to particular sections of the file. Nor are such boundaries representative of, or otherwise influenced by, the format/layout or content of the corresponding executable file. For example, a portable executable (PE) file comprising a DOS header section, a fields section, and a data directories section will not be divided along boundaries corresponding to those particular sections. Instead, each of the sections may be split into various chunks, some of which may comprise data from different sections of the file. The individual chunks, thus, do not represent sections of the file, and are not influenced (except coincidentally) by the format, layout or content of the corresponding executable file.

In contrast, the present application teaches that static data points are points of reference in a received executable file. The points of reference represent sections, subsections, or categories of an executable file:

> A static data point may be a point of reference used to evaluate an executable file. As examples, static data points include, but are not limited to: header information, section information, import and export information, certificate information, resource information, string and flag information, legal information, comments, and/or program information (e.g., APIs and DLLs), among other examples. Static data points may be organized into categories that identify a type of static data point. Categories of static data points comprise, but are not limited to: numeric

> values, nominal values string sequences, byte sequences, and/or Boolean values, among other examples.

Specification, para. [0017]. Although such points of reference may exist in the executable files processed in Wojnowicz, Wojnowicz does not describe the identification of such points of reference, or suggest the use of such points of reference in determining entropy. Nor would Wojnowicz provide such a teaching, as the file chunks boundaries would ignore such points of reference; thereby, frustrating the techniques of the present application. As such, Wojnowicz provides no equivalent teachings of static data points that are points of reference representing sections of an executable file. Accordingly, Wojnowicz does not anticipate claim 1 as amended.

The other independent claims recite similar limitations and are allowable over the recited reference for at least the same or similar reasons. For example, claim 10 as amended recites, *inter alia*:

> extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein one or more of the plurality of static data points are points of reference representing sections of the executable file, wherein the points of reference are used to evaluate the executable file

Claim 19 as amended recites, *inter alia*:

> extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein one or more of the plurality of static data points are points of reference representing sections of the executable file, wherein the points of reference are used to evaluate the executable file

The dependent claims, i.e. claims 2 and 11, incorporate all of the limitations of the above independent claims, respectively, and are allowable over Wojnowicz for at least the same reasons. As such, Applicants respectfully request that the Examiner withdraw the rejection and allow claims 1, 2, 10, 11 and 19 at the Examiner's earliest convenience.

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

Claims 3, 4, 12 and 13

Claims 3, 4, 12 and 13 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Tuvell. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

Claims 3, 4, 12 and 13 depend from claims 1 and 10, respectively. As previously discussed, claims 1 and 10 are allowable over Wojnowicz. Tuvell does not cure the deficiencies of Wojnowicz, nor does the Office Action refer to it for such. Tuvell relates to a system for detecting malware on a limited access mobile platform in a mobile network. The system uses feature sets describing various non-executable portions of malware-infected and malware-free applications, and compares an application on the limited access mobile platform to the features sets. A match of the features in a suspect application to one of the feature sets provides an indication as to whether the suspect application is malware-infected or malware-free. *Tuvell*, para. [0019]. The Office Action refers to Tuvell as disclosing the use of a feature set to detect malware. *Office Action*, pg. 12. Without conceding to the correctness of this characterization, Applicants submit that Tuvell does not teach the above-recited limitations. For example, Tuvell does not teach identifying static data points that are points of reference to sections in a file, or using data points to evaluate a file by grouping the static data points into categories and generating feature vectors based thereon. Thus, Tuvell fails to teach at least "wherein one or more of the plurality of static data points are points of reference representing sections of the executable file, wherein the points of reference are used to evaluate the executable file," as recited in claims 1 and 10 as amended. As such, Applicants respectfully request withdrawal of the rejections and allowance of claims 3, 4, 12 and 13 at the Examiner's earliest convenience.

Claims 5 and 14

Claims 5 and 14 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Tuvell, and further in view of Gilbert. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

Claims 5 and 14 depend from claims 1 and 10, respectively. As previously discussed, claims 1 and 10 are allowable over the combination of Wojnowicz and Tuvell. Gilbert does not cure their deficiencies, nor does the Office Action refer to it for such. Gilbert teaches a method for analyzing visual and non-visual elements associated with candidate data files to determine whether the files are malware. In the method, a visual element (e.g., icon) is extracted from the candidate file, and the icon's image is compared to a group of reference images associated with trusted entities. If the icon's image matches a reference image, the candidate file may be malware masquerading as trusted software. The non-visual elements associated with the candidate file are used, in combination with the visual elements, to determine whether the candidate file is malware. *Gilbert*, col. 2, ll. 29-46. The Office Action refers to Gilbert as disclosing the determination of whether the difference between the quantitative identity of an icon image and the quantitative identity of a reference image is less than a threshold difference. *Office Action*, pg. 15. Without conceding to the correctness of this characterization, Applicants submit that Gilbert does not teach the above-recited limitations. For example, Gilbert does not teach identifying static data points that are points of reference to sections in a file, or using data points to evaluate a file by grouping the static data points into categories and generating feature vectors based thereon. Thus, Gilbert fails to teach at least "wherein one or more of the plurality of static data points are points of reference representing sections of the executable file, wherein the points of reference are used to evaluate the executable file," as recited in claims 1 and 10 as

amended. As such, Applicants respectfully request withdrawal of the rejections and allowance of claims 5 and 14 at the Examiner's earliest convenience.

Claims 6 and 15

Claims 6 and 15 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Thomas. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

Claims 6 and 15 depend from claims 1 and 10, respectively. As previously discussed, claims 1 and 10 are allowable over Wojnowicz. Thomas does not cure the deficiencies of Wojnowicz, nor does the Office Action refer to it for such. Thomas teaches a method of detecting malicious software (malware), which includes receiving a file and storing a memory baseline for a system. The method also includes copying the file to the system, executing the file on the system, terminating operation of the system, and storing a post-execution memory map. The memory baseline and the post-execution memory map are then analyzed and determination is made as to whether the file includes malware. *Thomas*, para. [0005]. The Office Action refers to Thomas as disclosing the identification and classification of malware families. *Office Action*, pp. 16-17. Without conceding to the correctness of this characterization, Applicants submit that Thomas does not teach the above-recited limitations. For example, Thomas does not teach identifying static data points that are points of reference to sections in a file, or using data points to evaluate a file by grouping the static data points into categories and generating feature vectors based thereon. Thus, Thomas fails to teach at least "wherein one or more of the plurality of static data points are points of reference representing sections of the executable file, wherein the points of reference are used to evaluate the executable file," as recited in claim 1 as amended. As such, Applicants respectfully request withdrawal of the rejections and allowance of claims 6 and 15 at the Examiner's earliest convenience

Claims 7 and 16

Claims 7 and 16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Tuvell, and further in view of Thomas. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

Claims 7 and 16 depend from claims 1 and 10, respectively. As previously discussed, claims 1 and 10 are allowable over the combinations of Wojnowicz and Tuvell and Wojnowicz and Thomas. The further combination of Wojnowicz, Tuvell and Thomas does not cure their deficiencies of the individual combinations. For example, as discussed above, neither Tuvell nor Thomas teaches identifying static data points that are points of reference to sections in a file, or using data points to evaluate a file by grouping the static data points into categories and generating feature vectors based thereon. Thus, the recited references fail to teach at least "wherein one or more of the plurality of static data points are points of reference representing sections of the executable file, wherein the points of reference are used to evaluate the executable file," as recited in claims 1 and 10 as amended. As such, Applicants respectfully request withdrawal of the rejections and allowance of claims 7 and 16 at the Examiner's earliest convenience.

Claims 8, 9, 17, 18 and 20

Claims 8, 9, 17, 18 and 20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz in view of Gilbert. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made.

M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

Claims 8, 9, 17, 18 and 20 depend from claims 1, 10 and 19, respectively. As previously discussed, claims 1, 10 and 19 are allowable over the combinations of Wojnowicz, Tuvell and Gilbert. Removing Tuvell from the combination does not cure their deficiencies of Wojnowicz and Gilbert. For example, as discussed above, the combination of Wojnowicz nor Gilbert does not teach identifying static data points that are points of reference to sections in a file, or using data points to evaluate a file by grouping the static data points into categories and generating feature vectors based thereon. Thus, the recited references fail to teach at least "wherein one or more of the plurality of static data points are points of reference representing sections of the executable file, wherein the points of reference are used to evaluate the executable file," as recited in amended claims 1, 10 and 19 as amended. As such, Applicants respectfully request withdrawal of the rejections and allowance of claims 8, 9, 17, 18 and 20 at the Examiner's earliest convenience.

CONCLUSION

This Amendment fully responds to the Office Action mailed on April 20, 2018. Still, that Office Action may contain arguments and rejections that are not directly addressed by this Amendment due to the fact that they are rendered moot in light of the preceding arguments in favor of patentability. Hence, failure of this Amendment to directly address an argument raised in the Office Action should not be taken as an indication that the Applicant believes the argument has merit. Furthermore, the claims of the present application may include other elements, not discussed in this Amendment, which are not shown, taught, or otherwise suggested by the references of record. Accordingly, the preceding arguments in favor of patentability are advanced without prejudice to other bases of patentability.

This Amendment is filed concurrently with a Petition for Extension of Time. It is believed that no further fees are due with this Response. However, the Commissioner is hereby authorized to charge any deficiencies or credit any overpayment with respect to this patent application to deposit account number 13-2725.

In light of the above remarks and amendments, it is believed that the application is now in condition for allowance and such action is respectfully requested. Should any additional issues need to be resolved, the Examiner is requested to telephone the undersigned to attempt to resolve those issues.

Respectfully submitted,

Dated: September 20, 2018

/David D. Harrell/

David D. Harrell, Reg. No. 71,855
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1242

27488
PATENT TRADEMARK OFFICE

PTO/SB/22 (03-13)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): 04584.0168US01

Application Number: 14/709,875

Filed: 05-12-2015

For: AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS

Art Unit: 1593

Examiner: LAVELLE, GARY E

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☑ Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$ 600
☐ Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$
☐ Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐ Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

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

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 132725.

☑ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71. 37 CFR 3.73(b) statement is enclosed (Form PTO/SB/96).

☑ attorney or agent of record. Registration number 71855.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/David D. Harrell/ — Signature

2018-09-20 — Date

David D. Harrell — Typed or printed name

303-357-1242 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Privacy Act Statement

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

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

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

Electronic Patent Application Fee Transmittal

Application Number:	14709875
Filing Date:	12-May-2015
Title of Invention:	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS
First Named Inventor/Applicant Name:	Mauritius Schmidtler
Filer:	David Dwayne Harrell
Attorney Docket Number:	04584.0168US01

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

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

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 2 months with $0 paid	1252	1	600	600
Miscellaneous:				
			Total in USD ($)	**600**

Electronic Acknowledgement Receipt

EFS ID:	33784518
Application Number:	14709875
International Application Number:	
Confirmation Number:	1593
Title of Invention:	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS
First Named Inventor/Applicant Name:	Mauritius Schmidtler
Customer Number:	23552
Filer:	David Dwayne Harrell
Filer Authorized By:	
Attorney Docket Number:	04584.0168US01
Receipt Date:	20-SEP-2018
Filing Date:	12-MAY-2015
Time Stamp:	17:31:54
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$600
RAM confirmation Number	092118INTEFSW17325200
Deposit Account	132725
Authorized User	Elizabeth Pallardy

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

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 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		04584_0168US01_RespNFOA.PDF	151630 0db6a5c1e1beabb8025718937704611d0ec81dd9	yes	16

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Claims	2	6
Applicant Arguments/Remarks Made in an Amendment	7	16

Warnings:					
Information:					
2	Extension of Time	04584_0168US01_EOT.PDF	186229 029e31661c99433736fdbd44bc6450f581d91324	no	2
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30830 b5871b6fd82610d8de9af121e3cabcfa641629f8	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	368689		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
14/709,875	05/12/2015	

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

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

APPLICATION AS AMENDED – PART II

AMENDMENT **09/20/2018**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	X $100 =	0
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $460 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

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

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

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

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

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

SLIE
SHARON M. WEST

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/709,875	05/12/2015	Mauritius Schmidtler	04584.0168US01	1593

23552 7590 01/24/2019

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
LAVELLE, GARY E	

ART UNIT	PAPER NUMBER
2493	

NOTIFICATION DATE	DELIVERY MODE
01/24/2019	ELECTRONIC

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

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

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

USPTO23552@merchantgould.com

Office Action Summary	Application No. 14/709,875	Applicant(s) Schmidtler et al.	
	Examiner GARY E LAVELLE	Art Unit 2493	AIA Status Yes

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

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

Status

1)☑ Responsive to communication(s) filed on 20 September 2018.

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

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

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

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

Disposition of Claims*

5) ☑ Claim(s) 1-20 is/are pending in the application.

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

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-20 is/are rejected.

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

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

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

Application Papers

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

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

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

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

Priority under 35 U.S.C. § 119

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

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

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

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

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

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

Attachment(s)

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

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

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

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Status of claims

2. In communication filed 9/20/2018 Applicant amends claims 1, 10 and 19. Claims 1-20 are pending.

Response to Arguments

3. Applicant's arguments filed 9/20/2018 have been carefully considered.

4. The rejection of claims 1-20 under 35 USC § 112(a) have been withdrawn in view of the amendment.

5. With regard to claim 1, Applicant argues that Wojnowicz does not teach "wherein one or more of the plurality of static data points are points of reference representing sections of the executable file, wherein the points of reference are used to evaluate the executable file;" as recited in the claim as amended. Applicant notes that in Wojnowicz the fixed length boundaries upon which the files are split do not correspond to particular sections of the file. Nor are such boundaries representative of, or otherwise influenced by, the format/layout or content of the corresponding executable file. Applicant states that a selected example of a portable executable (PE) file comprising a DOS header section, a fields section, and a data directories section will not be divided

along boundaries corresponding to those particular sections and indicates that in Wojnowicz each of the sections may be split into various chunks, some of which may comprise data from different sections of the file. Applicant argues that for this reason the individual chunks of Wojnowicz do not represent sections of the file, and are not influenced (except coincidentally) by the format, layout or content of the corresponding executable file. Applicant's state that the points of reference in the present application represent sections, subsections or categories of an executable file.

Applicant presents a selected portion of the specification, para. [0017], [Remarks/Arguments, p. 9, last paragraph continued on p. 10]. Applicant concludes that although points of reference may exist in the executable files processed in Wojnowicz, Wojnowicz does not describe the identification of such points of reference, or suggest the use of such points of reference in determining entropy. Applicant argues that Wojnowicz would not provide such a teaching, as the file chunks boundaries would ignore such points of reference; thereby, frustrating the techniques of the present application. As such, Wojnowicz provides no equivalent teachings of static data points that are points of reference representing sections of an executable file. Accordingly, Wojnowicz does not anticipate claim 1 as amended. See [Remarks/Arguments, pp. 8 - 10].

The Examiner respectfully disagrees. The Applicant's specification indicates that the "executable file" may be a single encrypted file (for example, byte sequences of the original executable file which has been encrypted and packed) [0017-0018] including Table 1.1. It is noted that the chunks of code disclosed by Wojnowicz are encrypted or compressed ("packed") segments of an executable file. The Examiner respectfully

submits that, as such, the cited prior art teach the limitation argued by the Applicant. There is no indication in the claim that the sections of the recited "points of reference" are split at particular sections which perform a specific function or purpose, nor does the Examiner find such a requirement for the recited "section" in the instant specification.

Furthermore, and in addition, the Applicant's disclosure does not appear to disclose how such section identification and section specific splitting could be performed on an encrypted file without decrypting and/or for a packed file without unpacking.

Therefore, in response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., sections of the executable file corresponding to sections which perform a specific function or purpose, for example, the argued sections of the file influenced by the format, layout or content of the corresponding executable file [Remarks/Arguments, p. 9, first full paragraph] are not recited in the rejected claim(s). Furthermore, this argued premise is not supported by the specification. Rather, the Applicant's specification indicates that static data points may include, as examples, string information, program information and byte sequences [0017] as taught by the string of hexadecimal characters bundled into the chunk of Wojnowicz and utilized for entropy analysis [column 3, lines 1-23 and claim analysis below]. For these reasons, Applicant's arguments above are not persuasive.

Applicant submits that the other independent claims, specifically claims 10 and 19, recite similar limitations and should be allowable for the same or similar reasons. Applicant argues that claim 2 which depends from claim 1 and claim 11 which depends

from claim 10 incorporate the limitations of their respective independent claim and should be allowable for the same or similar reasons. See [Remarks/Arguments, p.10].

This argument is not persuasive for the same rational discussed with regard to claim 1, above.

With respect to dependent claims 3-9, 12-18 and 20, the claims stand rejected under 35 USC § 103(a) as being unpatentable under Wojnowicz in view of additional cited prior art of record. Applicant argues that each of the individual combinations do not overcome the alleged deficiencies of Wojnowicz. See [Remarks/Arguments, pp. 11 -16].

Applicant's arguments are not persuasive in view of the teachings of Wojnowicz based upon the same rational discussed with regard to claim 1, above and the rejections are maintained.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a)(2) the claimed invention was described in a patent issued under section 151, or in an application for patent published or deemed published under section 122(b), in which the patent or application, as the case may be, names another inventor and was effectively filed before the effective filing date of the claimed invention.

7. **Claims 1, 2, 10, 11 and 19** are rejected under 35 U.S.C. 102(a)(2) as being anticipated by Wojnowicz et al. (U.S. Patent No. 8,709,924) hereinafter Wojnowicz.

With respect to **claim 1**, Wojnowicz teach "a computer-implemented method" (computer systems include one or more data processors and memory storing

instructions that cause at least one processor to perform one or more of operations [column 1, lines 57-67]) "comprising:

extracting a plurality of static data points (chunks of code) from an executable file without decrypting or unpacking the executable file, wherein one or more of the plurality of static data points are points of reference representing sections of the executable file, wherein the points of reference are used to evaluate the executable file;" (The current subject matter addresses the issue of detecting malicious commands within portable executable files that are encrypted or compressed [column 2, lines 37-40]. The current subject matter is particularly useful for malware files that contain encrypted or compressed ("packed") segments which conceal malicious commands. Entropy analysis can be used in this regard [column 3, lines 1-6] and [abstract]. An entropy time series (ETS) is constructed for each file. To compute the entropy of an executable file, the original file, represented in hexadecimal (00hFFh), can be split into non-overlapping chunks of fixed length, typically 256 bytes (*i.e. points defined by the original executable file*). For each chunk of code, the entropy can then be computed [column 6, lines 4-26] and Fig. 1 and associated text. The current subject matter is particularly useful for malware files that contain encrypted or compressed ("packed") segments which conceal malicious commands. Entropy analysis can be used in this regard because files with high entropy are relatively likely to have encrypted or compressed sections inside them. *Thus, it is apparent that static data points are used without decrypting or unpacking*. In the context of software analysis, an executable file can be represented as a string of hexadecimals (00hFFh), where each observed hexadecimal character is considered to be an instantiation of a random variable (for example, with 256 possible values). A

string of these hexadecimal characters can be bundled up into a "chunk" of a file, and the statistical variation within that chunk can be estimated by computing the entropy within the chunk. Zero entropy means that the same character was repeated over and over (as might occur in a "padded" chunk of code) and maximum entropy means that a chunk consisted of entirely distinct values. Chunks of code that have been compressed or encrypted tend to have higher entropy than native code [column 3, lines 1-23].

"analyzing the executable file without decrypting or unpacking the executable file," (The current subject matter provides enhanced techniques for identifying malicious commands within code that are compressed and/or encrypted [column 2, lines 37-40] and [column 3, lines 1-3]. Entropy analysis can be used in this regard [column 3, lines 3-6] and [abstract]. See also [column 3, lines 45-59].

"wherein analyzing the executable file comprises applying a classifier to the plurality of static data points," (Based on entropic energy spectrum, a suspiciously structured entropy score (SSES) was derived. SSES can be combined with any number of additional features in a malware classifier. An entropy time series can characterize the amount of entropy over a chunk of code in a certain location of the file. The amount of entropic structure can then be quantified [column 2, line 50 through column 3, line 23] and [column 3, lines 32-38]. Wavelet-based classifiers may be used [column 5, lines 7-65]).

"wherein the classifier is trained from data that comprises known malicious executable files, known benign executable files and known unwanted executable files;" (The determination of whether nor not a file is likely to be malicious can be accomplished by generating, using at least one predictive model trained using data sets

comprising files known to contain malware. Files having a score above a pre-defined threshold are determined to be likely malicious and files having a score below the pre-defined threshold are determined to be not likely malicious [column 1, lines 32-39]. The data set comprised n=39,968 portable executable files from a data repository. 19,988 (50.01%) of these files were known to be malicious, and the remaining files were benign [column 5, line 66 through column 6, line 3]. *It is apparent that malicious executable malware is "unwanted"* [column 1, lines 23-31] and [column 1, lines 13-19].

"and

determining whether the executable file is harmful based on the analysis." (The determination of whether nor not a file is likely to be malicious can be accomplished by generating, using at least one predictive model trained using data sets comprising files known to contain malware. A suspiciously structured entropy score for each file such that files having a score above a pre-defined threshold are determined to be likely malicious [column 1, lines 32-39]).

With respect to **claim 2**, Wojnowicz teach "the computer-implemented method according to claim 1, wherein the extracting the plurality of static data points further comprises classifying the extracted static data points according to a type of data (file size) extracted from the executable file," (A wavelet based classifier strategy may use wavelet coefficients as features in a classifier. Such wavelet coefficients can be used as features within any machine learning or statistical classifier, for example, logistic regression or lasso logistic regression, decision trees, support vector machines, etc. [column 5, lines 8-16]. Two files A & B belonging to the same file size category [column 8, lines 11-17 and 25-28] and Fig. 2). "and

encoding the extracted static data points for the classifier based on the classification." (Data points may be pooled together into a "bin" and indexed *j* and *k* [column 6, lines 63-66] (*i.e. encoding*) Files A and B are placed in file size group J=5 [column 8, lines 48-50] and see Fig.2 and related text).

Claims 10 and 11 are computer-readable storage device versions of the method of Wojnowicz as discussed the analysis of claims 1 and 2 above and the claims are rejected on that basis.

Claim 19 is a system version of the method of Wojnowicz as discussed the analysis of claim 1 above and the claim is rejected on that basis.

Claim Rejections - 35 USC § 103

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

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102 of this title, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

9. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103 are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.

3. Resolving the level of ordinary skill in the pertinent art.

4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

10. **Claims 3, 4, 12 and 13** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wojnowicz in view of Tuvell et al. (U.S. Publication No. 2007/0240220).

With respect to **claim 3**, Wojnowicz teach the claimed subject matter as discussed in the analysis of claim 2 above the rejection of which is incorporated herein. In addition, Wojnowicz describes the use of wavelet-based classifiers and indicates that wavelet coefficients can be used as features within any machine learning or statistical classifier (logistic regression or lasso logistic regression, decision trees, support vector machines, etc.) [column 5, lines 9-15] and also discussed with regard to claim 1 above. Therefore, Wojnowicz teach "using support vector processing to determine whether the executable file is at least one of harmful, benign, and potentially unwanted." but may not specifically disclose "wherein analyzing the executable file further comprises generating a feature vector from the plurality of extracted static data points and evaluating the feature vector".

Tuvell, from the same or similar field of endeavor, teach "wherein analyzing the executable file further comprises generating a feature vector from the plurality of extracted static data points" (The information used to detect malware comprises a feature set selected from the list comprising program information or features such as file name, file size, vendor of the program and version of the program (*e.g. static data points*) [0104]. A feature set of the following three feature elements DLL1, DLL2, DLL3 and an input executable that contained only DLL1 and DLL3, the feature vector is 1 0 1.

Then, the probability of that specific executable being a virus with the feature vector 1 0 1 is then computed [0161]. See also [0336] and Fig. 9) "and

evaluating the feature vector using support vector processing to determine whether the executable file is at least one of harmful, benign, and potentially unwanted." (For example, with a feature set of the following three feature elements DLL1, DLL2, DLL3 and an input executable that contained only DLL1 and DLL3, the feature vector is 1 0 1. Then, the probability of that specific executable being a virus with the feature vector 1 0 1 is then computed [0161]. Probabilities are computed from the training data. Once the probabilities are calculated, a target executable is classified as a virus according to the probability model [0162]. A data structure is created 716 which nominally is one or more feature vectors describing the presence or absence of each feature element associated with each of the malware profiles. The feature vectors are compared to the malware profiles to determine if malware is present in a target application [0163] and Fig. 7. See also [0323], [0336] and Fig. 9. Once a malware feature set is sufficiently complete, two probability models are created 910 based on the feature sets: one for malware and the other for benign or malware-free programs. With these probability models, it is possible to compare 918 a target application with the probability models and distinguish malware-infected from malware-free programs [0323].)

Tuvell is analogous art directed to a system and method for detecting malware [abstract]. Based upon Wojnowicz in view of Tuvell it would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to utilize the teachings of Tuvell within the method of Wojnowicz with the motivation of

improving malware detection of polymorphic viruses that change their signatures every time they replicate (see Tuvell, [0009]) and also to improve operation on systems with limited storage and processing capacity (see Tuvell, [0011]) and also because all of the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination would have yielded predictable results to one of ordinary skill in the art at the time of the invention.

With respect to **claim 4**, Wojnowicz in view of Tuvell teach the claimed subject matter as discussed in the analysis of claim 3 above the rejection of which is incorporated herein. In addition, Tuvell teach "wherein generating the at least one feature vector comprises selectively setting features of the classifier based on the plurality of extracted static data points." (The information used to detect malware comprises a feature set selected from the list comprising program information or features such as file name, file size, vendor of the program and version of the program (*e.g. static data points*) [0104]. Each of the feature elements in a pre-defined feature set are derived 916 from the target application. The result is represented in a binary feature set vector, or feature vector, with a "1" indicating that the procedure is present in the searched executable, and a "0" otherwise [0336] and Fig. 9. For example, feature set of the following three feature elements DLL1, DLL2, DLL3 and an input executable that contained only DLL1 and DLL3, the feature vector is 1 0 1 [0161]) with the same motivation as discussed in the analysis of claim 3 above.

Claims 12 and 13 are computer-readable storage device versions of the method of Wojnowicz and Tuvell as discussed the analysis of claims 3 and 4, respectively above, and the claims are rejected on that basis.

11. **Claims 5 and 14** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wojnowicz in view of Tuvell and further in view of Gilbert et al. (U.S. Patent No. 9,197,663) hereinafter Gilbert.

With respect to **claim 5**, Wojnowicz in view of Tuvell teach the claimed subject matter including "wherein features of the feature vector are selectively turned on or off based on evaluation of"..."a value of a static data point" as discussed in the analysis of claim 4 above the rejection of which is incorporated herein but may not specifically disclose "based on evaluation of whether a value of a static data point from the plurality of extracted static data points is within a predetermined range."

Gilbert, from the same or similar field of endeavor, teach "evaluation of whether a value of a static data point from the plurality of extracted static data points is within a predetermined range." (Gilbert identifies malware by combining an analysis of visual and non-visual information associated with the software packages. The non-visual elements can include data identifying a publisher, filenames, external function calls, registered operating system functions, operating system filenames, registry key, system file value, application filenames, library filenames, file size, provider, vendor tags and path names. The visual elements can include an icon (*i.e. static data points*) [column 2, lines 17-20 and 47-52]. Performing the comparison of the icon image and the reference image may involve determining whether the difference between the quantitative identity of the icon image and the quantitative identity of the reference image is less than a

threshold difference (*i.e. a range*) [column 3, lines 26-30]. See also [column 20, lines 44-61].

Gilbert is analogous art directed to candidate files which are analyzed to determine whether the candidate files are malware [abstract]. Based upon Wojnowicz in view of Tuvell in view of Gilbert it would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to utilize the teachings of Gilbert within the method of Wojnowicz and Tuvell with the motivation of improving the issues of privacy and data security and also to avoid detrimental effects on the operation of the computer and/or network on which it resides and also because the transmission and operation of the spyware consume bandwidth and memory and also because users often experience a degradation in system performance, instability, and even total system failure (See Gilbert [column 4, line 64 through column 5, line 3]) and also because all of the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination would have yielded predictable results to one of ordinary skill in the art at the time of the invention.

Claim 14 is a computer-readable storage device version of the method of Wojnowicz and Tuvell as discussed the analysis of claim 5 above and the claim is rejected on that basis.

12. **Claims 6 and 15** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wojnowicz in view of Thomas et al. (U.S. Publication No. 2012/0079596) hereinafter Thomas.

With respect to **claim 6**, Wojnowicz teach the claimed subject matter as discussed in the analysis of claim 2 above the rejection of which is incorporated herein but may not specifically disclose “wherein the classifying the at least one static data point comprises classifying the plurality of extracted static data points into categories comprising numeric values, nominal values, string or byte sequences, and Boolean values.”

Thomas, from the same or similar field of view, teach “wherein the classifying the at least one static data point comprises classifying the plurality of extracted static data points into categories" (The malware detection and analysis system can identify and classify malware families. [0239]) “comprising numeric values” (file size [0175], [0225] and [0272]), “nominal values” (file type [0038], [0175], [0225] and [0272], and resource, [0191, table 4] and [0257]), “string or byte sequences” (original file [0250] and section name [0191, table 4], imports, exports [0195 and Fig. 8], original file name and comments [0250], [0251] and [0267]), “and Boolean values” (Boolean values [0062] and [0078], entry point [0095], resource and section name [0191, table 4] and [0269]).

Thomas is analogous art directed to detecting malicious software/malware [abstract]. Based upon Wojnowicz in view of Thomas it would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to utilize the classification of Thomas within the method of Wojnowicz with the same motivation as discussed in the analysis of claim 3 above and also with the motivation of providing the improvement of allowing the analysis to go much deeper into the heart of the operating system while not being disruptive since operation occurs on a memory dump once the system is frozen or powered down to detect attempts for malware to

hide in the stealthiest ways (see Thomas, [0023]) and also because Wojnowicz indicates that SSES can be combined with any number of additional features in a malware classifier of choice [column 2, lines 63-64].

Claim 15 is a computer-readable storage device version of the method of Wojnowicz and Thomas as discussed the analysis of claim 6 above and the claim is rejected on that basis.

13. **Claims 7 and 16** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wojnowicz in view of Tuvell and further in view of Thomas.

With respect to **claim 7**, Wojnowicz in view of Tuvell in view of Thomas teach the claimed subject matter including the classification of the plurality of extracted static data points as discussed in the analysis of claim 6 above the rejection of which is incorporated herein. In addition, Tuvell teach "wherein analyzing the executable file further comprises generating at least one feature vector from the plurality of extracted static data points," (The information used to detect malware comprises a feature set selected from the list comprising program information or features such as file name, file size, vendor of the program and version of the program (*e.g. static data points*) [0104]. Each of the feature elements in a pre-defined feature set are derived 916 from the target application. The result is represented in a binary feature set vector, or feature vector, with a "1" indicating that the procedure is present in the searched executable, and a "0" otherwise [0336] and Fig. 9. For example, feature set of the following three feature elements DLL1, DLL2, DLL3 and an input executable that contained only DLL1 and DLL3, the feature vector is 1 0 1 [0161]).

"wherein features of the generated feature vector are weighted based at least upon the classified categories and the plurality of extracted static data points." (The heuristic rules are derived from a classification [0020]. Wherein said rule comprises one or more weights, each said weight assigned to a feature element [claim 6]) with the same motivation as discussed in the analysis of claims 3 and 6 above.

Claim 16 is a computer-readable storage device version of the method of Wojnowicz, Tuvell and Thomas as discussed the analysis of claim 7 above and the claim is rejected on that basis.

14. **Claims 8, 9, 17, 18 and 20** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wojnowicz in view of Gilbert.

With respect to **claim 8**, Wojnowicz teach the claimed subject matter as discussed in the analysis of claim 1 above the rejection of which is incorporated herein. In addition, Wojnowicz teach "wherein determining whether the executable file is harmful further comprises…when a determined probability value that the executable file is harmful exceeds a threshold value." (Files having a score above a pre-defined threshold are determined to be likely malicious [column 1, lines 32-39]) but does not specifically disclose "preventing execution of the executable file".

Gilbert, from the same or similar field of endeavor, teach "preventing execution of the executable file" (Anti-virus and anti-spyware software detects, quarantines, and in some cases removes software, such as malware, that is malicious in nature and generally unwanted from a computer or computer [column 2, lines 17-28]).

Gilbert is analogous art directed to candidate files which are analyzed to determine whether the candidate files are malware [abstract]. Based upon Wojnowicz in view of Gilbert it would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to quarantine or eliminate the files of Gilbert within the method of Wojnowicz with the motivation of improving the issues of privacy and data security and also to avoid detrimental effects on the operation of the computer and/or network on which it resides and also because the transmission and operation of the spyware consume bandwidth and memory and also because users often experience a degradation in system performance, instability, and even total system failure (See Gilbert [column 4, line 64 through column 5, line 3]).

With respect to **claim 9**, Wojnowicz in view of Gilbert teach the claimed subject matter as discussed in the analysis of claim 8 above the rejection of which is incorporated herein. In addition, Gilbert teach "wherein the threshold value is set based on predetermined false positive range data." (The threshold value may be tuned, automatically or manually, based on the performance of malware identification system 100, for example, malware detection rate, false positive rate, etc. The threshold value may be set such that two images are determined to match when the difference between the images is less than approximately 40%, (i.e. *a range*) for example, the threshold value may be set to 0.4 [column 9, lines 21-34]) with the same motivation as discussed in the analysis of claim 8 above and also because all of the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the

combination would have yielded predictable results to one of ordinary skill in the art at the time of the invention.

The limitations of **claims 17, 18 and 20** are rejected in the analysis of claims 8 and 9 above and the claims are rejected on that basis.

Conclusion

15. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Gary Lavelle whose telephone number is 571 270-7575 and whose direct facsimile number is 571 270-8575. The examiner can normally be reached on Monday, Tuesday and Thursday 9AM - 6PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Carl Colin can be reached at 571-272-3862. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

17. 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.

Gary Lavelle
Examiner, Art Unit 2493
/gl/

/CARL G COLIN/
Supervisory Patent Examiner, Art Unit 2493

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/709,875	Schmidtler et al.
	Examiner	**Art Unit**
	GARY E LAVELLE	2493

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

CLAIMS

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

CLAIM		DATE								
Final	Original	11/27/2016	03/16/2017	04/16/2018	01/17/2019					
	1	✓	✓	✓	✓					
	2	✓	✓	✓	✓					
	3	✓	✓	✓	✓					
	4	✓	✓	✓	✓					
	5	✓	✓	✓	✓					
	6	✓	✓	✓	✓					
	7	✓	✓	✓	✓					
	8	✓	✓	✓	✓					
	9	✓	✓	✓	✓					
	10	✓	✓	✓	✓					
	11	✓	✓	✓	✓					
	12	✓	✓	✓	✓					
	13	✓	✓	✓	✓					
	14	✓	✓	✓	✓					
	15	✓	✓	✓	✓					
	16	✓	✓	✓	✓					
	17	✓	✓	✓	✓					
	18	✓	✓	✓	✓					
	19	✓	✓	✓	✓					
	20	✓	✓	✓	✓					

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/709,875	Schmidtler et al.
	Examiner	Art Unit
	GARY E LAVELLE	2493

CPC - Searched*		
Symbol	Date	Examiner
G06F21/565, G06F99/005 and G06F221/033	11/27/2016	Gary Lavelle

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

	/GARY LAVELLE/ Examiner.Art Unit 2493

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/709,875	Schmidtler et al.
	Examiner	Art Unit
	GARY E LAVELLE	2493

Search Notes		
Search Notes	**Date**	**Examiner**
Inventor search	11/27/2016	Gary Lavelle
NPL search (Google, ACM and IEEE with seach terms including: malware | malicious | virus, classify, static data points, feature vector, packed, encrypted...)	11/25/2016	Gary Lavelle
East search (see attached search history listing)	11/27/2016	Gary Lavelle
Inventor search updated	3/19/2017	Gary Lavelle
NPL search updated (Google, ACM and IEEE with new search terms including: static reference points...)	3/19/2017	Gary Lavelle
East search (see attached search history listing)	3/20/2017	Gary Lavelle
Inventor search updated	04/16/2018	Gary Lavelle
NPL search above updated (Google, ACM and IEEE with new search terms including: define file points of reference...)	04/10/2018	Gary Lavelle
G06F21/565, G06F99/005 and G06F221/033 EAST search updated (see attached search history listing included with this form to determine the scope of search)	04/16/2018	Gary Lavelle
Inventor search updated	01/17/2019	Gary Lavelle
NPL search above updated	01/17/2019	Gary Lavelle
G06F21/565, G06F99/005 and G06F221/033 EAST search updated (see attached search history listing included with this form to determine the scope of search)	01/17/2019	Gary Lavelle

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**

	/GARY LAVELLE/ Examiner.Art Unit 2493

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	5	((Mauritius) near2 (Schmidtler)).INV. and (classif$5 or categor$5) and (malware or malicious or virus)	US-PGPUB; USPAT	NEAR	ON	2019/01/17 10:10
L1	59	((Mauritius) near2 (Schmidtler)).INV.	US-PGPUB; USPAT	NEAR	ON	2019/01/17 10:10
L5	17	(G06F21/565 or G06F99/005 or G06F221/033).cpc. and (malware or malicious or virus) and weight$5 and feature adj vector and(classif$5 or categor$5)and (header section import export certificate resource string flag legal comment program API DLL)and (@pd or @ptad or @prad or @ad or @rlad) <"20151205" and referenc$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/01/17 10:17
L7	17	(G06F21/565 or G06F99/005 or G06F221/033).cpc. and (malware or malicious or virus) and weight$5 and feature adj vector and(classif$5 or categor$5)and (header section import export certificate resource string flag legal comment program API DLL)and (@pd or @ptad or @prad or @ad or @rlad) <"20151205" and referenc$4 and (encrypt$5 or decrypt$5 or pack$4 or compress$5 or unpack$4 or decompress$5)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/01/17 10:19
L6	17	(G06F21/565 or G06F99/005 or G06F221/033).cpc. and (malware or malicious or virus) and weight$5 and feature adj vector and(classif$5 or categor$5)and (header section import export certificate resource string flag legal comment program API DLL)and (@pd or @ptad or @prad or @ad or @rlad) <"20151205" and referenc$4 and (encrypt$5 or decrypt$5 or pack$4 or compress$5)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/01/17 10:19
L8	4	(G06F21/565 or G06F99/005 or G06F221/033).cpc. and (Numeric adj values file adj size linker adj version code adj size OS adj version image adj version subsystem adj version file adj version adj number size adj of adj stackr size adj of file adj OS adj image "PE header time" Section adj Entropy section adj count)and (Nominal adj values initialize Un-initialize entry adj point subsystem file adj subtype language file adj flags adj masks file adj flags product adj name size adj of adj heapr file adj type machine adj type PE adj type Sections adj count DLL adj count DLL adj functions data adj directory export adj count "Earliest Data	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/01/17 10:23

		Byte" resources resources adj language resource adj Encoding resource adj code adj page resource adj size DLL adj characteristics resource adj size DLL adj characteristics) and (Strings/Byte adj sequences Comments company adj name file adj descriptioninternal adj name legal adj copyright original adj file private adj build special adj build product adj version file adj version package adj code product adj code export adj DLL adj name assembly adj version "Certificate Issuer" Certificate adj Subject Imports Exports Section adj Names non-resource adj section adj strings non-resource adj section adj strings) and (Boolean adj values "Address Of Entry Point Anomaly" Image adj Base adj Anomaly "Section Alignment Anomaly" "Size Of Code Mismatch Anomaly" "Low Import Count Anomaly" "Entry Point Anomaly" certificate adj Validity Certificate adj Exception "Code Characteristics Anomaly" "Code Name Anomaly" Count adj Anomaly "Data Characteristics Anomaly" Data adj Name adj Anomaly Export adj Exception "Large Number of DLLs Anomaly" "flag DLL Name Anomaly" "Number of Functions Anomaly" "Function Name Anomaly" "PE Header Anomaly" "High Section Count Anomaly" "PE Magic Validity" Resource adj Exception "VR Code Ratio Anomaly" Import adj Exception) and (@pd or @ptad or @prad or @ad or @rlad)<"20151205" and (encrypt$5 or decrypt$5 or pack$4 or compress$5 or unpack$4 or decompress$5)				
L10	4	(G06F21/565 or G06F99/005 or G06F221/033).cpc. and (decrypt$5 or unpack$4 or decompress$4) (classif$6 or categor$6)same train$4 (reference or static) with data adj point and (@pd or @ptad or @prad or @ad or @rlad)<"20151205"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2019/01/17 10:38
L9	34	(decrypt$5 or unpack$4 or decompress$4) (classif$6 or categor$6)same train$4 (reference or static) with data adj point and (@pd or @ptad or @prad or @ad or @rlad) <"20151205"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2019/01/17 10:38
L11	30	(decrypt$5 or unpack$4 or decompress$4) (classif$6 or categor$6)same train$4 (reference or static) with data adj point and (@pd or @ptad or @prad or @ad or @rlad) <"20151205" not l10	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2019/01/17 10:39
L12	2	((Gaurav) near2 (Dalal)).INV.	US-PGPUB; USPAT	NEAR	ON	2019/01/17 10:44
L13	2	((Reza) near2 (Yoosoofmiya)).INV.	US-PGPUB; USPAT	NEAR	ON	2019/01/17 10:45

EAST Search History (Interference)

< This search history is empty>

1/ 17/ 2019 10:48:24 AM
C:\ Users\ glavelle\ Documents\ EAST\ Workspaces\ 14709875.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/709,875	05/12/2015	Mauritius Schmidtler	04584.0168US01	1593

23552 7590 04/08/2019

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
LAVELLE, GARY E	

ART UNIT	PAPER NUMBER
2493	

NOTIFICATION DATE	DELIVERY MODE
04/08/2019	ELECTRONIC

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

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

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

USPTO23552@merchantgould.com

Applicant-Initiated Interview Summary	Application No. 14/709,875	Applicant(s) Schmidtler et al.		
	Examiner GARY E LAVELLE	Art Unit 2493	AIA (First Inventor to File) Status Yes	Page 1 of 2

All participants (applicant, applicants representative, PTO personnel):

1. GARY E LAVELLE (Examiner); Telephonic

2. David Harrell (Attorney of Record); Telephonic

Date of Interview: 28 March 2019

Claims Discussed: Claim 1

Prior Art Discussed: Wojnowicz (U.S. Patent 9,465,940)

Amendment proposed: Applicant provided a proposed amendment to claim 1 for discussion purposes apparently to overcome the current 102 rejection.

Issues Discussed:

Item(s) under 35 U.S.C. 112:
I was noted that the proposed claim amendment to claim 1 recited "labeled ate points" in line 11. It was indicated that this is a typographical error intended to recite - - labeled data points - -.

Item(s) under 35 U.S.C. 102:
The proposed claim amendment to claim 1 recites, in part, "...wherein the plurality of static data points represent predefined character strings in the executable file;" in the fourth and fifth line of the claim. It was noted that the prior art of Wojnowicz teach this feature (column 3, lines 9-16) where an executable file can be represented as a string of hexadecimal characters, where a string of these hexadecimal characters can be bundled up into a chunk of a file. Differences between the Applicant's invention and the prior art with regard to this feature were discussed along with further claim amendments which may distinguish over the prior art. Specific claim language was not presented. Agreement was not reached.

The proposed claim amendment to claim 1 recites, in part, "...wherein the classifier is trained to classify the plurality of static data points based on labeled data points...". Under the broadest reasonable interpretation, it was noted that this limitation may be interpreted to indicate that the classification may be based on the data points (which are labeled) as opposed to being based upon a label. Wojnowicz teach this feature (column 6, lines 63-66) which indicates that data points may be pooled together in a bin and indexed. This feature was discussed along with further claim amendments which may distinguish over the prior art. Specific claim language was not presented. Agreement was not reached.

Attachment(s): Agenda, Proposed Amendments,

/GARY E LAVELLE/ Examiner, Art Unit 2493	/CARL G COLIN/ Supervisory Patent Examiner, Art Unit 2493

Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04
Please further see:
MPEP 713.04
Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)
37 CFR § 1.2 Business to be transacted in writing

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

TO: Examiner Gary Lavelle

FROM: David Harrell (Reg. No. 71,855)

DATE: April 1, 2019

RE: Agenda for Examiner Interview on Thursday, March 28, 2019 at 3:00pm EST

Application No: 14/709,875
Docket No.: 04584.0168US01
Filing Date: May 12, 2015
Title: AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS

"FOR DISCUSSION PURPOSES ONLY – NOT FOR OFFICIAL ENTRY"

I. Discuss § 103 Rejection:

a. Discuss Wojnowicz et al. (U.S. Pat. No. 8,709,924)

b. Discuss additional cited art if/as necessary.

II. Discuss proposed claim amendment:

1. (~~Previously Presented~~ Currently Amended) A computer-implemented method comprising:

extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the plurality of static data points represent predefined character strings in the executable file ~~one or more of the plurality of static data points are points of reference representing sections of the executable file, wherein the points of reference are used to evaluate the executable file~~;

analyzing ,using a classifier, the plurality of static data points ~~executable file without decrypting or unpacking the executable file, wherein analyzing the executable file comprises applying a classifier to the plurality of static data points~~, wherein the classifier is trained to classify the plurality of static data points based on labeled ate points from ~~data that comprises~~

known malicious executable files, known benign executable files and known unwanted executable files; and

determining whether the executable file is harmful based on the analysis.

Sophos Ex. 1003
Page 295 of 456

Doc code: RCEX
Doc description: Request for Continued Examination (RCE)

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

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

Application Number	14709875	Filing Date	2015-05-12	Docket Number (if applicable)	04584.0168US01	Art Unit	2493
First Named Inventor	Mauritius Schmidtler			Examiner Name	LAVELLE, GARY E		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☐ Other _____

☒ Enclosed

- ☒ Amendment/Reply
- ☐ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____ (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 132725

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

Applicant Signature

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

Signature of Registered U.S. Patent Practitioner			
Signature	/David D. Harrell/	Date (YYYY-MM-DD)	2019-04-24
Name	David D. Harrell	Registration Number	71855

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

Electronic Patent Application Fee Transmittal

Application Number:	14709875
Filing Date:	12-May-2015
Title of Invention:	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS
First Named Inventor/Applicant Name:	Mauritius Schmidtler
Filer:	David Dwayne Harrell/Elizabeth Pallardy
Attorney Docket Number:	04584.0168US01

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

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

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
RCE- 2ND AND SUBSEQUENT REQUEST	1820	1	1900	1900
		Total in USD ($)		**1900**

Electronic Acknowledgement Receipt

EFS ID:	35822640
Application Number:	14709875
International Application Number:	
Confirmation Number:	1593
Title of Invention:	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS
First Named Inventor/Applicant Name:	Mauritius Schmidtler
Customer Number:	23552
Filer:	David Dwayne Harrell/Elizabeth Pallardy
Filer Authorized By:	David Dwayne Harrell
Attorney Docket Number:	04584.0168US01
Receipt Date:	24-APR-2019
Filing Date:	12-MAY-2015
Time Stamp:	17:48:35
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$1900
RAM confirmation Number	042519INTEFSW17494100
Deposit Account	132725
Authorized User	Elizabeth Pallardy
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 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		04584_0168US01_RespFOA.PDF	146224 82f871d908e907a70007d938772941dfc9931990	yes	14
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Amendment Submitted/Entered with Filing of CPA/RCE		1	1	
	Claims		2	6	
	Applicant Arguments/Remarks Made in an Amendment		7	14	
Warnings:					
Information:					
2	Request for Continued Examination (RCE)	04584_0168US01_RCE.PDF	697619 f4e3ff52076bc912a676528e0adf54a41c29e811	no	3
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30781 0f194b553042b4e9ab864cf3aa23199b0fa9ad42	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	874624		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Mauritius Schmidtler et al.	Examiner:	Lavelle, Gary E.
Serial No.:	14/709,875	Group Art Unit:	2493
Filed:	May 12, 2015	Docket No.:	04584.0168US01
Title:	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS		

AMENDMENT & RESPONSE TO FINAL OFFICE ACTION

Mail Stop After Final
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Commissioner:

In response to the Final Office Action mailed January 24, 2019, please amend the above-identified application as follows:

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

Remarks/Arguments begin on page 7 of this paper.

Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (Currently Amended) A computer-implemented method comprising:

extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the plurality of static data points represent predefined character strings in the executable file ~~one or more of the plurality of static data points are points of reference representing sections of the executable file, wherein the points of reference are used to evaluate the executable file~~;

analyzing the plurality of static data points using a classifier ~~executable file without decrypting or unpacking the executable file, wherein analyzing the executable file comprises applying a classifier to the plurality of static data points, wherein the classifier is~~ trained to classify the plurality of static data points based on a collection of data comprising ~~from data that comprises~~ known malicious executable files, known benign executable files and known unwanted executable files, wherein the collection of data comprises the plurality of static data points; and

determining whether the executable file is harmful based on the analysis.

2. (Original) The computer-implemented method according to claim 1, wherein the extracting the plurality of static data points further comprises classifying the extracted static data points according to a type of data extracted from the executable file, and encoding the extracted static data points for the classifier based on the classification.

3. (Original) The computer-implemented method according to claim 2, wherein analyzing the executable file further comprises generating a feature vector from the plurality of extracted static data points and evaluating the feature vector using support vector processing to determine whether the executable file is at least one of harmful, benign, and potentially unwanted.

4. (Original) The computer-implemented method according to claim 3, wherein generating the at least one feature vector comprises selectively setting features of the classifier based on the plurality of extracted static data points.

5. (Original) The computer-implemented method according to claim 4, wherein features of the feature vector are selectively turned on or off based on evaluation of whether a value of a static data point from the plurality of extracted static data points is within a predetermined range.

6. (Original) The computer-implemented method according to claim 2, wherein the classifying the at least one static data point comprises classifying the plurality of extracted static data points into categories comprising numeric values, nominal values, string or byte sequences, and Boolean values.

7. (Original) The computer-implemented method according to claim 6, wherein analyzing the executable file further comprises generating at least one feature vector from the plurality of extracted static data points, wherein features of the generated feature vector are weighted based at least upon the classified categories and the plurality of extracted static data points.

8. (Original) The computer-implemented method according to claim 1, wherein determining whether the executable file is harmful further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value.

9. (Original) The computer-implemented method according to claim 8, wherein the threshold value is set based on predetermined false positive range data.

10. (Currently Amended) A computer-readable storage device containing instructions, that when executed on at least one processor, causing the processor to execute a process comprising:

extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the plurality of static data points represent predefined

character strings in the executable file ~~one or more of the plurality of static data points are points of reference representing sections of the executable file, wherein the points of reference are used to evaluate the executable file~~;

analyzing the plurality of static data points using a classifier ~~executable file without decrypting or unpacking the executable file, wherein analyzing the executable file comprises applying a classifier to the plurality of static data points, wherein the classifier is~~ trained to classify the plurality of static data points based on a collection of data comprising ~~from data that comprises~~ known malicious executable files, known benign executable files and known unwanted executable files, wherein the collection of data comprises the plurality of static data points; and

determining whether the executable file is harmful based on the analyzing of the executable file.

11. (Original) The computer-readable storage device according to claim 10, wherein the extracting of the plurality of static data points executed by the processor further comprises classifying the extracted static data points according to a type of data extracted from the executable file, and encoding the extracted static data points for the classifier based on the classifying.

12. (Original) The computer-readable storage device according to claim 11, wherein analyzing the executable file further comprises generating at least one feature vector from the plurality of extracted static data points and evaluating the feature vector using linear or nonlinear support vector processing to determine whether the executable file is at least one of harmful, benign, and potentially unwanted.

13. (Original) The computer-readable storage device according to claim 12, wherein generating the at least one feature vector comprises selectively setting features of the classifier based on the plurality of extracted static data points.

14. (Original) The computer-readable storage device according to claim 13, wherein features of the feature vector are selectively turned on or off based on evaluation of whether a value of a static data point from the plurality of extracted static data points is within a predetermined range.

15. (Original) The computer-readable storage device according to claim 11, wherein the classifying the at least one static data point comprises classifying the plurality of extracted static data points into categories comprising numeric values, nominal values, string or byte sequences, and Boolean values.

16. (Original) The computer-readable storage device according to claim 15, wherein analyzing the executable file further comprises generating a feature vector from the plurality of extracted static data points, wherein features of the generated feature vector are weighted based at least upon the classified categories and the plurality of extracted static data points.

17. (Original) The computer-readable storage device according to claim 10, wherein determining whether the executable file is harmful further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value.

18. (Original) The computer-readable storage device according to claim 17, wherein the threshold value is set based on predetermined false positive range data.

19. (Currently Amended) A system comprising:

at least one memory; and

at least one processor operatively connected with the memory and configured to perform operation of:

extracting a plurality of predefined character strings ~~static data points~~ from an executable file without decrypting or unpacking the executable file, ~~wherein one or more of the plurality of static data points are points of reference representing sections of the executable file, wherein the points of reference are used to evaluate the executable file~~;

analyzing the plurality of predefined character strings using a classifier ~~executable file without decrypting or unpacking the executable file, wherein analyzing the executable file comprises applying a classifier to the plurality of static data points, wherein the classifier is~~ trained to classify the plurality of predefined character strings based on a collection of data comprising ~~from data that comprises~~ known malicious executable files, known benign executable files and known unwanted executable files, wherein the collection of data comprises one or more of the plurality of predefined character strings; and

determining whether the executable file is harmful based on the analyzing of the executable file.

20. (Original) The system according to claim 19, wherein the determining further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value, and wherein the threshold value is set based on predetermined false positive range data.

REMARKS/ARGUMENTS

This Amendment and the following remarks are intended to fully respond to the Final Office Action dated January 24, 2019, hereinafter "Office Action." In that Office Action, claims 1-20 were examined and all claims were rejected. Claims 1, 2, 10, 11 and 19 were rejected under 35 U.S.C. § 102(a)(2) as allegedly anticipated by Wojnowicz et al. (U.S. Pat. No. 8,709,924; hereinafter "Wojnowicz"). Claims 3, 4, 12 and 13 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz in view of Tuvell et al. (U.S. Pat. Publ. No. 2007/0240220; hereinafter "Tuvell"). Claims 5 and 14 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Tuvell, and further in view of Gilbert et al. (U.S. Pat. No. 9,197,663; hereinafter "Gilbert"). Claims 6 and 15 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Thomas et al. (U.S. Pat. Publ. No. 2012/0079596; hereinafter "Thomas"). Claims 7 and 16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Tuvell, and further in view of Thomas. Claims 8, 9, 17, 18 and 20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz in view of Gilbert.

Reconsideration of these rejections, as they might apply to the original and amended claims in view of these remarks, is respectfully requested. In this Amendment, claims 1, 10, and 19 have been amended, and no claims have been canceled or added. Therefore, claims 1-20 remain present for examination.

Interview Summary

Examiner Gary Lavelle and Applicants' representative, Attorney David D. Harrell (Reg. No. 71,855), participated in a telephone interview on March 28, 2019 to discuss the cited references and the proposed claims. Although an agreement with respect to the ultimate allowability of the claims was not reached, it was agreed that the amendments discussed are likely to overcome the rejections.

Claim Rejections Under 35 U.S.C. § 102

Claims 1, 2, 10, 11 and 19 were rejected under 35 U.S.C. § 102(a)(2) as allegedly anticipated by Wojnowicz. Applicants respectfully traverse this rejection because either the Examiner failed to state a prima facie case of anticipation or the current amendments to the claims now render the Examiner's arguments moot. "Anticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim." Lindemann Mashinenfabrik GmbH v. Am. Hoist & Derrick Co., 730 F.2d 1452, 1458 (Fed. Cir. 1984); see also, MPEP § 2131. Applicants submit that the cited references do not disclose all of the elements of the rejected claims.

Non-limiting examples of the present application provide automatic threat detection of executable files based on static data analysis. In examples, a plurality of static data points may be extracted from an executable file without decrypting or unpacking the executable file. The executable file may then be analyzed without decrypting or unpacking the executable file. Analysis of the executable file may comprise applying a classifier to the plurality of extracted static data points. The classifier may be trained from data comprising known malicious executable files, known benign executable files and known unwanted executable files. Based upon analysis of the executable file, a determination can be made as to whether the executable file is harmful.

Turning specifically to the claims, without acquiescing to the propriety of the rejection and solely for the purpose of advancing prosecution, Applicants have amended the independent claims. The amended independent claims clarify that the data points extracted from the executable file represent predefined character strings, on which a classifier is trained to detect, extract, and analyze to classify a file as safe or malicious. For instance, claim 1 as amended recites, inter alia, "extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, *wherein the plurality of static data points represent predefined character strings in the executable file*" and "*analyzing the plurality of static data points using a classifier trained to classify the plurality of static data points based on a collection of data* comprising known malicious executable files, known benign executable files and known unwanted executable files, *wherein the collection of data comprises the plurality of static data points*."

Wojnowicz does not teach, at least, "*analyzing the plurality of static data points using a classifier trained to classify the plurality of static data points based on a collection of data comprising ... the plurality of static data points*," where such static data points "*represent predefined character strings in the executable file,*" as recited in claim 1 as amended. Wojnowicz describes a method for identifying malware using wavelet decomposition to determine software entropy. In the method, each of the data file in a set of received data files is split into non-overlapping file chunks of fixed length. The non-overlapping, fixed-length file chunks are represented as an entropy time series that reflects an amount of entropy across the file chunks for each file. A wavelet transform is applied to the corresponding entropy time series to generate an energy spectrum characterizing an amount of entropic energy at multiple scales of code resolution. A determination is then made as to whether the file is likely to be malicious based on the energy spectrum. *Wojnowicz*, col. 1, ll. 23-31.

Notably, as discussed in the examiner interview, the fixed-length file chunks do not represent predefined character strings. Instead, each fixed-length file chunk is, itself, a random (e.g. undefined) character string having no initial significance to the system of Wojnowicz. The entropy analysis performed on the random character string does not include a comparison of the random character string to a predefined character string. In contrast, claim 1 as amended specifies that the static data points represent one or more predefined character strings. The system of the present application is configured to identify the predefined character strings and the values associated therewith. Based on the presence of the predefined character strings and/or the corresponding values, the system determines whether a file is malicious. The portion of the file that does not correspond do the predefined character strings is not analyzed by the system. Thus, the system of the present application provides at least processing/computational improvements over the system of Wojnowicz.

Moreover, Wojnowicz does not disclose a learning classifier that is trained to identify and analyze static data points that represent such predefined character strings in order to determine whether a file is malicious. Instead, as described above, in Wojnowicz the entropy for each random character string in the fixed-length file chunk is calculated and used to determine

whether a file is malicious. Thus, for at least the foregoing reasons, Wojnowicz does not anticipate claim 1 as amended.

The other independent claims recite similar limitations and are allowable over the recited reference for at least the same or similar reasons. For example, claim 10 as amended recites, *inter alia*:

> analyzing the plurality of static data points using a classifier trained to classify the plurality of static data points based on a collection of data comprising known malicious executable files, known benign executable files and known unwanted executable files, wherein the collection of data comprises the plurality of static data points

Claim 19 as amended recites, *inter alia*:

> analyzing the plurality of predefined character strings using a classifier trained to classify the plurality of predefined character strings based on a collection of data comprising known malicious executable files, known benign executable files and known unwanted executable files, wherein the collection of data comprises one or more of the plurality of predefined character strings

The dependent claims, i.e. claims 2 and 11, incorporate all of the limitations of the above independent claims, respectively, and are allowable over Wojnowicz for at least the same reasons. As such, Applicants respectfully request that the Examiner withdraw the rejection and allow claims 1, 2, 10, 11 and 19 at the Examiner's earliest convenience.

Claim Rejections Under 35 U.S.C. §103

Claims 3, 4, 12 and 13

Claims 3, 4, 12 and 13 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz in view of Tuvell. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a), the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

Claims 3, 4, 12 and 13 depend from claims 1 and 10, respectively. As previously discussed, claims 1 and 10 are allowable over Wojnowicz. Tuvell does not cure the deficiencies of Wojnowicz, nor does the Office Action refer to it for such. Tuvell relates to a system for detecting malware on a limited access mobile platform in a mobile network. The system uses feature sets describing various non-executable portions of malware-infected and malware-free applications, and compares an application on the limited access mobile platform to the features sets. A match of the features in a suspect application to one of the feature sets provides an indication as to whether the suspect application is malware-infected or malware-free. *Tuvell*, para. [0019]. The Office Action refers to Tuvell as disclosing the use of a feature set to detect malware. *Office Action*, pg. 10. Without conceding to the correctness of this characterization, Applicants submit that Tuvell does not teach or suggest the distinguishing features of claims 1 and 10 discussed above. As such, Applicants respectfully request withdrawal of the rejections and allowance of claims 3, 4, 12 and 13 at the Examiner's earliest convenience.

Claims 5 and 14

Claims 5 and 14 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Tuvell, and further in view of Gilbert. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

Claims 5 and 14 depend from claims 1 and 10, respectively. As previously discussed, claims 1 and 10 are allowable over the combination of Wojnowicz and Tuvell. Gilbert does not cure their deficiencies, nor does the Office Action refer to it for such. Gilbert teaches a method for analyzing visual and non-visual elements associated with candidate data files to determine whether the files are malware. In the method, a visual element (e.g., icon) is extracted from the candidate file, and the icon's image is compared to a group of reference images associated with trusted entities. If the icon's image matches a reference image, the candidate file may be malware masquerading as trusted software. The non-visual elements associated with the candidate file are used, in combination with the visual elements, to determine whether the candidate file is malware. *Gilbert*, col. 2, ll. 29-46. The Office Action refers to Gilbert as

disclosing the determination of whether the difference between the quantitative identity of an icon image and the quantitative identity of a reference image is less than a threshold difference. *Office Action*, pg. 13. Without conceding to the correctness of this characterization, per the discussion above Applicants submit that Gilbert does not teach or suggest the distinguishing features of claims 1 and 10 discussed above. As such, Applicants respectfully request withdrawal of the rejections and allowance of claims 5 and 14 at the Examiner's earliest convenience.

Claims 6 and 15

Claims 6 and 15 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Thomas. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

Claims 6 and 15 depend from claims 1 and 10, respectively. As previously discussed, claims 1 and 10 are allowable over Wojnowicz. Thomas does not cure the deficiencies of Wojnowicz, nor does the Office Action refer to it for such. Thomas teaches a method of detecting malicious software (malware), which includes receiving a file and storing a memory baseline for a system. The method also includes copying the file to the system, executing the file on the system, terminating operation of the system, and storing a post-execution memory map. The memory baseline and the post-execution memory map are then analyzed and determination is made as to whether the file includes malware. *Thomas*, para. [0005]. The Office Action refers to Thomas as disclosing the identification and classification of malware families. *Office Action*, pg. 15. Without conceding to the correctness of this characterization, per the discussion above Applicants submit that Gilbert does not teach or suggest the distinguishing features of claims 1 and 10 discussed above. As such, Applicants respectfully request withdrawal of the rejections and allowance of claims 6 and 15 at the Examiner's earliest convenience

Claims 7 and 16

Claims 7 and 16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz, in view of Tuvell, and further in view of Thomas. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

Claims 7 and 16 depend from claims 1 and 10, respectively. As previously discussed, claims 1 and 10 are allowable over the combinations of Wojnowicz and Tuvell and Wojnowicz and Thomas. The further combination of Wojnowicz, Tuvell and Thomas does not cure their deficiencies of the individual combinations. As such, Applicants respectfully request withdrawal of the rejections and allowance of claims 7 and 16 at the Examiner's earliest convenience.

Claims 8, 9, 17, 18 and 20

Claims 8, 9, 17, 18 and 20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wojnowicz in view of Gilbert. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

Claims 8, 9, 17, 18 and 20 depend from claims 1, 10 and 19, respectively. As previously discussed, claims 1, 10 and 19 are allowable over the combinations of Wojnowicz, Tuvell and Gilbert. Removing Tuvell from the combination does not cure their deficiencies of Wojnowicz and Gilbert. As such, Applicants respectfully request withdrawal of the rejections and allowance of claims 8, 9, 17, 18 and 20 at the Examiner's earliest convenience.

CONCLUSION

This Amendment fully responds to the Final Office Action mailed on January 24, 2019. Still, that Office Action may contain arguments and rejections that are not directly addressed by this Amendment due to the fact that they are rendered moot in light of the preceding arguments in favor of patentability. Hence, failure of this Amendment to directly address an argument raised in the Office Action should not be taken as an indication that the Applicant believes the argument has merit. Furthermore, the claims of the present application may include other elements, not discussed in this Amendment, which are not shown, taught, or otherwise suggested by the references of record. Accordingly, the preceding arguments in favor of patentability are advanced without prejudice to other bases of patentability.

It is believed that no further fees are due with this Response. However, the Commissioner is hereby authorized to charge any deficiencies or credit any overpayment with respect to this patent application to deposit account number 13-2725.

In light of the above remarks and amendments, it is believed that the application is now in condition for allowance and such action is respectfully requested. Should any additional issues need to be resolved, the Examiner is requested to telephone the undersigned to attempt to resolve those issues.

Respectfully submitted,

Dated: April 24, 2019

/David D. Harrell/

David D. Harrell, Reg. No. 71,855
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1242

27488
PATENT TRADEMARK OFFICE

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/709,875	Filing Date 05/12/2015	☐ To be Mailed

ENTITY: ☑ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $80 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $420 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	04/24/2019	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0		x $100 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0		x $460 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

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

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

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

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.
14/709,875	05/12/2015	Mauritius Schmidtler	04584.0168US01	1593

23552 7590 07/17/2019

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2493	

NOTIFICATION DATE	DELIVERY MODE
07/17/2019	ELECTRONIC

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

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

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

USPTO23552@merchantgould.com

Office Action Summary	Application No. 14/709,875	Applicant(s) Schmidtler et al.	
	Examiner MICHAEL J SIMITOSKI	Art Unit 2493	AIA (FITF) Status Yes

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

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

Status

1)☑ Responsive to communication(s) filed on 24 April 2019.

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

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

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

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

Disposition of Claims*

5) ☑ Claim(s) 1-20 is/are pending in the application.

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

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-4,6-13 and 15-20 is/are rejected.

8) ☑ Claim(s) 5 and 14 is/are objected to.

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

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

Application Papers

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

11)☑ The drawing(s) filed on 12 May 2015 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

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

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

Priority under 35 U.S.C. § 119

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

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

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

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

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

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

Attachment(s)

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

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

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

4) ☐ Other: _____.

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

DETAILED ACTION

2. The response of 4/24/2019 was received and considered.

3. Claims 1-20 are pending.

Continued Examination Under 37 CFR 1.114

4. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 4/24/2019 has been entered.

Response to Arguments

5. Applicant's arguments with respect to claims 1-20 have been considered but are moot because the arguments do not apply to any of the references being used in the current rejection.

Claim Rejections - 35 USC § 102

6. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a)(1) the claimed invention was patented, described in a printed publication, or in public use, on sale or otherwise available to the public before the effective filing date of the claimed invention.

8. Claims 1-2, 10-11 and 19 are rejected under 35 U.S.C. 102(a)(1) as being anticipated by "Detection of Packed Malware" by Devi et al. (**Devi**).

Regarding claim 1, Devi discloses extracting a plurality of static data points (SOC, SOUID, SOSR, NSS, p. 25) from an executable file (PE file, p. 24, ¶4) without decrypting or unpacking the executable file (detecting packed malware, §5.2), wherein the plurality of static data points represent predefined character strings in the executable file (NSS represents section names, p. 25, §5.2, last paragraph); analyzing the plurality of static data points using a classifier (using Weka to classify, §5.2.1) trained to classify the plurality of static data points based on a collection of data comprising from data that comprises known malicious executable files, known benign executable files and known unwanted executable files (extracted features from malwares and benign executables, §5, ¶¶1-2), wherein the collection of data comprises the plurality of static data points (features were extracted from executables, §5, ¶¶1-2 and feature set is used in second phase classification, §5.2); and determining whether the executable file is harmful based on the analysis (determining packed malware or packed benign, §5.2).

Regarding claims 2 and 11, Devi discloses wherein the extracting the plurality of static data points further comprises classifying the extracted static data points according to a type of data extracted from the executable file (SOC, SOUID, SOSR, NSS, p. 25), and encoding the extracted static data points for the classifier based on the classification (feature set is used in second phase classification, §5.2).

Regarding claim 10, the claim is similar in scope to claim 1 and is therefore rejected using a similar rationale.

Regarding claim 19, the claim is similar in scope to claim 1 and is therefore rejected using a similar rationale.

Claim Rejections - 35 USC § 103

9. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

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

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

11. Claims 3 and 12 are rejected under 35 U.S.C. 103 as being unpatentable over **Devi**, as applied to claims 2 and 11 above, in view of "Efficient Malicious Code Detection Using N-Gram Analysis and SVM" by Choi et al. (**Choi**).

Regarding claims 3 and 12, Devi discloses wherein analyzing the executable file further comprises generating a feature vector (set of features, §5.2) from the plurality of extracted static data points and evaluating the feature vector using machine learning (§5, ¶3) to determine whether the executable file is at least one of harmful, benign, and potentially unwanted (§5.2). Note that while Devi does not explicitly disclose the term "feature vector" with respect to the second classification, "feature vector" is taught in the first classification to include the features used to classify executable types using

the analysis (§5.1). The limitation "feature vector", while not recited verbatim, is taught in the features used to classify the executable in the second classification. Devi lacks support vector processing. However, Choi teaches that SVM is a known machine learning classifier for determining malware (p. 620, §C). Therefore, it would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to modify Devi to include evaluating the feature vector using support vector processing. One of ordinary skill in the art would have been motivated to perform such a modification to utilize a known method of determining malware using machine learning, as taught by Choi.

12. Claims 4 and 13 are rejected under 35 U.S.C. 103 as being unpatentable over **Devi** and **Choi**, as applied to claims 3 and 12 above, in view of U.S. Patent Application Publication 2009/0013405 to **Schipka**.

Regarding claims 4 and 13, Devi, as modified above, lacks wherein generating the at least one feature vector comprises selectively setting features of the classifier based on the plurality of extracted static data points. However, Schipka teaches determining whether a file is malware using a feature set, including determining a file format of the input file to determine the features associated with that format (¶¶53-54, ¶¶61-64) and a classifier using machine learning techniques to classify the file as malicious or benign based on the determined features (¶64). This allows the classifier to utilize the features of a particular file type to correctly classify the file. Therefore, it would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to modify Devi, as modified above, such that generating the at least one feature vector comprises selectively setting features of the classifier based on the plurality of extracted static data points. One of ordinary skill in the art would have been motivated to perform such a modification to classify the executable based on the features of the executable, as taught by Schipka.

13. Claims 6 and 15 are rejected under 35 U.S.C. 103 as being unpatentable over **Devi**, as applied to claims 2 and 11 above, in view of U.S. Patent Application Publication 2012/0079596 to Thomas et al. (**Thomas**).

Regarding claims 6 and 15, Devi lacks wherein the classifying the at least one static data point comprises classifying the plurality of extracted static data points into categories comprising numeric values, nominal values, string or byte sequences, and Boolean values. However, Thomas, from the same or similar field of view, teaches "wherein the classifying the at least one static data point comprises classifying the plurality of extracted static data points into categories" (The malware detection and analysis system can identify and classify malware families. [0239]) "comprising numeric values" (file size [0175], [0225] and [0272]), "nominal values" (file type [0038], [0175], [0225] and [0272], and resource, [0191, table 4] and [0257]), "string or byte sequences" (original file [0250] and section name [0191, table 4], imports, exports [0195 and Fig. 8], original file name and comments [0250], [0251] and [0267]), "and Boolean values" (Boolean values [0062] and [0078], entry point [0095], resource and section name [0191, table 4] and [0269]). Thomas is analogous art directed to detecting malicious software/malware [abstract]. Based upon Devi in view of Thomas it would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to utilize the classification of Thomas within the method of Devi such that classifying the at least one static data point comprises classifying the plurality of extracted static data points into categories comprising numeric values, nominal values, string or byte sequences, and Boolean values. One of ordinary skill in the art would have been motivated to perform such a modification to utilize known executable features to classify the files, as taught by Thomas.

14. Claims 7 and 16 are rejected under 35 U.S.C. 103 as being unpatentable over **Devi** and **Thomas**, as applied to claims 6 and 15 above, in view of U.S. Patent 8,510,836 to **Nachenberg**.

Regarding claims 7 and 16, Devi, as modified above, discloses wherein analyzing the executable file further comprises generating at least one feature vector from the plurality of extracted static data points (set of features, Devi, §5.2), but lacks wherein features of the generated feature vector are weighted based at least upon the classified categories and the plurality of extracted static data points. However, Nachenberg teaches that it was known to apply weights to features of a feature set based on the type of information (col. 9, lines 53-65). Therefore, it would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to modify Devi, as modified above, such that analyzing the executable file further comprises generating at least one feature vector from the plurality of extracted static data points, wherein features of the generated feature vector are weighted based at least upon the classified categories and the plurality of extracted static data points. One of ordinary skill in the art would have been motivated to perform such a modification to utilize a relative importance of various features, as taught by Nachenberg.

15. Claims 8-9, 17-18 and 20 are rejected under 35 U.S.C. 103 as being unpatentable over **Devi**, as applied to claims 1, 10 and 19 above, in view of U.S. Patent 9,197,663 to Gilbert et al. (**Gilbert**).

Regarding claims 8 and 17, Devi lacks, but Gilbert teaches wherein determining whether the executable file is harmful further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value (Gilbert, col. 2, lines 17-28). Therefore, it would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to modify Devi such that determining whether the executable file is harmful further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value. One of

ordinary skill in the art would have been motivated to perform such a modification to protect the computer system from executing malware, as taught by Gilbert.

Regarding claims 9, 18 and 20, Devi lacks, but Gilbert teaches wherein the threshold value is set based on predetermined false positive range data (tuning threshold based on false positive rate, col. 9, lines 21-34). Therefore, it would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed invention to modify Gilbert such that the threshold value is set based on predetermined false positive range data. One of ordinary skill in the art would have been motivated to perform such a modification to tune the threshold for determining malware to minimize false positives, as taught by Gilbert.

Allowable Subject Matter

16. Claims 5 and 14 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL J SIMITOSKI whose telephone number is (571)272-3841. The examiner can normally be reached on Monday - Friday, 7:00-3:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Carl Colin can be reached on 571-272-38623862. 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.

/Michael Simitoski/
Primary Examiner, Art Unit 2493

July 11, 2019

Notice of References Cited	Application/Control No. 14/709,875	Applicant(s)/Patent Under Reexamination Schmidtler et al.	
	Examiner MICHAEL J SIMITOSKI	Art Unit 2493	Page 1 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20180365573-A1	12-2018	Sultana; Salmin	G06N5/04	1/1
*	B	US-20170262633-A1	09-2017	Miserendino; Scott	G06F21/566	1/1
*	C	US-20160156646-A1	06-2016	Hsueh; Frank Chijeen	G06F21/563	726/1
*	D	US-20160021174-A1	01-2016	DE LOS SANTOS VILCHEZ; Sergio	H04L43/10	709/201
*	E	US-20140310517-A1	10-2014	CHRISTODORESCU; MIHAI	H04L41/142	713/160
*	F	US-20130291111-A1	10-2013	Zhou; Hongyi	G06F21/566	726/23
*	G	US-20120227105-A1	09-2012	FRIEDRICHS; OLIVER	G06F21/564	726/22
*	H	US-20100082642-A1	04-2010	Forman; George	G06F16/35	707/749
*	I	US-20090300765-A1	12-2009	Moskovitch; Robert	G06F21/562	726/24
*	J	US-20090274376-A1	11-2009	Selvaraj; Sathiya Keerthi	G06K9/00442	382/224
*	K	US-20090013405-A1	01-2009	Schipka; Maksym	G06F21/562	726/22
*	L	US-8510836-B1	08-2013	Nachenberg; Carey S.	H04L63/145	706/12
	M					

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Bost, Raphael, et al. "Machine learning classification over encrypted data." NDSS. Vol. 4324. 2015. (Year: 2015)
	V	Choi, Junho, et al. "Efficient malicious code detection using n-gram analysis and SVM." 2011 14th International Conference on Network-Based Information Systems. IEEE, 2011. (Year: 2011)
	W	Devi, Dhruwajita, and Sukumar Nandi. "Detection of packed malware." Proceedings of the First International Conference on Security of Internet of Things. ACM, 2012. (Year: 2012)
	X	Dube, Thomas, et al. "Malware target recognition via static heuristics." Computers & Security 31.1 (2012): 137-147. (Year: 2012)

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 14/709,875	Applicant(s)/Patent Under Reexamination Schmidtler et al.	
	Examiner MICHAEL J SIMITOSKI	Art Unit 2493	Page 2 of 2

U.S. PATENT DOCUMENTS

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

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Merkel, Ronny, et al. "Statistical detection of malicious pe-executables for fast offline analysis." IFIP International Conference on Communications and Multimedia Security. Springer, Berlin, Heidelberg, 2010. (Year: 2010)
	V	Singla, Sanjam, et al. "A Novel Approach to Malware Detection using Static Classification." International Journal of Computer Science and Information Security 13.3 (2015): 1. (Year: 2015)
	W	Tabish, S. Momina, M. Zubair Shafiq, and Muddassar Farooq. "Malware detection using statistical analysis of byte-level file content. " Proceedings of the ACM SIGKDD Workshop on CyberSecurity and Intelligence Informatics. ACM, 2009. (Year: 2009)
	X	Treadwell, Scott, and Mian Zhou. "A heuristic approach for detection of obfuscated malware." 2009 IEEE International Conference on Intelligence and Security Informatics. IEEE, 2009. (Year: 2009)

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/709,875	Schmidtler et al.
	Examiner	Art Unit
	MICHAEL J SIMITOSKI	2493

CPC - Searched*		
Symbol	Date	Examiner
G06F21/565, G06F99/005 and G06F221/033	11/27/2016	Gary Lavelle
G06F 21/562,565; 2221/033; 8/53 | G06N 20/00	07/11/2019	MJS

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

/Michael Simitoski/ Primary Examiner, Art Unit 2493	

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/709,875	Schmidtler et al.
	Examiner	Art Unit
	MICHAEL J SIMITOSKI	2493

Search Notes		
Search Notes	**Date**	**Examiner**
Inventor search	11/27/2016	Gary Lavelle
NPL search (Google, ACM and IEEE with seach terms including: malware | malicious | virus, classify, static data points, feature vector, packed, encrypted...)	11/25/2016	Gary Lavelle
East search (see attached search history listing)	11/27/2016	Gary Lavelle
Inventor search updated	3/19/2017	Gary Lavelle
NPL search updated (Google, ACM and IEEE with new search terms including: static reference points...)	3/19/2017	Gary Lavelle
East search (see attached search history listing)	3/20/2017	Gary Lavelle
Inventor search updated	04/16/2018	Gary Lavelle
NPL search above updated (Google, ACM and IEEE with new search terms including: define file points of reference...)	04/10/2018	Gary Lavelle
G06F21/565, G06F99/005 and G06F221/033 EAST search updated (see attached search history listing included with this form to determine the scope of search)	04/16/2018	Gary Lavelle
Inventor search updated	01/17/2019	Gary Lavelle
NPL search above updated	01/17/2019	Gary Lavelle
G06F21/565, G06F99/005 and G06F221/033 EAST search updated (see attached search history listing included with this form to determine the scope of search)	01/17/2019	Gary Lavelle
EAST, NPL and Inventor searches performed	07/11/2019	
Consulted Global dossier and Common Citation Document	07/11/2019	

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
G06F	21/562,565; 2221/033; 8/53	07/11/2019	MJS
G06N	20/00	07/11/2019	MJS

/Michael Simitoski/ Primary Examiner, Art Unit 2493	

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/709,875	Schmidtler et al.
	Examiner	**Art Unit**
	MICHAEL J SIMITOSKI	2493

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

CLAIMS

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

CLAIM		DATE								
Final	Original	11/27/2016	03/16/2017	04/16/2018	01/17/2019	07/11/2019				
	1	✓	✓	✓	✓	✓				
	2	✓	✓	✓	✓	✓				
	3	✓	✓	✓	✓	✓				
	4	✓	✓	✓	✓	✓				
	5	✓	✓	✓	✓	O				
	6	✓	✓	✓	✓	✓				
	7	✓	✓	✓	✓	✓				
	8	✓	✓	✓	✓	✓				
	9	✓	✓	✓	✓	✓				
	10	✓	✓	✓	✓	✓				
	11	✓	✓	✓	✓	✓				
	12	✓	✓	✓	✓	✓				
	13	✓	✓	✓	✓	✓				
	14	✓	✓	✓	✓	O				
	15	✓	✓	✓	✓	✓				
	16	✓	✓	✓	✓	✓				
	17	✓	✓	✓	✓	✓				
	18	✓	✓	✓	✓	✓				
	19	✓	✓	✓	✓	✓				
	20	✓	✓	✓	✓	✓				

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	14/709875.app.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/09 05:38
S2	41718	(G06F21/562 OR G06F21/565 OR G06F2221/033 OR G06F8/53 OR G06N20/00).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/09 05:38
S6	95	((("Schmidtler") near3 ("Mauritius"))).INV. ((("Dalal") near3 ("Gaurav"))).INV. ((("Yoosoofmiya") near3 ("Reza"))).INV.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/09 05:39
S7	4	S6 and (unpack$4 near3 file)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/09 05:40
S8	27	(static near4 analysis) near5 (encrypted packed)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/09 05:41
S9	1	(static near4 analysis) near5 (encrypted packed) and ((machine near2 learn$4) (classifier near4 train$4))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/09 05:43
S10	18	("20100192222" | "9465940" | "9197663" | "20120079596" | "8719924" | "20140165203" | "20070240220").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/09 05:44
S11	4	S10 and train$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/09 05:45
S12	6	S10 and (train$4 learn$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/09 05:45
S13	364	(G06F21/562 OR G06F21/565 OR G06F2221/033 OR G06F8/53).CPC. AND (G06N20/00).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/09 05:45
S14	215	(G06F21/562 OR G06F21/563 OR G06F21/564 OR G06F21/565).CPC. AND (G06N20/00).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/09 05:47
S15	84	S14 and @ad<"20150512"	US-PGPUB; USPAT;	OR	ON	2019/07/09 05:47

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S16	4	(US-20090300765-$ or US-20130291111-$ or US-20160156646-$).did. or (EP-2182458-$).did.	US-PGPUB; FPRS	OR	ON	2019/07/09 09:42
S17	2	S16 and (encrypt$4 decrypt$4 pack$4 unpack$4 (windows adj portable) pe!)	US-PGPUB; FPRS	OR	ON	2019/07/09 09:43
S18	144	(character adj string) with (encrypted packed compressed) near2 (executable file)	US-PGPUB; FPRS	OR	ON	2019/07/09 16:40
S19	0	(character adj string) with (encrypted packed compressed) near2 (executable file) and classifier	US-PGPUB; FPRS	OR	ON	2019/07/09 16:47
S20	41718	(G06F21/562 OR G06F21/565 OR G06F2221/033 OR G06F8/53 OR G06N20/00).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/10 06:45
S21	77	S20 and (packed near (file executable))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/10 06:45
S22	3	S20 and (packed near (file executable)) and (train$4 near3 (packed encrypted compressed))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/10 06:47
S23	147	(machine near2 learn$4) and train$4 with (encrypted packed obfuscated)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/10 16:29
S24	56	(machine near2 learn$4) and train$4 with (encrypted packed obfuscated) and (vector feature) with (encrypted packed obfuscated)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/10 17:18
S25	4	classify$4 with malicious with benign with (unwanted undesirable)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 05:57
S26	10	(classify$4 classifi$7) with malicious with benign with (unwanted undesirable)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 05:57
S27	29	(("20150128263" | "20130304676" | "20120227105" | "20040111453" | "20090013405" | "20160072833" | "20090282485" | "20160021174" | "20150213365" | "20140181792" | "20130347094" | "20150154397").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 06:02
S28	3	"20090013405".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 06:07
S29	6736	(feature adj vector) and svm	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 10:09
S30	5881	(set$4 disabl$4 ignor$4) near3 (feature) with (classifier)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 11:42

S31	47	(set$4 disabl$4 ignor$4) near3 (feature) with (classifier) same (feature) near4 (range)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 11:43
S32	2	(disabl$4 ignor$4) near3 (feature) with (classifier) same (feature) near4 (threshold range)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 12:34
S33	1853	(feature) with includ$4 with (vector) with (threshold range)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 12:35
S34	393	(feature) with includ$4 with (vector) with (threshold range) near3 (point feature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 12:35
S35	74	(feature) with includ$4 with (vector) with (threshold range) near3 (point feature) and (machine adj learning)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 12:35
S36	3	"20120079596".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 13:20
S37	303	malware and (categor$8 classif$8 type) with weight$4 with feature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 13:31
S38	263	malware and (categor$8 classif$8 type) with weight$4 with feature and (svm (machine adj learning))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 13:32
S39	13	(machine adj learning) and malware and ((prevent$4 block$4) near2 execut$4) with threshold	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 14:21
S40	220	(machine adj learning) and (feature adj vector) and (ignor$4) near2 (feature (data adj point))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 14:38
S41	6	(machine adj learning) and (feature adj vector) and (ignor$4) near2 (feature (data adj point)) with (range threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 14:38
S42	0	(machine adj learning) and (feature adj vector) and (disregard$4) near2 (feature (data adj point)) with (range threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 14:50
S43	969	range near2 (data value) with (turn$4 adj off)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 15:32
S44	2	range near2 (data value) with (turn$4 adj off) with classifier	US-PGPUB; USPAT;	OR	ON	2019/07/11 15:33

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S45	24	((disabl$4) (turn$4 adj off)) with feature with classifier	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 15:34
S46	190	((exclu$4) (turn$4 adj off)) with feature with classifier	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 15:59
S47	187	((exclu$4)) with feature with classifier	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 15:59
S48	17	((exclu$4)) with feature with classifier with (range threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 15:59
S49	9	(machine adj learning) and (feature adj vector) and (exclu$4) near2 (feature (data adj point)) with (range threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 16:03
S50	22	((exclu$4)) with feature with classifier same (range threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 16:04
S51	16	(US-20090300765-$ or US-20130291111-$ or US-20160156646-$ or US-20140310517-$ or US-20120227105-$ or US-20160021174-$ or US-20090013405-$ or US-20090274376-$ or US-20120079596-$ or US-20180365573-$ or US-20100082642-$ or US-20170262633-$).did. or (US-9465940-$ or US-8510836-$ or US-9197663-$).did. or (EP-2182458-$).did.	US-PGPUB; USPAT; FPRS	OR	ON	2019/07/11 16:07

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S52	21382	(G06F21/562 OR G06F21/565 OR G06F2221/033 OR G06F8/53 OR G06N20/00).CPC.	US-PGPUB; USPAT	OR	ON	2019/07/11 16:08
S53	4	S52 and (((turn$4 adj off) disregard$4 exclu$4 ignor$4) near2 (feature)).clm. and range.clm.	US-PGPUB; USPAT	OR	ON	2019/07/11 16:09
S54	4	S52 and (((turn$4 adj off) disregard$4 exclu$4 ignor$4) near2 (feature)).clm. and classifier.clm.	US-PGPUB; USPAT	OR	ON	2019/07/11 16:10

7/ 11/ 2019 4:11:33 PM
C:\ Users\ msimitoski\ Documents\ EAST\ Workspaces\ 14\ 14_709875_threat_detection_static_analysis_without_decrypting_unpacking.wsp

Classification of packed executables for accurate computer virus detection

Search within citing articles

Bitshred: feature hashing malware for scalable triage and semantic analysis

J Jang, D Brumley, S Venkataraman - ... of the 18th ACM conference on ..., 2011 - dl.acm.org

The sheer volume of new malware found each day is growing at an exponential pace. This growth has created a need for automatic malware triage techniques that determine what malware is similar, what malware is unique, and why. In this paper, we present BitShred, a ...

☆ 99 Cited by 246 Related articles All 10 versions »

Opcode sequences as representation of executables for data-mining-based unknown malware detection

I Santos, F Brezo, X Ugarte-Pedrero, PG Bringas - Information Sciences, 2013 - Elsevier

Malware can be defined as any type of malicious code that has the potential to harm a computer or network. The volume of malware is growing faster every year and poses a serious global security threat. Consequently, malware detection has become a critical topic ...

☆ 99 Cited by 238 Related articles All 6 versions

Malware detection using statistical analysis of byte-level file content

SM Tabish, MZ Shafiq, M Farooq - ... of the ACM SIGKDD Workshop on ..., 2009 - dl.acm.org

Commercial anti-virus software are unable to provide protection against newly launched (aka" zero-day") malware. In this paper, we propose a novel malware detection technique which is based on the analysis of byte-level file content. The novelty of our approach ...

☆ 99 Cited by 168 Related articles All 7 versions »

Pe-miner: Mining structural information to detect malicious executables in realtime

MZ Shafiq, SM Tabish, F Mirza, M Farooq - International Workshop on ..., 2009 - Springer

In this paper, we present an accurate and realtime PE-Miner framework that automatically extracts distinguishing features from portable executables (PE) to detect zero-day (ie previously unknown) malware. The distinguishing features are extracted using the structural ...

☆ 99 Cited by 147 Related articles All 18 versions »

McBoost: Boosting scalability in malware collection and analysis using statistical classification of executables

R Perdisci, A Lanzi, W Lee - 2008 Annual Computer Security ..., 2008 - ieeexplore.ieee.org

In this work, we propose Malware Collection Booster (McBoost), a fast statistical malware detection tool that is intended to improve the scalability of existing malware collection and analysis approaches. Given a large collection of binaries that may contain both hitherto ...

☆ 99 Cited by 137 Related articles All 11 versions

Dynamical behavior of computer virus on Internet

X Han, Q Tan - Applied Mathematics and Computation, 2010 - Elsevier

In this paper, we presented a computer virus model using an SIRS model and the threshold value R 0 determining whether the disease dies out is obtained. If R 0 is less than one, the disease-free equilibrium is globally asymptotically stable. By using the time delay as a ...

☆ 99 Cited by 134 Related articles All 4 versions

A close look on n-grams in intrusion detection: anomaly detection vs. classification

C Wressnegger, G Schwenk, D Arp... - Proceedings of the 2013 ..., 2013 - dl.acm.org

Detection methods based on n-gram models have been widely studied for the identification of attacks and malicious software. These methods usually build on one of two learning schemes: anomaly detection, where a model of normality is constructed from n-grams, or ...

☆ 99 Cited by 72 Related articles All 17 versions »

A static, packer-agnostic filter to detect similar malware samples

G Jacob, PM Comparetti, M Neugschwandtner... - ... on Detection of ..., 2012 - Springer

The steadily increasing number of malware variants is a significant problem, clogging the input queues of automated analysis tools. The generation of malware variants is made easy by automatic packers and polymorphic engines, which produce by encryption and ...

☆ 99 Cited by 67 Related articles All 19 versions »

Dexhunter: toward extracting hidden code from packed android applications

Y Zhang, X Luo, H Yin - European Symposium on Research in Computer ..., 2015 - Springer

The rapid growth of mobile application (or simply app) economy provides lucrative and profitable targets for hackers. Among OWASP's top ten mobile risks for 2014, the lack of binary protections makes it easy to reverse, modify, and repackage Android apps. Recently ...

☆ 99 Cited by 62 Related articles All 5 versions »

PE-probe: leveraging packer detection and structural information to detect malicious portable executables

MZ Shafiq, S Tabish, M Farooq - ... of the Virus Bulletin Conference (VB), 2009 - nexginrc.org

The number of executable malware and the sophistication of their destructive ability has exponentially increased in past couple of years. Malware writers use sophisticated code obfuscation and encryption (aka packing) techniques to circumvent signatures–derived from ...

☆ 99 Cited by 60 Related articles All 5 versions »

Comparing files using structural entropy

I Sorokin - Journal in computer virology, 2011 - Springer

One of the main trends in the modern anti-virus industry is the development of algorithms that help estimate the similarity of files. Since malware writers tend to use increasingly complex techniques to protect their code such as obfuscation and polymorphism, anti-virus ...

☆ 99 Cited by 54 Related articles All 4 versions »

Webwitness: Investigating, categorizing, and mitigating malware download paths

T Nelms, R Perdisci, M Antonakakis... - 24th {USENIX} Security ..., 2015 - usenix.org

Most modern malware download attacks occur via the browser, typically due to social engineering and driveby downloads. In this paper, we study the "origin" of malware download attacks experienced by real network users, with the objective of improving ...

☆ 99 Cited by 52 Related articles All 11 versions »

Security Busters: Web browser security vs. rogue sites

N Virvilis, A Mylonas, N Tsalis, D Gritzalis - Computers & Security, 2015 - Elsevier

URL blacklists are used by the majority of modern web browsers as a means to protect users from rogue web sites, ie those serving malware and/or hosting phishing scams. There is a plethora of URL blacklists/reputation services, out of which Google's Safe Browsing and ...

☆ 99 Cited by 43 Related articles All 5 versions

Lines of malicious code: insights into the malicious software industry

M Lindorfer, A Di Federico, F Maggi... - Proceedings of the 28th ..., 2012 - dl.acm.org

Malicious software installed on infected computers is a fundamental component of online crime. Malware development thus plays an essential role in the underground economy of cyber-crime. Malware authors regularly update their software to defeat defenses or to ...

☆ 99 Cited by 41 Related articles All 19 versions

Collective classification for packed executable identification

I Santos, X Ugarte-Pedrero, B Sanz... - Proceedings of the 8th ..., 2011 - dl.acm.org

Malware is any software designed to harm computers. Commercial anti-virus are based on signature scanning, which is a technique effective only when the malicious executables have been previously analysed and identified. Malware writers employ several techniques ...

☆ 99 Cited by 39 Related articles All 7 versions »

Measuring and detecting malware downloads in live network traffic

P Vadrevu, B Rahbarinia, R Perdisci, K Li... - ... on Research in ..., 2013 - Springer

In this paper, we present AMICO, a novel system for measuring and detecting malware downloads in live web traffic. AMICO learns to distinguish between malware and benign file downloads from the download behavior of the network users themselves. Given a labeled ...

☆ 99 Cited by 38 Related articles All 9 versions »

Experimental study of fuzzy hashing in malware clustering analysis

Y Li, SC Sundaramurthy, AG Bardas, X Ou... - 8th Workshop on Cyber ..., 2015 - usenix.org

Malware triaging is the process of analyzing malicious software applications' behavior to develop detection signatures. This task is challenging, especially due to the enormous number of samples received by the vendors with limited amount of analyst time. Triaging ...

☆ 99 Cited by 35 Related articles All 6 versions »

Pattern recognition techniques for the classification of malware packers

L Sun, S Versteeg, S Boztaş, T Yann - Australasian Conference on ..., 2010 - Springer

Packing is the most common obfuscation method used by malware writers to hinder malware detection and analysis. There has been a dramatic increase in the number of new packers and variants of existing ones combined with packers employing increasingly ...

☆ 99 Cited by 35 Related articles All 11 versions »

Sigmal: A static signal processing based malware triage

D Kirat, L Nataraj, G Vigna, BS Manjunath - Proceedings of the 29th ..., 2013 - dl.acm.org

In this work, we propose SigMal, a fast and precise malware detection framework based on signal processing techniques. SigMal is designed to operate with systems that process large amounts of binary samples. It has been observed that many samples received by such ...

☆ 99 Cited by 34 Related articles All 14 versions

Global stability of a delayed SIRS computer virus propagation model

Y Muroya, Y Enatsu, H Li - International Journal of Computer ..., 2014 - Taylor & Francis

International Journal of Computer Mathematics, 2014 Vol. 91, No. 3, 347–367, http://dx.doi.org /10.1080/00207160.2013.790534 ... Global stability of a delayed SIRS computer virus propagation model ... Yoshiaki Muroyaa*, Yoichi Enatsub† and Huaixing Lic ... (Received 12 September ...

☆ 99 Cited by 33 Related articles All 5 versions

Opem: A static-dynamic approach for **machine-learning**-based **malware** detection

I Santos, J Devesa, F Brezo, J Nieves... - ... Joint Conference CISIS' ..., 2013 - Springer

... that have been either **compressed** or cyphered) [6] or complex obfuscation tech- niques [7]. On the contrary ... The **machine-learning** classifiers achieved high performance in classifying unknown **malware** ... First, regarding the static approach, it cannot counter **packed malware** ...

☆ 99 Cited by 98 Related articles All 4 versions »

Malware scanning of **compressed** computer files

NJ Hursey, WA McEwan - US Patent 7,107,617, 2006 - Google Patents

... 04-20, 2007-11-08, Boney Matthew L, Method and system for detecting a **compressed** pestware executable ... US20080028388A1 (en) *, 2006-07-26, 2008-01-31, Michael Burtscher, System and method for analyzing **packed** files ... Embedded anti-**virus** scanner for a network adapter ...

☆ 99 Cited by 210 Related articles All 4 versions »

Static **malware** analysis using **machine learning** methods

HV Nath, BM Mehtre - International Conference on Security in Computer ..., 2014 - Springer

... 25. Lyda, R., Hamrock, J.: Using entropy analysis to find **encrypted** and **packed** mal- ware ... IEEE (2001) 36. Shabtai, A., Moskovitch, R., Elovici, Y., Glezer, C.: Detection of malicious code by applying **machine learning** classifiers on static features: A state-of-the-art survey ...

☆ 99 Cited by 50 Related articles All 4 versions »

Semi-supervised learning for unknown **malware** detection

I Santos, J Nieves, PG Bringas - International Symposium on Distributed ..., 2011 - Springer

... 3. Kang, M., Poosankam, P., Yin, H.: Renovo: A hidden code extractor for **packed** exe- cutables ... **Virus** Bulletin (2001) 8. Moskovitch, R., Stopel, D., Feher, C., Nissim, N., Elovici, Y.: Unknown malcode detec ... Schapire, R.: The boosting approach to **machine learning**: An overview ...

☆ 99 Cited by 68 Related articles All 9 versions »

Machine learning for android **malware** detection using permission and api calls

N Peiravian, X Zhu - ... 25th international conference on tools with ..., 2013 - ieeexplore.ieee.org

... In our design, the permission is extracted from each App's profile information and the APIs are extracted from the **packed** App file by ... 10] Breiman, L. Bagging Predictors , **Machine Learning** 26, No ... [12] J. Kephart and W. Arnold, Automatic extraction of computer **virus** signatures In ...

☆ 99 Cited by 177 Related articles All 4 versions

Collective classification for **packed** executable identification

I Santos, X Ugarte-Pedrero, B Sanz... - Proceedings of the 8th ..., 2011 - dl.acm.org

... [9] G. Holmes, A. Donkin, and IH Witten. Weka: a **machine learning** workbench. pages 357–361, August 1994. [10] L. Julus ... [13] R. Lyda and J. Hamrock. Using entropy analysis to find **encrypted** and **packed malware**. IEEE Security & Privacy, 5(2):40–45, 2007 ...

☆ 99 Cited by 39 Related articles All 7 versions »

Malware and **machine learning**

C LeDoux, A Lakhotia - Intelligent Methods for Cyber Warfare, 2015 - Springer

... input. 5.2 Packing. Packing is a process whereby an arbitrary executable is taken and **encrypted** and **compressed** into a "**packed**" form that must be uncompressed and decrypted, ie "unpacked", before execution. This ...

☆ 99 Cited by 20 Related articles All 4 versions »

Malwise—an effective and efficient classification system for **packed** and polymorphic **malware**

S Cesare, Y Xiang, W Zhou - IEEE Transactions on Computers, 2012 - ieeexplore.ieee.org

... entropy of the analyzed data is low, then it is presumed that no more **compressed** or **encrypted** data are left to be unpacked ... CESARE ET AL.: MALWISE—AN EFFECTIVE AND EFFICIENT CLASSIFICATION SYSTEM FOR **PACKED** AND POLYMORPHIC **MALWARE** ...

☆ 99 Cited by 89 Related articles All 7 versions

Semi-supervised learning for **packed** executable detection

X Ugarte-Pedrero, I Santos, PG Bringas... - ... on Network and ..., 2011 - ieeexplore.ieee.org

... [21] R. Lyda and J. Hamrock, "Using entropy analysis to find **encrypted** and **packed** ... [24] Y. Singh, A. Kaur, and R. Malhotra, "Comparative analysis of regression and **machine learning** methods for ... [25] R. Perdisci, A. Lanzi, and W. Lee, "Classification of **packed** executables for ...

☆ 99 Cited by 11 Related articles All 5 versions

Image visualization based **malware** detection

K Kancherla, S Mukkamala - 2013 IEEE Symposium on ..., 2013 - ieeexplore.ieee.org

... Keywords- **Malware** Detection; **Machine Learning**; Support Vector Machines (SVMs); Textures based Features ... Static analysis is computationally efficient but performance is affected by **packed** or **encrypted malware** ...

☆ 99 Cited by 32 Related articles All 2 versions

Malware analysis and classification: A survey

E Gandotra, D Bansal, S Sofat - Journal of Information Security, 2014 - file.scirp.org

... This is a useful tech- nique to analyze **packed** executables which are ... obfuscation techniques, which transform the **malware** binaries into self **compressed** and uniquely ... Several Artificial Intel- ligence techniques, particularly **machine-learning** based techniques have been used in ...

☆ 99 Cited by 173 Related articles All 5 versions »

Detection of **packed malware**

D Devi, S Nandi - Proceedings of the First International Conference on ..., 2012 - dl.acm.org

... The new program embeds an **encrypted** version of the input executable and a decryption routine ... section [2]. As reported in [2], the combined data ie the code and the data section is **compressed** into a single section of the resulting **packed** binary and stored in section UPX1 ...

☆ 99 Cited by 9 Related articles »

Malware scanning of **compressed** computer files

NJ Hursey, WA McEwan - US Patent 7,234,165, 2007 - Google Patents

... System and method for analyzing **packed** files ... **Compressed** data pattern matching ... US9292688B2 (en) *, 2012-09-26, 2016-03-22, Northrop Grumman Systems Corporation, System and method for automated **machine-learning**, zero-day **malware** detection ...

☆ 99 Cited by 18 Related articles All 2 versions »

Malware detection methods for fixed and mobile networks

G McWilliams - Centre for Secure Information Technologies ..., 2013 - docbox.etsi.org

... Android applications are written in Java and packaged along with data and resource files into a single **compressed** .apk package ... Static analysis coupled with **machine learning** is an effective tool for ... Content-type: text/html actual content garbage (**encrypted**/obfuscated) ...

☆ 99 Cited by 21 Related articles All 2 versions »

Malware detection using **machine learning**

D Gavrilut, M Cimpoesu, D Anton... - ... on Computer Science ..., 2009 - ieeexplore.ieee.org

... 2. A **machine learning** system based firstly on one-sided perceptrons, and then on feature mapped one-sided ... We also use clean files that are **packed** or have the same form or the same ... The **malware** files in the training dataset have been taken from the **Virus** Heaven collection ...

☆ 99 Cited by 70 Related articles All 8 versions

Opcode-sequence-based semi-supervised unknown **malware** detection

I Santos, B Sanz, C Laorden, F Brezo... - ... Intelligence in Security for ..., 2011 - Springer

... Y., Kaur, A., Malhotra, R.: Comparative analysis of regression and **machine learning** methods for ... M., Poosankam, P., Yin, H.: Renovo: A hidden code extractor for **packed** executables ... R., Lee, W.: Polyunpack: Automating the hidden-code extraction of unpack-executing **malware** ...

☆ 99 Cited by 33 Related articles All 12 versions »

Using entropy analysis to find **encrypted** and **packed malware**

R Lyda, J Hamrock - IEEE Security & Privacy, 2007 - ieeexplore.ieee.org

... Limitations of the approach It's infeasible to absolutely determine if a sample contains **compressed** or **encrypted** bytes ... Figure 3. Total number of **encrypted** sections over the six-year study period ... 2006; www.virusbtn. com/virusbulletin/archive/2006/03/vb200603-**packed** ...

☆ 99 Cited by 297 Related articles All 10 versions

Detecting **packed** executables using steganalysis

C Burgess, F Kurugollu, S Sezer... - 2014 8th European ..., 2014 - ieeexplore.ieee.org

... With packing, an input file is **encrypted** and **compressed** and stored within ... bitmap images coupled with the use of a blind steganalysis technique [12] to generate features which are used in conjunction with **machine learning** algorithms in order to detect **packed** executables ...

☆ 99 Cited by 9 Related articles All 2 versions

Using opcode sequences in single-class learning to detect unknown **malware**

I Santos, F Brezo, B Sanz, C Laorden, PG Bringas - IET information security, 2011 - IET

... Since our method would not be able to detect **packed** executable, we removed any **packed** **malware** before selecting the ... believe that our results will have a strong impact on the study of unknown **malware** detection, which usually relies on supervised **machine learning** ...

☆ 99 Cited by 38 Related articles All 13 versions »

A survey on heuristic **malware** detection techniques

Z Bazrafshan, H Hashemi, SMH Fard... - The 5th Conference on ..., 2013 - ieeexplore.ieee.org

... Then, the engine and **malware** are **encrypted** using the produced algorithm and new decryption key is connected to them ... Springer, Berlin. 2006. [40] Z. Zhao, "A **virus** detection scheme ... [41] TM Mitchell, "**Machine learning** and data mining," Commun. ACM, vol. 42, no. 11, 1999 ...

☆ 99 Cited by 101 Related articles All 4 versions »

Using entropy analysis to find encrypted and **packed malware**

R Lyda, J Hamrock - IEEE Security & Privacy, 2007 - ieeexplore.ieee.org

... Numbers," Random.org, June 1999; www.random. org/essay.html. 5. A. Stephan, "Improving Proactive **Detection** of **Packed Malware**," Virus Bulletin, 01 Mar. 2006; www.virusbtn. com/virusbulletin/archive/2006/03/vb200603-**packed** ...

☆ 99 Cited by 297 Related articles All 10 versions

Classification of **packed** executables for accurate computer virus **detection**

R Perdisci, A Lanzi, W Lee - Pattern recognition letters, 2008 - Elsevier

... http://peid.has.it), (very likely) the most used signature-based **detector** for **packed** ... afterwards scanned by an anti-virus software, therefore improving virus **detection** accuracy while ... R. Lyda, J. HamrockUsing entropy analysis to find encrypted and **packed malware**. IEEE Security ...

☆ 99 Cited by 171 Related articles All 10 versions

Omniunpack: Fast, generic, and safe unpacking of **malware**

L Martignoni, M Christodorescu... - Twenty-Third Annual ..., 2007 - ieeexplore.ieee.org

... Requirements for Signatures We identify three requirements that the signatures used by the **malware detector** have to satisfy to guaran- tee accurate **detection**. First, the signature needs to characterize the real malicious payload, not the **packed** code or the unpack- 436 Page 7 ...

☆ 99 Cited by 252 Related articles All 12 versions

Malware detection using statistical analysis of byte-level file content

SM Tabish, MZ Shafiq, M Farooq - ... of the ACM SIGKDD Workshop on ..., 2009 - dl.acm.org

... ARCHITECTURE OF PROPOSED TECH- NIQUE In this section, we explain our data mining based **malware detection** ... We first describe the benign and then the **malware** dataset used in our experiments ... to note that in this work we are not differentiating between **packed** and non ...

☆ 99 Cited by 168 Related articles All 7 versions »

Revealing **packed malware**

W Yan, Z Zhang, N Ansari - ieee seCurity & PrivaCy, 2008 - ieeexplore.ieee.org

... However, viruses have used packers widely to avoid **detection**, and packers are increasingly in corporated into some **malware** families. Reportedly, among 735 malwares collected for the Wild List in March 2006, more than 92 percent were **packed** by crypters and packers from ...

☆ 99 Cited by 118 Related articles All 11 versions

Automatic generation of string signatures for **malware detection**

K Griffin, S Schneider, X Hu, TC Chiueh - ... advances in intrusion **detection**, 2009 - Springer

... **Malware Detection** ... Hancock begins by recursively unpacking **malware** files using Symantec's un- packing engine. It rejects files that are **packed** and cannot be unpacked, according to this engine, PEiD [1], and entropy analysis, and stores 48-byte sequences from these files in a ...

☆ 99 Cited by 190 Related articles All 10 versions »

Opcode sequences as representation of executables for data-mining-based unknown **malware detection**

I Santos, F Brezo, X Ugarte-Pedrero, PG Bringas - Information Sciences, 2013 - Elsevier

... are limited as they count certain bytes in the **malware** body; because most of the common transformations operate at the source level, these **detection** methods can be easily thwarted [14]. These approaches were also used by Perdisci et al. [54] to detect **packed** executables ...

☆ 99 Cited by 238 Related articles All 6 versions

PE File Header analysis-based **packed** PE file **detection** technique (PHAD)

Y Choi, I Kim, J Oh, J Ryou - International Symposium on ..., 2008 - ieeexplore.ieee.org

... The **packed** file **detection** rate of PHAD was approximately 93.59%, which is much higher than that of PEiD, which currently is the mostly commonly used **packed** file **detector**. PHAD is also very effective because it checks only the selected eight features ...

☆ 99 Cited by 41 Related articles All 4 versions

Opem: A static-dynamic approach for machine-learning-based **malware detection**

I Santos, J Devesa, F Brezo, J Nieves... - ... Joint Conference CISIS' ..., 2013 - Springer
... The future development of this **malware detection** system will be concentrated in three main research areas ... First, we will focus on facing **packed** executables using a dynamic unpacker ... analysis and the static dynamic in order to improve the results of this hybrid **malware detector** ...
☆ 99 Cited by 98 Related articles All 4 versions »

Semi-supervised learning for unknown **malware detection**

I Santos, J Nieves, PG Bringas - International Symposium on Distributed ..., 2011 - Springer
... **Packed malware** is produced by cyphering the payload of the executable and having it deciphered when finally loaded into memory. Indeed, broadly-used static **detection** methods can deal with **packed malware** only by using the signatures of the packers ...
☆ 99 Cited by 68 Related articles All 9 versions »

A survey on techniques in **detection** and analyzing **malware** executables

K Mathur, S Hiranwal - International Journal of Advanced ..., 2013 - pdfs.semanticscholar.org
... **Malware Detector** Signature or Behavior ... **Malware Detection** ... **Packed malware** codes can be treated as subset of obfuscated codes which are compressed and cannot be analyzed so, consequently unpacking phase is necessary to reveal the overall semantic of the code [11]. VII ...
☆ 99 Cited by 70 Related articles »

Malwise—an effective and efficient classification system for **packed** and polymorphic **malware**

S Cesare, Y Xiang, W Zhou - IEEE Transactions on Computers, 2012 - ieeexplore.ieee.org
... Identification of **malware** variants is essential to a **detection** system and is made possible by identifying invariant characteristics in related samples. To classify the **packed** and polymorphic **malware**, this paper proposes a novel system, named Malwise, for **malware** classification ...
☆ 99 Cited by 89 Related articles All 7 versions

A heuristic approach for **detection** of obfuscated **malware**

S Treadwell, M Zhou - 2009 IEEE International Conference on ..., 2009 - ieeexplore.ieee.org
... Among all 65 confirmed **packed malware** samples, we obtain 89.2% or higher **detection** rate with risk threshold of 3. Among all 144 **malware** samples, we flagged 84 suspicious files (58.3% **detection** rate) with threshold of 3, which is a reasonable result for us since our **detection** ...
☆ 99 Cited by 51 Related articles All 3 versions

Classification of **malware** using structured control flow

S Cesare, Y Xiang - Proceedings of the Eighth Australasian Symposium ..., 2010 - dl.acm.org
... 4.3 Entropy Analysis to Detect Completion of Hidden Code Extraction **Detection** of the original entry ... any newly written memory is executed, then the hidden code in the **packed** binary being ... approach, multiple layers or stages of hidden code may be present, and **malware** may be ...
☆ 99 Cited by 139 Related articles All 5 versions

Detection of **packed malware**

D Devi, S Nandi - Proceedings of the First International Conference on ..., 2012 - dl.acm.org
Packing is the most popular obfuscation technique used by malware writers' community in present scenario. The traditional signature-based anti-virus software had played a major role in malware detection, until the dawn of the trend of packed malware. Hence to evade ...
☆ 99 Cited by 9 Related articles »

McBoost: Boosting scalability in **malware** collection and analysis using statistical classification of executables

R Perdisci, A Lanzi, W Lee - 2008 Annual Computer Security ..., 2008 - ieeexplore.ieee.org
... and generalization abil- ity than other classification algorithms and signature-based **detection** approaches [13 ... of hidden-code extracted (using our unpacker) from **packed malware** and **packed** benign executables ... the results of modules A and B (ie, of the packer **detector** and the ...
☆ 99 Cited by 137 Related articles All 11 versions

Signature generation and **detection** of **malware** families

VS Sathyanarayan, P Kohli... - ... Conference on Information ..., 2008 - Springer
... cannot be detected. We now formally state our **malware detection** algo- rithm. The algorithm is composed of two parts: the signature generator SIGNA- TURE GENERATE (Algorithm 2) and the **detector** DETECT (Algorithm 3) ...
☆ 99 Cited by 111 Related articles All 11 versions »

A fast flowgraph based classification system for **packed** and polymorphic **malware** on the endhost

S Cesare, Y Xiang - 2010 24th IEEE International Conference ..., 2010 - ieeexplore.ieee.org
... **Detection** of variants is possible even when more significant changes to the **malware** source code are ... real content [7, 8]. Code packing is a post-processing transformation applied to **malware** after compilation. At runtime in a **packed** binary, the original content is revealed for ...
☆ 99 Cited by 57 Related articles All 5 versions

Malware detection based on structural and behavioural features of api calls

M Alazab, R Layton, S Venkataraman, P Watters - 2010 - ro.ecu.edu.au
... A **malware detector** scans the system in various locations for characteristic byte sequences or signature (s ... performed the verification and validation of our proposed method for **malware detection** based on ... If the existing tools are unable to unpack a **packed malware** that uses an ...
☆ 99 Cited by 59 Related articles All 8 versions »

PE-probe: leveraging packer **detection** and structural information to detect malicious portable executables

MZ Shafiq, S Tabish, M Farooq - ... of the Virus Bulletin Conference (VB), 2009 - nexginrc.org
... architecture of our PE-Probe **malware detection** system. Figure 1 shows the detailed architecture of PE-Probe. To remove the bias of structural features towards **packed**/non- **packed** executables, we have utilized two modules: 1. A non-signature based packer **detector** (M-1) to ...
☆ 99 Cited by 60 Related articles All 5 versions »

Related searches

computer virus detection packed **executables**

unknown malware detection

malware detection **string signatures**

malware detection **opcode sequence**

packed **executable identification**

machine learning based malware detection

malware detection **system**

malware detection **byte level**

malware detection **dynamic analysis**

file detection malware **forensics**

malware detection **automatic generation**

malware detection **file content**

malware detection **collective classification**

malware detection **semi-supervised learning**

malware detection **statistical analysis**

malware detection **data mining**

Detection of packed malware

Search within citing articles

Packer detection for multi-layer executables using entropy analysis

M Bat-Erdene, T Kim, H Park, H Lee - Entropy, 2017 - mdpi.com

Packing algorithms are broadly used to avoid anti-malware systems, and the proportion of packed malware has been growing rapidly. However, just a few studies have been conducted on detection various types of packing algorithms in a systemic way. Following this ...

☆ 99 Cited by 9 Related articles All 7 versions »

Machine learning aided static malware analysis: A survey and tutorial

A Shalaginov, S Banin, A Dehghantanha ... - Cyber Threat ..., 2018 - Springer

Malware analysis and detection techniques have been evolving during the last decade as a reflection to development of different malware techniques to evade network-based and host-based security protections. The fast growth in variety and number of malware species made ...

☆ 99 Cited by 5 Related articles All 6 versions »

The Effect of Code Obfuscation on Authorship Attribution of Binary Computer Files

S Hendrikse - 2017 - nsuworks.nova.edu

In many forensic investigations, questions linger regarding the identity of the authors of the software specimen. Research has identified methods for the attribution of binary files that have not been obfuscated, but a significant percentage of malicious software has been ...

☆ 99 Cited by 3 Related articles All 3 versions »

Lutte contre les botnets: analyse et stratégie

É Freyssinet - 2015 - hal.sorbonne-universite.fr

Les botnets, ou réseaux d'ordinateurs infectés par un code malveillant et connectés à un système de commande et de contrôle, constituent l'un des premiers outils de la délinquance sur Internet aujourd'hui. Ils permettent de concrétiser le développement d'un nouveau type ...

☆ 99 Cited by 1 Related articles All 17 versions »

Pin 을 이용한 안티디버깅 우회 설계 및 구현

홍수화 , 박용수 - 인터넷정보학회논문지, 2016 - papersearch.net

Pin 은 프로그램 동적 분석 도구를 생성할 수 있는 프레임워크로, 리눅스와 윈도우에서 사용자 영역의 프로그램 분석을 수행할 수 있게 한다. 역공학 방지 프로그램이나 악성코드는 프로그램 분석을 방해하는 안티디버깅이 적용되어 있기 때문에 Pin 을 사용한 분석이 어렵다. 본 ...

☆ 99 Cited by 1 Related articles All 3 versions »

Reverse Engineering Reverse Engineering Analysis Forensic Malware WEBC2-Div

RF Walilulu - Journal of Informatics, Information System ..., 2018 - journal.ittelkom-pwt.ac.id

At this paper focus on Malicious Software also known as Malware APT1 (Advance Persistent Threat) codename WEBC2-DIV the most variants malware has criteria consists of Virus, Worm, Trojan, Adware, Spyware, Backdoor either Rootkit. Although, malware could ...

☆ 99 Related articles »

On-line Shared Platform Evaluation Framework for Advanced Persistent Threats.

D Sohn, T Lee, J Kwak - KSII Transactions on Internet & ..., 2019 - search.ebscohost.com

Advanced persistent threats (APTs) are constant attacks of specific targets by hackers using intelligent methods. All current internal infrastructures are constantly subject to APT attacks created by external and unknown malware. Therefore, information security officers require a ...

☆ 99 Related articles All 2 versions

Reverse Engineering Analysis Statis Forensic Malware Webc2-Div

RF Wailulu, THI Alam - Insect (Informatics and Security) ..., 2018 - ejournal.um-sorong.ac.id

At this paper focus on Malicious Software also known as Malware APT1 (Advance Persistent Threat) codename WEBC2-DIV the most variants malware has criteria consists of Virus, Worm, Trojan, Adware, Spyware, Backdoor either Rootkit. Although, malware could ...

☆ 99 Related articles »

Reverse Engineering Analysis Forensic Malware WEBC2-DIV

RF Wailulu, THI Alam - KOMIK (Konferensi Nasional ..., 2018 - ejurnal.stmik-budidarma.ac.id

At this paper focus on Malicous Software also known as Malware APT1 (Advance Persistent Threat) codename WEBC2-DIV the most variants malware has criteria consists of Virus, Worm, Trojan, Adware, Spyware, Backdoor either Rootkit. Although, malware could ...

☆ 99 Related articles All 4 versions »

A heuristic approach for detection of obfuscated malware

Search within citing articles

Malware target recognition via static heuristics

T Dube, R Raines, G Peterson, K Bauer, M Grimaila... - Computers & ..., 2012 - Elsevier

Organizations increasingly rely on the confidentiality, integrity and availability of their information and communications technologies to conduct effective business operations while maintaining their competitive edge. Exploitation of these networks via the introduction ...

☆ 99 Cited by 34 Related articles All 5 versions

Exposé: Discovering potential binary code re-use

BH Ng, A Prakash - 2013 IEEE 37th Annual Computer Software ..., 2013 - ieeexplore.ieee.org

The use of third-party libraries in deployed applications can potentially put an organization's intellectual property at risk due to licensing restrictions requiring disclosure or distribution of the resulting software. Binary applications that are statically linked to buggy version (s) of a ...

☆ 99 Cited by 27 Related articles All 4 versions

Malware target recognition of unknown threats

TE Dube, RA Raines, MR Grimaila... - IEEE Systems ..., 2012 - ieeexplore.ieee.org

Organizations traditionally use signature-based commercial antivirus products as a frontline defense against malware, but advanced persistent threats craft custom malicious tools to achieve their objectives. Organizations safeguarding sensitive information have difficulty in ...

☆ 99 Cited by 20 Related articles All 3 versions

Statistical detection of malicious pe-executables for fast offline analysis

R Merkel, T Hoppe, C Kraetzer, J Dittmann - IFIP International Conference ..., 2010 - Springer

While conventional malware detection approaches increasingly fail, modern heuristic strategies often perform dynamically, which is not possible in many applications due to related effort and the quantity of files. Based on existing work from [1] and [2] we analyse an ...

☆ 99 Cited by 20 Related articles All 15 versions »

Malware detection in cloud computing

SS Hatem, MM El-Khouly - Int J Adv Comput Sci Appl, 2014 - pdfs.semanticscholar.org

Antivirus software is one of the most widely used tools for detecting and stopping malicious and unwanted files. However, the long term effect of traditional host based antivirus is questionable. Antivirus software fails to detect many modern threats and its increasing ...

☆ 99 Cited by 19 Related articles All 5 versions »

Obfuscation of stuxnet and flame malware

R Goyal, S Sharma... - Latest Trends in ..., 2012 - pdfs.semanticscholar.org

Malware is defined as a sequence of instructions performing actions intended by an attacker or hacker without the consent of the owner when executed. This paper gives overview of three main malwares: Stuxnet, Flame and MyDoom and obfuscation of these malware. The ...

☆ 99 Cited by 16 Related articles All 2 versions »

Instructions-based detection of sophisticated obfuscation and packing

M Saleh, EP Ratazzi, S Xu - 2014 IEEE Military ..., 2014 - ieeexplore.ieee.org

Every day thousands of malware are released online. The vast majority of these malware employ some kind of obfuscation ranging from simple XOR encryption, to more sophisticated anti-analysis, packing and encryption techniques. Dynamic analysis methods can unpack ...

☆ 99 Cited by 12 Related articles All 11 versions

PEAL—packed executable analysis

V Laxmi, MS Gaur, P Faruki, S Naval - International Conference on ..., 2011 - Springer

The proliferation of packed malware has posed a serious threat to computers connected to Internet across the globe. Packers are popular tools used by malware authors to hide malicious payloads that bypass traditional signature antiviruses (AV). Packing being the ...

☆ 99 Cited by 10 Related articles All 5 versions »

Malware type recognition and cyber situational awareness

T Dube, R Raines, G Peterson, K Bauer... - 2010 IEEE Second ..., 2010 - ieeexplore.ieee.org

Current technologies for computer network and host defense do not provide suitable information to support strategic and tactical decision making processes. Although pattern-based malware detection is an active research area, the additional context of the type of ...

☆ 99 Cited by 10 Related articles All 6 versions »

The study of evasion of packed pe from static detection

M Baig, P Zavarsky, R Ruhl... - World Congress on ..., 2012 - ieeexplore.ieee.org

Static detection of packed portable executables (PEs) relies primarily on structural properties of the packed PE, and also on anomalies in the packed PE caused by packing tools. This paper outlines weaknesses in this method of detection. We show that these structural ...

☆ 99 Cited by 10 Related articles All 3 versions

Detecting packed executables using steganalysis

C Burgess, F Kurugollu, S Sezer... - 2014 8th European ..., 2014 - ieeexplore.ieee.org

This paper proposes a novel method of detecting packed executable files using steganalysis, primarily targeting the detection of obfuscated malware through packing. Considering that over 80% of malware in the wild is packed, detection accuracy and low ...

☆ 99 Cited by 9 Related articles All 2 versions

A static heuristic approach to detecting malware targets

M Zakeri, F Faraji Daneshgar... - Security and ..., 2015 - Wiley Online Library

Nowadays malware writers usually employ several obfuscation techniques to evade detection. The number of variants detected each day has been increasing significantly. Unfortunately traditional detection approaches such as signature scanning are becoming ...

☆ 99 Cited by 8 Related articles All 2 versions »

A Novel Approach to Malware Detection using Static Classification

S Singla, E Gandotra, D Bansal... - International Journal of ..., 2015 - academia.edu

Malware, commonly called computer virus, is one of the top security threats to the computer systems around the globe. These are evolving at a very rapid pace and are continually finding new ways to exploit and infect the systems of various enterprises and businesses ...

☆ 99 Cited by 7 Related articles »

Malicious data classification using structural information and behavioral specifications in executables

S Kumar, CR Krishna, N Aggarwal... - ... Recent Advances in ..., 2014 - ieeexplore.ieee.org

With the rise in the underground Internet economy, automated malicious programs popularly known as malwares have become a major threat to computers and information systems connected to the internet. Properties such as self healing, self hiding and ability to deceive ...

☆ 99 Cited by 7 Related articles All 3 versions

A novel malware target recognition architecture for enhanced cyberspace situation awareness

TE Dube - 2011 - apps.dtic.mil

The rapid transition of critical business processes to computer networks potentially exposes organizations to digital theft or corruption by advanced competitors. One tool used for these tasks is malware, because it circumvents legitimate authentication mechanisms. Malware is ...

☆ 99 Cited by 7 Related articles All 5 versions »

Metamorphic malware analysis and detection methods

P Vinod, V Laxmi, MS Gaur - Cyber security, cyber crime and cyber ..., 2011 - igi-global.com

The term 'malware'is collectively used for any program which accesses the system through surreptitious (often unauthorized) means, with malicious intent, resulting in data loss and/or corruption. Some examples are viruses, worms, trojans, botnets etc. Malware is becoming a ...

☆ 99 Cited by 5 Related articles All 4 versions »

A heuristics-based static analysis approach for detecting packed pe binaries

R Arora, A Singh, H Pareek, UR Edara - International Journal of Security ..., 2013 - earticle.net

Malware authors evade the signature based detection by packing the original malware using custom packers. In this paper, we present a static heuristics based approach for the detection of packed executables. We present 1) the PE heuristics considered for analysis ...

☆ 99 Cited by 10 Related articles All 5 versions »

The threat of obfuscated zero day polymorphic malwares: An analysis

B Wanswett, HK Kalita - 2015 International Conference on ..., 2015 - ieeexplore.ieee.org

When a Zero day malware crops up and with the advent of polymorphism and obfuscation, such malware poses a serious threat to unsuspecting victims of such attack. In this paper we will analyze the current scenario of such a malware threat that is obfuscated and ...

☆ 99 Cited by 4 Related articles

REDIR: automated static detection of obfuscated anti-debugging techniques

AJ Smith, RF Mills, AR Bryant... - ... and Systems (CTS), 2014 - ieeexplore.ieee.org

Reverse Code Engineering (RCE) to detect anti-debugging techniques in software is a very difficult task. Code obfuscation is an anti-debugging technique makes detection even more challenging. The Rule Engine Detection by Intermediate Representation (REDIR) system for ...

☆ 99 Cited by 4 Related articles All 7 versions »

Detecting and classifying morphed malwares: A survey

S Singla, E Gandotra, D Bansal, S Sofat - International Journal of ..., 2015 - Citeseer

In this era, most of the antivirus companies are facing immense difficulty in detecting morphed malwares as they conceal themselves from detection. Malwares use various techniques to camouflage themselves so as to increase their lifetime. These obscure ...

☆ 99 Cited by 4 Related articles All 4 versions »

Opem: A static-dynamic approach for **machine-learning**-based malware detection

I Santos, J Devesa, F Brezo, J Nieves... - ... Joint Conference CISIS' ..., 2013 - Springer

... and the analysis and detection is usually fast [5]. However, they are not resilient to **packed malware** (executables Á ... The resulting **vector** for each pro- gram's trace is a finite sequence of bits, a proper ... A Static-Dynamic Approach for **Machine-Learning**-Based Malware Detection ...

☆ 99 Cited by 99 Related articles All 4 versions »

Semi-supervised learning for unknown malware detection

I Santos, J Nieves, PG Bringas - International Symposium on Distributed ..., 2011 - Springer

... as a vectorial function such as F : X → Rc to assign a **vector** Fi to ... Indeed, broadly-used static detection methods can deal with **packed malware** only by using the signatures of ... While **machine-learning** meth- ods are a suitable approach for unknown malware, they require a high ...

☆ 99 Cited by 68 Related articles All 9 versions »

Static malware analysis using **machine learning** methods

HV Nath, BM Mehtre - International Conference on Security in Computer ..., 2014 - Springer

... In case of **obfuscated malware**, each module would be decrypted only if that module is executed ... Page 6. Static Malware Analysis Using **Machine Learning** Methods 445 ... This method is used mainly to identify the packed and **encrypted malware**. It was proposed by Lyda at el ...

☆ 99 Cited by 50 Related articles All 4 versions »

Malware behavioural detection and vaccine development by using a support **vector** model classifier

P Wang, YS Wang - Journal of Computer and System Sciences, 2015 - Elsevier

... k-NN algorithm is among the simplest of all **machine learning** algorithms using instance-based ... the offset of a hyperplane from the origin along the normal **vector** W. Generally ... incorporating malware behavioural analysis in the AMDS is suitable for **encrypted malware** detection by ...

☆ 99 Cited by 31 Related articles All 3 versions

Zero-day malware detection based on supervised learning algorithms of API call signatures

M Alazab, S Venkatraman, P Watters... - Proceedings of the Ninth ..., 2011 - dl.acm.org

... 2006, researchers (Kolter & Maloof 2006) described the use of **machine learning** and data ... Kolter found that support **vector** machine performed exceptionally well and fast as compared ... Hence, for the **obfuscated malware** detection system, this research adopts SVM as a classifier ...

☆ 99 Cited by 114 Related articles All 7 versions

Image visualization based malware detection

K Kancherla, S Mukkamala - 2013 IEEE Symposium on ..., 2013 - ieeexplore.ieee.org

... Keywords- Malware Detection; **Machine Learning**; Support **Vector** Machines (SVMs); Textures based Features ... analysis is more efficient and is not affected by packed or **encrypted malware** ... However they did not consider **packed malware** (variety of packers) in their experiment ...

☆ 99 Cited by 32 Related articles All 2 versions

Using opcode sequences in single-class learning to detect unknown malware

I Santos, F Brezo, B Sanz, C Laorden, PG Bringas - IET Information security, 2011 - IET

... Semi-supervised learning is a type of **machine-learning** technique that is especially useful when a ... prediction, each test instance e [U is compared with each prototype **vector** e [P ... would not be able to detect packed executable, we removed any **packed malware** before selecting ...

☆ 99 Cited by 38 Related articles All 13 versions »

Malware detection based on structural and behavioural features of api calls

M Alazab, R Layton, S Venkataraman, P Watters - 2010 - ro.ecu.edu.au

... If the existing tools are unable to unpack a **packed malware** that uses an unknown packing algorithm, this ... the similarities and the distance of unknown malware with known behaviour so that **obfuscated malware** could be ... Support-**vector** network", **Machine Learning**, 20, 273-297 ...

☆ 99 Cited by 59 Related articles All 8 versions »

A survey on heuristic malware detection techniques

Z Bazrafshan, H Hashemi, SMH Fard... - The 5th Conference on ..., 2013 - ieeexplore.ieee.org

... Usually, a transformation engine is embedded in the **encrypted malware** that at any change ... They used this feature **vector** in order to detect **obfuscated malware** variants and to this ... method based on OpCode sequences [23] and trained several **machine learning** classifiers by ...

☆ 99 Cited by 101 Related articles All 4 versions »

Opcode sequences as representation of executables for data-mining-based unknown malware detection

I Santos, F Brezo, X Ugarte-Pedrero, PG Bringas - Information Sciences, 2013 - Elsevier

... In a previous work [66], we presented an approach focused on detecting **obfuscated malware** variants using ... Decision tree classifiers are a type of **machine-learning** classifiers that can be graphically ... Formally, the optimal hyperplane is represented by a **vector** w and a scalar m ...

☆ 99 Cited by 238 Related articles All 6 versions

Malware detection using adaptive data compression

Y Zhou, WM Inge - Proceedings of the 1st ACM workshop on Workshop ..., 2008 - dl.acm.org

... limitation of signature based anti-virus software is their susceptibility to **obfuscated malware** ... Several **machine learning** techniques have been investi- gated for identifying unknown malicious executables ... naive Bayes [14], k-nearest neigh- bor, support **vector** machines, decision ...

☆ 99 Cited by 47 Related articles All 3 versions »

Malware detection and classification based on extraction of API sequences

D Uppal, R Sinha, V Mehra ... - ... Conference on Advances ..., 2014 - ieeexplore.ieee.org

... obfuscation techniques, simply frauds antivirus scanners, thereby, decreasing the **obfuscated malware** detection rate ... comes the oligomorphic malware- they are the advancement of **encrypted malware**, such that ... of this approach was only that it does not work for **packed malware** ...

☆ 99 Cited by 24 Related articles All 2 versions

Reform: Relevant features for malware analysis

P Vinod, V Laxmi, MS Gaur - 2012 26th International ..., 2012 - ieeexplore.ieee.org

... The detection rate of 92% was reported for **obfuscated malware** executables ... http://www.virustotal.com/stats.html. [2] Open Source **Machine Learning** Software Weka. http://www ... [14] Yan, Wei and Zhang, Zheng and Ansari, Nirwan, Revealing **Packed Malware**, In Proc ...

☆ 99 Cited by 12 Related articles All 4 versions

Detecting packed executables using steganalysis

C Burgess, F Kurugollu, S Sezer... - 2014 8th European ..., 2014 - ieeexplore.ieee.org

... J. Hamrock, "Using Entropy Analysis to Find Encrypted and **Packed Malware**," Security & ... and Mian Zhou, "A Heuristic Approach for Detection of **Obfuscated Malware**," in Intelligence ... of Packed Executables Using Support **Vector** Machines," in **Machine Learning** and Cybernetics ...

☆ 99 Cited by 9 Related articles All 2 versions

An accurate packer identification method using support **vector** machine

R Isawa, T Ban, S Guo, D Inoue... - IEICE Transactions on ..., 2014 - search.ieice.org

... Our method applies string- kernel-based support **vector** machine (SVM): it can measure the ... key words: malware analysis, pack, unpack, **machine learning**, SVM ... 3] incur sig- nificant performance overhead because of monitoring each instruction of the **packed malware** program [5 ...

☆ 99 Cited by 3 Related articles All 6 versions

Mining control flow graph as api call-grams to detect portable executable malware

P Faruki, V Laxmi, MS Gaur, P Vinod - Proceedings of the Fifth ..., 2012 - dl.acm.org

... Moreover this approach did not work for **packed malware** ... Weka library has implemented set of pattern recognition, **machine learning** and clustering algorithms to perform bi- nary classification ... The proposed approach works well against the code **obfuscated malware** ...

☆ 99 Cited by 29 Related articles All 3 versions »

Mads: malicious android applications detection through string analysis

B Sanz, I Santos, J Nieves, C Laorden... - ... Conference on Network ..., 2013 - Springer

... Indeed, static detection methods can deal with **packed malware** only by using the signatures of the packers ... 57–64 (1995) 25. Quinlan, J.: C4.5 programs for **machine learning** ... Amari, S., Wu, S.: Improving support **vector** machine classifiers by modifying kernel functions ...

☆ 99 Cited by 22 Related articles All 7 versions

An efficient block-discriminant identification of **packed malware**

S Naval, V Laxmi, MS Gaur - Sadhana, 2015 - Springer

... Normalized FVT used as an input to **machine learning** classifiers (We have used WEKA ... is conducted to check the detection accuracy of our model with **packed malware** and native ... M vs N B : This experiment is performed to evaluate PEAL in the presence of **encrypted malware** ...

☆ 99 Cited by 7 Related articles All 6 versions »

Evolution and detection of polymorphic and metamorphic malwares: A survey

A Sharma, SK Sahay - arXiv preprint arXiv:1406.7061, 2014 - arxiv.org

... joined with the **encrypted malware** body to construct a new variant of malware [14] ... [25] Mitchell, TM "**Machine learning**", Burr Ridge, IL ... [30] Xu, M., Wu, L., Qi, S., Xu, J., Zhang, H., Ren, Y. and Zheng, N. "A similarity metric method of **obfuscated malware** using function-call graph ...

☆ 99 Cited by 43 Related articles All 8 versions »

Detection of **packed malware**

D Devi, S Nandi - Proceedings of the First International Conference on ..., 2012 - dl.acm.org

... It classifies the input packed executables as **packed malware** or packed benign executables respectively. Windows portable executable file has a large number of features ... It is a popular suite of **machine learning** software written in Java ... The feature **vector** consisting of these 2 ...

☆ 99 Cited by 9 Related articles »

Semi-supervised **learning** for unknown malware detection

I Santos, J Nieves, PG Bringas - International Symposium on Distributed ..., 2011 - Springer

... Indeed, broadly-used static detection methods can deal with **packed malware** only by using the signatures of the ... First, we plan to extend our study of semi-supervised **learning** approaches by applying more ... Second, we will use different features for **training** these kinds of models ...

☆ 99 Cited by 68 Related articles All 9 versions »

Collective classification for unknown malware detection

I Santos, C Laorden, PG Bringas - Proceedings of the ..., 2011 - ieeexplore.ieee.org

... results of FPR lower than 5%, Collective Forest only needs to be **trained** with a ... **Training** the model through supervised machine-**learning** algorithms can be a problem itself because ... First, because of the static nature of the proposed method, it cannot counter **packed malware** ...

☆ 99 Cited by 40 Related articles All 8 versions »

Opem: A static-dynamic approach for machine-**learning**-based malware detection

I Santos, J Devesa, F Brezo, J Nieves ... - ... Joint Conference CISIS' ..., 2013 - Springer

... and detection is usually fast [5]. However, they are not resilient to **packed malware** (executables Á ... step, we conducted the **learning** phase of the algorithms with the **training** datasets, applying ... In particular, the best overall results were obtained by SVM **trained** with Polynomial ...

☆ 99 Cited by 99 Related articles All 4 versions »

Using opcode sequences in single-class **learning** to detect unknown malware

I Santos, F Brezo, B Sanz, C Laorden, PG Bringas - IET Information security, 2011 - IET

... Since our method would not be able to detect packed executable, we removed any **packed malware** before selecting the 1000 malicious executables ... The use of supervised machine-**learning** algorithms for model **training** can be problematic because supervised **learning** ...

☆ 99 Cited by 38 Related articles All 13 versions »

Collective classification for packed executable identification

I Santos, X Ugarte-Pedrero, B Sanz... - Proceedings of the 8th ..., 2011 - dl.acm.org

... in order to guarantee results of TPR lower than 5%, Collective Forest only needs to be **trained** with, at ... with accuracy, CollectiveIBK was the only one that was highly sensitive to the increase of the **training** dataset ... Using entropy analysis to find encrypted and **packed malware** ...

☆ 99 Cited by 39 Related articles All 7 versions »

Opcode sequences as representation of executables for data-mining-based unknown malware detection

I Santos, F Brezo, X Ugarte-Pedrero, PG Bringas - Information Sciences, 2013 - Elsevier

... There are several **training** algorithms that are typically used to **learn** the graph structure of these trees ... each validation step, we conducted the **learning** phase of each algorithm with each **training** dataset, applying different parameters or **learning** algorithms depending ...

☆ 99 Cited by 238 Related articles All 6 versions

Evolving computational intelligence system for malware detection

K Demertzis, L Iliadis - International Conference on Advanced Information ..., 2014 - Springer

... The aim of the one-pass **learning** method is to create a repository of **trained** output neurons during the presentation of **training** samples ... or unpacked executables with minimum computational power combined with the ECF method in order to detect **packed malware** ...

☆ 99 Cited by 26 Related articles All 3 versions »

Behavioral detection of malware on mobile handsets

A Bose, X Hu, KG Shin, T Park - ... of the 6th international conference on ..., 2008 - dl.acm.org

... in cooperation with a service provider, develops a behavior classifier **trained** by the ... Upon receiving the signature, the detection agent performs machine-**learning** classification with the pre ... 6, we show that malicious behavior can be detected more accurately by **training** an SVM ...

☆ 99 Cited by 348 Related articles All 15 versions »

Opcode-sequence-based semi-supervised unknown malware detection

I Santos, B Sanz, C Laorden, F Brezo... - ... Intelligence in Security for ..., 2011 - Springer

... Specifically, the best overall results were obtained with a **training** set containing 90% of labelled ... In particular, a preliminary test with a Bayesian Network **trained** with Hill climber shows an ... of the static nature of the features we used with LLGC, it cannot counter **packed malware** ...

☆ 99 Cited by 33 Related articles All 12 versions »

Using entropy analysis to find encrypted and **packed malware**

R Lyda, J Hamrock - IEEE Security & Privacy, 2007 - ieeexplore.ieee.org

... Table 1. Computed statistical measures based on four **training** sets ... 5. A. Stephan, "Improving Proactive Detection of **Packed Malware**," Virus Bulletin, 01 Mar ... His research interests include applying machine-**learning** mechanisms for classifying malware samples based on ...

☆ 99 Cited by 298 Related articles All 10 versions

Malware detection based on structural and behavioural features of api calls

M Alazab, R Layton, S Venkataraman, P Watters - 2010 - ro.ecu.edu.au

... Swets and Pickett, 1982), which is commonly used to estimate how well the **trained** SVM model ... Among the four basic types of kernels used by SVM to map the **training** vectors to ... If the existing tools are unable to unpack a **packed malware** that uses an unknown packing algorithm ...

☆ 99 Cited by 59 Related articles All 8 versions »

Malware detection using statistical analysis of byte-level file content

SM Tabish, MZ Shafiq, M Farooq - ... of the ACM SIGKDD Workshop on ..., 2009 - dl.acm.org

... architecture of our malware detection technique in Section 3. We discuss the dataset in Section 4. We re- port the results of pilot studies in Section 5. In Section 6, we discuss the knowledge discovery process of the proposed technique by visualizing the **learning** models of data ...

☆ 99 Cited by 168 Related articles All 7 versions »

Application of string kernel based support vector machine for malware packer identification

T Ban, R Isawa, S Guo, D Inoue... - The 2013 International ..., 2013 - ieeexplore.ieee.org

... Then, in the ith of the 10 cross-validation iterations, a classifier is **trained** using the complementary set of the ... the best generalization performance on a wide range of (C, γ) combinations with a reasonable computing cost: **training** performed on ... machine-**learning**-based approach ...

☆ 99 Cited by 11 Related articles All 2 versions

Control flow-based opcode behavior analysis for Malware detection

Y Ding, W Dai, S Yan, Y Zhang - Computers & Security, 2014 - Elsevier

... two hundred features with high document frequency values are selected from each class of **training** samples (see ... **trained** using Text-feature-set1, and the prefix "TXT2" represents the classifier is **trained** using Text ... If **packed malware** cannot be unpacked, our method is ineffective ...

☆ 99 Cited by 36 Related articles All 3 versions

Image visualization based malware detection

K Kancherla, S Mukkamala - 2013 IEEE Symposium on ..., 2013 - ieeexplore.ieee.org

... However they did not consider **packed malware** (variety of packers) in their experiment ... Of this 70% of the samples are used for **training** and remaining 30% are used for testing. In **learning** phase we estimate the parameters for SVM ...

☆ 99 Cited by 32 Related articles All 2 versions

McBoost: Boosting scalability in malware collection and analysis using statistical classification of executables

R Perdisci, A Lanzi, W Lee - 2008 Annual Computer Security ..., 2008 - ieeexplore.ieee.org

... A Multi-Layer Perceptron (MLP) classifier that uses these features is **trained** to distinguish between packed and non ... The only difference is that the **training** dataset is made of a collection of hidden-code extracted (using our unpacker) from **packed malware** and packed ...

☆ 99 Cited by 137 Related articles All 11 versions

Classification of packed executables for accurate computer virus detection

R Perdisci, A Lanzi, W Lee - Pattern recognition letters, 2008 - Elsevier

... We first **trained** each classifier on the **training** dataset, and then computed the accuracy on ... classification results, according to the cross-validation experiments on the **training** dataset ... R. Lyda, J. HamrockUsing entropy analysis to find encrypted and **packed malware**. IEEE Security ...

☆ 99 Cited by 171 Related articles All 10 versions

Improving malware classification: bridging the static/dynamic gap

B Anderson, C Storlie, T Lane - Proceedings of the 5th ACM workshop on ..., 2012 - dl.acm.org

... The goal of classical kernel- based **learning** with support vector machines is to **learn** the weight ... 4: Heatmap for all six kernels combined with the weights found using multiple kernel **learning** ... This helps to prevent over-fitting the **training** data and allows for better generalization ...

☆ 99 Cited by 100 Related articles All 5 versions »

Detection of packed executables using support vector machines

TY Wang, CH Wu - ... Conference on Machine Learning and ..., 2011 - ieeexplore.ieee.org

... [10] E. Osuna, R. Freund and F. Girosit, "**Training** Support Vector ... 81-106, 1986. [16] A. Stepan, "Improving Proactive Detection of **Packed Malware**," 2006; http ... [18] S. Tong and D. Koller, "Support Vector Machine Active **Learning** with Applications to Text Classification," J. Mach ...

☆ 99 Cited by 3 Related articles All 4 versions

Malware detection and classification based on extraction of API sequences

D Uppal, R Sinha, V Mehra ... - ... Conference on Advances ..., 2014 - ieeexplore.ieee.org

... Page 3. The drawback of this approach was only that it does not work for **packed malware**. In this research we proposed a novel approach to determine maliciousness in an input sample ... Stage 1 Machine **learning** techniques and Data Mining Methods **Training** data Classify ...

☆ 99 Cited by 24 Related articles All 2 versions

Related searches

machine learning **based** malware **detection**

unknown malware **detection semi-supervised** learning

malware **detection machine** learning **techniques**

Image visualization based malware detection

K Kancherla, S Mukkamala - 2013 IEEE Symposium on ..., 2013 - ieeexplore.ieee.org

... Features Extraction **Machine Learning** ... Recent approaches allow a wide class of **models** of varying complexity to be chosen ... Then the task of learning amounts to selecting the sought-after **model** of optimal complexity and estimating parameters from training data [6 and 7]. Within ...

☆ 99 Cited by 32 Related articles All 2 versions

Malware detection and classification based on extraction of API sequences

D Uppal, R Sinha, V Mehra... - ... Conference on Advances ..., 2014 - ieeexplore.ieee.org

... Then comes the oligomorphic malware- they are the advancement of **encrypted malware**, such that, only the decryptor is ... C. **Machine Learning** Algorithms for classification Various **machine learning** algorithms were used to construct the proposed **model** for classification ...

☆ 99 Cited by 24 Related articles All 2 versions

Evolution and detection of polymorphic and metamorphic malwares: A survey

A Sharma, SK Sahay - arXiv preprint arXiv:1406.7061, 2014 - arxiv.org

... joined with the **encrypted malware** body to construct a new variant of malware [14] ... for the detection of malwares; Signature matching [22], Heuristic approach [20], **Machine learning** [28] and ... Austin, TH, Filiol, E., Josse, and Stamp, SM "Exploring Hidden Markov **Models** for Virus ...

☆ 99 Cited by 43 Related articles All 8 versions »

Classification of polymorphic and metamorphic malware samples based on their behavior

K Tsyganok, E Tumoyan, L Babenko... - Proceedings of the Fifth ..., 2012 - dl.acm.org

... execution graph, analysis of disassembly code using neural networks or other **machine learning** techniques, etc ... This can be concluded from the fact that the described **models** are statistical ... analysis of related work, the following requirement to the addressed **model** and method ...

☆ 99 Cited by 13 Related articles »

A survey on heuristic malware detection techniques

Z Bazrafshan, H Hashemi, SMH Fard... - The 5th Conference on ..., 2013 - ieeexplore.ieee.org

... Usually, a transformation engine is embedded in the **encrypted malware** that at any change ... Some researchers set out to improve the precision of **machine learning** through the features ... They proposed a semi parametric classification **model** for combining file content and file ...

☆ 99 Cited by 101 Related articles All 4 versions »

An efficient block-discriminant identification of packed malware

S Naval, V Laxmi, MS Gaur - Sadhana, 2015 - Springer

... 0x 1E960000, 0x34960000, ... are the byte features for which both the **models** are implemented ... Normalized FVT used as an input to **machine learning** classifiers (We have used WEKA ... N B : This experiment is conducted to check the detection accuracy of our **model** with packed ...

☆ 99 Cited by 7 Related articles All 6 versions »

Overview of malware analysis and detection

A Makandar, A Patrot - International Journal of Computer ..., 2015 - pdfs.semanticscholar.org

... behaviors are identified in one of them such as **encrypted malware**, polymorphic malware ... Proceedings of 12th International Conference on **Machine Learning**, San Francisco, pp ... of the ACM SIGMETRICS/International Conference on Measurement and **Modeling** of Computer ...

☆ 99 Cited by 12 Related articles »

Enhancing Malware Detection Accuracy through Graph Based **Model**

K Muthumanickam, E Ilavarasan - Journal of Advances in ..., 2014 - journaljamcs.com

... and analyze malicious code attac s, still they suffer the adaptation of ineffective **models** ... As our **model** only concentrates on important native system calls which are countable in ... Using spatio-temporal information in api calls with **machine learning** algorithms for malware detection ...

☆ 99 Cited by 1 Related articles All 2 versions »

Method for recognizing malicious file

MC Chiu, MW Wu, CC Wang, CK Hsu... - US Patent App. 14 ..., 2014 - Google Patents

... Once the normal file is executed, the **encrypted malware** could be executed simultaneously and ... a method of detecting malicious software using generic signature, and **machine learning** methods ... US20070152854A1 (en), 2007-07-05, Forgery detection using entropy **modeling** ...

☆ 99 Cited by 3 Related articles All 2 versions »

Combining dynamic and static analysis for malware detection

A Damodaran - 2015 - scholarworks.sjsu.edu

... 2.2.3.1 Hidden Markov **Model** Hidden Markov **Models** are generally used for statistical based pattern analysis ... tion on HMM and its usage in malware detection. A Hidden Markov **Model** is a **machine learning model** to represent probability distributions over sequence of obser ...

☆ 99 Cited by 1 Related articles All 3 versions

Platform Neutral Sandbox for Analyzing Android Malware and Resource Hoggers

A Malware - researchgate.net

In this paper, we propose an automated, scalable, and dynamic analysis framework incorporating static anti anti-analysis techniques to detect the analysis environment aware Android malware and Resource Hogger apps. The proposed framework can automatically ...

☆ 99 Related articles All 2 versions »

Comparative analysis of voting schemes for ensemble-based malware detection

RK Shahzad, N Lavesson - Journal of Wireless Mobile Networks ..., 2013 - diva-portal.org

... amount of research for classification tasks has applied techniques ranging from statistical methods to **machine learning** like supervised ... used for detecting the malicious behavior [2]. In some cases, the decision from an individual **model** or even from several **models** may be ...

☆ 99 Cited by 19 Related articles All 4 versions »

Static malware analysis using **machine learning** methods

HV Nath, BM Mehtre - International Conference on Security in Computer ..., 2014 - Springer

... This **model** could be extended to any stage, in which the final or intermediate payload could be malware, which belongs to any of these families ... Static Malware Analysis Using **Machine Learning** Methods ... This method is used mainly to identify the packed and **encrypted malware** ...

☆ 99 Cited by 50 Related articles All 4 versions »

Droidolytics: robust feature signature for repackaged android apps on official and third party android markets

P Faruki, V Laxmi, V Ganmoor... - 2013 2nd ..., 2013 - ieeexplore.ieee.org

... more than 0.1 million normal and 426 malware apps with **machine learning** approach to ... An- droid permission **model** also specifies permissions based on categories but still manifest ... A methodology for Empirical analysis of Permission-Based Security **models** and its application ...

☆ 99 Cited by 14 Related articles All 3 versions

Anticipating dormant functionality in malware: A semantics based approach

M Noor, H Abbas - 2013 International Symposium on ..., 2013 - ieeexplore.ieee.org

... and difficult than mere detection of malicious behavior, as identification requires **machine learning** to differentiate ... x Extracting Genotype **Models** by locating the blocks (genotype) of the code, that is ... The genotype **model** is based on structural attributes of the code and is not ...

☆ 99 Cited by 4 Related articles All 5 versions

Using entropy analysis to find encrypted and packed malware

R Lyda, J Hamrock - IEEE Security & Privacy, 2007 - ieeexplore.ieee.org

... As such, our method- ology computes entropy at a naïve **model** level, in ... His research interests include applying **machine-learning** mechanisms for classifying malware samples based ... researcher in malware-analysis trends, applying mathematical and statistical **models** to study ...

☆ 99 Cited by 298 Related articles All 10 versions

Maitland: analysis of packed and **encrypted malware** via paravirtualization extensions

CA Benninger - 2012 - dspace.library.uvic.ca

... develop new ways of detecting and analyzing packed and **encrypted malware**. Meth ... Binary signature analysis involves generating a sig- nature or **model** which represents a particular piece of malicious behavior (or code) and some variations of it ...

☆ 99 Cited by 2 Related articles All 2 versions »

Malware behavioural detection and vaccine development by using a support vector **model** classifier

P Wang, YS Wang - Journal of Computer and System Sciences, 2015 - Elsevier

... k-NN algorithm is among the simplest of all **machine learning** algorithms using instance ... developed by Vapnik in 1995 (AT&T Labs), are supervised learning **models** associated with ... processes were included in the learning process: data analysis, **model** parameter determination ...

☆ 99 Cited by 31 Related articles All 3 versions

Metamorphic code generation from LLVM bytecode

T Tamboli, TH Austin, M Stamp - Journal of Computer Virology and ..., 2014 - Springer

... Hidden Markov **models** can be viewed as a **machine learning** technique. We can train an HMM to fit a given observation sequence. The resulting **model** can then be used to score an unknown sequence to measure its similarity to the training data ...

☆ 99 Cited by 11 Related articles All 8 versions »

Towards automating malware classification and characterization

AK Seewald - ... Sicherheit, Schutz und Zuverlässigkeit. Beiträge der ..., 2008 - dl.gi.de

... binary stream with maximum entropy and thus minimum compressibility, so all **encrypted malware** samples are ... As the **model** of instance-based learning is not easily understandable, we also ... All **machine learning** experiments were done within WEKA [FW05] using ten-fold cross ...

☆ 99 Cited by 5 Related articles All 9 versions »

BNS **feature** scaling: an improved representation over tf-idf for svm text classification

G Forman - Proceedings of the 17th ACM conference on ..., 2008 - dl.acm.org

... This solution improves a number of **feature** selection metrics that otherwise **ignore** strong negative ... two standard performance measures: accuracy for its historical standard in **machine learning** research and ... We had to **disable** its **feature** space normalization **feature**, otherwise it re ...

☆ 99 Cited by 139 Related articles All 8 versions »

A study of distance-based **machine learning** algorithms

D Wettschereck - 1994 - ir.library.oregonstate.edu

... Page 4. A Study of Distance-Based **Machine Learning** Algorithms by ... FWMI), or learned **feature** weights (kNN FWVSM). 77 4.9. The performance of the k-nearest neighbor algorithms with and without **features** weights when trained on the original **features** or the pca-**features** ...

☆ 99 Cited by 177 Related articles All 6 versions »

CSO-based **feature** selection and parameter optimization for support vector machine

KC Lin, HY Chien - 2009 Joint Conferences on Pervasive ..., 2009 - ieeexplore.ieee.org

... problems have been frequently investigated in the domains of data mining and **machine learning** ... SVM [7]. However, these approaches only consider the parameter optimization but **ignore** the optimized ... separate the dataset to training and testing set with selected **feature** subset ...

☆ 99 Cited by 34 Related articles All 2 versions »

CSL: A cost-sensitive learning system for sensing and grasping objects

M Tan - ... ., IEEE International Conference on Robotics and ..., 1990 - ieeexplore.ieee.org

... This is beyond **machine learning** methods because they usually **ignore** robot execution costs and ... Col- lecting exhaustive object descriptions would allow using existing **machine learning** methods, but this can ... sensing pro- cedure H-scan-lo produces a value of **feature** Width-deg ...

☆ 99 Cited by 43 Related articles All 2 versions

Comparison of **feature** ranking methods based on information entropy

W Duch, T Wieczorek, J Biesiada ... - 2004 IEEE International ..., 2004 - ieeexplore.ieee.org

... classification algorithms have inherent ability to focus on relevant **features** and **ignore** irrelevant ones ... neural networks with strong regularization of the input layer may **turn off** the irrelevant ... and "abalone" data, both taken from the UCI repository of **machine learning** databases [IO ...

☆ 99 Cited by 77 Related articles All 9 versions »

Feature shaping for linear SVM classifiers

G Forman, M Scholz, S Rajaram - Proceedings of the 15th ACM SIGKDD ..., 2009 - dl.acm.org

... But the field of **machine learning** is about getting the computer to better handle any sort of input fea- ture without careful, manual data preparation by an expen- sive domain ... We used its default options, except that we had to **disable** its internal **feature range** normalization (-N 2 ...

☆ 99 Cited by 39 Related articles All 7 versions »

Learning a meta-level prior for **feature** relevance from multiple related tasks

SI Lee, V Chatalbashev, D Vickrey... - ... on **Machine learning**, 2007 - dl.acm.org

... Appearing in Proceedings of the 24th International Conference on **Machine Learning**, Corvallis, OR, 2007 ... where, for simplicity of notation, we **ignore** the bias (inter- cept) term, under the ... remainder of our evaluation to those tasks which exhibit an average **feature** relevance **range** ...

☆ 99 Cited by 148 Related articles All 14 versions »

Genetic algorithms and **machine learning**

DE Goldberg, JH Holland - **Machine learning**, 1988 - Springer

... It would **ignore** the fact that all these creations have become possible only after three ... fifth paper, Belew and Forrest compare symbolic and subsymbolic approaches to **machine learning**, using a ... [In complex domains] one expects perpetual novelty to be a characteristic **feature** ...

☆ 99 Cited by 2116 Related articles All 7 versions »

On **feature** selection: learning with exponentially many irreverent **features** as training examples

AY Ng - 1998 - dspace.mit.edu

... fying the "irrelevant" **features**, and most learning algorithms will automatically learn to **ignore** the uirrelevant ... for **feature** selection in classification, which comes mostly from the **Machine Learning** literature ... a "similar" manner — for example, when X = Rf , then for two **feature** sets _F ...

☆ 99 Cited by 181 Related articles All 11 versions »

Machine learning with R

B Lantz - 2013 - books.google.com

... relationships amongfeatures – the correlation matrix Visualizingrelationships among **features** – the scatterplot matrix ... Boostrap method, reliability, design of experiments, **machine learning** and data ... reada collection offree technicalarticles, signup fora **range** offree newslettersand ...

☆ 99 Cited by 305 Related articles All 10 versions »

Machine learning: a probabilistic perspective

KP Murphy - 2012 - books.google.com

... structure 13 1.3.4 Matrix completion 14 1.4 Some basic concepts in **machine learning** 16 1.4 ... prediction 87 3.5.3 The log-sum-exp trick 88 3.5.4 **Feature** selection using ... equivalent to Bayes model averaging Experimental comparison 584 16.7.1 Low-dimensional **features** 584 16.7 ...

☆ 99 Cited by 5089 Related articles All 21 versions »

A review and empirical evaluation of **feature** weighting methods for a class of lazy learning algorithms

D Wettschereck, DW Aha, T Mohri - Artificial Intelligence Review, 1997 - Springer

... Second, we focus on classification as the performance task and **ignore** issues concerning ... and closed loop in statistics, and as wrapperand filter models in **machine learning** (eg, John ... discretize continuous **features** and binarize discrete **features** (ie, each discrete **feature** f defined ...

☆ 99 Cited by 870 Related articles All 18 versions »

Learning relational probability trees

J Neville, D Jensen, L Friedland, M Hay - Proceedings of the ninth ACM ..., 2003 - dl.acm.org

... Many techniques common to **machine learning**, data mining, and statistical modeling rely on the underlying assumption that data instances are ... We have shown that **feature** selection will be biased when relational learning algorithms **ignore** common characteristics of ...

☆ 99 Cited by 274 Related articles All 14 versions »

Machine learning applications in genetics and genomics

MW Libbrecht, WS Noble - Nature Reviews Genetics, 2015 - nature.com

... we recommend you use a more up to date browser (or **turn off** compatibility mode ... 29 trained a collection of **machine learning** methods to distinguish among various types of genomic ... Moreover, replacing a single averaged **feature** with 100 separate **features** may be problematic ...

☆ 99 Cited by 475 Related articles All 10 versions

Feature selection using dynamic weights for classification

X Sun, Y Liu, M Xu, H Chen, J Han, K Wang - Knowledge-Based Systems, 2013 - Elsevier

... However, it is likely to **ignore features** which as a group have strong discriminatory ... **Feature** selection helps improve the performance of **machine learning** algorithms by selecting a small ... As discussed earlier, most of the traditional **feature** selection methods disregard the intrinsic ...

☆ 99 Cited by 48 Related articles All 4 versions

Machine learning and data mining

TM Mitchell - Communications of the ACM, 1999 - ri.cmu.edu

... In this article, we focus primarily on the role of **machine learning** algorithms in the data mining ... portion of the figure illustrates a typical patient record, where \?" indicates that the **feature** value is ... a result, the current state of the art in medical outcomes analysis is to **ignore** the image ...

☆ 99 Cited by 427 Related articles All 22 versions »

The pyramid match kernel: Efficient learning with sets of **features**

K Grauman, T Darrell - Journal of Machine Learning Research, 2007 - jmlr.org

... However, this representation poses a challenge to many conventional **machine learning** techniques, since sets may ... form of the **features**, discard information by replacing inputs with prototypical **features**, **ignore** important co ... 2005), and D is the value of the maximal **feature range** ...

☆ 99 Cited by 395 Related articles All 9 versions »

Conditional random fields: Probabilistic models for segmenting and labeling sequence data

J Lafferty, A McCallum, FCN Pereira - 2001 - repository.upenn.edu

... The definitive version was published in Proceedings of the 18th International Conference on **Machine Learning** 2001 (ICML ... Thus, states with a single outgoing tran- sition effectively **ignore** their observations ... For example, a Boolean vertex **feature** gk might be true if the word Xi is ...

☆ 99 Cited by 12437 Related articles All 77 versions »

Feature weighting for lazy learning algorithms

DW Aha - Feature Extraction, Construction and Selection, 1998 - Springer

... We focus primarily on contributions to **machine learning** and case-based reasoning ... mentioned here use either a filter or wrapper model to set **feature** weights, we tend to **ignore** feedback methods ... Lo- cal **feature** weighting methods include methods that weight **features** by class1 ...

☆ 99 Cited by 148 Related articles All 7 versions »

Machine learning with R

B Lantz - 2015 - books.google.com

... also read a collection of free technical articles, sign up for a **range** of free ... Types of **machine learning** algorithms 19 Matching input data to algorithms 21 **Machine learning** with R ... 97 Classification with Naive Bayes 98 The Laplace estimator 100 Using numeric **features** with Naive ...

☆ 99 Cited by 144 Related articles All 3 versions »

Combining lexicon and learning based approaches for concept-level sentiment analysis

A Mudinas, D Zhang, M Levene - ... of the first international workshop on ..., 2012 - dl.acm.org

... but also", and **exclude** them as sentiment negations ... 3.4 Learning-based Sentiment Evaluation The supervised **machine learning** algorithm used in our system is the linear SVM implementation in LibSVM2 with L2 ... For example, the **feature** _Large_ is **excluded** from this calculation ...

☆ 99 Cited by 166 Related articles All 6 versions »

A methodological approach to the classification of dermoscopy images

ME Celebi, HA Kingravi, B Uddin, H Iyatomi... - ... Medical Imaging and ..., 2007 - Elsevier

... 3d). After the **exclusion** of these images, 564 images remained in the image set ... **Feature** selection is an important preprocessing step in many **machine-learning** tasks ... **Feature** selection algorithms can be classified into two main categories according to their evaluation criteria ...

☆ 99 Cited by 440 Related articles All 10 versions

Toward personalized care management of patients at risk: the diabetes case study

H Neuvirth, M Ozery-Flato, J Hu, J Laserson... - Proceedings of the 17th ..., 2011 - dl.acm.org

... K-nearest neighbor (kNN) is another algorithm often used in **machine learning** applications ... This **excluded** 1604 samples, which represent 35% of the dataset ... selection test appropriate for each algorithm with a bound of 0.05 on the p-value, the LR filter **excludes** significantly more ...

☆ 99 Cited by 54 Related articles All 7 versions »

Migration and stopover in a small pelagic seabird, the Manx shearwater *Puffinus puffinus*: insights from **machine learning**

T Guilford, J Meade, J Willis ... - ... of the Royal ..., 2009 - royalsocietypublishing.org

... We believe that this and similar **machine learning** techniques may have considerable usage in helping to extract more information from extant and ... across the globe at the equinoxes, erroneous location estimates are often seen around these periods and these were **excluded** ...

☆ 99 Cited by 194 Related articles All 14 versions »

Representation of elderly persons and women in published randomized trials of acute coronary syndromes

PY Lee, KP Alexander, BG Hammill, SK Pasquali ... - Jama, 2001 - jamanetwork.com

... Regression line represents the average increase in percentage of women as the average mean age among the trials increases. Table 1. **Characteristics** of Trials (N = 593) ... Image description not available. Table 2. Enrollment and **Exclusion** of Elderly Patients in Clinical Trials of ...

☆ 99 Cited by 868 Related articles All 9 versions »

Hierarchical metabolomics demonstrates substantial compositional similarity between genetically modified and conventional potato crops

GS Catchpole, M Beckmann, DP Enot... - Proceedings of the ..., 2005 - National Acad Sciences

... Subscriptions FAQ; Open Access; Recommend PNAS to Your Librarian. Log in; Log out; My Cart. Main menu. Home; Articles: Current; Latest Articles; Special **Features**; Colloquia; Collected Articles; PNAS Classics; Archive. Front Matter; News: For the Press; ...

☆ 99 Cited by 388 Related articles All 21 versions »

Predictive analytics model for power consumption in manufacturing

SJ Shin, J Woo, S Rachuri - Procedia Cirp, 2014 - Elsevier

... However, the current scheme of STEP-NC **excludes** both machine tool specification and G- code ... The accuracy drop- off implies the **machine learning** performance is not good to predict a ... the use of a simulator and not through actual machining, the **exclusion** of optimization ...

☆ 99 Cited by 76 Related articles All 8 versions »

Quality of anticoagulation management among patients with atrial fibrillation: results of a review of medical records from 2 communities

GP Samsa, DB Matchar, LB Goldstein... - Archives of internal ..., 2000 - jamanetwork.com

... **of-range**; B), and INR of less than 1.50 (low **out-of-range**; C). Practice sites are described in the "Practices" subsection of the "Subjects and Methods" section. Percentages have been rounded and may not sum 100. Table 1 ... Demographic and Clinical **Characteristics** of Patients ...

☆ 99 Cited by 373 Related articles All 7 versions

The influence of patient adherence on anticoagulation control with warfarin: results from the International Normalized Ratio Adherence and Genetics (IN-RANGE) ...

SE Kimmel, Z Chen, M Price, CS Parker... - Archives of Internal ..., 2007 - jamanetwork.com

... B indicates INR below range; A, INR above range; and O, INR **out of range**. *Multivariable P<.001. †Multivariable P = .04 for comparison of adherent vs nonadherent. Table 1 ... Demographic and Clinical **Characteristics** of the Study Cohort. Demographic and Clinical ...

☆ 99 Cited by 281 Related articles All 10 versions

A mobility-assisted protocol for supervised learning of link quality estimates in wireless networks

EF Flushing, J Nagi, GA Di Caro - ... International Conference on ..., 2012 - ieeexplore.ieee.org

... In idle state, a node **excludes** itself from the network, reducing in this way the number of ... H(D) is the entropy of D. En- tropy has been widely used in **machine learning** prob- lems ... we ran also experiments with a simplified version of the protocol, in which we **excluded** node mobility ...

☆ 99 Cited by 32 Related articles All 7 versions

Reinforcement learning for context awareness and intelligence in wireless networks: Review, new **features** and open issues

KLA Yau, P Komisarczuk, PD Teal - Journal of Network and Computer ..., 2012 - Elsevier

... The phrase 'unsupervised' means the **machine-learning** technique enables a host to learn knowledge about its ... a subset of actions in adherence to a set of rules that **exclude** actions that ... Table 1 summarizes the approaches and references for each component and **feature** ...

☆ 99 Cited by 94 Related articles All 8 versions

Development of a nomogram for prediction of vaginal birth after cesarean delivery

WA Grobman, Y Lai, MB Landon, CY Spong... - Obstetrics & ..., 2007 - journals.lww.com

OBJECTIVE: To develop a model based on factors available at the first prenatal visit that predicts c.

☆ 99 Cited by 237 Related articles All 8 versions »

Applying reinforcement learning to small scale combat in the real-time strategy game StarCraft: Broodwar

S Wender, I Watson - 2012 IEEE Conference on Computational ..., 2012 - ieeexplore.ieee.org

... The **characteristics** exhibited by RTS games such as adversarial planning, incomplete information combined ... 3] make RTS games a great test bed for unsupervised **machine learning** techniques such ... This **excludes** many high level planning actions, such as actions that are given ...

☆ 99 Cited by 96 Related articles All 3 versions

Medical data mining: knowledge discovery in a clinical data warehouse.

JC Prather, DF Lobach, LK Goodwin... - Proceedings of the ..., 1997 - ncbi.nlm.nih.gov

... searching the data using statistical queries, neural networks, or other **machine learning** methods [2 ... Table 1. **Characteristics** of the production system database and the clinical data warehouse ... data ina sample dataset represented legal values that were **excluded** because they ...

☆ 99 Cited by 293 Related articles All 12 versions »

Detection of early plant stress responses in hyperspectral images

J Behmann, J Steinrücken, L Plümer - ISPRS Journal of Photogrammetry ..., 2014 - Elsevier

... based on a single VI is not suitable, as too much information is **excluded**. • The **machine learning** approaches with compressed **features** achieve good results with compact models, but ... Approaches which extract a maximum of information by enhanced **feature** sets or detect ...

☆ 99 Cited by 85 Related articles All 7 versions

Range and AGC normalization in airborne discrete-return LiDAR intensity data for forest canopies

I Korpela, HO Ørka, J Hyyppä, V Heikkinen... - ISPRS Journal of ..., 2010 - Elsevier

... Echoes lower than 40% from the top were **excluded** ... of 80 **features** were computed for each of the 8 sensor × echo type combinations, **excluding** some combinations of ... based on the use of the Gini importance measure in the Random Forest **machine-learning** algorithm (Breiman ...

☆ 99 Cited by 68 Related articles All 5 versions

Predictive analytics with Microsoft Azure **machine learning**

R Barga, V Fontama, WH Tok, L Cabrera-Cordon - 2015 - Springer

... Scoring Your Data in Azure **Machine Learning** and Visualizing in powerbi.com ... **Feature** Hashing ... Identifying the Right **Features** ...

☆ 99 Cited by 68 Related articles All 8 versions »

First documented rhythm and clinical outcome from in-hospital cardiac arrest among children and adults

VM Nadkarni, GL Larkin, MA Peberdy, SM Carey... - Jama, 2006 - jamanetwork.com

... Table 1. Patient **Characteristics** of Pediatric and Adult Cardiac Arrests ... Image description not available. Table 2. Event **Characteristics** of Pediatric and Adult Cardiac Arrests ...

☆ 99 Cited by 1049 Related articles All 12 versions

Support vector regression based prediction of global solar radiation on a horizontal surface

K Mohammadi, S Shamshirband, MH Anisi... - Energy Conversion and ..., 2015 - Elsevier

... achieve further accuracy, for the omitted months the sunshine duration data were also **excluded** from the ... Results in the higher-dimensional **feature** space correspond to the results of the original, lower ... x and x i are vectors in the input space, ie vectors of **features** computed from ...

☆ 99 Cited by 86 Related articles All 8 versions

A global **machine learning** based scoring function for protein structure prediction

E Faraggi, A Kloczkowski - Proteins: Structure, Function, and ..., 2014 - Wiley Online Library

... Critically important for any **machine learning** is the presentation of the data in a machine usable ... A common approach to parameterization is to multiply each **feature** by a parameter optimized ... For testing purposes, the newer CASP results are **excluded** as will be described below ...

☆ 99 Cited by 21 Related articles All 8 versions »

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Mauritius Schmidtler et al.	Examiner:	Simitoski, Michael J.
Serial No.:	14/709,875	Group Art Unit:	2493
Filed:	May 12, 2015	Docket No.:	04584.0168US01
Title:	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS		

AMENDMENT & RESPONSE TO NON-FINAL OFFICE ACTION

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

Dear Commissioner:

In response to the Non-Final Office Action mailed July 17, 2019, please amend the above-identified application as follows:

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

Remarks/Arguments begin on page 7 of this paper.

Electronic Acknowledgement Receipt

EFS ID:	37291082
Application Number:	14709875
International Application Number:	
Confirmation Number:	1593
Title of Invention:	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS
First Named Inventor/Applicant Name:	Mauritius Schmidtler
Customer Number:	23552
Filer:	David Dwayne Harrell/Elizabeth Pallardy
Filer Authorized By:	David Dwayne Harrell
Attorney Docket Number:	04584.0168US01
Receipt Date:	26-SEP-2019
Filing Date:	12-MAY-2015
Time Stamp:	17:06:03
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		04584-0168US01_RespNFOA.PDF	145903 4faff39148d34ec605bb114504e310cc4466d935	yes	11

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Applicant Arguments/Remarks Made in an Amendment	7	11
	Claims	2	6
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Warnings:			
Information:			
	Total Files Size (in bytes):	145903	

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.

REMARKS/ARGUMENTS

This Amendment and the following remarks are intended to fully respond to the Non-Final Office Action dated July 17, 2019, hereinafter "Office Action." In that Office Action, claims 1-20 were examined and all claims were rejected. Specifically, claims 5 and 14 were objected to for various informalities. Claims 1, 2, 10, 11, and 19 were rejected under 35 U.S.C. § 102(a)(1) as allegedly anticipated by "Detection of Packed Malware" by Devi et al. (hereinafter "Devi"). Claims 3 and 12 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Devi as applied to claims 2 and 11 above, in view of "Efficient Malicious Code Detection Using N-Gram Analysis and SVM" by Choi et al. (hereinafter "Choi"). Claims 4 and 13 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Devi and Choi as applied to claims 3 and 12 above, in view of Schipka (U.S. Pat. Publ. No. 2009/0013405; hereinafter "Schipka"). Claims 6 and 15 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Devi as applied to claims 2 and 11 above, in view of Thomas et al. (U.S. Pat. Publ. No. 2012/0079596; hereinafter "Thomas"). Claims 7 and 16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Devi and Thomas as applied to claims 6 and 15 above in view of Nachenberg (U.S. Pat. No. 8,510,836; hereinafter "Nachenberg"). Claims 8, 9, 17, 18, and 20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Devi, as applied to claims 1, 10, and 19 above, in view of Gilbert et al. (U.S. Pat. No. 9,197,663; hereinafter "Gilbert").

Reconsideration of these rejections, as they might apply to the original and amended claims in view of these remarks, is respectfully requested. In this Amendment, claims 1, 3, 10, 12, and 19 have been amended, claims 5 and 14 have been canceled, and claims 21 and 22 have been added. Therefore, claims 1-4, 6-13, and 15-22 remain present for examination.

Interview Summary

Examiner Michael J. Simitoski and Applicants' representative, Attorney David D. Harrell (Reg. No. 71,855), participated in a telephone interview on September 23, 2019 to discuss the cited references and the proposed claims. It was agreed that the proposed claims are likely to overcome the rejections.

Allowable Subject Matter

Claims 5 and 14 are indicated in the Office Action as allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. Applicants acknowledge with appreciation Examiner's allowance of claims 5 and 14. Applicants have amended the independent claims to include the allowable subject matter of previously pending claims 5 and 14. For example, claim 1 as amended recites, *inter alia*:

> generating a feature vector from the plurality of static data points using a classifier trained to classify the plurality of static data points based on a collection of data comprising known malicious executable files, known benign executable files, and known unwanted executable files, wherein the collection of data comprises at least a portion of the plurality of static data points, and wherein one or more features of the feature vector are selectively turned on or off based on whether a value of one or more static data points from the plurality of extracted static data points is within a predetermined range

Claim 10 as amended recites, *inter alia*:

> generating a feature vector from the plurality of static data points using a classifier trained to classify the plurality of static data points based on a collection of data comprising known malicious executable files, known benign executable files and known unwanted executable files, wherein the collection of data comprises at least a portion of the plurality of static data points, and wherein one or more features of the feature vector are selectively turned on or off based on whether one or more values of one or more static data points from the plurality of extracted static data points is within a predetermined range

Claim 19 as amended recites, *inter alia*:

> generating a feature vector from the plurality of predefined character strings using a classifier trained to classify the plurality of predefined character strings based on a collection of data comprising known malicious executable files, known benign executable files and known unwanted executable files, wherein the collection of data comprises at least a portion of one or more of the plurality of predefined character strings, and wherein one or more features of the feature vector are selectively turned on or off based on whether a value of one or more predefined character strings from the plurality of predefined character strings is within a predetermined range

Accordingly, Applicants submit that claims 1, 10, and 19 as amended are allowable. Claims 2-9, 11-18, and 20 ultimately depend from claims 1, 10, and 19, respectively. As such, Applicants respectfully request the allowance of claims 1-20.

Claim Rejections Under 35 U.S.C. §103

Claims 1, 2, 10, 11, and 19

Claims 1, 2, 10, 11, and 19 were rejected under 35 U.S.C. § 102(a)(1) as allegedly anticipated by Devi. As previously discussed, independent claims 1, 10, and 19 have been amended to include the allowable subject matter of previously pending claims 5 and 14. Claims 2 and 11 depend from claims 1 and 10, respectively. Thus, Applicants submit that claims 1, 2, 10, 11, and 19 are in condition for allowance, and that the 103 rejection is moot. As such, Applicants respectfully request withdrawal of the rejections of claims 1, 2, 10, 11, and 19.

Claims 3 and 12

Claims 3 and 12 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Devi as applied to claims 2 and 11 above, in view of Choi. As previously discussed, independent claims 1 and 10 have been amended to include the allowable subject matter of previously pending claims 5 and 14. Claims 3 and 12 depend from claims 1 and claim 10, respectively. Thus, Applicants submit that claims 3 and 12 are in condition for allowance, and that the 103 rejection is moot. As such, Applicants respectfully request withdrawal of the rejections of claims 3 and 12.

Claims 4 and 13

Claims 4 and 13 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Devi and Choi as applied to claims 3 and 12 above, in view of Schipka. As previously discussed, independent claims 1 and 10 have been amended to include the allowable subject matter of previously pending claims 5 and 14. Claims 4 and 13 depend from claims 1 and 10, respectively. Thus, Applicants submit that claims 4 and 13 are in condition for allowance, and that the 103 rejection is moot. As such, Applicants respectfully request withdrawal of the rejections of claims 4 and 13.

Claims 6 and 15

Claims 6 and 15 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Devi as applied to claims 2 and 11 above, in view of Thomas. As previously discussed, independent claims 1 and 10 have been amended to include the allowable subject matter of previously pending claims 5 and 14. Claims 6 and 15 depend from claims 1 and 10, respectively. Thus, Applicants submit that claims 6 and 15 are in condition for allowance, and that the 103 rejection is moot. As such, Applicants respectfully request withdrawal of the rejections of claims 6 and 15.

Claims 7 and 16

Claims 7 and 16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Devi and Thomas as applied to claims 6 and 15 above in view of Nachenberg. As previously discussed, independent claims 1 and 10 have been amended to include the allowable subject matter of previously pending claims 5 and 14. Claims 7 and 16 depend from claims 1 and 10, respectively. Thus, Applicants submit that claims 7 and 16 are in condition for allowance, and that the 103 rejection is moot. As such, Applicants respectfully request withdrawal of the rejections of claims 7 and 16.

Claims 8, 9, 17, 18, and 20

Claims 8, 9, 17, 18, and 20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Devi, as applied to claims 1, 10, and 19 above, in view of Gilbert. As previously discussed, independent claims 1, 10, and 19 have been amended to include the allowable subject matter of previously pending claims 5 and 14. Claims 8, 9, 17, 18, and 20 depend from claims 1, 10, and 19, respectively. Thus, Applicants submit that claims 8, 9, 17, 18, and 20 are in condition for allowance, and that the 103 rejection is moot. As such, Applicants respectfully request withdrawal of the rejections of claims 8, 9, 17, 18, and 20.

CONCLUSION

This Amendment fully responds to the Office Action mailed on July 17, 2019. Still, that Office Action may contain arguments and rejections that are not directly addressed by this Amendment due to the fact that they are rendered moot in light of the preceding arguments in favor of patentability. Hence, failure of this Amendment to directly address an argument raised in the Office Action should not be taken as an indication that the Applicant believes the argument has merit. Furthermore, the claims of the present application may include other elements, not discussed in this Amendment, which are not shown, taught, or otherwise suggested by the references of record. Accordingly, the preceding arguments in favor of patentability are advanced without prejudice to other bases of patentability.

It is believed that no further fees are due with this Response. However, the Commissioner is hereby authorized to charge any deficiencies or credit any overpayment with respect to this patent application to deposit account number 13-2725.

In light of the above remarks and amendments, it is believed that the application is now in condition for allowance and such action is respectfully requested. Should any additional issues need to be resolved, the Examiner is requested to telephone the undersigned to attempt to resolve those issues.

Respectfully submitted,

Dated: September 26, 2019

/David D. Harrell/

David D. Harrell, Reg. No. 71,855
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1242

27488
PATENT TRADEMARK OFFICE

Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (Currently Amended)A computer-implemented method comprising:

extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the plurality of static data points represent predefined character strings in the executable file;

~~analyzing~~ generating a feature vector from the plurality of static data points using a classifier trained to classify the plurality of static data points based on a collection of data comprising known malicious executable files, known benign executable files, and known unwanted executable files, wherein the collection of data comprises at least a portion of the plurality of static data points, and wherein one or more features of the feature vector are selectively turned on or off based on whether a value of one or more static data points from the plurality of extracted static data points is within a predetermined range; and

determining whether the executable file is harmful based on the analysis.

2. (Original) The computer-implemented method according to claim 1, wherein the extracting the plurality of static data points further comprises classifying the extracted static data points according to a type of data extracted from the executable file, and encoding the extracted static data points for the classifier based on the classification.

3. (Currently Amended) The computer-implemented method according to claim 2, wherein analyzing the executable file further comprises ~~generating a feature vector from the plurality of extracted static data points and~~ evaluating the feature vector using support vector processing to determine whether the executable file is at least one of harmful, benign, and potentially unwanted.

4. (Original) The computer-implemented method according to claim 3, wherein generating the at least one feature vector comprises selectively setting features of the classifier based on the plurality of extracted static data points.

5. (Canceled)

6. (Original) The computer-implemented method according to claim 2, wherein the classifying the at least one static data point comprises classifying the plurality of extracted static data points into categories comprising numeric values, nominal values, string or byte sequences, and Boolean values.

7. (Original) The computer-implemented method according to claim 6, wherein analyzing the executable file further comprises generating at least one feature vector from the plurality of extracted static data points, wherein features of the generated feature vector are weighted based at least upon the classified categories and the plurality of extracted static data points.

8. (Original) The computer-implemented method according to claim 1, wherein determining whether the executable file is harmful further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value.

9. (Original) The computer-implemented method according to claim 8, wherein the threshold value is set based on predetermined false positive range data.

10. (Currently Amended) A computer-readable storage device containing instructions, that when executed on at least one processor, causing the processor to execute a process comprising:

extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the plurality of static data points represent predefined character strings in the executable file;

generating a feature vector from ~~analyzing~~ the plurality of static data points using a classifier trained to classify the plurality of static data points based on a collection of data comprising known malicious executable files, known benign executable files and known unwanted executable files, wherein the collection of data comprises at least a portion of the plurality of static data points, and wherein one or more features of the feature vector are selectively turned on or off based on whether one or more values of one or more static data points from the plurality of extracted static data points is within a predetermined range; and

determining whether the executable file is harmful based on the analyzing of the executable file.

11. (Original) The computer-readable storage device according to claim 10, wherein the extracting of the plurality of static data points executed by the processor further comprises classifying the extracted static data points according to a type of data extracted from the executable file, and encoding the extracted static data points for the classifier based on the classifying.

12. (Currently Amended) The computer-readable storage device according to claim 11, wherein analyzing the executable file further comprises ~~generating at least one feature vector from the plurality of extracted static data points and~~ evaluating the feature vector using linear or nonlinear support vector processing to determine whether the executable file is at least one of harmful, benign, and potentially unwanted.

13. (Original) The computer-readable storage device according to claim 12, wherein generating the at least one feature vector comprises selectively setting features of the classifier based on the plurality of extracted static data points.

14. (Canceled)

15. (Original) The computer-readable storage device according to claim 11, wherein the classifying the at least one static data point comprises classifying the plurality of extracted static

data points into categories comprising numeric values, nominal values, string or byte sequences, and Boolean values.

16. (Original) The computer-readable storage device according to claim 15, wherein analyzing the executable file further comprises generating a feature vector from the plurality of extracted static data points, wherein features of the generated feature vector are weighted based at least upon the classified categories and the plurality of extracted static data points.

17. (Original) The computer-readable storage device according to claim 10, wherein determining whether the executable file is harmful further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value.

18. (Original) The computer-readable storage device according to claim 17, wherein the threshold value is set based on predetermined false positive range data.

19. (Currently Amended) A system comprising:

at least one memory; and

at least one processor operatively connected with the memory and configured to perform operation of:

extracting a plurality of predefined character strings from an executable file without decrypting or unpacking the executable file;

generating a feature vector from ~~analyzing~~ the plurality of predefined character strings using a classifier trained to classify the plurality of predefined character strings based on a collection of data comprising known malicious executable files, known benign executable files and known unwanted executable files, wherein the collection of data comprises at least a portion of one or more of the plurality of predefined character strings, and wherein one or more features of the feature vector are selectively turned on or off based on whether a value of one or more predefined character strings from the plurality of predefined character strings is within a predetermined range; and

determining whether the executable file is harmful based on the analyzing of the executable file.

20. (Original) The system according to claim 19, wherein the determining further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value, and wherein the threshold value is set based on predetermined false positive range data.

21. (New) The system according to claim 19, wherein the extracting the plurality of predefined character strings further comprises classifying the extracted plurality of predefined character strings according to a type of data extracted from the executable file, and encoding the extracted plurality of predefined character strings for the classifier based on the classification.

22. (New) The system according to claim 19, wherein determining whether the executable file is harmful further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value.

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.
14/709,875	05/12/2015	Mauritius Schmidtler	04584.0168US01	1593

23552 7590 09/30/2019

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2493	

NOTIFICATION DATE	DELIVERY MODE
09/30/2019	ELECTRONIC

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

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

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

USPTO23552@merchantgould.com

Applicant-Initiated Interview Summary	Application No. 14/709,875	Applicant(s) Schmidtler et al.		
	Examiner MICHAEL J SIMITOSKI	Art Unit 2493	AIA (First Inventor to File) Status Yes	Page 1 of 2

All participants (applicant, applicants representative, PTO personnel):

1. MICHAEL J SIMITOSKI (Primary Examiner); Telephonic

2. David Harrell, Reg. No. 71,855 (Attorney of Record); Telephonic

Date of Interview: 23 September 2019

Claims Discussed: 1

Prior Art Discussed: Devi

Amendment proposed: See attached agenda

Issues Discussed:

Item(s) under 35 U.S.C. 103:
Applicant proposed an amendment to the claims (see attached agenda). The Examiner noted that, based on the prior search and consideration, the amendment would likely place claim 1 in condition for allowance.

Attachment(s): Agenda, Proposed Amendments,

/Michael Simitoski/ Primary Examiner, Art Unit 2493	

Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04
Please further see:
MPEP 713.04
Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)
37 CFR § 1.2 Business to be transacted in writing

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

TO: Examiner Gary Lavelle

FROM: David Harrell (Reg. No. 71,855)

DATE: September 18, 2019

RE: Agenda for Examiner Interview on Monday, September 23, 2019 at 1:00pm EST

Application No: 14/709,875
Docket No.: 04584.0168US01
Filing Date: May 12, 2015
Title: AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS

"FOR DISCUSSION PURPOSES ONLY – NOT FOR OFFICIAL ENTRY"

I. Discuss § 103 Rejection:

a. Discuss "Detection of Packed Malware" by Devi

b. Discuss additional cited art if/as necessary.

II. Discuss proposed claim amendment:

1. (Currently Amended)A computer-implemented method comprising:

extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the plurality of static data points represent predefined character strings in the executable file;

~~analyzing~~ generating a feature vector from the plurality of static data points using a classifier trained to classify the plurality of static data points based on a collection of data comprising known malicious executable files, known benign executable files, and known unwanted executable files, wherein the collection of data comprises at least a portion of the plurality of static data points, and wherein features of the feature vector are selectively turned on or off based on whether a value of a static data point from the plurality of extracted static data points is within a predetermined range; and

determining whether the executable file is harmful based on the analysis.

Sophos Ex. 1003
Page 385 of 456

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/709,875	Filing Date 05/12/2015	☐ To be Mailed

ENTITY: ☑ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $80 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $420 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	10/26/2019	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0		x $100 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0		x $460 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

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

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

23552 7590 11/14/2019
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	PAPER NUMBER
2493	

DATE MAILED: 11/14/2019

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/709,875	05/12/2015	Mauritius Schmidtler	04584.0168US01	1593

TITLE OF INVENTION: AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1000	$0.00	$0.00	$1000	02/14/2020

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: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

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

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

23552 7590 11/14/2019

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

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

Certificate of Mailing or Transmission

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

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/709,875	05/12/2015	Mauritius Schmidtler	04584.0168US01	1593

TITLE OF INVENTION: AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1000	$0.00	$0.00	$1000	02/14/2020

EXAMINER	ART UNIT	CLASS-SUBCLASS
SIMITOSKI, MICHAEL J	2493	726-023000

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

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

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 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 must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). 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. Fees submitted: ❑ Issue Fee ❑ Publication Fee (if required) ❑ Advance Order - # of Copies _____

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

❑ Electronic Payment via EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

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

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

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

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

Sophos Ex. 1003
Page 388 of 456

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.
14/709,875	05/12/2015	Mauritius Schmidtler	04584.0168US01	1593

23552 7590 11/14/2019

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	PAPER NUMBER
2493	

DATE MAILED: 11/14/2019

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

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

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

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

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

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

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

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

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

Notice of Allowability	Application No. 14/709,875	Applicant(s) Schmidtler et al.	
	Examiner MICHAEL J SIMITOSKI	Art Unit 2493	AIA (FITF) Status Yes

-- 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 Applicant's remarks dated 9/26/2019.
   ☐ 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 See Continuation Sheet . 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. 11/1/2019.
5. ☑ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/Michael Simitoski/
Primary Examiner, Art Unit 2493

Continuation of 3. The allowed claim(s) is/are: 1-2,6-11,13 and 15-24

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

DETAILED ACTION

2. The response of 9/26/2019 was received and considered.

3. Claims 1-4, 6-13 and 15-22 are pending.

EXAMINER'S AMENDMENT

4. 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 David Harrell, 71,855, on 11/1/2019.

The application has been amended as follows:

Please **REPLACE ALL CLAIMS** with the listing in the attached **Office Action Appendix**.

Allowable Subject Matter

5. Claims 1-2, 6-11, 13 and 15-24 are allowed.

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

a. Applicant's remarks (9/26/2019, p. 8) are persuasive. The prior art fails to teach generating a feature vector from the plurality of static data points using a classifier trained to classify the plurality of static data points based on a collection of data comprising known

malicious executable files, known benign executable files, and known unwanted executable files, wherein one or more features of the feature vector are selectively turned on or off based on whether a value of one or more static data points from the plurality of extracted static data points is within a predetermined range and evaluating the feature vector using support vector processing to determine whether the executable file is harmful, in combination with the remaining elements of the claims as a whole.

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

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL J SIMITOSKI whose telephone number is (571)272-3841. The examiner can normally be reached on Monday - Friday, 7:00-3:00.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Carl Colin can be reached on 571-272-3862. 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.

/Michael Simitoski/
Primary Examiner, Art Unit 2493

November 4, 2019

Examiner-Initiated Interview Summary	**Application No.** 14/709,875	**Applicant(s)** Schmidtler et al.		
	Examiner MICHAEL J SIMITOSKI	**Art Unit** 2493	**AIA (First Inventor to File) Status** Yes	**Page** **1 of** 2

All participants (applicant, applicants representative, PTO personnel):

1. MICHAEL J SIMITOSKI (Primary Examiner); Telephonic

2. David Harrell, 71,855 (Attorney of Record); Telephonic

Date of Interview: 01 November 2019

Claims Discussed: Claims 1, 3-4, 10, 12-13 and 19

Amendment proposed: See attached Examiner's amendment

Issues Discussed:

Claim Interpretation and/or scope:
The Examiner contacted Applicant to discuss the response dated 9/26/2019. Applicant incorporated allowable subject matter from (for example), claim 5 into claim 1, but omitted some of the intervening claim language of claims 3 and 4. The Examiner maintained that without an evaluating step providing a connection between the claimed feature vector and the previously recited "determining", the claim was missing essential elements. Applicant agreed to the attached Examiner's amendments to place the application in condition for allowance.

Attachment(s): Proposed Amendments,

/Michael Simitoski/ Primary Examiner, Art Unit 2493	

Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04
Please further see:
MPEP 713.04
Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)
37 CFR § 1.2 Business to be transacted in writing

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.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/709,875	Schmidtler et al.
	Examiner	Art Unit
	MICHAEL J SIMITOSKI	2493

CPC - Searched*		
Symbol	Date	Examiner
G06F21/565, G06F99/005 and G06F221/033	11/27/2016	Gary Lavelle
G06F 21/562,565; 2221/033; 8/53 | G06N 20/00	11/04/2019	MJS

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

/Michael Simitoski/ Primary Examiner, Art Unit 2493	

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/709,875	Schmidtler et al.
	Examiner	Art Unit
	MICHAEL J SIMITOSKI	2493

Search Notes		
Search Notes	**Date**	**Examiner**
Inventor search	11/27/2016	Gary Lavelle
NPL search (Google, ACM and IEEE with seach terms including: malware | malicious | virus, classify, static data points, feature vector, packed, encrypted...)	11/25/2016	Gary Lavelle
East search (see attached search history listing)	11/27/2016	Gary Lavelle
Inventor search updated	3/19/2017	Gary Lavelle
NPL search updated (Google, ACM and IEEE with new search terms including: static reference points...)	3/19/2017	Gary Lavelle
East search (see attached search history listing)	3/20/2017	Gary Lavelle
Inventor search updated	04/16/2018	Gary Lavelle
NPL search above updated (Google, ACM and IEEE with new search terms including: define file points of reference...)	04/10/2018	Gary Lavelle
G06F21/565, G06F99/005 and G06F221/033 EAST search updated (see attached search history listing included with this form to determine the scope of search)	04/16/2018	Gary Lavelle
Inventor search updated	01/17/2019	Gary Lavelle
NPL search above updated	01/17/2019	Gary Lavelle
G06F21/565, G06F99/005 and G06F221/033 EAST search updated (see attached search history listing included with this form to determine the scope of search)	01/17/2019	Gary Lavelle
EAST, NPL and Inventor searches performed	11/04/2019	MJS
Consulted Global dossier and Common Citation Document	11/04/2019	MJS

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
G06F	21/562,565; 2221/033; 8/53	11/04/2019	MJS
G06N	20/00	11/04/2019	MJS

/Michael Simitoski/ Primary Examiner, Art Unit 2493	

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/709,875	Schmidtler et al.
	Examiner	**Art Unit**
	MICHAEL J SIMITOSKI	2493

CPC								
Symbol							**Type**	**Version**
G06F	/	21	/	565			F	2013-01-01
G06N	/	20	/	00			I	2019-01-01
G06F	/	21	/	562			I	2013-01-01
G06F	/	8	/	53			A	2013-01-01
G06F	/	2221	/	033			A	2013-01-01

CPC Combination Sets								
Symbol							**Type**	**Set**	**Ranking**	**Version**
	/		/							

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	20	
/Michael Simitoski/ Primary Examiner, Art Unit 2493	04 November 2019	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

U.S. Patent and Trademark Office

Part of Paper No.: 20191101

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/709,875	Schmidtler et al.
	Examiner	**Art Unit**
	MICHAEL J SIMITOSKI	2493

INTERNATIONAL CLASSIFICATION				
CLAIMED				
G06F	/	21	/	56
G06N	/	5	/	04
G06N20/00	/	20	/	00
G06F8/53	/	8	/	53

NON-CLAIMED				
G06F	/	11	/	30

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	20	
/Michael Simitoski/ Primary Examiner, Art Unit 2493	04 November 2019	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/709,875	Schmidtler et al.
	Examiner	**Art Unit**
	MICHAEL J SIMITOSKI	2493

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

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	10	10	17	19										
2	2	11	11	18	20										
	3		12	19	21										
3	4	12	13	20	22										
	5		14	8	23										
4	6	13	15	9	24										
5	7	14	16												
6	8	15	17												
7	9	16	18												

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	20	
/Michael Simitoski/ Primary Examiner, Art Unit 2493	04 November 2019	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S60	17	(machine adj learning) and (feature adj vector) and (ignor$4 exclu$4 (turn$4 adj off)) near2 (feature (data adj point)) with (range threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/11/04 10:49
S61	12	(machine adj learning) and (feature adj vector) and (exclu$4 (turn$4 adj off)) near2 (feature (data adj point)) with (range threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/11/04 10:49
S62	96	((("Schmidtler") near3 ("Mauritius"))).INV. ((("Dalal") near3 ("Gaurav"))).INV. ((("Yoosoofmiya") near3 ("Reza"))).INV.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/11/04 10:49
S63	4	S62 and (unpack$4 near3 file)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/11/04 10:49

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S66	24529	(G06F21/562 OR G06F21/565 OR G06F2221/033 OR G06F8/53 OR G06N20/00).CPC.	US-PGPUB; USPAT	OR	ON	2019/11/04 10:49
S67	5	S66 and (((turn$4 adj off) disregard$4 exclu$4 ignor$4) near2 (feature)).clm. and range.clm.	US-PGPUB; USPAT	OR	ON	2019/11/04 10:49
S68	5	S66 and (((turn$4 adj off) disregard$4 exclu$4 ignor$4) near2 (feature)).clm. and classifier.clm.	US-PGPUB; USPAT	OR	ON	2019/11/04 10:49

11/ 4/ 2019 11:01:01 AM
C:\ Users\ msimitoski\ Documents\ EAST\ Workspaces\ 14\ 14_709875_threat_detection_static_analysis_without_decrypting_unpacking.wsp

Bibliographic Data

Application No: 14/709,875

Foreign Priority claimed: ○ Yes ◉ No

35 USC 119 (a-d) conditions met: ☐ Yes ☑ No ☐ Met After Allowance

Verified and Acknowledged: /Michael Simitoski/ Examiner's Signature | Initials

Title: AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
05/12/2015	726	2493	04584.0168US01
RULE			

APPLICANTS

Webroot Inc., Broomfield, CO, UNITED STATES

INVENTORS

Mauritius Schmidtler Escondido, CA, UNITED STATES

Gaurav Dalal San Jose, CA, UNITED STATES

Reza Yoosoofmiya San Diego, CA, UNITED STATES

CONTINUING DATA

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

05/27/2015

STATE OR COUNTRY

UNITED STATES

ADDRESS

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903
UNITED STATES

FILING FEE RECEIVED

$730

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.
14/709,875	05/12/2015	Mauritius Schmidtler	04584.0168US01	1593

23552 7590 12/23/2019

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2493	

NOTIFICATION DATE	DELIVERY MODE
12/23/2019	ELECTRONIC

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

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

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

USPTO23552@merchantgould.com

Corrected ***Notice of Allowability***	**Application No.** 14/709,875	**Applicant(s)** Schmidtler et al.	
	Examiner MICHAEL J SIMITOSKI	**Art Unit** 2493	**AIA (FITF) Status** Yes

-- 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 Applicant's remarks dated 9/26/2019.
   ☐ 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 See Continuation Sheet . 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. 11/1/2019.
5. ☑ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/Michael Simitoski/
Primary Examiner, Art Unit 2493

Continuation of 3. The allowed claim(s) is/are: 1-2,6-11,13 and 15-24

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

DETAILED ACTION

2. The response of 9/26/2019 was received and considered.

3. Claims 1-4, 6-13 and 15-22 are pending.

EXAMINER'S AMENDMENT

4. 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 David Harrell, 71,855, on 11/1/2019.

The application has been amended as follows:

Please **REPLACE ALL CLAIMS** with the listing in the attached **Office Action Appendix**.

Allowable Subject Matter

5. Claims 1-2, 6-11, 13 and 15-24 are allowed.

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

a. Applicant's remarks (9/26/2019, p. 8) are persuasive. The prior art fails to teach generating a feature vector from the plurality of static data points using a classifier trained to classify the plurality of static data points based on a collection of data comprising known

malicious executable files, known benign executable files, and known unwanted executable files, wherein one or more features of the feature vector are selectively turned on or off based on whether a value of one or more static data points from the plurality of extracted static data points is within a predetermined range and evaluating the feature vector using support vector processing to determine whether the executable file is harmful, in combination with the remaining elements of the claims as a whole.

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

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL J SIMITOSKI whose telephone number is (571)272-3841. The examiner can normally be reached on Monday - Friday, 7:00-3:00.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Carl Colin can be reached on 571-272-3862. 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.

/Michael Simitoski/
Primary Examiner, Art Unit 2493

December 16, 2019

Examiner-Initiated Interview Summary	**Application No.** 14/709,875	**Applicant(s)** Schmidtler et al.		
	Examiner MICHAEL J SIMITOSKI	**Art Unit** 2493	**AIA (First Inventor to File) Status** Yes	**Page** **1 of** 2

All participants (applicant, applicants representative, PTO personnel):

1. MICHAEL J SIMITOSKI (Primary Examiner); Telephonic

2. David Harrell, 71,855 (Attorney of Record); Telephonic

Date of Interview: 01 November 2019

Claims Discussed: Claims 1, 3-4, 10, 12-13 and 19

Amendment proposed: See attached Examiner's amendment

Issues Discussed:

Claim Interpretation and/or scope:
The Examiner contacted Applicant to discuss the response dated 9/26/2019. Applicant incorporated allowable subject matter from (for example), claim 5 into claim 1, but omitted some of the intervening claim language of claims 3 and 4. The Examiner maintained that without an evaluating step providing a connection between the claimed feature vector and the previously recited "determining", the claim was missing essential elements. Applicant agreed to the attached Examiner's amendments to place the application in condition for allowance.

Attachment(s): Proposed Amendments,

/Michael Simitoski/ Primary Examiner, Art Unit 2493	

Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04
Please further see:
MPEP 713.04
Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)
37 CFR § 1.2 Business to be transacted in writing

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.

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/709,875	Schmidtler et al.
	Examiner	**Art Unit**
	MICHAEL J SIMITOSKI	2493

CPC								
Symbol							**Type**	**Version**
G06F	/	21	/	565			F	2013-01-01
G06N	/	20	/	00			I	2019-01-01
G06F	/	21	/	562			I	2013-01-01
G06F	/	8	/	53			A	2013-01-01
G06F	/	2221	/	033			A	2013-01-01

CPC Combination Sets								
Symbol							**Type**	**Set**	**Ranking**	**Version**
	/		/							

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	20	
/Michael Simitoski/ Primary Examiner, Art Unit 2493	16 December 2019	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

U.S. Patent and Trademark Office

Part of Paper No.: 20191216

Sophos Ex. 1003
Page 413 of 456

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/709,875	Schmidtler et al.
	Examiner	**Art Unit**
	MICHAEL J SIMITOSKI	2493

INTERNATIONAL CLASSIFICATION				
CLAIMED				
G06F	/	21	/	56
G06N	/	5	/	04
G06N20/00	/	20	/	00
G06F8/53	/	8	/	53

NON-CLAIMED				
G06F	/	11	/	30

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	20	
/Michael Simitoski/ Primary Examiner, Art Unit 2493	16 December 2019	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/709,875	Schmidtler et al.
	Examiner	**Art Unit**
	MICHAEL J SIMITOSKI	2493

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

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	10	10	17	19										
2	2	11	11	18	20										
	3		12	19	21										
3	4	12	13	20	22										
	5		14	8	23										
4	6	13	15	9	24										
5	7	14	16												
6	8	15	17												
7	9	16	18												

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	20	
/Michael Simitoski/ Primary Examiner, Art Unit 2493	16 December 2019	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

U.S. Patent and Trademark Office

Part of Paper No.: 20191216

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/709,875	Schmidtler et al.
	Examiner	Art Unit
	MICHAEL J SIMITOSKI	2493

CPC - Searched*		
Symbol	Date	Examiner
G06F21/565, G06F99/005 and G06F221/033	11/27/2016	Gary Lavelle
G06F 21/562,565; 2221/033; 8/53 | G06N 20/00	11/04/2019	MJS

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

/Michael Simitoski/ Primary Examiner, Art Unit 2493	

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/709,875	Schmidtler et al.
	Examiner	Art Unit
	MICHAEL J SIMITOSKI	2493

Search Notes		
Search Notes	**Date**	**Examiner**
Inventor search	11/27/2016	Gary Lavelle
NPL search (Google, ACM and IEEE with seach terms including: malware | malicious | virus, classify, static data points, feature vector, packed, encrypted...)	11/25/2016	Gary Lavelle
East search (see attached search history listing)	11/27/2016	Gary Lavelle
Inventor search updated	3/19/2017	Gary Lavelle
NPL search updated (Google, ACM and IEEE with new search terms including: static reference points...)	3/19/2017	Gary Lavelle
East search (see attached search history listing)	3/20/2017	Gary Lavelle
Inventor search updated	04/16/2018	Gary Lavelle
NPL search above updated (Google, ACM and IEEE with new search terms including: define file points of reference...)	04/10/2018	Gary Lavelle
G06F21/565, G06F99/005 and G06F221/033 EAST search updated (see attached search history listing included with this form to determine the scope of search)	04/16/2018	Gary Lavelle
Inventor search updated	01/17/2019	Gary Lavelle
NPL search above updated	01/17/2019	Gary Lavelle
G06F21/565, G06F99/005 and G06F221/033 EAST search updated (see attached search history listing included with this form to determine the scope of search)	01/17/2019	Gary Lavelle
EAST, NPL and Inventor searches performed	11/04/2019	MJS
Consulted Global dossier and Common Citation Document	11/04/2019	MJS

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
G06F	21/562,565; 2221/033; 8/53	11/04/2019	MJS
G06N	20/00	11/04/2019	MJS

/Michael Simitoski/ Primary Examiner, Art Unit 2493	

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Mauritius Schmidtler et al.	Examiner:	Simitoski, Michael J.
Serial No.:	14/709,875	Group Art Unit:	2493
Filed:	May 12, 2015	Docket No.:	04584.0168US01
Title:	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS		

Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (Currently Amended)A computer-implemented method comprising:

extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the plurality of static data points represent predefined character strings in the executable file;

~~analyzing~~ generating a feature vector from the plurality of static data points using a classifier trained to classify the plurality of static data points based on a collection of data comprising known malicious executable files, known benign executable files, and known unwanted executable files, wherein the collection of data comprises at least a portion of the plurality of static data points, and wherein one or more features of the feature vector are selectively turned on or off based on whether a value of one or more static data points from the plurality of extracted static data points is within a predetermined range; and

evaluating the feature vector using support vector processing to determine whether the executable file is harmful.

~~determining whether the executable file is harmful based on the analysis.~~

2. (Original) The computer-implemented method according to claim 1, wherein the extracting the plurality of static data points further comprises classifying the extracted static data points according to a type of data extracted from the executable file, and encoding the extracted static data points for the classifier based on the classification.

3. (Canceled)

4. (Original) The computer-implemented method according to claim [[3]]2, wherein generating the at least one feature vector comprises selectively setting features of the classifier based on the plurality of extracted static data points.

5. (Canceled)

6. (Original) The computer-implemented method according to claim 2, wherein the classifying the at least one static data point comprises classifying the plurality of extracted static data points into categories comprising numeric values, nominal values, string or byte sequences, and Boolean values.

7. (Original) The computer-implemented method according to claim 6, wherein analyzing the executable file further comprises generating at least one feature vector from the plurality of extracted static data points, wherein features of the generated feature vector are weighted based at least upon the classified categories and the plurality of extracted static data points.

8. (Original) The computer-implemented method according to claim 1, wherein determining whether the executable file is harmful further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value.

9. (Original) The computer-implemented method according to claim 8, wherein the threshold value is set based on predetermined false positive range data.

10. (Currently Amended) A computer-readable storage device containing instructions, that when executed on at least one processor, causing the processor to execute a process comprising:

extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the plurality of static data points represent predefined character strings in the executable file;

generating a feature vector from ~~analyzing~~ the plurality of static data points using a classifier trained to classify the plurality of static data points based on a collection of data comprising known malicious executable files, known benign executable files and known unwanted executable files, wherein the collection of data comprises at least a portion of the plurality of static data points, and wherein one or more features of the feature vector are selectively turned on or off based on whether one or more values of one or more static data points from the plurality of extracted static data points is within a predetermined range; and

evaluating the feature vector using support vector processing to determine whether the executable file is harmful.

~~determining whether the executable file is harmful based on the analyzing of the executable file.~~

11. (Original) The computer-readable storage device according to claim 10, wherein the extracting of the plurality of static data points executed by the processor further comprises classifying the extracted static data points according to a type of data extracted from the executable file, and encoding the extracted static data points for the classifier based on the classifying.

12. (Canceled)

13. (Original) The computer-readable storage device according to claim [[12]]11, wherein generating the at least one feature vector comprises selectively setting features of the classifier based on the plurality of extracted static data points.

14. (Canceled)

15. (Original) The computer-readable storage device according to claim 11, wherein the classifying the at least one static data point comprises classifying the plurality of extracted static data points into categories comprising numeric values, nominal values, string or byte sequences, and Boolean values.

16. (Original) The computer-readable storage device according to claim 15, wherein analyzing the executable file further comprises generating a feature vector from the plurality of extracted static data points, wherein features of the generated feature vector are weighted based at least upon the classified categories and the plurality of extracted static data points.

17. (Original) The computer-readable storage device according to claim 10, wherein determining whether the executable file is harmful further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value.

18. (Original) The computer-readable storage device according to claim 17, wherein the threshold value is set based on predetermined false positive range data.

19. (Currently Amended) A system comprising:

at least one memory; and

at least one processor operatively connected with the memory and configured to perform operation of:

extracting a plurality of predefined character strings from an executable file without decrypting or unpacking the executable file;

generating a feature vector from ~~analyzing~~ the plurality of predefined character strings using a classifier trained to classify the plurality of predefined character strings based on a collection of data comprising known malicious executable files, known benign executable files and known unwanted executable files, wherein the collection of data comprises at least a portion of one or more of the plurality of predefined character strings, and wherein one or more features of the feature vector are selectively turned on or off

based on whether a value of one or more predefined character strings from the plurality of predefined character strings is within a predetermined range; and

evaluating the feature vector using support vector processing to determine whether the executable file is harmful.

~~determining whether the executable file is harmful based on the analyzing of the executable file.~~

20. (Original) The system according to claim 19, wherein the determining further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value, and wherein the threshold value is set based on predetermined false positive range data.

21. (New) The system according to claim 19, wherein the extracting the plurality of predefined character strings further comprises classifying the extracted plurality of predefined character strings according to a type of data extracted from the executable file, and encoding the extracted plurality of predefined character strings for the classifier based on the classification.

22. (New) The system according to claim 19, wherein determining whether the executable file is harmful further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value.

23. (New) The computer-implemented method according to claim 1, wherein the plurality of static data points is extracted using a machine learning technique.

24. (New) The computer-implemented method according to claim 1, wherein a determination of whether the executable file is harmful is used to retrain the classifier.

Bibliographic Data

Application No: 14/709,875

Foreign Priority claimed: ○ Yes ◉ No

35 USC 119 (a-d) conditions met: ☐ Yes ☑ No ☐ Met After Allowance

Verified and Acknowledged: /Michael Simitoski/ Examiner's Signature | Initials

Title: AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
05/12/2015	726	2493	04584.0168US01
RULE			

APPLICANTS

Webroot Inc., Broomfield, CO, UNITED STATES

INVENTORS

Mauritius Schmidtler Escondido, CA, UNITED STATES

Gaurav Dalal San Jose, CA, UNITED STATES

Reza Yoosoofmiya San Diego, CA, UNITED STATES

CONTINUING DATA

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

05/27/2015

STATE OR COUNTRY

UNITED STATES

ADDRESS

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903
UNITED STATES

FILING FEE RECEIVED

$730

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.
14/709,875	05/12/2015	Mauritius Schmidtler	04584.0168US01	1593

23552 7590 01/24/2020

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2493	

NOTIFICATION DATE	DELIVERY MODE
01/24/2020	ELECTRONIC

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

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

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

USPTO23552@merchantgould.com

Corrected ***Notice of Allowability***	**Application No.** 14/709,875	**Applicant(s)** Schmidtler et al.	
	Examiner MICHAEL J SIMITOSKI	**Art Unit** 2493	**AIA (FITF) Status** Yes

-- 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 Applicant's remarks dated 9/26/2019.
   ☐ 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 See Continuation Sheet . 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. 11/1/2019.
5. ☑ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/Michael Simitoski/
Primary Examiner, Art Unit 2493

Continuation of 3. The allowed claim(s) is/are: 1-2,4,6-11,13 and 15-24

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

DETAILED ACTION

2. The response of 9/26/2019 was received and considered.

3. Claims 1-4, 6-13 and 15-22 are pending.

EXAMINER'S AMENDMENT

4. 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 David Harrell, 71,855, on 11/1/2019.

The application has been amended as follows:

Please **REPLACE ALL CLAIMS** with the listing in the attached **Office Action Appendix**.

Allowable Subject Matter

5. Claims 1-2, 4, 6-11, 13 and 15-24 are allowed.

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

a. Applicant's remarks (9/26/2019, p. 8) are persuasive. The prior art fails to teach generating a feature vector from the plurality of static data points using a classifier trained to classify the plurality of static data points based on a collection of data comprising known

malicious executable files, known benign executable files, and known unwanted executable files, wherein one or more features of the feature vector are selectively turned on or off based on whether a value of one or more static data points from the plurality of extracted static data points is within a predetermined range and evaluating the feature vector using support vector processing to determine whether the executable file is harmful, in combination with the remaining elements of the claims as a whole.

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

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL J SIMITOSKI whose telephone number is (571)272-3841. The examiner can normally be reached on Monday - Friday, 7:00-3:00.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Carl Colin can be reached on 571-272-3862. 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.

/Michael Simitoski/
Primary Examiner, Art Unit 2493

January 21, 2020

Examiner-Initiated Interview Summary	Application No. 14/709,875	Applicant(s) Schmidtler et al.		
	Examiner MICHAEL J SIMITOSKI	Art Unit 2493	AIA (First Inventor to File) Status Yes	Page 1 of 2

All participants (applicant, applicants representative, PTO personnel):

1. MICHAEL J SIMITOSKI (Primary Examiner); Telephonic

2. David Harrell, 71,855 (Attorney of Record); Telephonic

Date of Interview: 01 November 2019

Claims Discussed: Claims 1, 3-4, 10, 12-13 and 19

Amendment proposed: See attached Examiner's amendment

Issues Discussed:

Claim Interpretation and/or scope:
The Examiner contacted Applicant to discuss the response dated 9/26/2019. Applicant incorporated allowable subject matter from (for example), claim 5 into claim 1, but omitted some of the intervening claim language of claims 3 and 4. The Examiner maintained that without an evaluating step providing a connection between the claimed feature vector and the previously recited "determining", the claim was missing essential elements. Applicant agreed to the attached Examiner's amendments to place the application in condition for allowance.

Attachment(s): Proposed Amendments,

/Michael Simitoski/ Primary Examiner, Art Unit 2493	

Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04
Please further see:
MPEP 713.04
Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)
37 CFR § 1.2 Business to be transacted in writing

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.

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/709,875	Schmidtler et al.
	Examiner	**Art Unit**
	MICHAEL J SIMITOSKI	2493

CPC						
Symbol					**Type**	**Version**
G06F	/	21	/	565	F	2013-01-01
G06N	/	20	/	00	I	2019-01-01
G06F	/	21	/	562	I	2013-01-01
G06F	/	8	/	53	A	2013-01-01
G06F	/	2221	/	033	A	2013-01-01

CPC Combination Sets							
Symbol					**Type**	**Set**	**Ranking**	**Version**
	/		/					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	20	
/Michael Simitoski/ Primary Examiner, Art Unit 2493	21 January 2020	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

U.S. Patent and Trademark Office

Part of Paper No.: 20200121

Sophos Ex. 1003
Page 432 of 456

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/709,875	Schmidtler et al.
	Examiner	**Art Unit**
	MICHAEL J SIMITOSKI	2493

INTERNATIONAL CLASSIFICATION				
CLAIMED				
G06F	/	21	/	56
G06N	/	5	/	04
G06N20/00	/	20	/	00
G06F8/53	/	8	/	53

NON-CLAIMED				
G06F	/	11	/	30

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	20	
/Michael Simitoski/ Primary Examiner, Art Unit 2493	21 January 2020	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/709,875	Schmidtler et al.
	Examiner	**Art Unit**
	MICHAEL J SIMITOSKI	2493

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

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	10	10	17	19										
2	2	11	11	18	20										
	3		12	19	21										
3	4	12	13	20	22										
	5		14	8	23										
4	6	13	15	9	24										
5	7	14	16												
6	8	15	17												
7	9	16	18												

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	20	
/Michael Simitoski/ Primary Examiner, Art Unit 2493	21 January 2020	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/709,875	Schmidtler et al.
	Examiner	Art Unit
	MICHAEL J SIMITOSKI	2493

CPC - Searched*		
Symbol	Date	Examiner
G06F21/565, G06F99/005 and G06F221/033	11/27/2016	Gary Lavelle
G06F 21/562,565; 2221/033; 8/53 | G06N 20/00	11/04/2019	MJS

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

/Michael Simitoski/ Primary Examiner, Art Unit 2493	

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/709,875	Schmidtler et al.
	Examiner	Art Unit
	MICHAEL J SIMITOSKI	2493

Search Notes		
Search Notes	**Date**	**Examiner**
Inventor search	11/27/2016	Gary Lavelle
NPL search (Google, ACM and IEEE with seach terms including: malware | malicious | virus, classify, static data points, feature vector, packed, encrypted...)	11/25/2016	Gary Lavelle
East search (see attached search history listing)	11/27/2016	Gary Lavelle
Inventor search updated	3/19/2017	Gary Lavelle
NPL search updated (Google, ACM and IEEE with new search terms including: static reference points...)	3/19/2017	Gary Lavelle
East search (see attached search history listing)	3/20/2017	Gary Lavelle
Inventor search updated	04/16/2018	Gary Lavelle
NPL search above updated (Google, ACM and IEEE with new search terms including: define file points of reference...)	04/10/2018	Gary Lavelle
G06F21/565, G06F99/005 and G06F221/033 EAST search updated (see attached search history listing included with this form to determine the scope of search)	04/16/2018	Gary Lavelle
Inventor search updated	01/17/2019	Gary Lavelle
NPL search above updated	01/17/2019	Gary Lavelle
G06F21/565, G06F99/005 and G06F221/033 EAST search updated (see attached search history listing included with this form to determine the scope of search)	01/17/2019	Gary Lavelle
EAST, NPL and Inventor searches performed	11/04/2019	MJS
Consulted Global dossier and Common Citation Document	11/04/2019	MJS

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
G06F	21/562,565; 2221/033; 8/53	11/04/2019	MJS
G06N	20/00	11/04/2019	MJS

/Michael Simitoski/ Primary Examiner, Art Unit 2493	

Bibliographic Data

Application No: 14/709,875

Foreign Priority claimed: ○ Yes ◉ No

35 USC 119 (a-d) conditions met: ☐ Yes ☑ No ☐ Met After Allowance

Verified and Acknowledged: /Michael Simitoski/ Examiner's Signature | Initials

Title: AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
05/12/2015	726	2493	04584.0168US01
RULE			

APPLICANTS

Webroot Inc., Broomfield, CO, UNITED STATES

INVENTORS

Mauritius Schmidtler Escondido, CA, UNITED STATES

Gaurav Dalal San Jose, CA, UNITED STATES

Reza Yoosoofmiya San Diego, CA, UNITED STATES

CONTINUING DATA

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

05/27/2015

STATE OR COUNTRY

UNITED STATES

ADDRESS

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903
UNITED STATES

FILING FEE RECEIVED

$730

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Mauritius Schmidtler et al.	Examiner:	Simitoski, Michael J.
Serial No.:	14/709,875	Group Art Unit:	2493
Filed:	May 12, 2015	Docket No.:	04584.0168US01
Title:	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS		

Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (Currently Amended)A computer-implemented method comprising:

extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the plurality of static data points represent predefined character strings in the executable file;

~~analyzing~~ generating a feature vector from the plurality of static data points using a classifier trained to classify the plurality of static data points based on a collection of data comprising known malicious executable files, known benign executable files, and known unwanted executable files, wherein the collection of data comprises at least a portion of the plurality of static data points, and wherein one or more features of the feature vector are selectively turned on or off based on whether a value of one or more static data points from the plurality of extracted static data points is within a predetermined range; and

evaluating the feature vector using support vector processing to determine whether the executable file is harmful.

~~determining whether the executable file is harmful based on the analysis.~~

2. (Original) The computer-implemented method according to claim 1, wherein the extracting the plurality of static data points further comprises classifying the extracted static data points according to a type of data extracted from the executable file, and encoding the extracted static data points for the classifier based on the classification.

3. (Canceled)

4. (Original) The computer-implemented method according to claim [[3]]2, wherein generating the at least one feature vector comprises selectively setting features of the classifier based on the plurality of extracted static data points.

5. (Canceled)

6. (Original) The computer-implemented method according to claim 2, wherein the classifying the at least one static data point comprises classifying the plurality of extracted static data points into categories comprising numeric values, nominal values, string or byte sequences, and Boolean values.

7. (Original) The computer-implemented method according to claim 6, wherein analyzing the executable file further comprises generating at least one feature vector from the plurality of extracted static data points, wherein features of the generated feature vector are weighted based at least upon the classified categories and the plurality of extracted static data points.

8. (Original) The computer-implemented method according to claim 1, wherein determining whether the executable file is harmful further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value.

9. (Original) The computer-implemented method according to claim 8, wherein the threshold value is set based on predetermined false positive range data.

10. (Currently Amended) A computer-readable storage device containing instructions, that when executed on at least one processor, causing the processor to execute a process comprising:

extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the plurality of static data points represent predefined character strings in the executable file;

generating a feature vector from ~~analyzing~~ the plurality of static data points using a classifier trained to classify the plurality of static data points based on a collection of data comprising known malicious executable files, known benign executable files and known unwanted executable files, wherein the collection of data comprises at least a portion of the plurality of static data points, and wherein one or more features of the feature vector are selectively turned on or off based on whether one or more values of one or more static data points from the plurality of extracted static data points is within a predetermined range; and

evaluating the feature vector using support vector processing to determine whether the executable file is harmful.

~~determining whether the executable file is harmful based on the analyzing of the executable file.~~

11. (Original) The computer-readable storage device according to claim 10, wherein the extracting of the plurality of static data points executed by the processor further comprises classifying the extracted static data points according to a type of data extracted from the executable file, and encoding the extracted static data points for the classifier based on the classifying.

12. (Canceled)

13. (Original) The computer-readable storage device according to claim [[12]]11, wherein generating the at least one feature vector comprises selectively setting features of the classifier based on the plurality of extracted static data points.

14. (Canceled)

15. (Original) The computer-readable storage device according to claim 11, wherein the classifying the at least one static data point comprises classifying the plurality of extracted static data points into categories comprising numeric values, nominal values, string or byte sequences, and Boolean values.

16. (Original) The computer-readable storage device according to claim 15, wherein analyzing the executable file further comprises generating a feature vector from the plurality of extracted static data points, wherein features of the generated feature vector are weighted based at least upon the classified categories and the plurality of extracted static data points.

17. (Original) The computer-readable storage device according to claim 10, wherein determining whether the executable file is harmful further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value.

18. (Original) The computer-readable storage device according to claim 17, wherein the threshold value is set based on predetermined false positive range data.

19. (Currently Amended) A system comprising:

at least one memory; and

at least one processor operatively connected with the memory and configured to perform operation of:

extracting a plurality of predefined character strings from an executable file without decrypting or unpacking the executable file;

generating a feature vector from ~~analyzing~~ the plurality of predefined character strings using a classifier trained to classify the plurality of predefined character strings based on a collection of data comprising known malicious executable files, known benign executable files and known unwanted executable files, wherein the collection of data comprises at least a portion of one or more of the plurality of predefined character strings, and wherein one or more features of the feature vector are selectively turned on or off

based on whether a value of one or more predefined character strings from the plurality of predefined character strings is within a predetermined range; and

evaluating the feature vector using support vector processing to determine whether the executable file is harmful.

~~determining whether the executable file is harmful based on the analyzing of the executable file.~~

20. (Original) The system according to claim 19, wherein the determining further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value, and wherein the threshold value is set based on predetermined false positive range data.

21. (New) The system according to claim 19, wherein the extracting the plurality of predefined character strings further comprises classifying the extracted plurality of predefined character strings according to a type of data extracted from the executable file, and encoding the extracted plurality of predefined character strings for the classifier based on the classification.

22. (New) The system according to claim 19, wherein determining whether the executable file is harmful further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value.

23. (New) The computer-implemented method according to claim 1, wherein the plurality of static data points is extracted using a machine learning technique.

24. (New) The computer-implemented method according to claim 1, wherein a determination of whether the executable file is harmful is used to retrain the classifier.

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

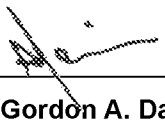
as my/our attorney(s) or agent(s) and to transact all business before the United States Patent and Trademark Office (USPTO) in connection with any and all patents and patent applications that are assigned to **Webroot Inc.** (the "assignee's patents/patent applications") in which they shall appear, any 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:	38539708
Application Number:	14709875
International Application Number:	
Confirmation Number:	1593
Title of Invention:	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS
First Named Inventor/Applicant Name:	Mauritius Schmidtler
Customer Number:	23552
Filer:	John L. Adair/Delia Narvaiz
Filer Authorized By:	John L. Adair
Attorney Docket Number:	04584.0168US01
Receipt Date:	10-FEB-2020
Filing Date:	12-MAY-2015
Time Stamp:	14:19:52
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	126961 50ab3093648a7505d565f42a50de6af35361bd49	no	1

Warnings:

Information:	
Total Files Size (in bytes):	126961

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
14/709,875	05/12/2015	Mauritius Schmidtler	04584.0168US01

CONFIRMATION NO. 1593

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

POA ACCEPTANCE LETTER

OC000000114667375

Date Mailed: 02/12/2020

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 02/10/2020.

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**.

/qnguyen/

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
14/709,875	05/12/2015	Mauritius Schmidtler	04584.0168US01

CONFIRMATION NO. 1593

POWER OF ATTORNEY NOTICE

23552
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

OC000000114667374

Date Mailed: 02/12/2020

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 02/10/2020.

- The Power of Attorney to you in this application has been revoked by the applicant. 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**.

/qnguyen/

TRANSMITTAL OF PAYMENT OF ISSUE FEE (LARGE Entity) 37 C.F.R. 1.311)	Docket No. OPEN7950

First Named Inventor **Mauritius Schmidtler**				
Application No.	Filing Date	Examiner	Group Art Unit	Confirmation No.
14/709,875	**05/12/2015**	**Michael J. Simitoski**	**2493**	**1593**

Title:

AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS

Mail Stop: Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Transmitted herewith are the following items in reference to the above-identified application:

- ☒ Issue Fee Transmittal Form PTOL-85
- ☒ Issue Fee: $1,000.00
- ☒ Comment on Allowance
- ☒ The Director is hereby authorized to charge Deposit Account No. 50-3183 of Sprinkle IP Law Group.
- ☒ The Director is hereby authorized to charge any deficiencies or credit any overpayments to Deposit Account No. 50-3183 of Sprinkle IP Law Group.

Bruce Johnson
Reg. No. 37,861

Customer No. 109422
Sprinkle IP Law Group
1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. (512) 637-9220
Fax. (512) 371-9088

Certificate of Transmission Under 37 C.F.R. § 1.8

I hereby certify that this correspondence is being deposited electronically with the U.S. Patent and Trademark Office using the United States Patent and Trademark Office's EFS-Web system on February 14, **2020**.

/Shenise Ramdeen/
Shenise Ramdeen

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (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)

109422 7590 11/14/2019

Sprinkle IP Law Group
1301 W. 25th Street, Suite 408
Austin, Texas 78705

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 transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

N/A--filed via EFS	(Typed or printed name)
	(Signature)
	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/709,875	05/12/2015	Mauritius Schmidtler	04584.0168US01	1593

TITLE OF INVENTION: AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1000	$0.00	$0.00	$1000	02/14/2020

EXAMINER	ART UNIT	CLASS-SUBCLASS
SIMITOSKI, MICHAEL J	2493	726-023000

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

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

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 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 Sprinkle IP Law Group
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 must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: Webroot, Inc.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Broomfield, COLORADO

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

4a. Fees submitted: ☒ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies .....

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

☒ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 50-3183

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

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

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

Authorized Signature ..... Date 2-12-2020

Typed or printed name Bruce Johnson Registration No. 37,361

Electronic Patent Application Fee Transmittal

Application Number:	14709875
Filing Date:	12-May-2015
Title of Invention:	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS
First Named Inventor/Applicant Name:	Mauritius Schmidtler
Filer:	John L. Adair/Shenise Ramdeen
Attorney Docket Number:	OPEN7950

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	1501	1	1000	1000

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**1000**

Electronic Acknowledgement Receipt

EFS ID:	38593762
Application Number:	14709875
International Application Number:	
Confirmation Number:	1593
Title of Invention:	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS
First Named Inventor/Applicant Name:	Mauritius Schmidtler
Customer Number:	109422
Filer:	John L. Adair/Shenise Ramdeen
Filer Authorized By:	John L. Adair
Attorney Docket Number:	OPEN7950
Receipt Date:	14-FEB-2020
Filing Date:	12-MAY-2015
Time Stamp:	14:40:57
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$1000
RAM confirmation Number	E20202DE41213738
Deposit Account	503183
Authorized User	Shenise Ramdeen

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

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 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	Post Allowance Communication - Incoming	OPEN7950_Comments02-14-20.pdf	44747 cbc7f1abfe39e4867552784 6dc602d71057cb912	no	1
Warnings:					
Information:					
2		OPEN7950_IssueFee02-14-20.pdf	114107 b0995dc201d34c68ff1f9752f93c42df7b2b6962	yes	2

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Transmittal Letter	1	1
Issue Fee Payment (PTO-85B)	2	2

Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30245 e1bc7579273bf1c3c3e310140f78a174d0bccc93	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	189099		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
Comments on Statement of Reasons for Allowance	Atty. Docket No. **OPEN7950**

First Named Inventor **Mauritius Schmidtler**	
Application No. **14/709,875**	Filing or 371 (c) Date **May 12, 2015**
Title **AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS**	
Group Art Unit **2493**	Examiner **Michael J. Simitoski**
Confirmation No. **1593**	

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

Dear Sir:

Certificate of Transmission Under 37 C.F.R. § 1.8

I hereby certify that this correspondence is being deposited electronically with the U.S. Patent and Trademark Office using the United States Patent and Trademark Office's EFS-Web system on February 14, **2020.**

Shenise Ramdeen

Applicant appreciates the Examiner's allowance of Claims 1-2, 4, 6-11, 13 and 15-24 of United States Patent Application No. 14/709,875. Applicant submits the record as a whole makes evident the reasons for allowance and that there are additional reasons for patentability not enumerated by the Examiner. While Applicant agrees with the Examiner's reasons for patentability to the extent such reasons are consistent with the record as a whole, Applicant does not acquiesce or agree to any characterization of the claims that place unwarranted limitations or interpretations upon the claims, especially to the extent such limitations or interpretations are inconsistent with the claim language, specification or prior prosecution history in this case.

The Director of the U.S. Patent and Trademark Office is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

Sprinkle IP Law Group

Bruce Johnson
Reg. No. 37,361

Dated: 2-13-2020

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. 512-637-9220
Fax. 512-371-9088

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.
14/709,875	03/24/2020	10599844	OPEN7950	1593

109422 7590 03/04/2020

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

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 95 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):

Mauritius Schmidtler, Escondido, CA;
Webroot Inc., Broomfield, CO;
Gaurav Dalal, San Jose, CA;
Reza Yoosoofmiya, San Diego, CA;

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.