SCORE Placeholder Sheet for IFW Content

Application Number: 16791649 Document Date: 02/14/2020

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.

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.

- Drawing

At the time of document entry (noted above):

- USPTO employees may access SCORE content via DAV or via the SCORE web page.
- External customers may access SCORE content via PAIR using the Supplemental Content tab.

Sophos Ex. 1002
Sophos Ltd. and Sophos Inc., v. Webroot Inc.
PGR2023-00031

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

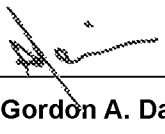
as my/our attorney(s) or agent(s) and to transact all business before the United States Patent and Trademark Office (USPTO) in connection with any and all patents and patent applications that are assigned to **Webroot Inc.** (the "assignee's patents/patent applications") in which they shall appear, any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

AUTOMATIC THREAT DETECTON OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS

CROSS-REFERENCE TO RELATED APPLICATION(S)

[0001] This application is a continuation of, and claims a benefit of priority from U.S. Patent Application No. 14/709,875, filed May 12, 2015, entitled "AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS," which is fully incorporated by reference herein.

BACKGROUND

[0002] 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

[0003] 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.

[0004] 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

[0005] 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.

[0006] Figure 1 illustrates an exemplary system 100 showing interaction of components for implementation threat detection as described herein.

[0007] Figure 2 illustrates an exemplary distributed system 200 showing interaction of components for implementation of exemplary threat detection as described herein.

[0008] Figure 3 illustrates an exemplary method 300 for implementation of threat detection systems and methods described herein.

[0009] Figure 4 illustrates one example of a suitable operating environment 400 in which one or more of the present examples may be implemented.

[0010] 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.

[0011] 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.

[0012] 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.

[0013] 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.

[0014] 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).

[0015] 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.

[0016] 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.

[0017] 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.).

[0018] 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

[0019] 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.

[0020] 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.

[0021] 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).

[0022] 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.

[0023] 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).

[0024] 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_0043006f007000790072006900670068007 4:0.4472135955
legalcopyright_002800430029:0.4472135955
legalcopyright_0043006f00720070002e:0.4472135955
legalcopyright_0031003900390035:0.4472135955
legalcopyright_004d006900630072006f0073006f00660074:0.4472135955
filesize_9965:1.0
PEHeaderAnomaly_False:1.0

[0025] 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.

[0026] 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.

[0027] 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.

[0028] 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.).

[0029] 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.

[0030] 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.

[0031] 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.

[0032] 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.

[0033] 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.

[0034] 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.

[0035] 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.

[0036] 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.

[0037] 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.

[0038] 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.

[0039] 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.

[0040] 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.

[0041] 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.

[0042] 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.

[0043] 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.

[0044] 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.

[0045] 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.

[0046] 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.

[0047] 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.

[0048] 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.

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.

FIG. 1

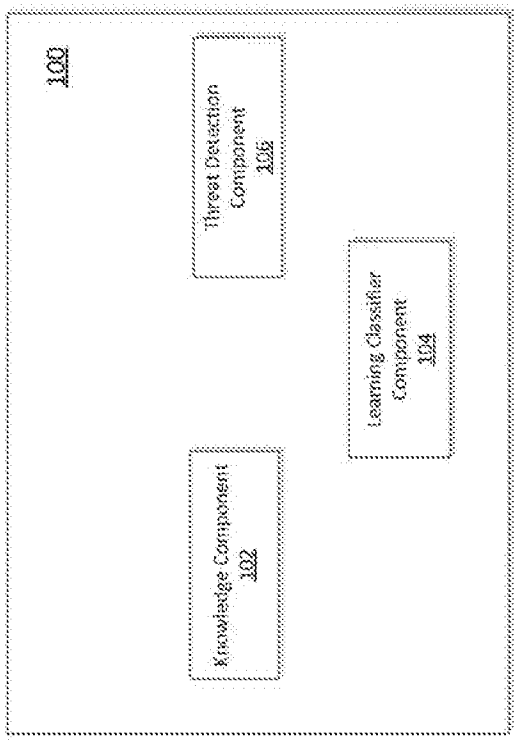

100
Threat Detection Component 106
Learning Classifier Component 104
Knowledge Component 102

FIG. 2

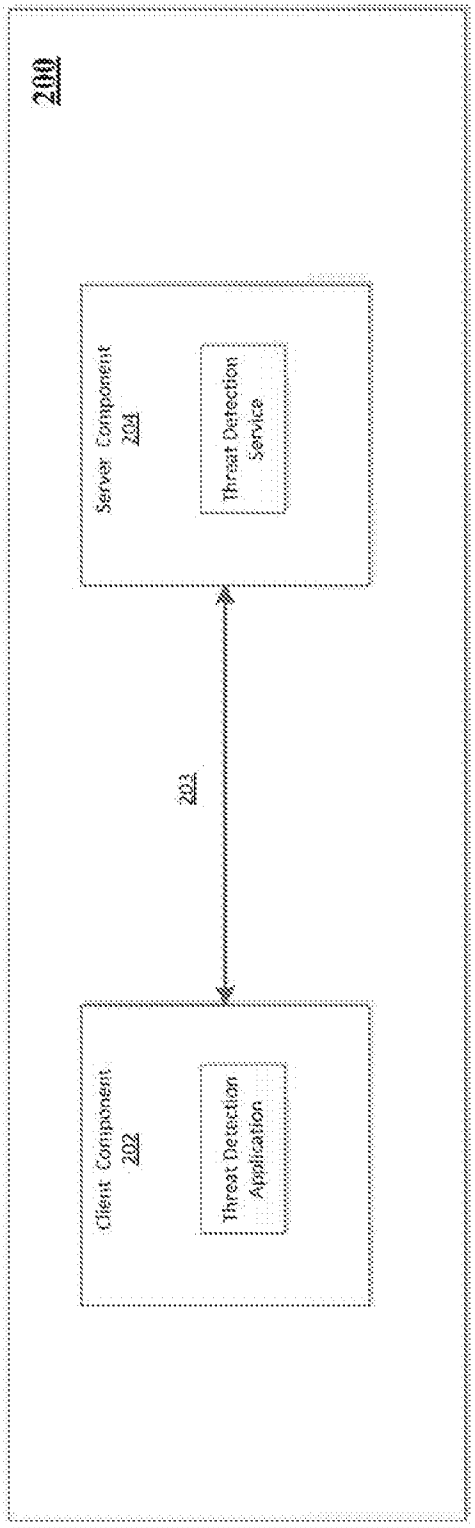
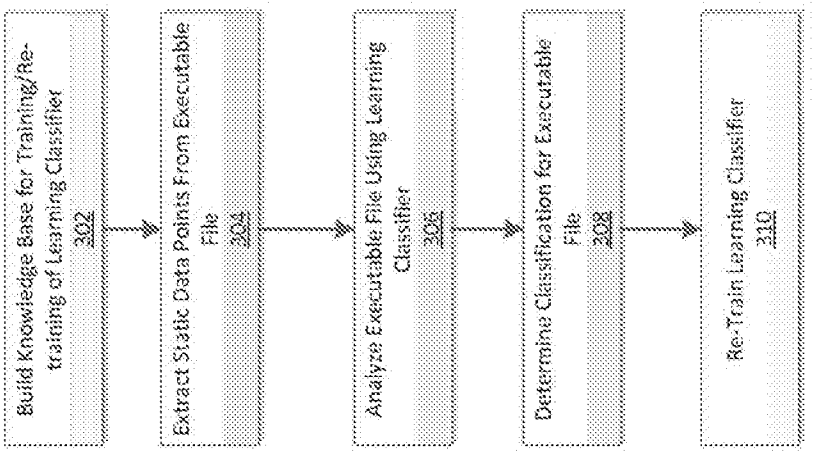

200
Server Component
204
Threat Detection
Service
223
Client Component
202
Threat Detection
Application

FIG. 3


300
Build Knowledge Base for Training/Re-training of Learning Classifier
302
Extract Static Data Points From Executable File
304
Analyze Executable File Using Learning Classifier
306
Determine Classification for Executable File
308
Re-Train Learning Classifier
310

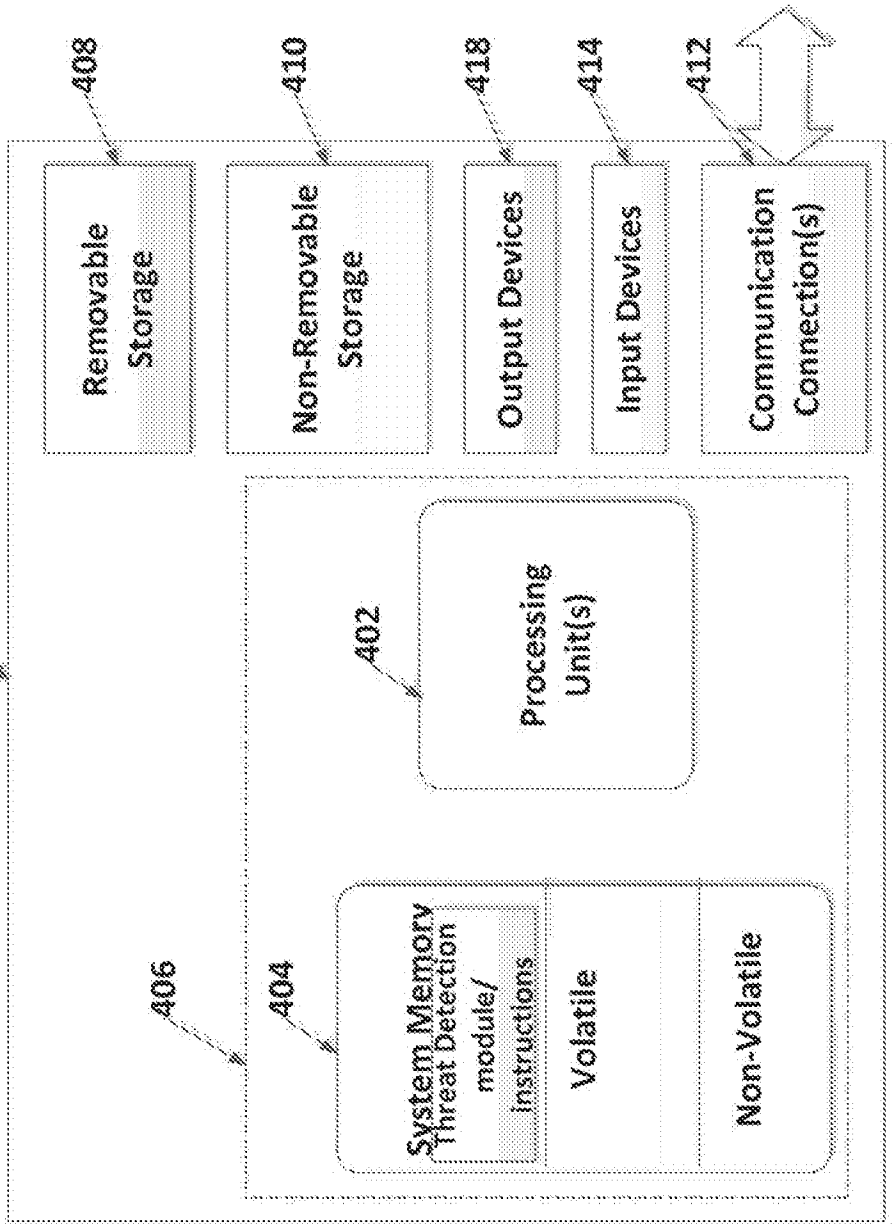

PAGE 4 OF 4
400
406
404
System Memory
Threat Detection
module/
instructions
Volatile
Non-Volatile
402
Processing
Unit(s)
408
Removable
Storage
410
Non-Removable
Storage
418
Output Devices
414
Input Devices
412
Communication
Connection(s)

FIG. 4

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Atty. Docket No. (Opt.) **OPEN7950-1**

Applicant **Mauritius Schmidtler**	
Application Number **Not Yet Assigned**	Filing or 371 (c) Date **Herewith**
For **AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS**	
Group Art Unit **Not Yet Assigned**	Examiner **Not Yet Assigned**
Confirmation Number **Not Yet Assigned**	

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

Certification of Transmission Under 37 C.F.R. 1.8

I hereby certify that this correspondence is being transmitted to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 via the U.S. Patent and Trademark Office Electronic Filing System (EFS-Web) on February 14 2020.

Shenise Ramdeen

Shenise Ramdeen

Dear Sir,

Applicant respectfully requests, pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, that the information listed on the attached SB08A/B form(s) be considered and cited in the examination of the above-identified application. A copy of U.S. Patent(s) and U.S. Patent Application Publication(s) listed on the attached SB08A form is not being submitted with this Information Disclosure Statement pursuant to the waiver of 37 C.F.R. § 1.98(a)(2)(i) by the U.S. Patent and Trademark Office. Where applicable, a copy of foreign patent document(s) as well as information listed on the attached SB08B form is enclosed for the convenience of the Examiner.

☒ This Information Disclosure Statement is being submitted within three months of the filing date of a national application other than a continued prosecution application under 37 C.F.R. § 1.53(d).

☐ This Information Disclosure Statement is being submitted within three months of the date of entry of the national stage as set forth in 37 C.F.R. § 1.491 in an international application;

☐ This Information Disclosure Statement is being submitted before the mailing of a First Office Action on the merits; or

☐ This Information Disclosure Statement is being submitted before the mailing of a First Office Action after the filing of a request for continued examination under 37 C.F.R. § 1.114.

Pursuant to 37 C.F.R. §§ 1.97(g) and (h), no representation is made that a search has been made or that this information is material to patentability of the present application.

Applicant does not believe any fees are due and owing at this time. If Applicant is in error, the Director is hereby authorized to deduct any and all appropriate fees from Deposit Account 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

SPRINKLE IP LAW GROUP
Attorneys for Applicant

Bruce Johnson
Reg. No. 37,361

Dated: 2-14-, 2020

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. (512) 637-9220
Fax. (512) 317-9088

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Application Number	Not Yet Assigned
Filing or 371 (c) Date:	Herewith
First Named Inventor	Mauritius Schmidtler
Group Art Unit	Not Yet Assigned
Examiner Name	Not Yet Assigned
Attorney Docket Number	OPEN7950-1

Sheet 1 of 1

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A1	20160335435	11-17-2016	Schmidtler et al.	
	A2	9465940	10-11-2016	Wijnowicz et al.	
	A3	20070240220	10-11-2007	Tuvell et al.	
	A4	20120079596	03-29-2012	Thomas et al.	
	A5	9197663	11-24-2015	Gilbert et al.	
	A6	8719924	05-06-2014	Williamson et sl.	
	A7	20140165203	06-12-2014	Friedrichs et al.	
	A8	20100192222	07-29-2010	Stokes et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT				Application Number	Not Yet Assigned
				Filing or 371 (c) Date:	Herewith
				First Named Inventor	Mauritius Schmidtler
				Group Art Unit	Not Yet Assigned
				Examiner Name	Not Yet Assigned
Sheet	1	of	2	Atty Docket Number	OPEN7950-1

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, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C1	Office Action issued for U.S. Patent Application No. 14/709,875 (OPEN7950), mailed December 8, 2016, 19 pages.	
	C2	SHABTAI ET AL., "Detection of Malicious Code by Applying Machine Learning Classifiers on Static Features: A State-of-the-Art Survery," Information Security Technical Report, Elsevier Advanced Technology, Amsterdam NL, vol. 14, No. 1, February 1, 2009, pp. 16-29, XP026144093, ISSN: 1363-4127.	
	C3	Office Action issued for U.S. Patent Application No. 14/709,875 (OPEN7950), mailed March 24, 2017, 21 pages.	
	C4	Office Action issued for U.S. Patent Application No. 14/709,875 (OPEN7950), mailed April 20, 2018, 22 pages.	
	C5	Office Action issued for U.S. Patent Application No. 14/709,875 (OPEN7950), mailed January 24, 2019, 21 pages.	
	C6	Office Action issued for U.S. Patent Application No. 14/709,875 (OPEN7950), mailed July 17, 2019, 12 pages.	
	C7	BOST, et al., "Machine learning classification over encrypted data." N DSS. Vol. 4324. 2015. (Year: 2015), 14 pages.	
	C8	CHOI, et al., "Efficient Malicious Code Detection Using N-Gram Analysis and SVM," 2011 14th International Conference on Network-Based Information Systems. IEEE, 2011, 4 pages.	
	C9	DEVI, Dhruwajita et al., "Detection of Packed Malware," Proceedings of the First International Conference on Security of Internet ofThings, ACM, 2012, 5 pages.	
	C10	DUBE, et al., "Malware Target Recognition Via Static Heuristics," Computers & Security 31.1, 2012, 11 pages.	
	C11	MERKEL, et al., Statistical Detection of Malicious Pe-Executables for Fast Offline Analysis," IFIP International Conference on Communications and Multimedia Security, Springer, Berlin, 2010, 12 pages.	

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT				Application Number	Not Yet Assigned
				Filing or 371 (c) Date:	Herewith
				First Named Inventor	Mauritius Schmidtler
				Group Art Unit	Not Yet Assigned
				Examiner Name	Not Yet Assigned
Sheet	2	of	2	Atty Docket Number	OPEN7950-1

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, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C12	SINGLA, et al., "A Novel Approach to Malware Detection Using Static Classification," International Journal of Computer Science and Information Security 13.3, 2015, 5 pages.	
	C13	TABISH, et al., "Malware Detection Using Statistical Analysis of Byte-Level File Content," Proceedings of the ACM SIGKDD Workshop on CyberSecurity and Intelligence Informatics, ACM, 2009, 9 pages.	
	C14	TREADWELL, et al., "A Heuristic Approach for Detection of Obfuscated Malware, 2009 IEEE International Conference on Intelligence and Security Informatics, 2009, 9 pages.	
	C15	Notice of Allowance issued for U.S. Patent Application No. 14/709,875 (OPEN7950), mailed November 14, 2019, 11 pages.	
	C16	Corrected Notice of Allowance issued for U.S. Patent Application No. 14/709,875 (OPEN7950), mailed December 23, 2019, 8 pages.	
	C17	Corrected Notice of Allowance issued for U.S. Patent Application No. 14/709,875 (OPEN7950), mailed January 24, 2020, 8 pages.	
	C18	International Patent Application No. PCT/US2016/032090, International Search Report and Written Opinion mailed July 29,2016, 13 pages.	
	C19	PERDISCI et al., "Classification of Packed Executables for Accurate Computer Virus Detection," Pattern Recognition Letters 29, 2008, 6 pages.	
	C20	PERDISCI et al., "McBoost: Boosting Scalability in Malware Collection and Analysis Using Statistical Classification of Executables," Annual Computer Security Applications, 2008, 10 pages.	
	C21	KHAN, et al., "Determining Malicious Executable Distinguishing Attributes and Low-Complexity Detection", J. ComputVirol, 7.2 (2011), 11 pgs.	
	C22	KOLTER, et al., "Learning to Detect and Classift Malicious Executables in the Wild", Journal of Machine Learning Research 7 (2006), 24 pages.	

Examiner Signature		Date Considered	

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
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:	OPEN7950-1

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
UTILITY APPLICATION FILING	1011	1	300	300
UTILITY SEARCH FEE	1111	1	660	660
UTILITY EXAMINATION FEE	1311	1	760	760
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**1720**

Electronic Acknowledgement Receipt

EFS ID:	38594566
Application Number:	16791649
International Application Number:	
Confirmation Number:	2519
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:	OPEN7950-1
Receipt Date:	14-FEB-2020
Filing Date:	
Time Stamp:	16:34:03
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$1720
RAM confirmation Number	E20202DG34296363
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	Application Data Sheet	OPEN7950-1_ADS02-14-20.pdf	620797 2825bba962be3f43e2561b4bd61c18590ffae04d	no	9
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
2	Oath or Declaration filed	OPEN7950-1_Oath02-14-20.pdf	171586 4f28871bca8a6e975758aa146c3329b8f78fed1a	no	3
Warnings:					
Information:					
3	Power of Attorney	OPEN7950-1_POA02-14-20.pdf	44148 483ca86916057c7e91f3c441a81572b82cab365e	no	1
Warnings:					
Information:					
4		OPEN7950-1_FiledApplication02-14-20.pdf	174076 7748e6a91b60b451ce02a2444012e96acc1dbfc1	yes	22

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	20
Claims	21	21
Abstract	22	22

Warnings:

Information:

5	Drawings-only black and white line drawings	OPEN7950-1_FiledDrawings02-14-20.pdf	332011 1d633c968924249c4d0e23a2e6dc9c40ecf8d276	no	4
Warnings:					
Information:					
6		OPEN7950-1_IDS02-14-20.pdf	164071 118d6d92994ec9ebddf5cfac2aa2f9affe746868	yes	5
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Transmittal Letter		1	2	
	Information Disclosure Statement (IDS) Form (SB08)		3	5	
Warnings:					
Information:					
7	Non Patent Literature	OPEN7950_C1.pdf	702490 3f335c24b06bc400d72191baa38c69c11cd41ff6	no	19
Warnings:					
Information:					
8	Non Patent Literature	OPEN7950_C2.pdf	1719385 796525e5e5e70416fc2ad8627e5d30b7e19daafa	no	14
Warnings:					
Information:					
9	Non Patent Literature	OPEN7950_C3.pdf	781562 944c7524b803ed26833ae5b4e5304180f9034a18	no	21
Warnings:					
Information:					
10	Non Patent Literature	OPEN7950_C4.pdf	884942 e0fab02868aca5183907833b24ede2a14024331e	no	22
Warnings:					
Information:					

11	Non Patent Literature	OPEN7950_C5.pdf	820960 437e64b32e21e6aa4220cbf842e142d07605f509	no	21
Warnings:					
Information:					
12	Non Patent Literature	OPEN7950_C6.pdf	426923 47f4221fea30f820c066d963380e362f11e6b30e	no	12
Warnings:					
Information:					
13	Non Patent Literature	OPEN7950_C7.pdf	1277253 bf4bab2cfc75976133fbb9ad8830f12ca7f18152	no	14
Warnings:					
Information:					
14	Non Patent Literature	OPEN7950_C8.pdf	343453 f2c71295b996fd5dbd4489b6c57ff2c9577551a0	no	4
Warnings:					
Information:					
15	Non Patent Literature	OPEN7950_C9.pdf	435471 85fc9b2366a2a1b5f145d066bbf151b59a57e434	no	5
Warnings:					
Information:					
16	Non Patent Literature	OPEN7950_C10.pdf	1114240 fa87567da86cd7531d40fb80e2626301c93b688e	no	11
Warnings:					
Information:					
17	Non Patent Literature	OPEN7950_C11.pdf	635421 01e1529896fe6971af826baed1a14e104442b947	no	12
Warnings:					
Information:					

18	Non Patent Literature	OPEN7950_C12.pdf	430406 441b6c164f58210428185bc86a910a9e70947503	no	5
Warnings:					
Information:					
19	Non Patent Literature	OPEN7950_C13.pdf	828210 b2bf24b6b3a913fe30e499928c8cde5487760084	no	9
Warnings:					
Information:					
20	Non Patent Literature	OPEN7950_C14.pdf	1137096 98f3a4d69903a4fa359fc6a7a9540a9993e4fe36	no	9
Warnings:					
Information:					
21	Non Patent Literature	OPEN7950_C15.pdf	478281 dfcefcaa9832d7a309eb12a06e23fa1e6e542ad5	no	11
Warnings:					
Information:					
22	Non Patent Literature	OPEN7950_C16.pdf	207618 4cfc835d593f90a4ea4080e32d9bf1990f19468e	no	8
Warnings:					
Information:					
23	Non Patent Literature	OPEN7950_C17.pdf	207622 f45d66af1a80d4c20dc1ff43a473c84a1f432c1b	no	8
Warnings:					
Information:					
24	Non Patent Literature	OPEN7950_C18.pdf	950001 0e812bd4ad8b64b5c3bd777279df34bba7ff863a	no	13
Warnings:					
Information:					

25	Non Patent Literature	OPEN7950_C19.pdf	980182 d60b7946ac106e791d68fd14342a8c5e59397c5d	no	6
Warnings:					
Information:					
26	Non Patent Literature	OPEN7950_C20.pdf	1407095 bbeb7c8287f3f44f889f87978426a20d911c68c9	no	10
Warnings:					
Information:					
27	Non Patent Literature	OPEN7950_C21.pdf	1172193 2affccc0f60d4824869946ab838e33c0cd072ae	no	11
Warnings:					
Information:					
28	Non Patent Literature	OPEN7950_C22.pdf	1502746 9d8deaed7fbd54194e832cff805e07a64598080d	no	24
Warnings:					
Information:					
29	Fee Worksheet (SB06)	fee-info.pdf	34939 a900978e9ff05d249b77dd2987fae3d22628be9f	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	19985178	

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.

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	OPEN7950-1
	Application Number	
Title of Invention	AUTOMATIC THREAT DETECTION 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	US

Mailing Address of Inventor:

Address 1	c/o Webroot Inc.
Address 2	385 Interlocken Crescent, Suite 800

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	US

Mailing Address of Inventor:

Address 1	Webroot Inc.
Address 2	385 Interlocken Crescent, Suite 800

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 (02-18)
Approved for use through 11/30/2020. 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	OPEN7950-1
	Application Number	
Title of Invention	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS	

City	San Diego	State/Province	CA	Country of Residence	US

Mailing Address of Inventor:

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

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

Correspondence Information:

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

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

Customer Number	109422		
Email Address	docketing@sprinklelaw.com	Add Email	Remove Email

Application Information:

Title of the Invention	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS		
Attorney Docket Number	OPEN7950-1	**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

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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	OPEN7950-1
	Application Number	
Title of Invention	AUTOMATIC THREAT DETECTION 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	109422		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim 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" field blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Continuation of	14/709875	2015-05-12

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

Foreign Priority Information:

This section allows for the applicant to claim 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. 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(i)(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).

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

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

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	OPEN7950-1
	Application Number	
Title of Invention	AUTOMATIC THREAT DETECTION 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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	OPEN7950-1
	Application Number	
Title of Invention	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is 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 State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	OPEN7950-1
	Application Number	
Title of Invention	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS	

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.

Applicant 1

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. ☒

Organization Name	Webroot Inc.

Mailing Address Information For Applicant:

Address 1	385 Interlocken Crescent		
Address 2	Suite 800		
City	Broomfield	**State/Province**	CO
Country	US	Postal Code	80021
Phone Number		Fax Number	
Email Address			

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

Assignee Information including Non-Applicant Assignee 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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	OPEN7950-1
	Application Number	
Title of Invention	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS	

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.

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

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		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.

Signature:

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature				Date (YYYY-MM-DD)	2020-02-14
First Name	Bruce	Last Name	Johnson	Registration Number	37361

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

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. 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	OPEN7950-1
	Application Number	
Title of Invention	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS	

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 CooperationTreaty.

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.

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: 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.

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 Yoosofmiya 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.

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
16/791,649	02/14/2020		1720	OPEN7950-1	1	1

CONFIRMATION NO. 2519

FILING RECEIPT

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

OC000000115102845

Date Mailed: 03/03/2020

Receipt is acknowledged of this non-provisional utility 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 FIRST INVENTOR, 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 corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction 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 provided that the request is grantable.

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 109422

Domestic Priority data as claimed by applicant

This application is a CON of 14/709,875 05/12/2015

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 Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 03/02/2020

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 16/791,649**

Projected Publication Date: 06/11/2020

Non-Publication Request: No

Early Publication Request: No

Title

AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS

Preliminary Class

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.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 16/791,649

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	300
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	660
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	760
TOTAL CLAIMS (37 CFR 1.16(i))	1 minus 20 =	*			OR	x 100 =	0.00
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1 minus 3 =	*				x 460 =	0.00
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	1720

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
PRELIMINARY AMENDMENT	Atty. Docket No. **OPEN7950-1**

First Named Inventor **Mauritius Schmidtler**	
Application Number **16/791,649**	Filing or 371(c) Date **February 14, 2020**
Title **AUTOMATIC THREAT OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS (AS AMENDED)**	
Group Art Unit **2493**	Confirmation No. **2519**

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

Dear Sir:

Certification of Transmission Under 37 C.F.R. 1.8

I hereby certify that this correspondence is being transmitted to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22312-1450 via the U.S. Patent and Trademark Office Electronic Filing System (EFS-Web) on April 9, 2020.

/Shenise Ramdeen/
Shenise Ramdeen

Prior to examination on the merits, please amend the above-identified U.S. patent application as follows:

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

Amendments to the Claims begin on page 4 of this paper.

Remarks begin on page 8 of this paper

Electronic Acknowledgement Receipt

EFS ID:	39115533
Application Number:	16791649
International Application Number:	
Confirmation Number:	2519
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:	Bruce Alan Johnson/Shenise Ramdeen
Filer Authorized By:	Bruce Alan Johnson
Attorney Docket Number:	OPEN7950-1
Receipt Date:	09-APR-2020
Filing Date:	14-FEB-2020
Time Stamp:	16:39:03
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		OPEN7950-1_PreliminaryAmendment04-09-20.pdf	47459 17f9e1226b00209 41ecc7e2c0235589c82f6 1100	yes	8

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Applicant Arguments/Remarks Made in an Amendment	8	8
	Claims	4	7
	Specification	2	3
	Preliminary Amendment	1	1
Warnings:			
Information:			
	Total Files Size (in bytes):	47459	

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.

CONCLUSION

In this Preliminary Amendment, the specification has been amended to include the most recent status of the parent U.S. Patent Application referenced in paragraph [0001]. Also in this Preliminary Amendment, the title has been amended and original claim 1 has been cancelled and new claims 2-21 have been added. Support for claims 2-21 can be found in the specification as originally filed, at least in paragraphs [0003], [0019] - [0023], and [0034] - [0035]. No new matter has been added. By this Preliminary Amendment, claims 2-21 are pending in the application.

Applicant believes that all the pending claims 2-21 are in allowable condition. Favorable consideration and prompt issuance of a Notice of Allowance is therefore respectfully requested. The Examiner is invited to contact the undersigned at the phone number indicated below with any questions or comments, or to otherwise facilitate expeditious and compact prosecution of the application.

Applicant does not believe any fee is due or owing. If Applicant is in error, 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
Attorneys for Applicant

/Bruce A Johnson/
Bruce A. Johnson
Reg. No. 37,361

Dated: April 7, 2020

1301 W. 25th Street
Suite 408
Austin, Texas 78705
Tel. (512) 637-9220
Fax. (512) 371-9088

AMENDMENTS TO THE CLAIMS:

Please amend the claims as set forth in the following listing. This listing of claims will replace all prior versions, and listings, of claims in the present application:

1. (Canceled)

2. (New) A computer-implemented method comprising:

identifying, by a knowledge module, static data points that may be indicative of either a harmful or benign executable file;

associating, by the knowledge module, the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting, by the knowledge module, a plurality of static data points from the identified executable file;

generating, by a classifier, a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files; and

providing the generated feature vector to one or more support vector machines to build a probabilistic model that indicates whether the executable file fits into one of the categories of files.

3. (New) The computer-implemented method according to claim 2, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

4. (New) The computer-implemented method according to claim 2, wherein the one or more support vector machines builds the probabilistic model by performing data analysis and pattern recognition on the one or more feature vectors.

5. (New) The computer-implemented method according to claim 2, wherein the probabilistic model indicates whether the executable file is harmful.

6. (New) The computer-implemented method according to claim 2, wherein the executable file is identified in response to a detected condition.

7. (New) The computer-implemented method according to claim 6, wherein the condition is user request for a file download.

8. (New) The computer-implemented method according to claim 6, wherein the condition is the detection of a new file attempting to execute.

9. (New) The computer-implemented method according to claim 2, wherein the plurality of static data points represent predefined character strings in the executable file.

10. (New) The computer-implemented method according to claim 2, 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.

11. (New) The computer-implemented method according to claim 2, wherein a determination of whether the executable file is harmful is used to retrain the classifier.

12. (New) A system comprising:

at least one memory; and

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

identifying static data points that may be indicative of either a harmful or benign executable file;

associating the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting a plurality of static data points from the identified executable file;

generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files; and

providing the generated feature vector to one or more support vector machines to build a probabilistic model that indicates whether the executable file fits into one of the categories of files.

13. (New) The system according to claim 12, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

14. (New) The system according to claim 12, wherein the one or more support vector machines builds the probabilistic model by performing data analysis and pattern recognition on the one or more feature vectors.

15. (New) The system according to claim 12, wherein the probabilistic model indicates whether the executable file is harmful.

16. (New) The system according to claim 12, wherein the plurality of static data points represent predefined character strings in the executable file.

17. (New) The system according to claim 12, 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.

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

identifying static data points that may be indicative of either a harmful or benign executable file;

associating the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting a plurality of static data points from the identified executable file;

generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files; and

providing the generated feature vector to one or more support vector machines to build a probabilistic model that indicates whether the executable file fits into one of the categories of files.

19. (New) The computer-readable storage device according to claim 18, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

20. (New) The computer-readable storage device according to claim 18, wherein the plurality of static data points represent predefined character strings in the executable file.

21. (New) The computer-readable storage device according to claim 18, 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.

AMENDMENTS TO THE TITLE

Please replace the title of the invention with the following amended title.

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

AMENDMENTS TO THE SPECIFICATION

On page 1 of the specification, please replace paragraph [0001] with the following replacement paragraph:

[0001] This application is a continuation of, and claims a benefit of priority from U.S. Patent Application No. 14/709,875, filed May 12, 2015, issued as U.S. Patent No. 10,599,844, entitled "AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS," which is fully incorporated by reference herein.

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 16/791,649	Filing Date 02/14/2020	☐ 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 $100 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $460 =	
☐ 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	04/09/2020	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".	/ANTHONY TYSON/
*** 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 NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
16/791,649	02/14/2020	Mauritius Schmidtler	OPEN7950-1

CONFIRMATION NO. 2519

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

PUBLICATION NOTICE

OC000000117670666

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

Publication No.US-2020-0184073-A1
Publication Date:06/11/2020

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 Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, 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 https://portal.uspto.gov/pair/PublicPair. 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.
16/791,649	02/14/2020	Mauritius Schmidtler	OPEN7950-1	2519

109422 7590 03/29/2021

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

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2493	

MAIL DATE	DELIVERY MODE
03/29/2021	PAPER

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

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

Office Action Summary	Application No. 16/791,649	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 14 February 2020 and 09 April 2020.

☐ 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) 2-21 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) 2-21 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 14 February 2020 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 IDS of 2/14/2020 was received and considered.

3. Claims 2-21 are pending.

Claim Rejections - 35 USC § 112

4. 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.

The following is a quotation of the first paragraph of pre-AIA 35 U.S.C. 112:

> 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 of carrying out his invention.

5. Claims 2-21 are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor or a joint inventor, or for applications subject to pre-AIA 35 U.S.C. 112, the inventor(s), at the time the application was filed, had possession of the claimed invention. The claims recite the limitation: "generating, by a classifier, a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data

comprising files known to fit into one of the plurality of categories of files". However, the specification does not teach using a classifier to generate the feature vector, but rather to use pre-processing to generate the feature vector for use by the classifier.

6. Claims 2-21 are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the enablement requirement. The claim(s) 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. However, the specification does not teach using a classifier to generate the feature vector, but rather to use pre-processing to generate the feature vector for use by the classifier. Therefore, the specification does not enable a skilled artisan to make and/or use the invention, as claimed.

Claim Rejections - 35 USC § 102

7. 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.

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)(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.

9. Claims 2-5, 9, 11-16 and 18-20 are rejected under 35 U.S.C. 102(a)(1) as being anticipated by "Detection of malicious code by applying machine learning classifiers on static features: A state-of-the-art survey." by Shabtai et al. (**Shabtai**).

Regarding claim 2, Shabtai discloses identifying, by a knowledge module (a skilled artisan would understand the reference is describing operations performed by computer software), static data points that may be indicative of either a harmful or benign executable file (training set is provided to the system, where a vector representing each file is extracted based on a vocabulary, p. 17, §2, p. 18, Fig. 1a); associating, by the knowledge module, the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files (create training set of benign and malicious files and input to a training algorithm, p. 17, §2); identifying an executable file to be evaluated (p. 17, §2, p. 18, Fig. 1b); extracting, by the knowledge module, a plurality of static data points from the identified executable file (file parsed and representative vector extracted, p. 17, §2, p. 18, Fig. 1a); generating, by a classifier, a feature vector from the plurality of static data points (representative vector extracted, p. 17, §2, p. 18, Fig. 1a) using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files (training data set is trained using malicious and benign files, p. 17, §2, p. 18, Fig. 1b); and providing the generated feature vector to one or more support vector machines to build a probabilistic model that indicates whether the executable file fits into one of the categories of files (feature vectors provided to classification algorithm, p. 18, Fig. 1b, including support vector machine, p. 20, §5).

Regarding claims 3, 13 and 19, Shabtai discloses wherein the plurality of static data points are extracted without decrypting or unpacking the executable file (Shabtai does not teach decryption or unpacking).

Regarding claims 4 and 14, Shabtai discloses wherein the one or more support vector machines builds the probabilistic model by performing data analysis and pattern recognition on the one or more feature vectors (recognize patterns in collection of byte n-grams derived from input file, p. 24, Table 1).

Regarding claims 5 and 15, Shabtai discloses wherein the probabilistic model indicates whether the executable file is harmful (classifier classifies file into the benign or malicious class, p. 20, §5).

Regarding claims 9, 16 and 20, Shabtai discloses wherein the plurality of static data points represent predefined character strings in the executable file (Portable Executable (PE) and String features, p. 19, §3).[1]

Regarding claim 11, Shabtai discloses wherein a determination of whether the executable file is harmful is used to retrain the classifier (Shabtai discloses acquiring new malicious files and updating (retraining) the classifiers accordingly, p. 26, §6.3).

Regarding claim 12, the claim is similar in scope to claim 2 and is therefore rejected using a similar rationale, noting again that a skilled artisan would understand the reference is describing operations performed by computer software.

Regarding claim 18, the claim is similar in scope to claim 2 and is therefore rejected using a similar rationale, noting again that a skilled artisan would understand the reference is describing operations performed by computer software.

Claim Rejections - 35 USC § 103

10. 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.

11. 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

[1] "A malware detection scheme based on mining format information" by Bai et al. teaches a similar concept.

> 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.

12. Claims 6-8 are rejected under 35 U.S.C. 103 as being unpatentable over **Shabtai**, as applied to claim 1 above, in view of US 2010/0293273 A1 to Basarrate et al. (**Basarrate**).

Regarding claims 6-8, Shabtai is silent regarding wherein the executable file is identified in response to a detected condition. However, Basarrate teaches that it was known for a virus scanner to detect a file being downloaded or executed (¶85)[2]. 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 Shabtai such that the executable file is identified in response to a detected condition. One of ordinary skill in the art would have been motivated to perform such a modification to utilize known triggers for file inspection, as taught by Basarrate. Note that a skilled artisan would have found such a teaching obvious specifically as it well known in the art of computer security to intercept and scan a potential threat when entering the system (downloading) and before allowing execution.

Double Patenting

13. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re*

[2] US 10,116,688 B1 to Yun and US 2011/0154490 A1 to DeLuca et al. teach a similar concept.

Goodman, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on nonstatutory double patenting provided the reference application or patent either is shown to be commonly owned with the examined application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. See MPEP § 717.02 for applications subject to examination under the first inventor to file provisions of the AIA as explained in MPEP § 2159. See MPEP § 2146 *et seq.* for applications not subject to examination under the first inventor to file provisions of the AIA. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO Internet website contains terminal disclaimer forms which may be used. Please visit www.uspto.gov/patent/patents-forms. The filing date of the application in which the form is filed determines what form (e.g., PTO/SB/25, PTO/SB/26, PTO/AIA/25, or PTO/AIA/26) should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

14. Claims 2-5 and 9-21 are rejected on the ground of nonstatutory double patenting as being unpatentable over claim of U.S. Patent No. 10,599,844 in view of Shabtai, per the table below.

15. Claims 6-8 are rejected on the ground of nonstatutory double patenting as being unpatentable over claim of U.S. Patent No. 10,599,844 in view of Shabtai and Basarrate, per the table below.

Note that removing limitations from the patent claims would have been obvious for reasons of breadth. Further, the patent claims anticipate the instant claims, with exceptions listed below.

16/791,649	10,599,844
2	1 – The patent claim lacks the "identifying" and "associating" steps of the instant application. However, those steps (as shown above) are taught in Shabtai (pp. 17-18) for preparing the system to extract the data points and for training the model. Therefore, the distinction would have been obvious to a skilled artisan.
3	1
4	1 – While the patent claim lacks performing data analysis and pattern recognition on the one or more feature vectors, this is taught in Shabtai (pp. 17-18) for determining if the file is harmful. Therefore, the distinction would have been obvious to a skilled artisan.
5	1
6 7 8	1 – The patent claim lacks determining a condition. However, as discussed above, Basarrate discloses this feature. Therefore, the distinction would have been obvious to a skilled artisan.
9	1
10	1
11	9
12	17 - The patent claim lacks the "identifying" and "associating" steps of the instant application. However, those steps (as shown above) are taught in Shabtai (pp. 17-18) for preparing the system to extract the data points and for training the model. Therefore, the distinction would have been obvious to a skilled artisan.
13	17
14	17 – While the patent claim lacks performing data analysis and pattern recognition on the one or more feature vectors, this is taught in Shabtai (pp. 17-18) for determining if the file is harmful. Therefore, the distinction would have been obvious to a skilled artisan.
15	17
16	17
17	17
18	10 – The patent claim lacks the "identifying" and "associating" steps of the instant application. However, those steps (as shown above) are taught in Shabtai (pp. 17-18) for preparing the system to extract the data points and for training the model. Therefore, the distinction would have been obvious to a skilled artisan.
19	10
20	10
21	10

Allowable Subject Matter

16. Claims 10, 17 and 21 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 and any remaining rejections above, not based on prior art, are overcome.

a. Regarding claims 10, 17 and 21, certain prior art related to machine learning teaches removing outliers in the selected data. For example, US 20110172504 A1 to Wegerich teaches ignoring feature data that varies more than a threshold in a system that uses biometric/sensor data. However, the prior art as a whole does not teach how such a feature would be applicable to the teachings of Shabtai.

Conclusion

17. 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 https://ppair-my.uspto.gov/pair/PrivatePair. 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

March 24, 2021

Notice of References Cited	Application/Control No. 16/791,649	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	G06N20/00	1/1
*	B	US-20170262633-A1	09-2017	Miserendino; Scott	G06F21/564	1/1
*	C	US-20160156646-A1	06-2016	Hsueh; Frank Chijeen	G06N20/00	726/1
*	D	US-20160021174-A1	01-2016	DE LOS SANTOS VILCHEZ; Sergio	H04W12/128	709/201
*	E	US-20140310517-A1	10-2014	CHRISTODORESCU; MIHAI	G06N20/00	713/160
*	F	US-20130291111-A1	10-2013	Zhou; Hongyi	G06F21/562	726/23
*	G	US-20120227105-A1	09-2012	FRIEDRICHS; OLIVER	G06F21/564	726/22
*	H	US-20110172504-A1	07-2011	Wegerich; Stephan W.	G16H50/30	600/301
*	I	US-20110154490-A1	06-2011	DeLuca; Lisa Seacat	G06F21/56	726/23
*	J	US-20100293273-A1	11-2010	Basarrate; Inaki Urzay	H04L61/2567	709/224
*	K	US-20100082642-A1	04-2010	Forman; George	G06F16/35	707/749
*	L	US-20090300765-A1	12-2009	Moskovitch; Robert	G06K9/6256	726/24
*	M	US-20090274376-A1	11-2009	Selvaraj; Sathiya Keerthi	G06K9/6269	382/224

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	Bai, Jinrong, Junfeng Wang, and Guozhong Zou. "A malware detection scheme based on mining format information." The Scientific World Journal 2014 (2014). (Year: 2014)
	V	
	W	
	X	

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

Notice of References Cited	Application/Control No. 16/791,649	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	US-20090013405-A1	01-2009	Schipka; Maksym	G06F21/562	726/22
*	B	US-20060037080-A1	02-2006	Maloof; Marcus A.	G06F21/562	726/24
*	C	US-20060026675-A1	02-2006	Cai; Dongming M.	G06F21/562	726/22
*	D	US-10116688-B1	10-2018	Yun; James	H04L63/145	1/1
*	E	US-8510836-B1	08-2013	Nachenberg; Carey S.	H04L63/145	726/23
*	F	US-8161548-B1	04-2012	Wan; Justin	G06K9/6228	726/22
	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	
	V	
	W	
	X	

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

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/791,649	Schmidtler et al.
	Examiner	Art Unit
	MICHAEL J SIMITOSKI	2493

CPC - Searched*		
Symbol	Date	Examiner
G06F 21/51,53,562,56,565,566; 2221/033; 8/53 | G06N 20/00,10 | H04L 63/145	03/24/2021	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.

Search Notes		
Search Notes	Date	Examiner
EAST, NPL and inventor search performed (see EAST and NPL search histories, attached and/or previously made of record)	03/24/2021	MJS
Consulted Common Citation Document and Global Dossier for related/family applications and prosecution histories	03/24/2021	MJS

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
G06F	21/51,53,562,56,565,566; 2221/033; 8/53	03/24/2021	MJS
G06N	20/00,10	03/24/2021	MJS
H04L	63/145	03/24/2021	MJS

/Michael Simitoski/ Primary Examiner, Art Unit 2493	

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/791,649	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	03/24/2021								
	1	-								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								

Bibliographic Data

Application No: 16/791,649

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.
02/14/2020	726	2493	OPEN7950-1
RULE			

APPLICANTS

Webroot Inc., Broomfield, CO,

INVENTORS

Mauritius Schmidtler, Escondido, CA, UNITED STATES

Gaurav Dalal, San Jose, CA, UNITED STATES

Reza Yoosoofmiya, San Diego, CA, UNITED STATES

CONTINUING DATA

This application is a CON of 14709875 05/12/2015 PAT 10599844

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

03/02/2020

STATE OR COUNTRY

UNITED STATES

ADDRESS

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

FILING FEE RECEIVED

$1,720

CCD view for US202016791649

#	CC	Cat.	Citation details
1	*US*		**Application N° US202016791649** (US16791649) - 14 February 2020
2	*US*		**Application N° US201514709875** (US14709875) - 12 May 2015
			National Search Report
			US9465940 B1 (CYLANCE INC [US]) - 11 October 2016
			US2007240220 A1 (TUVELL GEORGE, , et al) - 11 October 2007
			US2012079596 A1 (THOMAS RALPH [US], et al) - 29 March 2012
			US9197663 B1 (BIT9 INC [US]) - 24 November 2015
			US8719924 B1 (WILLIAMSON MATTHEW [US], et al) - 6 May 2014
			US2014165203 A1 (SOURCEFIRE INC [US]) - 12 June 2014
			US2010192222 A1 (MICROSOFT CORP [US]) - 29 July 2010
		X	US8709924 B2 (HANAWA HIROJI [US], et al) - 29 April 2014 * claim 1 | column 1 lines 57 - 67] | column 2 lines 37 - 40] | column 3 lines 1 - 6] abstract | column 6 lines
		Y	US2007240220 A1 (TUVELL GEORGE, , et al) - 11 October 2007 * [0104] | [0161] | [0336] Fig. 9 | [0162] | abs | [0163] Fig. 7 | [0323], [0336] Fig. 9 | [0323] | abstract |
		Y	US9197663 B1 (BIT9 INC [US]) - 24 November 2015 * column 2 lines 17 - 20 and 47 - 52] | column 3 lines 26 - 30] | column 20 lines 44 - 61] | abstract | colum
		Y	US2012079596 A1 (THOMAS RALPH [US], et al) - 29 March 2012 * [0239] | [0175], [0225] and [0272] | [0038], [0175], [0225] and [0272] | table 4] and [0257] | [0250] |
		A	US8719924 B1 (WILLIAMSON MATTHEW [US], et al) - 6 May 2014
		A	US2014165203 A1 (SOURCEFIRE INC [US]) - 12 June 2014
		A	US9465940 B1 (CYLANCE INC [US]) - 11 October 2016
		A	US2010192222 A1 (MICROSOFT CORP [US]) - 29 July 2010
			US8510836 B1 (NACHENBERG CAREY S [US], et al) - 13 August 2013
			US8719924 B1 (WILLIAMSON MATTHEW [US], et al) - 6 May 2014
			US9197663 B1 (BIT9 INC [US]) - 24 November 2015
			US9465940 B1 (CYLANCE INC [US]) - 11 October 2016
			US2007240220 A1 (TUVELL GEORGE, , et al) - 11 October 2007
			US2009013405 A1 (MESSAGELABS LTD [GB]) - 8 January 2009
			US2009274376 A1 (YAHOO INC [US]) - 5 November 2009
			US2009300765 A1 (DEUTSCHE TELEKOM AG [DE]) - 3 December 2009
			US2010082642 A1 (Forman George, , et al) - 1 April 2010
			US2010192222 A1 (MICROSOFT CORP [US]) - 29 July 2010
			US2012079596 A1 (THOMAS RALPH [US], et al) - 29 March 2012
			US2012227105 A1 (FRIEDRICHS OLIVER [US], et al) - 6 September 2012
			US2013291111 A1 (ZHOU HONGYI [CN], et al) - 31 October 2013
			US2014165203 A1 (SOURCEFIRE INC [US]) - 12 June 2014

Sophos Ex. 1002
Page 86 of 347

#	CC	Cat.	Citation details
			US2014310517 A1 (IBM [US]) - 16 October 2014
			US2016021174 A1 (TELEFONICA DIGITAL ESPANA SLU [ES]) - 21 January 2016
			US2016156646 A1 (HEWLETT PACKARD DEVELOPMENT CO [US]) - 2 June 2016
			US2017262633 A1 (BLUVECTOR INC [US]) - 14 September 2017
			US2018365573 A1 (INTEL CORP [US]) - 20 December 2018
			Detection of malicious code by applying machine learning classifiers on static features: A state-of-t Authors: Shabtai A, Moskovitch R, Elovici Y, Glezer C Publication data: Information Security Technical Report, 20090201 Elsevier Advanced Technology, AMSTERDAM, NL Source info: Vol: 14, Nr: 1, Page(s): 16 - 29
			Detection of malicious code by applying machine learning classifiers on static features: A state-of-t Authors: Shabtai A, Moskovitch R, Elovici Y, Glezer C Publication data: Information Security Technical Report, 20090201 Elsevier Advanced Technology, AMSTERDAM, NL Source info: Vol: 14, Nr: 1, Page(s): 16 - 29
			Non-patent literature - Bost, Raphael, et al. "Machine learning classification over encrypted data." NDSS. vol. 4324. 2015. (Year: 20
			Non-patent literature - Choi, Junho, et al. "Efficient malicious code detection using n-gram analysis and SVM." 2011 14th Internatior
			Non-patent literature - Devi, Dhruwajita, and Sukumar Nandi. "Detection of packed malware." Proceedings of the First International
			Non-patent literature - Dube, Thomas, et al. "Malware target recognition via static heuristics." Computers & Security 31.1 (2012): 1
			Non-patent literature - Merkel, Ronny, et al. "Statistical detection of malicious pe-executables for fast offline analysis." IFIP Internati
			Non-patent literature - Singla, Sanjam, et al. "A Novel Approach to Malware Detection using Static Classification." International Jour
			Non-patent literature - Tabish, S. Momina, M. Zubair Shafiq, and Muddassar Farooq. "Malware detection using statistical analysis of
			Non-patent literature - Treadwell, Scott, and Mian Zhou. "A heuristic approach for detection of obfuscated malware." 2009 IEEE Inte
			Applicant
			Non-patent literature - International Patent Application No. PCT/US2016/032090, International Search Report and Written Opinion d
			Non-patent literature - Perdisci et al. (2008) Pattern Recognition Letters 29:1941-1946 "Classification of packed executables for acc
			Non-patent literature - Perdisci et al. (2008) IEEE: Annual Computer Security Applications Conference 301-310 "McBoost: Boosting
			Non-patent literature - Khan, Hassan et al., "Determining Malicious Executable Distinguishing Attributes and Low-Complexity Detect
			Non-patent literature - Kolter, J. Zico et al., "Learning to Detect and Classift Malicious Executables in the Wild", Journal of Machine L
			Non-patent literature - International Patent Application No. PCT/US2016/032090, International Preliminary Report on Patentability d
3	WO		Application N° WO2016US32090 (WOUS2016032090) - 12 May 2016
			International Search Report
	A		US2010192222 A1 (MICROSOFT CORP [US]) - 29 July 2010 * sentences 3 - 6, paragraph [0019] * * sentences 9 - 11, paragraph [0032] *

Sophos Ex. 1002
Page 87 of 347

#	CC	Cat.	Citation details
		X I	*Classification of packed executables for accurate computer virus detection* Authors: Perdisci R, Lanzi A, Lee W Publication data: PATTERN RECOGNITION LETTERS, 20081015 ELSEVIER, AMSTERDAM, NL Source info: Vol: 29, Nr: 14, Page(s): 1941 - 1946 * page 1942, column left, lines 10 - 14, 41 - 42, 51 - 53; figure 1 * * page 1943, column left, lines 9 - 14 * * section 4 "Experiments"; page 1944, column right, lines 6 - 9, 24, 25, 28 * * page 1945; table 1 *
		A	*McBoost: Boosting Scalability in Malware Collection and Analysis Using Statistical Classification of* Authors: Roberto Perdisci, Andrea Lanzi, Wenke Lee Publication data: Computer Security Applications Conference, 2008. ACSAC 2008. Annual, 20081208 IEEE, Piscataway, Source info: Page(s): 301 - 310 * page 304, column left *

Search History

Report Run Date: 2021-03-25 UTC
Queries: 13
Markers: 0

Query #	Timestamp	Results	Page
1	2021-03-24 13:15 UTC	167	3
2	2021-03-24 13:16 UTC	47	4
3	2021-03-24 13:20 UTC	19,682	4
4	2021-03-24 13:20 UTC	0	4
5	2021-03-24 14:03 UTC	3,216,292	4
6	2021-03-24 14:03 UTC	37	4
7	2021-03-24 15:35 UTC	951,394	5
8	2021-03-24 15:35 UTC	231,944	5
9	2021-03-24 15:37 UTC	~231,166	5
10	2021-03-25 08:32 UTC	3,217,372	5
11	2021-03-25 08:33 UTC	3,217,372	5
12	2021-03-25 08:33 UTC	29,530	6
13	2021-03-25 08:35 UTC	808	6

Content: Patents + NPL (188)

US Patents | US Designs | US Applications | EPO Patents | EPO Applications | China Patents | China Applications | Japan Patents | Japan Applications | Korea Patents | Korea Applications | WIPO Applications | Argentina Patents | Argentina Applications | Brazil Patents | Brazil Applications | Canada Patents | Canada Applications | Chile Patents | Chile Applications | Colombia Applications | Costa Rica Applications | Cuba Patents | Cuba Applications | Dominican Republic Applications | Ecuador Patents | Ecuador Applications | El Salvador Applications | Guatemala Applications | Honduras Applications | Mexico Patents | Mexico Applications | Nicaragua Patents | Panama Applications | Peru Applications | Trinidad & Tobago Patents | Uruguay Applications | Austria Patents | Austria Applications | Belarus Patents | Belgium Patents | Belgium Applications | Bosnia & Herzegovina Patents | Bosnia & Herzegovina Applications | Bulgaria Patents | Bulgaria Applications | Croatia Patents | Croatia Applications | Czech Republic Patents | Czech Republic Applications | Czechoslovakia Patents | Czechoslovakia Applications | Denmark Patents | Denmark Applications | Estonia Patents | Estonia Applications | EUIPO Patents | Finland Patents | Finland Applications | France Patents | France Applications | Germany Patents | Germany Applications | Great Britain Patents | Great Britain Applications | Greece Patents | Greece Applications | Hungary Patents | Hungary Applications | Iceland Patents | Iceland Applications | Ireland Patents | Ireland Applications | Italy Patents | Italy Applications | Latvia Patents | Latvia Applications | Lithuania Patents | Lithuania Applications | Luxembourg Patents | Malta Patents | Monaco Patents | Montenegro Patents | Montenegro Applications | Netherlands Patents | Netherlands Applications | Norway Patents | Norway Applications | Poland Patents | Poland Applications | Portugal Patents | Portugal Applications | Republic of Moldova Patents | Republic of Moldova Applications | Romania Patents | Romania Applications | San Marino Patents | San Marino Applications | Serbia Patents | Serbia Applications | Slovakia Patents | Slovakia Applications | Slovenia Patents | Spain Patents | Spain Applications | Sweden Patents | Sweden Applications | Switzerland Patents | Switzerland Applications | Ukraine Patents | Yugoslavia/Serbia and Montenegro Patents | Yugoslavia/Serbia and Montenegro Applications | Armenia Patents | Australia Patents | Australia Applications | Cyprus Patents | Gulf Cooperation Council Patents | Hong Kong Patents | India Patents | India Applications | Indonesia Patents | Indonesia Applications | Israel Applications | Jordan Patents | Kyrgyzstan Patents | Macao Applications | Malaysia Patents | Mongolia Patents | New Zealand Patents | Philippines Patents | Philippines Applications | Saudi Arabia Patents | Singapore Patents | Singapore Applications | Taiwan Patents | Taiwan Applications | Tajikistan Patents | Tajikistan Applications | Thailand Applications | Uzbekistan Patents | Vietnam Patents | Algeria Patents | ARIPO Patents | ARIPO Applications | Egypt Patents | Kenya Patents | Malawi Patents | Morocco Patents | Morocco Applications | OAPI Patents | South Africa Patents | Tunisia Applications | Zambia Patents | Zimbabwe Patents | EAPO Patents | EAPO Applications | Georgia Patents | Georgia Applications | Kazakhstan Patents | Kazakhstan Applications | Russia Patents | Russia Applications | Turkey Patents | Turkey Applications | IEEE Xplore Publications: IEEE Periodicals | IEEE Xplore Publications: IEEE Conferences | IEEE Xplore Publications: IEEE Standards | IEEE Xplore Publications: IEEE Early Access | IEEE Xplore Publications: SMPTE Periodicals | IEEE Xplore Publications: SMPTE Conferences | IEEE Xplore Publications: SMPTE Standards | IEEE Xplore Publications: MIT Press eBooks | IEEE Xplore Publications: Wiley-IEEE eBooks | IEEE Xplore Publications: IBM Periodicals | IEEE Xplore Publications: URSI Periodicals | IEEE Xplore Publications: VDE Conferences | IEEE Xplore Publications: Periodicals from China | IP.com Prior Art Database: The IP.com Journal | IP.com Prior Art Database: Internet Society RFC | IP.com Prior Art Database: IBM TDB Archive | IP.com Prior Art Database: Legacy Journals | IP.com Prior Art Database: Software Patent Institute | OnePetro.org: Periodicals at OnePetro.org | OnePetro.org: Conferences at OnePetro.org | OnePetro.org: Standards at OnePetro.org | Other Literature: IBM Redbooks | Other Literature: PubMed Central | Other Literature: arXiv.org

1 **2021-03-24 13:15 UTC | 167 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Text
tabish decision tree

Sophos Ex. 1002
Page 91 of 347

Concept Modifiers: None

Filters: None

2 **2021-03-24 13:16 UTC | 47 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Same as Query 1

Concept Modifiers: None

Filters (1):
Title+Abstract+Body/Description+Related Terms limited to: malware

3 **2021-03-24 13:20 UTC | 19,682 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Text
malware decision tree

Concept Modifiers: None

Filters: Same as Query 2

4 **2021-03-24 13:20 UTC | 0 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Same as Query 3

Concept Modifiers: None

Filters (1):
Authors/Inventors limited to: tabish

5 **2021-03-24 14:03 UTC | 3,216,292 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Text
detection of malicious code machine learning classifiers

Concept Modifiers: None

Filters: None

6 **2021-03-24 14:03 UTC | 37 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Same as Query 5

Concept Modifiers: None

Filters (1):
Authors/Inventors limited to: moskovitch

7 **2021-03-24 15:35 UTC | 951,394 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Text
"feature vector" classifier

Concept Modifiers: None

Filters: None

8 **2021-03-24 15:35 UTC | 231,944 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Same as Query 7

Concept Modifiers: None

Filters (1):
Title+Abstract+Body/Description+Related Terms limited to: SVM

9 **2021-03-24 15:37 UTC | ~231,166 results from**

De-Dup: Simple Family Numbers (PAT only) | **Cut-off:** None | **Sort:** Relevance

Main Concept: Same as Query 7

Concept Modifiers: None

Filters: Same as Query 8

10 **2021-03-25 08:32 UTC | 3,217,372 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Text
machine learning data points

Concept Modifiers: None

Filters: None

11 **2021-03-25 08:33 UTC | 3,217,372 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Same as Query 10

Concept Modifiers: None

Filters: None

12 **2021-03-25 08:33 UTC | 29,530 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Same as Query 10

Concept Modifiers: None

Filters: Same as Query 2

13 **2021-03-25 08:35 UTC | 808 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Same as Query 10

Concept Modifiers: None

Filters (2):
Title+Abstract+Body/Description+Related Terms limited to: malware
Title+Abstract+Body/Description+Related Terms limited to: "portable executable"

Summaries with Thumbnails

Report Run Date: 2021-03-25
Results included: 6
Results Priority Date Range: 2009-01-23 to 2016-07-05
Results Publication Date Range: 2010-07-29 to 2019-04-01

Publication contains information from a representative family member.

Sophos Ex. 1002
Page 95 of 347

Selected Documents

Publication #	Title
9020524	Malware Classification of Portable Executables using Tree-Based Ensemble Machine Learning
8718647	Machine Learning-Based Analysis of Program Binaries: A Comprehensive Study
US20180013772	Automatic Inline Detection based on Static Data
WO2018009537A1	Automatic inline detection based on static data
8359287	Machine Learning and Deep Learning Methods for Cybersecurity
US20100192222	Malware detection using multiple classifiers

9020524 | **Publication Date: 2019-04-01** |

Malware Classification of Portable Executables using Tree-Based Ensemble Machine Learning



Abstract:
The impact of malware and its role in cyber attacks is well known in this current day and age where there is a consistent barrage of cyber attacks on a daily basis. Techniques that can identify the malware that is obfuscated, or has the capabilities to stay hidden, are needed to combat these malware based cyber attacks. In the current study, an attempt is made to study different tree-based ensemble machine learning techniques that can identify malware among windows portable executable (PE) files and the features of importance in the identification of malware. The datasets used in the present research includes both malicious (489 files) and benign (700) portable executable files. The PE file metadata extracted as raw and calculated features (54 features) from the PE file headers. Six different Tree-based ensemble Machine Learning techniques, Bagging Decision Tree Classifier (BDT), Random Forest Classifier (RFC), Extra Trees Classifier (ETC), AdaBoost Classifier (ABC), Gradient Boosting...

8718647 | **Publication Date: 2019-01-01** |

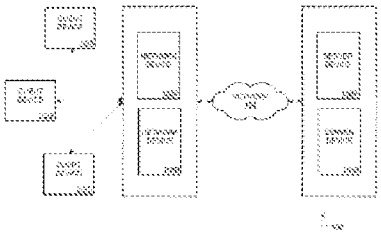
Machine Learning-Based Analysis of Program Binaries: A Comprehensive Study



Abstract:
Binary code analysis is crucial in various software engineering tasks, such as malware detection, code refactoring, and plagiarism detection. With the rapid growth of software complexity and the increasing number of heterogeneous computing platforms, binary analysis is particularly critical and more important than ever. Traditionally adopted techniques for binary code analysis are facing multiple challenges, such as the need for cross-platform analysis, high scalability and speed, and improved fidelity, to name a few. To meet these challenges, machine learning-based binary code analysis frameworks attract substantial attention due to their automated feature extraction and drastically reduced efforts needed on large-scale programs. In this paper, we provide the taxonomy of machine learning-based binary code analysis, describe the recent advances and key findings on the topic, and discuss the key challenges and opportunities. Finally, we present our thoughts for future directions on this...

US20180013772 | **Publication Date: 2018-01-11** | **Priority Date: 2016-07-05**

Automatic Inline Detection based on Static Data



Abstract:
Examples of the present disclosure describe systems and methods of automatic inline detection based on static data. In aspects, a file being received by a recipient device may be analyzed using an inline parser. The inline parser may identify sections of the file and feature vectors may be created for the identified sections. The feature vectors may be used to calculate a score corresponding to the malicious status of the file as the information is being analyzed. If a score is determined to exceed a predetermined threshold, the file download process may be terminated. In aspects, the received files, file fragments, feature vectors and/or additional data may be collected and analyzed to build a probabilistic model used to identify potentially malicious files.

Current Assignees: WEBROOT INC

WO2018009537A1 | **Publication Date: 2018-01-11** | **Priority Date: 2016-07-05**

Automatic inline detection based on static data

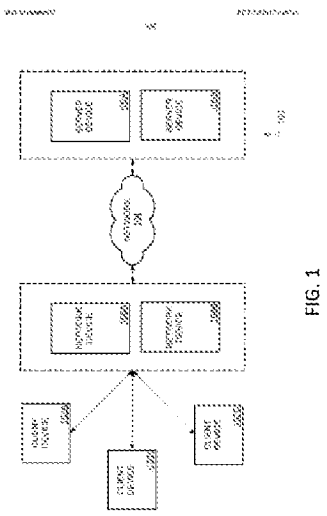


FIG. 1

Abstract:
Examples of the present disclosure describe systems and methods of automatic inline detection based on static data. In aspects, a file being received by a recipient device may be analyzed using an inline parser. The inline parser may identify sections of the file and feature vectors may be created for the identified sections. The feature vectors may be used to calculate a score corresponding to the malicious status of the file as the information is being analyzed. If a score is determined to exceed a predetermined threshold, the file download process may be terminated. In aspects, the received files, file fragments, feature vectors and/or additional data may be collected and analyzed to build a probabilistic model used to identify potentially malicious files.

Current Assignees: WEBROOT INC

8359287 | **Publication Date: 2018-01-01** |

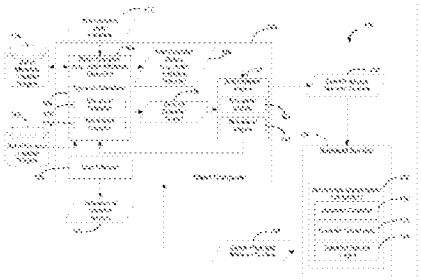
Machine Learning and Deep Learning Methods for Cybersecurity

Image not currently available

Abstract:
With the development of the Internet, cyber-attacks are changing rapidly and the cyber security situation is not optimistic. This survey report describes key literature surveys on machine learning (ML) and deep learning (DL) methods for network analysis of intrusion detection and provides a brief tutorial description of each ML/DL method. Papers representing each method were indexed, read, and summarized based on their temporal or thermal correlations. Because data are so important in ML/DL methods, we describe some of the commonly used network datasets used in ML/DL, discuss the challenges of using ML/DL for cybersecurity and provide suggestions for research directions.

US20100192222 | **Publication Date: 2010-07-29** | **Priority Date: 2009-01-23**

Malware detection using multiple classifiers



Abstract:
A method of identifying a malware file using multiple classifiers is disclosed. The method includes receiving a file at a client computer. The file includes static metadata. A set of metadata classifier weights are applied to the static metadata to generate a first classifier output. A dynamic classifier is initiated to evaluate the file and to generate a second classifier output. The method includes automatically identifying the file as potential malware based on at least the first classifier output and the second classifier output.

Current Assignees: MICROSOFT TECH LICENSING LLC

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	41,718	(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$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/09 05:45
S13	364	(G06F21/562 OR G06F21/565 OR G06F2221/033 OR G06F8/53).CPC. AND (G06N20/00).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/09 05:45
S14	215	(G06F21/562 OR G06F21/563 OR G06F21/564 OR G06F21/565).CPC. AND (G06N20/00).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/09 05:47
S15	84	S14 and @ad<"20150512"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/09 05:47
S16	4	(US-20090300765-$ 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	41,718	(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	6,736	(feature adj vector) and svm	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 10:09
S30	5,881	(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	1,853	(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; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 15:33
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
S55	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 16:12

S56	18	("20100192222" | "9465940" | "9197663" | "20120079596" | "8719924" | "20140165203" | "20070240220").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 16:12
S57	13	S55 not S56	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/11 16:12
S58	9	(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	2019/10/09 10:53
S59	14	(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	2019/10/09 10:53
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$4 near3 file)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/11/04 10:49
S64	16	(US-20090300765-$ 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	2019/11/04 10:50
S65	27	("20090274376" | "20090300765" | "20120227105" | "8510836" | "20100192222" | "20090013405" | "20100082642" | "9465940" | "20130291111" | "9197663" | "20140310517" | "20170262633" | "20120079596" | "8719924" | "20160156646" | "20180365573" | "20140165203" | "20070240220" | "20160021174").PN.	US-PGPUB; USPAT; FPRS	OR	ON	2019/11/04 11:00
S69	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	2019/11/04 11:02
S70	27	("20090274376" | "20090300765" | "20120227105" | "8510836" | "20100192222" | "20090013405" | "20100082642" | "9465940" | "20130291111" | "9197663" | "20140310517" | "20170262633" | "20120079596" | "8719924" | "20160156646" | "20180365573" | "20140165203" | "20070240220" | "20160021174").PN.	US-PGPUB; USPAT; FPRS	OR	ON	2019/11/04 11:02
S71	28	S69 S70	US-PGPUB; USPAT;	OR	ON	2019/11/04 11:02

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S72	132	(@ad<"20150512" @prad<"20150512") and (classif$8) near3 (benign malign$3 malicious harmless harmful malware) and (model) near4 (benign malign$3 malicious harmless harmful malware) and (bayesian (support adj2 vector))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/02/25 06:20
S73	129	(@ad<"20150512" @prad<"20150512") and (classif$8) near3 (benign malign$3 malicious harmless harmful malware) and (model) near4 (benign malign$3 malicious harmless harmful malware) and (bayesian (support adj2 vector)) and (features! (feature adj vectors!))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/02/25 06:20
S74	87,813	(support adj vector)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/23 14:31
S79	21,615	(file executable) near3 (harmful malicious virus malware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/23 14:57
S80	613	S74 and S79	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/23 14:57
S81	739	(file executable) near3 (harmful malicious virus malware) and (file executable) near3 (harmless benign)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/23 14:58
S82	157	S74 and S81	US-PGPUB; USPAT; USOCR;	OR	ON	2021/03/23 14:58

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S83	87,813	(support adj vector)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 06:42
S84	739	(file executable) near3 (harmful malicious virus malware) and (file executable) near3 (harmless benign)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 06:42
S85	157	S83 and S84	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 06:42
S86	157	S85	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 06:42
S88	118	S86 and (points! features! attributes! characteristics!) near4 (determin$6 identif$8 select$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 06:43
S89	0	tabish.in. and j48	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 09:14
S90	0	tabish.in. and decision adj tree	US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	ON	2021/03/24 09:14

			JPO; DERWENT; IBM_TDB			
S91	0	(shabtai and moskovitch).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 09:48
S92	0	(glezer and moskovitch).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 09:49
S93	24	(elovici and moskovitch).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 09:49
S94	10	(elovici and moskovitch).in. and (training) and (testing)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 09:49
S95	2	(elovici and moskovitch).in. and (training) and (testing) and (support adj vector)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 09:51
S96	62,631	train$4 same feature near2 (select$4 extract$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 10:23
S98	161	train$4 with classifier with (malicious benign) same feature near2 (select$4 extract$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2021/03/24 10:24

			DERWENT; IBM_TDB			
S99	260	train$4 with classifier with (malicious benign) and feature near2 (select$4 extract$4) with classifier	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 10:43
S100	80	train$4 with classifier with (malicious benign) with (feature vector) and (feature vector) near2 (select$4 extract$4) with classifier and (feature vector) same (svm (support adj vector))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 10:44
S101	18	train$4 with classifier with (malicious benign) with (feature vector) and (feature vector) near2 (select$4 extract$4) with classifier and (feature vector) same (svm (support adj vector)) and (feature vector) with (narrow$4 reduc$4 limit$4) with (classifier)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 10:46
S102	33	train$4 with classifier with (malicious benign) with (feature vector) and (feature vector) near2 (select$4 extract$4) with classifier and (feature vector) same (svm (support adj vector)) and (feature vector) with (narrow$4 reduc$4 limit$4) same (classifier)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 10:46
S103	174	train$4 with classifier with (malicious benign) and (feature vector) near2 (select$4 extract$4) with classifier and (feature with vector)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 11:34
S104	234	virus near4 scan$4 with trigger$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 12:44
S105	9	virus near4 scan$4 with trigger$4 with download$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2021/03/24 12:44

			DERWENT; IBM_TDB			
S106	77	virus near4 scan$4 with download$4 with execut$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 12:45
S107	69	(@ad<"20150512" @prad<"20150512") and virus near4 scan$4 with download$4 with execut$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 12:46
S108	215	(@ad<"20150512" @prad<"20150512") and ((virus near4 scan$4) (antivirus) (anti adj virus) (malware near2 scan$4)) and detect$4 near4 download$4 and detect$4 near4 execut$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 12:57
S109	33	(@ad<"20150512" @prad<"20150512") and ((virus near4 scan$4) (antivirus) (anti adj virus) (malware near2 scan$4)) and trigger$4 near4 download$4 and trigger$4 near4 execut$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 13:01
S110	122	(@ad<"20150512" @prad<"20150512") and ((virus near4 scan$4) (antivirus) (anti adj virus) (malware near2 scan$4)) and response near4 download$4 and response near4 execut$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 13:02
S111	48	S110 AND ((G06F21/53 OR G06F21/566 OR G06F21/51 OR G06F21/56 OR H04L63/145).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 13:06
S112	28	(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;	OR	ON	2021/03/24 13:21

			DERWENT; IBM_TDB			
S113	35	(machine adj learning) and (feature adj vector) and (exclu$4 ignor$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	2021/03/24 13:26
S114	7	(@ad<"20150512" @prad<"20150512") and (machine adj learning) and (feature adj vector) and (exclu$4 ignor$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	2021/03/24 13:30
S115	61	(@ad<"20150512" @prad<"20150512") and ((support adj vector) (machine adj learning)) and (exclu$4 ignor$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	2021/03/24 13:32
S116	143	(@ad<"20150512" @prad<"20150512") and ((support adj vector) (machine adj learning)) and (exclu$4 ignor$4 filter$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	2021/03/24 13:32
S117	0	(antivirus malware) and (@ad<"20150512" @prad<"20150512") and ((support adj vector) (machine adj learning)) and (exclu$4 ignor$4 filter$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	2021/03/24 14:04
S118	7	(antivirus malware) and (@ad<"20150512" @prad<"20150512") and ((support adj vector) (machine adj learning)) and (exclu$4 ignor$4 filter$4 (turn$4 adj off)) near2 (feature outlier data point) with (range threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 14:06
S119	112	((("Schmidtler") near3 ("Mauritius"))).INV. ((("Dalal") near3 ("Gaurav"))).INV. ((("Yoosoofmiya") near3 ("Reza"))).INV.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2021/03/24 14:29

			DERWENT; IBM_TDB			
S120	9	S119 and benign	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 14:30
S121	7	S119 and benign and feature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 14:30
S122	1	(14/709875).APP.	USPAT; USOCR	OR	ON	2021/03/24 14:30
S123	8	("20070240220" | "20100192222" | "20120079596" | "20140165203" | "20160335435" | "8719924" | "9197663" | "9465940").PN.	US-PGPUB; USPAT	OR	ON	2021/03/24 14:57
S124	23	(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-$ or US-20060026675-$ or US-20060037080-$ or US-20100293273-$ or US-20110154490-$ or US-20110172504-$).did. or (US-9465940-$ or US-8510836-$ or US-9197663-$ or US-8161548-$ or US-10116688-$).did. or (EP-2182458-$).did.	US-PGPUB; USPAT; FPRS	OR	ON	2021/03/24 14:57
S125	20	S124 not S123	US-PGPUB; USPAT; FPRS	OR	ON	2021/03/24 14:57
S126	2	14/709875.app.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 14:58

S127	98,499	(G06F21/562 OR G06F21/565 OR G06F2221/033 OR G06F8/53 OR G06N20/00 OR G06N20/10).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 14:59
S128	143,892	(G06F21/51,53,562,56,565,566 OR G06F2221/033 OR G06F8/53 OR G06N20/00 OR G06N20/10 OR H04L63/145).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/03/24 15:00

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S52	21,382	(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
S66	24,529	(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

3/24/2021 3:08:59 PM
C:\Users\msimitoski\Documents\EAST\Workspaces\16\16_791649_threat_detection_static_analysis_without_decrypting_unpacking.wsp

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	Not Yet Assigned
				Filing or 371 (c) Date:	Herewith
				First Named Inventor	Mauritius Schmidtler
				Group Art Unit	Not Yet Assigned
				Examiner Name	Not Yet Assigned
Sheet	1	of	1	Attorney Docket Number	OPEN7950-1

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A1	20160335435	11-17-2016	Schmidtler et al.	
	A2	9465940	10-11-2016	Wijnowicz et al.	
	A3	20070240220	10-11-2007	Tuvell et al.	
	A4	20120079596	03-29-2012	Thomas et al.	
	A5	9197663	11-24-2015	Gilbert et al.	
	A6	8719924	05-06-2014	Williamson et sl.	
	A7	20140165203	06-12-2014	Friedrichs et al.	
	A8	20100192222	07-29-2010	Stokes et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature		Date Considered	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MS/

INFORMATION DISCLOSURE STATEMENT				Application Number	Not Yet Assigned
				Filing or 371 (c) Date:	Herewith
				First Named Inventor	Mauritius Schmidtler
				Group Art Unit	Not Yet Assigned
				Examiner Name	Not Yet Assigned
Sheet	1	of	2	Atty Docket Number	OPEN7950-1

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, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C1	Office Action issued for U.S. Patent Application No. 14/709,875 (OPEN7950), mailed December 8, 2016, 19 pages.	
	C2	SHABTAI ET AL., "Detection of Malicious Code by Applying Machine Learning Classifiers on Static Features: A State-of-the-Art Survery," Information Security Technical Report, Elsevier Advanced Technology, Amsterdam NL, vol. 14, No. 1, February 1, 2009, pp. 16-29, XP026144093, ISSN: 1363-4127.	
	C3	Office Action issued for U.S. Patent Application No. 14/709,875 (OPEN7950), mailed March 24, 2017, 21 pages.	
	C4	Office Action issued for U.S. Patent Application No. 14/709,875 (OPEN7950), mailed April 20, 2018, 22 pages.	
	C5	Office Action issued for U.S. Patent Application No. 14/709,875 (OPEN7950), mailed January 24, 2019, 21 pages.	
	C6	Office Action issued for U.S. Patent Application No. 14/709,875 (OPEN7950), mailed July 17, 2019, 12 pages.	
	C7	BOST, et al., "Machine learning classification over encrypted data." N DSS. Vol. 4324. 2015. (Year: 2015), 14 pages.	
	C8	CHOI, et al., "Efficient Malicious Code Detection Using N-Gram Analysis and SVM," 2011 14th International Conference on Network-Based Information Systems. IEEE, 2011, 4 pages.	
	C9	DEVI, Dhruwajita et al., "Detection of Packed Malware," Proceedings of the First International Conference on Security of Internet ofThings, ACM, 2012, 5 pages.	
	C10	DUBE, et al., "Malware Target Recognition Via Static Heuristics," Computers & Security 31.1, 2012, 11 pages.	
	C11	MERKEL, et al., Statistical Detection of Malicious Pe-Executables for Fast Offline Analysis," IFIP International Conference on Communications and Multimedia Security, Springer, Berlin, 2010, 12 pages.	

Examiner Signature		Date Considered	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MS/

INFORMATION DISCLOSURE STATEMENT				Application Number	Not Yet Assigned
				Filing or 371 (c) Date:	Herewith
				First Named Inventor	Mauritius Schmidtler
				Group Art Unit	Not Yet Assigned
				Examiner Name	Not Yet Assigned
Sheet	2	of	2	Atty Docket Number	OPEN7950-1

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, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C12	SINGLA, et al., "A Novel Approach to Malware Detection Using Static Classification," International Journal of Computer Science and Information Security 13.3, 2015, 5 pages.	
	C13	TABISH, et al., "Malware Detection Using Statistical Analysis of Byte-Level File Content," Proceedings of the ACM SIGKDD Workshop on CyberSecurity and Intelligence Informatics, ACM, 2009, 9 pages.	
	C14	TREADWELL, et al., "A Heuristic Approach for Detection of Obfuscated Malware, 2009 IEEE International Conference on Intelligence and Security Informatics, 2009, 9 pages.	
	C15	Notice of Allowance issued for U.S. Patent Application No. 14/709,875 (OPEN7950), mailed November 14, 2019, 11 pages.	
	C16	Corrected Notice of Allowance issued for U.S. Patent Application No. 14/709,875 (OPEN7950), mailed December 23, 2019, 8 pages.	
	C17	Corrected Notice of Allowance issued for U.S. Patent Application No. 14/709,875 (OPEN7950), mailed January 24, 2020, 8 pages.	
	C18	International Patent Application No. PCT/US2016/032090, International Search Report and Written Opinion mailed July 29,2016, 13 pages.	
	C19	PERDISCI et al., "Classification of Packed Executables for Accurate Computer Virus Detection," Pattern Recognition Letters 29, 2008, 6 pages.	
	C20	PERDISCI et al., "McBoost: Boosting Scalability in Malware Collection and Analysis Using Statistical Classification of Executables," Annual Computer Security Applications, 2008, 10 pages.	
	C21	KHAN, et al., "Determining Malicious Executable Distinguishing Attributes and Low-Complexity Detection", J. ComputVirol, 7.2 (2011), 11 pgs.	
	C22	KOLTER, et al., "Learning to Detect and Classift Malicious Executables in the Wild", Journal of Machine Learning Research 7 (2006), 24 pages.	

Examiner Signature	/Michael Simitoski/	Date Considered	03/24/2021

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MS/

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.
16/791,649	02/14/2020	Mauritius Schmidtler	OPEN7950-1	2519

109422 7590 06/11/2021

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

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2493	

MAIL DATE	DELIVERY MODE
06/11/2021	PAPER

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

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

Applicant-Initiated Interview Summary	Application No. 16/791,649	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)	Title	Type
MICHAEL J SIMITOSKI	Primary Examiner	Telephonic
Mark Berrier, 35,066	Attorney of Record	

Date of Interview: 08 June 2021

Issues Discussed:

35 U.S.C. 112

Applicant contacted the Examiner to discuss the attached agenda. Regarding the §112 rejection, Applicant pointed to ¶¶34-35 of the specification. The Examiner noted that, given the ordinary meaning of "classifier", the specification did not appear to teach the classifier outputting a feature vector. However , Applicant and the Examiner agreed that the combined creation of the feature vector and the classification of data points could be pointed to by the same element that Applicant has named "classifier ".

35 U.S.C. 103

Applicant incorporated some limitations of allowable claim 10 into claim 2. The Examiner suggested that Applicant incorporate that the selective turning on/off of features are based on the data point, to avoid a rejection using the prior art discussing simply disregarding/ignoring features of a data set as a means to avoid skewing classification (for example Wegerich).

Non-statutory Double Patenting

The Examiner noted that a double patenting rejection remained applicable to the proposed amended claim.

☑ Attachment

/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.

Applicant-Initiated Interview Summary	**Application No.** 16/791,649	**Applicant(s)** Schmidtler et al.		
	Examiner MICHAEL J SIMITOSKI	**Art Unit** 2493	**AIA (First Inventor to File) Status** Yes	**Page** **2 of 2**

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
PROPOSED AGENDA	Atty. Docket No. **OPEN7950-1**

First Named Inventor **Mauritius Schmidtler**	
Application Number **16/791,649**	Date Filed **February 14, 2020**
Title **AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS**	
Group Art Unit **2493**	Examiner **Michael J. Simitoski**
Confirmation Number: **2519**	

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

Dear Sir:

The Applicant wishes to discuss the claim rejections and the cited prior art. More specifically, the Applicant wishes to discuss the following items:

- support in the written description for the limitation "generating, by a classifier, a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files", which is believed to be disclosed at paragraphs 34-35 (and claims 1-3 of the parent application, which is incorporated by reference);
- distinctions between the cited prior art (Shabtai) and a proposed amendment to a representative claim, which includes a limitation that features of the feature vector are selectively turned on or off.

To facilitate this discussion, the Applicant is including with this proposed agenda a proposed amendment to representative independent claim 2. Support for the proposed amendment can be found in claim 10 of the application as filed. The Applicant would also welcome any suggestions or guidance from the Examiner as to clarifications to the claim language which would advance prosecution of the application.

Respectfully submitted,

Sprinkle IP Law Group
Attorneys for Applicants

/Mark L. Berrier/

Mark L. Berrier
Reg. No. 35,066

Date: June 1, 2021

1301 W. 25th Street, Suite 408
Austin, TX 78705
Tel. (512) 637-9220
Fax. (512) 371-9088

PROPOSED AMENDMENT (NOT FOR ENTRY)

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

identifying, by a knowledge module, static data points that may be indicative of either a harmful or benign executable file;

associating, by the knowledge module, the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting, by the knowledge module, a plurality of static data points from the identified executable file;

generating, by a classifier, a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein features of the feature vector are selectively turned on or off; and

providing the generated feature vector to one or more support vector machines to build a probabilistic model that indicates whether the executable file fits into one of the categories of files.

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 16/791,649	Filing Date 02/14/2020	☐ 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 $100 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $460 =	
☐ 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	06/17/2021	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 $480 =	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".	/JACQUELYN L WILLIAMS/
*** 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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
REPLY TO OFFICE ACTION DATED 03/29/2021	Atty. Docket No. **OPEN7950-1**

First Named Inventor **Mauritius Schmidtler**	
Application Number **16/791,649**	Date Filed **February 14, 2020**
Title **AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS**	
Group Art Unit **2493**	Examiner **Michael J. Simitoski**
Confirmation Number: **2519**	

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 **June 17, 2021.**

/Delia Narvaiz/
Delia Narvaiz

This paper is submitted in response to the Official Action mailed on March 29, 2021, the Examiner Interview held on June 8, 2021, and the Interview Summary mailed on June 11, 2021. Please reconsider the above-identified application in view of the following amendments and remarks.

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

Remarks/Arguments begin on page 6 of this paper.

AMENDMENTS TO THE CLAIMS:

Please amend the claims as set forth in the following listing. This listing of claims will replace all prior versions, and listings, of claims in the present application:

1. (Canceled)

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

identifying, by a knowledge module, static data points that may be indicative of either a harmful or benign executable file;

associating, by the knowledge module, the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting, by the knowledge module, a plurality of static data points from the identified executable file;

generating, by a classifier, a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off based on information associated with one or more of the plurality of extracted static data points; and

providing the generated feature vector to one or more support vector machines to build a probabilistic model that indicates whether the executable file fits into one of the categories of files.

3. (Previously Presented) The computer-implemented method according to claim 2, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

4. (Previously Presented) The computer-implemented method according to claim 2, wherein the one or more support vector machines builds the probabilistic model by performing data analysis and pattern recognition on the one or more feature vectors.

5. (Previously Presented) The computer-implemented method according to claim 2, wherein the probabilistic model indicates whether the executable file is harmful.

6. (Previously Presented) The computer-implemented method according to claim 2, wherein the executable file is identified in response to a detected condition.

7. (Previously Presented) The computer-implemented method according to claim 6, wherein the condition is user request for a file download.

8. (Previously Presented) The computer-implemented method according to claim 6, wherein the condition is the detection of a new file attempting to execute.

9. (Previously Presented) The computer-implemented method according to claim 2, wherein the plurality of static data points represent predefined character strings in the executable file.

10. (Currently Amended) The computer-implemented method according to claim 2, wherein the one or more features of the feature vector are selectively turned on or off based at least in part on evaluation of whether a value of one of ~~a static data point from~~ the plurality of extracted static data points is within a predetermined range.

11. (Previously Presented) The computer-implemented method according to claim 2, wherein a determination of whether the executable file is harmful is used to retrain the classifier.

12. (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:

identifying static data points that may be indicative of either a harmful or benign executable file;

associating the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting a plurality of static data points from the identified executable file;

generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector

are selectively turned on or off based on information associated with one or more of the plurality of extracted static data points; and

providing the generated feature vector to one or more support vector machines to build a probabilistic model that indicates whether the executable file fits into one of the categories of files.

13. (Previously Presented) The system according to claim 12, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

14. (Previously Presented) The system according to claim 12, wherein the one or more support vector machines builds the probabilistic model by performing data analysis and pattern recognition on the one or more feature vectors.

15. (Previously Presented) The system according to claim 12, wherein the probabilistic model indicates whether the executable file is harmful.

16. (Previously Presented) The system according to claim 12, wherein the plurality of static data points represent predefined character strings in the executable file.

17. (Currently Amended) The system according to claim 12, wherein the one or more features of the feature vector are selectively turned on or off based at least in part on evaluation of whether a value of one of ~~a static data point from~~ the plurality of extracted static data points is within a predetermined range.

18. (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:

identifying static data points that may be indicative of either a harmful or benign executable file;

associating the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting a plurality of static data points from the identified executable file;

generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off based on information associated with one or more of the plurality of extracted static data points; and

providing the generated feature vector to one or more support vector machines to build a probabilistic model that indicates whether the executable file fits into one of the categories of files.

19. (Previously Presented) The computer-readable storage device according to claim 18, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

20. (Previously Presented) The computer-readable storage device according to claim 18, wherein the plurality of static data points represent predefined character strings in the executable file.

21. (Currently Amended) The computer-readable storage device according to claim 18, wherein the one or more features of the feature vector are selectively turned on or off based at least in part on evaluation of whether a value of one of ~~a static data point from~~ the plurality of extracted static data points is within a predetermined range.

REMARKS

The Applicant appreciates the time taken by the Examiner to review the Applicant's present application. This application has been carefully reviewed in light of the Official Action mailed on March 29, 2021 ("Office Action"), the Examiner Interview held on June 8, 2021, and the Examiner's Interview Summary mailed on June 11, 2021. The Applicant does not acquiesce to the Examiner's rejections, claim interpretations or other statements in the Office Action. However, in order to expedite prosecution, the Applicant has amended claims 2, 10, 12, 17, 18 and 21. No new matter has been added. Claims 2-21 therefore remain pending in the application. The Applicant respectfully requests reconsideration and favorable action in this case.

Interview Summary

A telephonic interview was conducted on June 8, 2021 between Examiner Simitoski and Attorney Berrier. The Applicant appreciates the time and effort taken by Examiner Simitoski to review the Applicant's present application and discuss the pending claims and the cited prior art.

During the interview, the rejections under 35 U.S.C. §§ 112 and 103 were discussed. The Attorney pointed out disclosure in the specification of support for the limitation mentioned in the §112 rejection, and the Examiner suggested a clarification regarding selectively turning features on and off relating to a data point. No specific agreement was reached as to allowability.

Rejections under 35 U.S.C. § 112

Claims 2-21 stand rejected under 35 U.S.C. § 112, first paragraph. The Office Action alleges that the claims fail to comply with the written description requirement and the enablement requirement. In particular, the Office Action alleges that "the specification does not teach using a classifier to generate the feature vector, but rather to use pre-processing to generate the feature vector for use by the classifier."

The Applicant points out that, as discussed in the June 8 interview, the limitation "generating, by a classifier, a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files" is disclosed at paragraphs 34-35 of the specification (as well as claims 1-3 of the parent application, which is incorporated by reference into the present application). Paragraphs 34-35 disclose, *inter alia*,

"Operation 306 comprises applying a learning classifier … 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 … In one example, operation 306 comprises generating at least one feature vector from the plurality of static data points … the learning classifier can uniquely generate a feature vector for analysis of the executable file".

The rejected claims therefore comply with the written description and enablement requirements, so the Applicant respectfully requests that the rejection of the claims under Because the limitation 35 U.S.C. § 112, first paragraph be withdrawn.

Rejections under 35 U.S.C. § 102

Claims 2-5, 9, 11-16 and 18-20 stand rejected as anticipated by *Detection of Malicious Code by Applying Machine Learning Classifiers on Static Features: A State-of-the-Art Survey* ("Shabtai").

The Applicant points out that independent claims 2, 12 and 18 have been amended to include limitations which were previously included in dependent claims 10, 17 and 21, which were acknowledged in the Office Action to be directed to allowable subject matter. The limitations added to the independent claims specify that one or more features of the feature vector are selectively turned on or off based on information associated with one or more of the plurality of extracted static data points. As discussed with the examiner during the June 8 interview, these newly added limitations of the independent claims are believed to patentably distinguish the claims from the cited prior art. Because the dependent claims depend from and incorporate the limitations of the independent claims, they are likewise believed to be patentably distinguished from the cited prior art. Accordingly, the Applicant respectfully requests withdrawal of the rejections under 35 U.S.C. § 102.

Rejections under 35 U.S.C. § 103

Claims 6-8 stand rejected as obvious over Shabtai in view of U.S. Publication No. 2010/0293273 ("Basarrate").

As noted above, claim 2 has been amended to include limitations which were previously included in dependent claim 10, which the Office Action pointed out is directed to allowable subject matter. Because claim 2 is believed to be allowable, claims 6-8, which depend from and

incorporate the limitations of the claim 2, are patentably distinguished from the cited prior art in the same manner as claim 2. Accordingly, the Applicant respectfully requests withdrawal of the rejection of claims 6-8 under 35 U.S.C. § 103.

Double Patenting Rejection

Claims 2-5 and 19-21 stand rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over the claims of U.S. Patent No. 10,599,844, in view of Shabtai.

Claims 6-8 stand rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over the claims of U.S. Patent No. 10,599,844, in view of Shabtai and Basarrate.

The Office Action includes a table indicating portions of the claims that are not disclosed by U.S. Patent No. 10,599,844 (the '844 Patent), but are alleged to be disclosed by either Shabtai or Basarrate. The Applicant notes that while the table indicates portions of the Shabtai and Basarrate references that are alleged to disclose the missing features, neither the table nor the text of the double patenting rejection explains the motivation for a person of ordinary skill in the art to modify the claims of the '844 Patent with the teachings of Shabtai and/or Basarrate. Consequently, the double patenting rejection does not establish the obviousness of the instant claims with respect to the '844 Patent. Accordingly, the Applicant respectfully requests that the rejection be withdrawn.

Allowable Subject Matter

Applicant appreciates the Examiner's acknowledgement that claims 10, 17 and 21 include allowable subject matter. As pointed out above, independent claims 2, 12 and 18 have been amended to include limitations of claims 10, 17 and 21, respectively, and are therefore believed to be in condition for allowance.

Conclusion

The Applicant has now made an earnest attempt to place this case in condition for allowance. Other than as explicitly set forth above, this reply does not include an acquiescence to statements, assertions, assumptions, conclusions, or any combination thereof in the Office Action. For the foregoing reasons and for other reasons clearly apparent, Applicant respectfully requests full allowance of all pending claims. The Examiner is invited to telephone the undersigned at the number listed below for prompt action in the event any issues remain.

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
Attorneys for Applicant

/Mark L. Berrier/

Mark L. Berrier
Reg. No. 35,066

Date: June 17, 2021

1301 W. 25th Street, Suite 408
Austin, TX 78705
Tel. (512) 637-9220
Fax. (512) 371-9088

Electronic Acknowledgement Receipt

EFS ID:	43022368
Application Number:	16791649
International Application Number:	
Confirmation Number:	2519
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:	Mark Louis Berrier/Delia Narvaiz
Filer Authorized By:	Mark Louis Berrier
Attorney Docket Number:	OPEN7950-1
Receipt Date:	17-JUN-2021
Filing Date:	14-FEB-2020
Time Stamp:	18:45:51
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		OPEN7950-1_ROA_061721.pdf	130117 ca5de934090c7b6c659e5fb188ee15c687d979d6	yes	9

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	5
	Applicant Arguments/Remarks Made in an Amendment	6	9
Warnings:			
Information:			
	Total Files Size (in bytes):	130117	

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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	16/791,649
				Filing or 371 (c) Date:	February 13, 2020
				First Named Inventor	Mauritius Schmidtler
				Group Art Unit	2493
				Examiner Name	Michael J. Simitoski
Sheet	1	of	1	Attorney Docket Number	OPEN7950-1

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A9	10599844	03-23-2020	Schmidtler et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature		Date Considered	

Electronic Acknowledgement Receipt

EFS ID:	43031899
Application Number:	16791649
International Application Number:	
Confirmation Number:	2519
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:	Mark Louis Berrier/Delia Narvaiz
Filer Authorized By:	Mark Louis Berrier
Attorney Docket Number:	OPEN7950-1
Receipt Date:	18-JUN-2021
Filing Date:	14-FEB-2020
Time Stamp:	18:14:28
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	OPEN7950-1_IDS_061821.pdf	98802 f8ba33540ce666c95902ff4acc9f8ebf2261d068	no	3

Warnings:

Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	OPEN7950-1_SB08A.pdf	83155 0619a75f86e3ac4c108a478daa3468e96e4e1092	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
			Total Files Size (in bytes):	181957	

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	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Atty. Docket No. **OPEN7950-1**

First Named Inventor **Mauritius Schmidtler**	
Application Number **16/791,649**	Filing or 371 (c) Date **February 13, 2020**
Title **AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS**	
Group Art Unit **2493**	Examiner **Michael J. Simitoski**
Confirmation Number **2519**	

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

Certification of Transmission Under 37 C.F.R. 1.8

I hereby certify that this correspondence is being transmitted to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 via the U.S. Patent and Trademark Office Electronic Filing System (EFS-Web) on **June 18, 2021**.

/Delia Narvaiz/
Delia Narvaiz

Dear Sir,

Applicant respectfully requests, pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, that the information listed on the attached SB08A/B form(s) be considered and cited in the examination of the above-identified application. A copy of U.S. Patent(s) and U.S. Patent Application Publication(s) listed on the attached SB08A form is not being submitted with this Information Disclosure Statement pursuant to the waiver of 37 C.F.R. § 1.98(a)(2)(i) by the U.S. Patent and Trademark Office. Where applicable, a copy of foreign patent document(s) as well as information listed on the attached SB08B form is enclosed for the convenience of the Examiner.

☐ This Information Disclosure Statement is being submitted within three months of the filing date of a national application other than a continued prosecution application under 37 C.F.R. § 1.53(d).

☐ This Information Disclosure Statement is being submitted within three months of the date of entry of the national stage as set forth in 37 C.F.R. § 1.491 in an international application;

☐ This Information Disclosure Statement is being submitted before the mailing of a First Office Action on the merits; or

☐ This Information Disclosure Statement is being submitted before the mailing of a First Office Action after the filing of a request for continued examination under 37 C.F.R. § 1.114.

☒ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(b) and before the mailing date of any of a final action under 37 C.F.R. § 1.113, a notice of allowance under 37 C.F.R. § 1.311, or an action that otherwise closes prosecution in the application, and is accompanied by one of:

☒ The statement specified in 37 C.F.R. § 1.97(e); or

☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $240 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

Pursuant to 37 C.F.R. § 1.97(e), Applicant hereby states:

☐ 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; 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 C.F.R. § 1.56(c) more than three months prior to the filing of the information disclosure statement.

Pursuant to 37 C.F.R. §§ 1.97(g) and (h), no representation is made that a search has been made or that this information is material to patentability of the present application.

Applicant does not believe any fees are due and owing at this time. If Applicant is in error, the Director is hereby authorized to deduct any and all appropriate fees from Deposit Account 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

SPRINKLE IP LAW GROUP
Attorneys for Applicant

/Mark L. Berrier/

Mark L. Berrier
Reg. No. 35,066

Dated: June 18, 2021

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. (512) 637-9220
Fax. (512) 317-9088

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

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT**
Application Number	16791649
Filing Date	14-Feb-2020
First Named Inventor	Mauritius Schmidtler
Attorney Docket Number	OPEN7950-1
Title of Invention	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS

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

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

Owner	Percent Interest
WEBROOT INC.	100%

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

10599844

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

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

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

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

Applicant claims the following fee status:

○ Small Entity

○ Micro Entity

◉ Regular Undiscounted

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

THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES

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

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

Registration Number 35066

○ A sole inventor

○ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application

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

Signature	/Mark L. Berrier/
Name	Mark L. Berrier

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

Electronic Patent Application Fee Transmittal

Application Number:	16791649
Filing Date:	14-Feb-2020
Title of Invention:	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS
First Named Inventor/Applicant Name:	Mauritius Schmidtler
Filer:	Mark Louis Berrier/Delia Narvaiz
Attorney Docket Number:	OPEN7950-1

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
STATUTORY OR TERMINAL DISCLAIMER	1814	1	170	170
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**170**

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

Application No.: 16791649

Filing Date: 14-Feb-2020

Applicant/Patent under Reexamination: Schmidtler

Electronic Terminal Disclaimer filed on August 11, 2021

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

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

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt

EFS ID:	43487268
Application Number:	16791649
International Application Number:	
Confirmation Number:	2519
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:	Mark Louis Berrier/Delia Narvaiz
Filer Authorized By:	Mark Louis Berrier
Attorney Docket Number:	OPEN7950-1
Receipt Date:	11-AUG-2021
Filing Date:	14-FEB-2020
Time Stamp:	18:01:27
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$170
RAM confirmation Number	E20218AI01242305
Deposit Account	503183
Authorized User	Delia Narvaiz

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	Terminal Disclaimer-Filed (Electronic)	eTerminal-Disclaimer.pdf	41333 07cc6fa1a846dbf1dd5a72159a85b01e54faeffd	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	38134 d7356b968316d784b70fabd38f2924bc360595d6	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	79467		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

109422 7590 08/18/2021
Sprinkle IP Law Group/OPEN
1301 W. 25th Street, Suite 408
Austin, TX 78705

EXAMINER
SIMITOSKI, MICHAEL J

ART UNIT	PAPER NUMBER
2493	

DATE MAILED: 08/18/2021

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/791,649	02/14/2020	Mauritius Schmidtler	OPEN7950-1	2519

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	$1200	$0.00	$0.00	$1200	11/18/2021

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)

109422 7590 08/18/2021
Sprinkle IP Law Group/OPEN
1301 W. 25th Street, Suite 408
Austin, TX 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.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/791,649	02/14/2020	Mauritius Schmidtler	OPEN7950-1	2519

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	$1200	$0.00	$0.00	$1200	11/18/2021

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. 1002
Page 152 of 347

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.
16/791,649	02/14/2020	Mauritius Schmidtler	OPEN7950-1	2519

109422 7590 08/18/2021

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

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2493	

DATE MAILED: 08/18/2021

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. 16/791,649	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 reply dated 6/17/2021.
   ☐ 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 2-21 . 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. 8/11/2021.
5. ☐ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/Michael Simitoski/
Primary Examiner, Art Unit 2493

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 6/17/2021 was received and considered.

3. Claims 2-21 are pending.

Response to Amendment

4. Applicant's remarks (pp. 6-7) regarding the rejections under 35 U.S.C. §112 are persuasive.

Terminal Disclaimer

5. The terminal disclaimer filed on 8/11/2021 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of **10,599,844** has been reviewed and is accepted. The terminal disclaimer has been recorded.

Allowable Subject Matter

6. Claims 2-21 are allowed.

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

a. Applicant's remarks (p. 7) regarding the rejections under 35 U.S.C. §103 are persuasive. While the prior art shows ignoring outlier features to avoid skewing results (e.g. Wegerich), the prior art fails to selectively turn on or off features of a feature vector based on information associated with one or more of extracted data points, as recited in 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

8. 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 https://ppair-my.uspto.gov/pair/PrivatePair. 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

August 11, 2021

Examiner-Initiated Interview Summary	**Application No.** 16/791,649	**Applicant(s)** Schmidtler et al.		
	Examiner MICHAEL J SIMITOSKI	**Art Unit** 2493	**AIA (First Inventor to File) Status** Yes	**Page** 1 of 1

All Participants (applicant, applicants representative, PTO personnel)	**Title**	**Type**
MICHAEL J SIMITOSKI	Primary Examiner	In-Person
Mark Berrier, 35,066	Attorney of Record	

Date of Interview: 11 August 2021

Issues Discussed:

Non-statutory Double Patenting

The Examiner contacted Applicant to discuss the outstanding double patenting rejections in view of the most recent amendments. Applicant agreed to file a terminal disclaimer to obviate the rejections and place the application in condition for allowance.

/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
	16/791,649	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
G06N	/	20	/	10		I	2019-01-01
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	11 August 2021	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

U.S. Patent and Trademark Office

Part of Paper No.: 20210811

Sophos Ex. 1002
Page 159 of 347

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/791,649	Schmidtler et al.
	Examiner	**Art Unit**
	MICHAEL J SIMITOSKI	2493

INTERNATIONAL CLASSIFICATION				
CLAIMED				
G06F	/	21	/	56
G06N	/	5	/	04

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	11 August 2021	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

U.S. Patent and Trademark Office

Part of Paper No.: 20210811

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/791,649	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	9	10	18	19										
1	2	10	11	19	20										
2	3	11	12	20	21										
3	4	12	13												
4	5	13	14												
5	6	14	15												
6	7	15	16												
7	8	16	17												
8	9	17	18												

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	20	
/Michael Simitoski/ Primary Examiner, Art Unit 2493	11 August 2021	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/791,649	Schmidtler et al.
	Examiner	Art Unit
	MICHAEL J SIMITOSKI	2493

CPC - Searched*		
Symbol	Date	Examiner
G06F 21/51,53,562,56,565,566; 2221/033; 8/53 | G06N 20/00,10 | H04L 63/145	08/11/2021	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.

Search Notes		
Search Notes	Date	Examiner
EAST, NPL and inventor search performed (see EAST and NPL search histories, attached and/or previously made of record)	08/11/2021	MJS
Consulted Common Citation Document and Global Dossier for related/family applications and prosecution histories	08/11/2021	MJS

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
G06F	21/51,53,562,56,565,566; 2221/033; 8/53	08/11/2021	MJS
G06N	20/00,10	08/11/2021	MJS
H04L	63/145	08/11/2021	MJS

/Michael Simitoski/ Primary Examiner, Art Unit 2493	

Bibliographic Data

Application No: 16/791,649

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.
02/14/2020	726	2493	
RULE			

APPLICANTS

Webroot Inc., Broomfield, CO,

INVENTORS

Mauritius Schmidtler, Escondido, CA, UNITED STATES

Gaurav Dalal, San Jose, CA, UNITED STATES

Reza Yoosoofmiya, San Diego, CA, UNITED STATES

CONTINUING DATA

This application is a CON of 14709875 05/12/2015 PAT 10599844

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

03/02/2020

STATE OR COUNTRY

UNITED STATES

ADDRESS

FILING FEE RECEIVED

$1,720

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Application Number	16/791,649
Filing or 371 (c) Date:	February 13, 2020
First Named Inventor	Mauritius Schmidtler
Group Art Unit	2493
Examiner Name	Michael J. Simitoski
Sheet 1 of 1	Attorney Docket Number: OPEN7950-1

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A9	10599844	03-23-2020	Schmidtler et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature	/Michael Simitoski/	Date Considered	08/11/2021

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MS/

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S132	7	(antivirus malware) and (@ad<"20150512" @prad<"20150512") and ((support adj vector) (machine adj learning)) and (exclu$4 ignor$4 filter$4 (turn$4 adj off)) near2 (feature outlier data point) with (range threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/08/10 11:58
S133	1	("10599844").PN.	US-PGPUB; USPAT	OR	ON	2021/08/10 11:59
S134	7	(antivirus malware) and (@ad<"20150512" @prad<"20150512") and ((support adj vector) (machine adj learning)) and (exclu$4 ignor$4 filter$4 (turn$4 adj off)) near2 (feature outlier data point) with (range threshold)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/08/11 06:04
S135	119	((("Schmidtler") near3 ("Mauritius"))).INV. ((("Dalal") near3 ("Gaurav"))).INV. ((("Yoosoofmiya") near3 ("Reza"))).INV.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/08/11 06:07
S136	14	S135 and benign	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/08/11 06:07
S137	38	(machine adj learning) and (feature adj vector) and (exclu$4 ignor$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	2021/08/11 06:34
S138	29	(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	2021/08/11 06:34
S139	163	(feature) with includ$4 with (vector) with (threshold range) near3 (point feature) and (machine adj learning)	US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	ON	2021/08/11 06:34

			JPO; DERWENT; IBM_TDB			
S140	267	((exclu$4) (turn$4 adj off)) with feature with classifier	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/08/11 06:34

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S141	49,873	(G06F21/562 OR G06F21/565 OR G06F2221/033 OR G06F8/53 OR G06N20/00).CPC.	US-PGPUB; USPAT	OR	ON	2021/08/11 06:51
S142	11	S141 and (((turn$4 adj off) disregard$4 exclu$4 ignor$4) near2 (feature)).clm. and classifier.clm.	US-PGPUB; USPAT	OR	ON	2021/08/11 06:51

8/11/2021 6:53:50 AM
C:\Users\msimitoski\Documents\EAST\Workspaces\16\16_791649_threat_detection_static_analysis_without_decrypting_unpacking.wsp

Search History

Report Run Date: 2021-08-11 UTC
Queries: 4
Markers: 0

Sophos Ex. 1002
Page 167 of 347

Query #	Timestamp	Results	Page
1	2021-08-11 10:43 UTC	3,973,142	3
2	2021-08-11 10:43 UTC	16,412,199	4
3	2021-08-11 10:43 UTC	~16,411,075	4
4	2021-08-11 10:44 UTC	~320,629	4

Content: Patents + NPL (187)

US Patents | US Designs | US Applications | EPO Patents | EPO Applications | China Patents | China Applications | Japan Patents | Japan Applications | Korea Patents | Korea Applications | WIPO Applications | Argentina Patents | Argentina Applications | Brazil Patents | Brazil Applications | Canada Patents | Canada Applications | Chile Patents | Chile Applications | Colombia Applications | Costa Rica Applications | Cuba Patents | Cuba Applications | Dominican Republic Applications | Ecuador Patents | Ecuador Applications | El Salvador Applications | Guatemala Applications | Honduras Applications | Mexico Patents | Mexico Applications | Nicaragua Patents | Panama Applications | Peru Applications | Trinidad & Tobago Patents | Uruguay Applications | Austria Patents | Austria Applications | Belarus Patents | Belgium Patents | Belgium Applications | Bosnia & Herzegovina Patents | Bosnia & Herzegovina Applications | Bulgaria Patents | Bulgaria Applications | Croatia Patents | Croatia Applications | Czech Republic Patents | Czech Republic Applications | Czechoslovakia Patents | Czechoslovakia Applications | Denmark Patents | Denmark Applications | Estonia Patents | Estonia Applications | EUIPO Patents | Finland Patents | Finland Applications | France Patents | France Applications | Germany Patents | Germany Applications | Great Britain Patents | Great Britain Applications | Greece Patents | Greece Applications | Hungary Patents | Hungary Applications | Iceland Patents | Iceland Applications | Ireland Patents | Ireland Applications | Italy Patents | Italy Applications | Latvia Patents | Latvia Applications | Lithuania Patents | Lithuania Applications | Luxembourg Patents | Malta Patents | Monaco Patents | Montenegro Patents | Montenegro Applications | Netherlands Patents | Netherlands Applications | Norway Patents | Norway Applications | Poland Patents | Poland Applications | Portugal Patents | Portugal Applications | Republic of Moldova Patents | Republic of Moldova Applications | Romania Patents | Romania Applications | San Marino Patents | San Marino Applications | Serbia Patents | Serbia Applications | Slovakia Patents | Slovakia Applications | Slovenia Patents | Spain Patents | Spain Applications | Sweden Patents | Sweden Applications | Switzerland Patents | Switzerland Applications | Ukraine Patents | Yugoslavia/Serbia and Montenegro Patents | Yugoslavia/Serbia and Montenegro Applications | Armenia Patents | Australia Patents | Australia Applications | Cyprus Patents | Gulf Cooperation Council Patents | Hong Kong Patents | India Patents | India Applications | Indonesia Patents | Indonesia Applications | Israel Applications | Jordan Patents | Kyrgyzstan Patents | Macao Applications | Malaysia Patents | Mongolia Patents | New Zealand Patents | Philippines Patents | Philippines Applications | Saudi Arabia Patents | Singapore Patents | Singapore Applications | Taiwan Patents | Taiwan Applications | Tajikistan Patents | Tajikistan Applications | Thailand Applications | Uzbekistan Patents | Vietnam Patents | Algeria Patents | ARIPO Patents | ARIPO Applications | Egypt Patents | Kenya Patents | Malawi Patents | Morocco Patents | Morocco Applications | OAPI Patents | South Africa Patents | Tunisia Applications | Zambia Patents | Zimbabwe Patents | EAPO Patents | EAPO Applications | Georgia Patents | Georgia Applications | Kazakhstan Patents | Kazakhstan Applications | Russia Patents | Russia Applications | Turkey Patents | Turkey Applications | IEEE Xplore Publications: IEEE Periodicals | IEEE Xplore Publications: IEEE Conferences | IEEE Xplore Publications: IEEE Standards | IEEE Xplore Publications: IEEE Early Access | IEEE Xplore Publications: SMPTE Periodicals | IEEE Xplore Publications: SMPTE Conferences | IEEE Xplore Publications: SMPTE Standards | IEEE Xplore Publications: MIT Press eBooks | IEEE Xplore Publications: Wiley-IEEE eBooks | IEEE Xplore Publications: IBM Periodicals | IEEE Xplore Publications: URSI Periodicals | IEEE Xplore Publications: VDE Conferences | IEEE Xplore Publications: Periodicals from China | IP.com Prior Art Database: The IP.com Journal | IP.com Prior Art Database: Internet Society RFC | IP.com Prior Art Database: IBM TDB Archive | IP.com Prior Art Database: Legacy Journals | IP.com Prior Art Database: Software Patent Institute | OnePetro.org: Periodicals at OnePetro.org | OnePetro.org: Conferences at OnePetro.org | Other Literature: IBM Redbooks | Other Literature: PubMed Central | Other Literature: arXiv.org

1 **2021-08-11 10:43 UTC | 3,973,142 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Text
turn off feature vector training

Sophos Ex. 1002
Page 169 of 347

Concept Modifiers: None

Filters: None

2 **2021-08-11 10:43 UTC | 16,412,199 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Text
ignore data point feature vector

Concept Modifiers: None

Filters: None

3 **2021-08-11 10:43 UTC | ~16,411,075 results from**

De-Dup: Simple Family Numbers (PAT only) | **Cut-off:** None | **Sort:** Relevance

Main Concept: Same as Query 2

Concept Modifiers: None

Filters: None

4 **2021-08-11 10:44 UTC | ~320,629 results from**

De-Dup: Simple Family Numbers (PAT only) | **Cut-off:** None | **Sort:** Relevance

Main Concept: Same as Query 2

Concept Modifiers: None

Filters (1):
Title+Abstract+Body/Description+Related Terms limited to: outlier

Sophos Ex. 1002
Page 170 of 347

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	16791649	Filing Date	2020-02-14	Docket Number (if applicable)	OPEN7950-1	Art Unit	2493
First Named Inventor	Mauritius Schmidtler			Examiner Name	Michael J. Simitoski		

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 503183

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	/John L. Adair/	Date (YYYY-MM-DD)	2021-11-18
Name	John L. Adair	Registration Number	48828

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
SUPPLEMENTAL AMENDMENT	Atty. Docket No. (Opt.) **OPEN7950-1**

First Named Inventor **Mauritius Schmidtler**	
Application Number **16/791,649**	Date Filed **February 14, 2020**
Title **AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS**	
Group Art Unit **2493**	Examiner **Michael J. Simitoski**
Confirmation Number **2519**	

Mail Stop: Issue Fee

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

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 **November 18, 2021.**

/Shenise Ramdeen/
Shenise Ramdeen

Please amend the above-identified application as follows.

AMENDMENTS TO THE CLAIMS:

Please amend the claims as set forth in the following listing. This listing of claims will replace all prior versions, and listings, of claims in the present application:

1. (Canceled)

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

identifying, by a knowledge module, static data points that may be indicative of either a harmful or benign executable file;

associating, by the knowledge module, the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting, by the knowledge module, a plurality of static data points from the identified executable file;

generating~~, by a classifier,~~ a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off based on information associated with one or more of the plurality of extracted static data points; and

providing the generated feature vector to one or more support vector machines to build a probabilistic model that indicates whether the executable file fits into one of the categories of files.

3. (Previously Presented) The computer-implemented method according to claim 2, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

4. (Previously Presented) The computer-implemented method according to claim 2, wherein the one or more support vector machines builds the probabilistic model by performing data analysis and pattern recognition on the one or more feature vectors.

5. (Previously Presented) The computer-implemented method according to claim 2, wherein the probabilistic model indicates whether the executable file is harmful.

6. (Previously Presented) The computer-implemented method according to claim 2, wherein the executable file is identified in response to a detected condition.

7. (Currently Amended) The computer-implemented method according to claim 6, wherein the detected condition is user request for a file download.

8. (Currently Amended) The computer-implemented method according to claim 6, wherein the detected condition is the detection of a new file attempting to execute.

9. (Previously Presented) The computer-implemented method according to claim 2, wherein the plurality of static data points represent predefined character strings in the executable file.

10. (Previously Presented) The computer-implemented method according to claim 2, wherein the one or more features of the feature vector are selectively turned on or off based at least in part on evaluation of whether a value of one of the plurality of extracted static data points is within a predetermined range.

11. (Previously Presented) The computer-implemented method according to claim 2, wherein a determination of whether the executable file is harmful is used to retrain the classifier.

12. (Previously Presented) A system comprising:

at least one memory; and

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

identifying static data points that may be indicative of either a harmful or benign executable file;

associating the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting a plurality of static data points from the identified executable file;

generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files

known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off based on information associated with one or more of the plurality of extracted static data points; and

providing the generated feature vector to one or more support vector machines to build a probabilistic model that indicates whether the executable file fits into one of the categories of files.

13. (Previously Presented) The system according to claim 12, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

14. (Previously Presented) The system according to claim 12, wherein the one or more support vector machines builds the probabilistic model by performing data analysis and pattern recognition on the one or more feature vectors.

15. (Previously Presented) The system according to claim 12, wherein the probabilistic model indicates whether the executable file is harmful.

16. (Previously Presented) The system according to claim 12, wherein the plurality of static data points represent predefined character strings in the executable file.

17. (Previously Presented) The system according to claim 12, wherein the one or more features of the feature vector are selectively turned on or off based at least in part on evaluation of whether a value of one of the plurality of extracted static data points is within a predetermined range.

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

identifying static data points that may be indicative of either a harmful or benign executable file;

associating the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting a plurality of static data points from the identified executable file;

generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off based on information associated with one or more of the plurality of extracted static data points; and

providing the generated feature vector to one or more support vector machines to build a probabilistic model that indicates whether the executable file fits into one of the categories of files.

19. (Previously Presented) The computer-readable storage device according to claim 18, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

20. (Previously Presented) The computer-readable storage device according to claim 18, wherein the plurality of static data points represent predefined character strings in the executable file.

21. (Previously Presented) The computer-readable storage device according to claim 18, wherein the one or more features of the feature vector are selectively turned on or off based at least in part on evaluation of whether a value of one of the plurality of extracted static data points is within a predetermined range.

22. (New) A computer-implemented method comprising:

identifying static data points that may be indicative of either a harmful or benign executable file;

associating the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting a plurality of static data points from the executable file;

generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off based on information associated with one or more of the plurality of extracted static data points; and

evaluating the feature vector using a machine learning model to determine whether the executable file fits into one of the categories of files.

23. (New) The computer-implemented method according to claim 22, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

24. (New) The computer-implemented method according to claim 22, wherein the machine learning model comprises an artificial neural network.

25. (New) The computer-implemented method according to claim 22, wherein the machine learning model comprises a support vector machine.

26. (New) The computer-implemented method according to claim 22, wherein the machine learning model comprises a machine learning decision tree.

27. (New) The computer-implemented method according to claim 22, wherein the machine learning model comprises a Bayesian network.

28. (New) The computer-implemented method according to claim 22, wherein evaluating the feature vector using the machine learning model comprises evaluating the feature vector using support vector processing.

29. (New) The computer-implemented method according to claim 22, wherein the machine learning model comprises a clustering model.

30. (New) The computer-implemented method according to claim 22, wherein the executable file is identified in response to a detected condition.

31. (New) The computer-implemented method according to claim 30, wherein the detected condition is user request for a file download.

32. (New) The computer-implemented method according to claim 30, wherein the detected condition is the detection of a new file attempting to execute.

33. (New) The computer-implemented method according to claim 22, wherein the plurality of static data points represent predefined character strings in the executable file.

34. (New) The computer-implemented method according to claim 22, wherein the one or more features of the feature vector are selectively turned on or off based at least in part on evaluation of whether a value of one of the plurality of extracted static data points is within a predetermined range.

35. (New) The computer-implemented method according to claim 22, wherein a determination of whether the executable file is harmful is used to retrain the classifier.

36. (New) The computer-implemented method according to claim 22, further comprising preventing execution of the executable file based on classifying the executable file as harmful.

37. (New) A computer-readable storage device containing instructions, that when executed on a processor, cause the processor to execute a process comprising:

identifying static data points that may be indicative of either a harmful or benign executable file;

associating the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting a plurality of static data points from the executable file;

generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off based on information associated with one or more of the plurality of extracted static data points; and

evaluating the feature vector using a machine learning model to determine whether the executable file fits into one of the categories of files.

38. (New) The computer-readable storage device according to claim 37, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

39. (New) The computer-readable storage device according to claim 37, wherein the machine learning model comprises an artificial neural network.

40. (New) The computer-readable storage device according to claim 37, wherein the machine learning model comprises a support vector machine.

41. (New) The computer-readable storage device according to claim 37, wherein the machine learning model comprises a machine learning decision tree.

42. (New) The computer-readable storage device according to claim 37, wherein the machine learning model comprises a Bayesian network.

43. (New) The computer-readable storage device according to claim 37, wherein evaluating the feature vector using the machine learning model comprises evaluating the feature vector using support vector processing.

44. (New) The computer-readable storage device according to claim 37, wherein the machine learning model comprises a clustering model.

45. (New) The computer-readable storage device according to claim 37, wherein the executable file is identified in response to a detected condition.

46. (New) The computer-readable storage device according to claim 45, wherein the detected condition is user request for a file download.

47. (New) The computer-readable storage device according to claim 45, wherein the detected condition is the detection of a new file attempting to execute.

48. (New) The computer-readable storage device according to claim 37, wherein the plurality of static data points represent predefined character strings in the executable file.

49. (New) The computer-implemented method according to claim 2, wherein the one or more features of the feature vector are selectively turned on or off based at least in part on

evaluation of whether a value of one of the plurality of extracted static data points is within a predetermined range.

50. (New) The computer-readable storage device according to claim 37, wherein a determination of whether the executable file is harmful is used to retrain the classifier.

51. (New) The computer-readable storage device according to claim 37, further comprising preventing execution of the executable file based on classifying the executable file as harmful.

REMARKS

Applicant appreciates the time taken by the Examiner to review the present amendment. Claim 2 is amended to address the fact that claim 2 as allowed recited "a classifier" twice: "generating, by **a classifier**, a feature vector from the plurality of static data points using **a classifier**" (emphasis added). The relevant portion of claim 2 now matches the corresponding portion of claim 14. As such, claim 2 should still be allowable.

Claims 7 and 8 have been amended to address minor informalities.

Claims 22-51 have been added. No new subject matter has been added. The application as filed, for example, teaches that various machine learning techniques may be used. *See e.g.,* Application at [0022] and [0025].

The Commissioner is hereby authorized to charge any deficiencies or credit any overpayment to Deposit Account No. 50-3183.

Respectfully submitted,

Sprinkle IP Law Group

/John L. Adair/

John L. Adair
Reg. No. 48,828

Dated: November 18, 2021

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. 512-637-9220
Fax. 512-371-9088

Electronic Patent Application Fee Transmittal

Application Number:	16791649
Filing Date:	14-Feb-2020
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:	OPEN7950-1

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:				
CLAIMS IN EXCESS OF 20	1202	30	100	3000
INDEPENDENT CLAIMS IN EXCESS OF 3	1201	2	480	960
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
RCE- 1ST REQUEST	1801	1	1360	1360
		Total in USD ($)		**5320**

Electronic Acknowledgement Receipt

EFS ID:	44322075
Application Number:	16791649
International Application Number:	
Confirmation Number:	2519
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:	OPEN7950-1
Receipt Date:	18-NOV-2021
Filing Date:	14-FEB-2020
Time Stamp:	19:19:47
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$5320
RAM confirmation Number	E2021AHJ20150635
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	OPEN7950-1_Comments11-18-21.pdf	20560 99d448a5ffa9a601dec3b40adf53ef933e398127	no	1
Warnings:					
Information:					
2	Request for Continued Examination (RCE)	OPEN7950-1_RCE11-18-21.pdf	39414 ff53a8188e702c5969ae435ee4b9be34f5454646	no	3
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
3		OPEN7950-1_SuppAmend11-18-21.pdf	47584 194c8145f462bbe6ca1e6a08744852c83a0889b4	yes	10

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment Submitted/Entered with Filing of CPA/RCE	1	1
Claims	2	9
Applicant Arguments/Remarks Made in an Amendment	10	10

Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	42630 a72f0a917249cc51878f459c66529e7b665a0299	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	150188	

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. **OPEN7950-1**

First Named Inventor **Mauritius Schmidtler**	
Application No. **16/791,649**	Filing or 371 (c) Date **February 14, 2020**
Title **AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS**	
Group Art Unit **2493**	Examiner **Michael J. Simitoski**
Confirmation No. **2519**	

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

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 **November 18, 2021.**

/Shenise Ramdeen/
Shenise Ramdeen

Dear Sir:

Applicant appreciates the Examiner's allowance of Claims 2-21 of United States Patent Application No. 16/791,649. 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. Applicant does not acquiesce or agree to the statement that "the prior art shows ignoring outlier features to avoid skewing results (e.g. Wegerich)."

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

/John L. Adair/

John L. Adair
Reg. No. 48,828

Dated: November 18, 2021

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. 512-637-9220
Fax. 512-371-9088

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 16/791,649	Filing Date 02/14/2020	☐ 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 $100 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $460 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	11/18/2021	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 50	Minus	** 20	= 30		x $100 =	3000
	Independent (37 CFR 1.16(h))	* 5	Minus	*** 3	= 2		x $480 =	960
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	3960

		(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.	SLIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/RANELL D GRAY/
*** 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.
16/791,649	02/14/2020	Mauritius Schmidtler	OPEN7950-1	2519

109422 7590 12/21/2021

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

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2493	

NOTIFICATION DATE	DELIVERY MODE
12/21/2021	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):

USPTOMAIL@SPRINKLELAW.COM

Office Action Summary	Application No. 16/791,649	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 18 November 2021.

☐ 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) 2-51 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) 2-9,11-16,18-20,22-33,35-48 and 50-51 is/are rejected.

8) ☑ Claim(s) 10,17,21,34 and 49 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 14 February 2020 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 12/16/2021.

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. Claims 2-51 are pending.

Continued Examination Under 37 CFR 1.114

3. 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 allowance or after an Office action under *Ex Parte Quayle*, 25 USPQ 74, 453 O.G. 213 (Comm'r Pat. 1935). 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, prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on 11/18/2021 has been entered.

Response to Amendment

4. Applicant's remarks (11/18/2021) were received. The Examiner notes that US 2010/0082642 A1 to Forman et al. (Forman) teaches controlling machine learning classification results by excluding features of a query whose associated number of classifiers exceed a threshold (¶47). 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 Shabtai such that one or more features of the feature vector are selectively turned on or off based on information associated with one or more of the plurality of extracted static data points (based on the data point being associated with too many classifiers in the machine learning model) to avoid a situation in which too many classifiers are returned for a query, as taught by Forman.

5. Claim 49 is a duplicate of claim 10. The Examiner believes claim 49 was intended to depend from claim 37. If so, the preamble should be amended to reflect "computer-readable storage device".

Claim Objections

6. Claim 49 is objected to because of the following informalities:

a. Claim 49 is a duplicate of claim 10. The Examiner believes claim 49 was intended to depend from claim 37. If so, the preamble should be amended to reflect "computer-readable storage device".

Appropriate correction is required.

Claim Rejections - 35 USC § 103

7. 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.

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, 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. Claim 2-5, 9, 11-16, 18-20, 22-28, 33, 35, 37-43, 48 and 50 are rejected under 35 U.S.C. 103 as being unpatentable over "Detection of malicious code by applying machine learning classifiers on static features: A state-of-the-art survey." by Shabtai et al. (**Shabtai**) in view of US 2010/0082642 A1 to Forman et al. (**Forman**).

Regarding claim 2, Shabtai discloses identifying, by a knowledge module (a skilled artisan would understand the reference is describing operations performed by computer software), static data points that may be indicative of either a harmful or benign executable file (training set is provided to the system, where a vector representing each file is extracted based on a vocabulary, p. 17, §2, p. 18, Fig. 1a); associating, by the knowledge module, the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files (create training set of benign and malicious files and input to a training algorithm, p. 17, §2); identifying an executable file to be evaluated (p. 17, §2, p. 18, Fig. 1b); extracting, by the knowledge module, a plurality of static data points from the identified executable file (file parsed and representative vector extracted, p. 17, §2, p. 18, Fig. 1a); generating a feature vector from the plurality of static data points (representative vector extracted, p. 17, §2, p. 18, Fig. 1a) using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files (training data set is trained using malicious and benign files, p. 17, §2, p. 18, Fig. 1b); and providing the generated feature vector to one or more support vector machines to build a probabilistic model that indicates whether the executable file fits into one of the categories of files (feature vectors provided to classification algorithm, p. 18, Fig. 1b, including support vector machine, p. 20, §5). Shabtai lacks wherein one or more features of the feature vector are selectively turned on or off based on information associated with one or more of the plurality of extracted static data points. However, Forman teaches controlling machine learning classification results by excluding features of a query whose associated number of classifiers exceed a threshold (¶47). 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 Shabtai such that one or more features of the feature vector are selectively turned on or off based on information associated with one or more of the plurality of extracted static data points (based on the data point being associated with too many classifiers in the machine learning

model). One of ordinary skill in the art would have been motivated to perform such a modification to avoid a situation in which too many classifiers are returned for a query, as taught by Forman.

Regarding claim 12, the claim is similar in scope to claim 2 and is therefore rejected using a similar rationale, noting again that a skilled artisan would understand the reference is describing operations performed by computer software.

Regarding claim 18, the claim is similar in scope to claim 2 and is therefore rejected using a similar rationale, noting again that a skilled artisan would understand the reference is describing operations performed by computer software.

Regarding claim 22, the claim is similar in scope to claim 2 and is therefore rejected using a similar rationale, noting again that a skilled artisan would understand the reference is describing operations performed by computer software.

Regarding claim 37, the claim is similar in scope to claim 2 and is therefore rejected using a similar rationale, noting again that a skilled artisan would understand the reference is describing operations performed by computer software.

Regarding claims 3, 13, 19, 23 and 38, Shabtai discloses wherein the plurality of static data points are extracted without decrypting or unpacking the executable file (Shabtai does not teach decryption or unpacking).

Regarding claims 4 and 14, Shabtai discloses wherein the one or more support vector machines builds the probabilistic model by performing data analysis and pattern recognition on the one or more feature vectors (recognize patterns in collection of byte n-grams derived from input file, p. 24, Table 1).

Regarding claims 5 and 15, Shabtai discloses wherein the probabilistic model indicates whether the executable file is harmful (classifier classifies file into the benign or malicious class, p. 20, §5).

Regarding claims 9, 16, 20, 33 and 48, Shabtai discloses wherein the plurality of static data points represent predefined character strings in the executable file (Portable Executable (PE) and String features, p. 19, §3).[1]

Regarding claims 11, 35 and 50, Shabtai discloses wherein a determination of whether the executable file is harmful is used to retrain the classifier (Shabtai discloses acquiring new malicious files and updating (retraining) the classifiers accordingly, p. 26, §6.3).

Regarding claims 24 and 39, Shabtai discloses wherein the machine learning model comprises an artificial neural network (p. 20, §5).

Regarding claims 25, 28, 40 and 43, Shabtai discloses wherein the machine learning module comprises a support vector machine (p. 20, §5).

Regarding claims 26 and 41, Shabtai discloses wherein the machine learning model comprises a machine learning decision tree (p. 20, §5).

Regarding claims 27 and 42, Shabtai discloses wherein the machine learning model comprises a Bayesian network (p. 20, §5).

10. Claims 6-8, 30-32, 36, 45-47 and 51 are rejected under 35 U.S.C. 103 as being unpatentable over **Shabtai** and **Forman**, as applied to claim 1 above, in view of US 2010/0293273 A1 to Basarrate et al. (**Basarrate**).

Regarding claims 6-8, 30-32 and 45-47, Shabtai, as modified above, is silent regarding wherein the executable file is identified in response to a detected condition. However, Basarrate teaches that it was known for a virus scanner to detect a file being downloaded or executed (¶85)[2]. Therefore, it would have been obvious to one having ordinary skill in the art before the effective filing date of the claimed

[1] "A malware detection scheme based on mining format information" by Bai et al. teaches a similar concept.
[2] US 10,116,688 B1 to Yun and US 2011/0154490 A1 to DeLuca et al. teach a similar concept.

invention to modify Shabtai, as modified above, such that the executable file is identified in response to a detected condition. One of ordinary skill in the art would have been motivated to perform such a modification to utilize known triggers for file inspection, as taught by Basarrate. Note that a skilled artisan would have found such a teaching obvious specifically as it well known in the art of computer security to intercept and scan a potential threat when entering the system (downloading) and before allowing execution.

Regarding claims 36 and 51, Shabtai, as modified above, lacks preventing execution of the executable file based on classifying the executable file as harmful. However, Basarrate teaches recommending an action based on a classification, including erasing the file or putting it in quarantine (¶93). 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 Shabtai, as modified above, to include preventing execution of the executable file based on classifying the executable file as harmful. One of ordinary skill in the art would have been motivated to perform such a modification to avoid the file infecting the host system, as taught by Basarrate.

11. Claims 29 and 44 are rejected under 35 U.S.C. 103 as being unpatentable over **Shabtai** and **Forman**, as applied to claim 1 above, in view of US 2015/0213365 A1 to Ideses et al. (**Ideses**).

Regarding claims 29 and 44, Shabtai, as modified above, lacks wherein the machine learning model comprises a clustering model. However, Ideses teaches that it was known to detect malware (¶45) by classification using a trained machine learning model, including "Neural Networks, Support Vector Machines, Decision Trees, Hard/Soft Thresholding, Naive Bayes Classifiers, or any other suitable classification system and/or method. Alternatively or additionally, the classifier is trained (and/or machine learning takes place) based on unsupervised learning, for example, k-Nearest Neighbors (KNN) clustering, Gaussian Mixture Model (GMM) parameterization, or other suitable unsupervised methods"

(¶105). 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 Shabtai, as modified above, such that the machine learning model comprises a clustering model. One of ordinary skill in the art would have been motivated to perform such a modification to utilize a known method of classifying software, as taught by Ideses.

Allowable Subject Matter

12. Claims 10, 17, 21, 34 and 49 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 and any remaining rejections above, not based on prior art, are overcome.

b. Regarding claims 10, 17, 21, 34 and 49, certain prior art related to machine learning teaches removing outliers in the selected data. For example, US 20110172504 A1 to Wegerich teaches ignoring feature data that varies more than a threshold in a system that uses biometric/sensor data. However, the prior art as a whole does not teach how a skilled artisan would include selectively turning one or off the claimed feature vector based at least in part on evaluation of whether a value of one of the plurality of extracted static data points is within a predetermined range within the context of Shabtai.

Conclusion

13. 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 https://ppair-my.uspto.gov/pair/PrivatePair. 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, 2021

Examiner-Initiated Interview Summary	**Application No.** 16/791,649	**Applicant(s)** Schmidtler et al.		
	Examiner MICHAEL J SIMITOSKI	**Art Unit** 2493	**AIA (First Inventor to File) Status** Yes	**Page** 1 of 1

All Participants (applicant, applicants representative, PTO personnel)	**Title**	**Type**
MICHAEL J SIMITOSKI	Primary Examiner	Telephonic
Mark Berrier, 35066	Attorney of Record	

Date of Interview: 16 December 2021

Issues Discussed:

35 U.S.C. 103

The Examiner noted that the independent claims would be rejected in view of Shabtai and Forman (see attached Office Action), but claims 10, 17, 21, 34 and 49 would be objected to as allowable. Applicant and the Examiner were unable to reach an agreement within the timeframe required by the Examiner and, as such, the attached Office Action is submitted.

Objections

The Examiner noted that claim 49 appears to be a duplicate of claim 2. The Examiner believes that claim 49 should depend from claim 37.

/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.

Notice of References Cited	Application/Control No. 16/791,649	Applicant(s)/Patent Under Reexamination Schmidtler et al.	
	Examiner MICHAEL J SIMITOSKI	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-9465940-B1	10-2016	Wojnowicz; Michael	G06F21/565	1/1
*	B	US-20160225017-A1	08-2016	Wong; Jimmy K.	G06Q30/0247	1/1
*	C	US-9197663-B1	11-2015	Gilbert; Mark	G06F21/552	1/1
*	D	US-20150213365-A1	07-2015	IDESES; Ianir	H04L67/125	706/12
*	E	US-20120079596-A1	03-2012	Thomas; Ralph	G06F21/566	726/24
	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	
	V	
	W	
	X	

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

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/791,649	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	03/24/2021	12/16/2021							
	1	-	-							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	O							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16	✓	✓							
	17	✓	O							
	18	✓	✓							
	19	✓	✓							
	20	✓	✓							
	21	✓	O							
	22		✓							
	23		✓							
	24		✓							
	25		✓							
	26		✓							
	27		✓							
	28		✓							
	29		✓							
	30		✓							
	31		✓							
	32		✓							
	33		✓							
	34		O							
	35		✓							
	36		✓							
	37		✓							
	38		✓							
	39		✓							
	40		✓							
	41		✓							
	42		✓							

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/791,649	Schmidtler et al.
	Examiner	**Art Unit**
	MICHAEL J SIMITOSKI	2493

CLAIM		DATE								
Final	Original	03/24/2021	12/16/2021							
	43		✓							
	44		✓							
	45		✓							
	46		✓							
	47		✓							
	48		✓							
	49		O							
	50		✓							
	51		✓							

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/791,649	Schmidtler et al.
	Examiner	Art Unit
	MICHAEL J SIMITOSKI	2493

CPC - Searched*		
Symbol	Date	Examiner
G06F 21/51,53,562,56,565,566; 2221/033; 8/53 | G06N 20/00,10 | H04L 63/145	12/16/2021	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.

Search Notes		
Search Notes	Date	Examiner
EAST, NPL and inventor search performed (see EAST and NPL search histories, attached and/or previously made of record)	12/16/2021	MJS
Consulted Common Citation Document and Global Dossier for related/family applications and prosecution histories	12/16/2021	MJS

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
G06F	21/51,53,562,56,565,566; 2221/033; 8/53	12/16/2021	MJS
G06N	20/00,10	12/16/2021	MJS
H04L	63/145	12/16/2021	MJS

/Michael Simitoski/ Primary Examiner, Art Unit 2493	

Search History

Report Run Date: 2021-12-16 UTC
Queries: 5
Markers: 0

Sophos Ex. 1002
Page 206 of 347

Query #	Timestamp	Results	Page
1	2021-12-16 15:03 UTC	2,094,963	3
2	2021-12-16 15:04 UTC	977,509	4
3	2021-12-16 15:04 UTC	~976,337	4
4	2021-12-16 15:04 UTC	~824,018	4
5	2021-12-16 15:05 UTC	~15,442	4

Content: Patents + NPL (187)

US Patents | US Designs | US Applications | EPO Patents | EPO Applications | China Patents | China Applications | Japan Patents | Japan Applications | Korea Patents | Korea Applications | WIPO Applications | Argentina Patents | Argentina Applications | Brazil Patents | Brazil Applications | Canada Patents | Canada Applications | Chile Patents | Chile Applications | Colombia Applications | Costa Rica Applications | Cuba Patents | Cuba Applications | Dominican Republic Applications | Ecuador Patents | Ecuador Applications | El Salvador Applications | Guatemala Applications | Honduras Applications | Mexico Patents | Mexico Applications | Nicaragua Patents | Panama Applications | Peru Applications | Trinidad & Tobago Patents | Uruguay Applications | Austria Patents | Austria Applications | Belarus Patents | Belgium Patents | Belgium Applications | Bosnia & Herzegovina Patents | Bosnia & Herzegovina Applications | Bulgaria Patents | Bulgaria Applications | Croatia Patents | Croatia Applications | Czech Republic Patents | Czech Republic Applications | Czechoslovakia Patents | Czechoslovakia Applications | Denmark Patents | Denmark Applications | Estonia Patents | Estonia Applications | EUIPO Patents | Finland Patents | Finland Applications | France Patents | France Applications | Germany Patents | Germany Applications | Great Britain Patents | Great Britain Applications | Greece Patents | Greece Applications | Hungary Patents | Hungary Applications | Iceland Patents | Iceland Applications | Ireland Patents | Ireland Applications | Italy Patents | Italy Applications | Latvia Patents | Latvia Applications | Lithuania Patents | Lithuania Applications | Luxembourg Patents | Malta Patents | Monaco Patents | Montenegro Patents | Montenegro Applications | Netherlands Patents | Netherlands Applications | Norway Patents | Norway Applications | Poland Patents | Poland Applications | Portugal Patents | Portugal Applications | Republic of Moldova Patents | Republic of Moldova Applications | Romania Patents | Romania Applications | San Marino Patents | San Marino Applications | Serbia Patents | Serbia Applications | Slovakia Patents | Slovakia Applications | Slovenia Patents | Spain Patents | Spain Applications | Sweden Patents | Sweden Applications | Switzerland Patents | Switzerland Applications | Ukraine Patents | Yugoslavia/Serbia and Montenegro Patents | Yugoslavia/Serbia and Montenegro Applications | Armenia Patents | Australia Patents | Australia Applications | Cyprus Patents | Gulf Cooperation Council Patents | Hong Kong Patents | India Patents | India Applications | Indonesia Patents | Indonesia Applications | Israel Applications | Jordan Patents | Kyrgyzstan Patents | Macao Applications | Malaysia Patents | Mongolia Patents | New Zealand Patents | Philippines Patents | Philippines Applications | Saudi Arabia Patents | Singapore Patents | Singapore Applications | Taiwan Patents | Taiwan Applications | Tajikistan Patents | Tajikistan Applications | Thailand Applications | Uzbekistan Patents | Vietnam Patents | Algeria Patents | ARIPO Patents | ARIPO Applications | Egypt Patents | Kenya Patents | Malawi Patents | Morocco Patents | Morocco Applications | OAPI Patents | South Africa Patents | Tunisia Applications | Zambia Patents | Zimbabwe Patents | EAPO Patents | EAPO Applications | Georgia Patents | Georgia Applications | Kazakhstan Patents | Kazakhstan Applications | Russia Patents | Russia Applications | Turkey Patents | Turkey Applications | IEEE Xplore Publications: IEEE Periodicals | IEEE Xplore Publications: IEEE Conferences | IEEE Xplore Publications: IEEE Standards | IEEE Xplore Publications: IEEE Early Access | IEEE Xplore Publications: SMPTE Periodicals | IEEE Xplore Publications: SMPTE Conferences | IEEE Xplore Publications: SMPTE Standards | IEEE Xplore Publications: MIT Press eBooks | IEEE Xplore Publications: Wiley-IEEE eBooks | IEEE Xplore Publications: IBM Periodicals | IEEE Xplore Publications: URSI Periodicals | IEEE Xplore Publications: VDE Conferences | IEEE Xplore Publications: Periodicals from China | IP.com Prior Art Database: The IP.com Journal | IP.com Prior Art Database: Internet Society RFC | IP.com Prior Art Database: IBM TDB Archive | IP.com Prior Art Database: Legacy Journals | IP.com Prior Art Database: Software Patent Institute | OnePetro.org: Periodicals at OnePetro.org | OnePetro.org: Conferences at OnePetro.org | Other Literature: IBM Redbooks | Other Literature: PubMed Central | Other Literature: arXiv.org

1 **2021-12-16 15:03 UTC | 2,094,963 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Text
machine learning ignore features

Sophos Ex. 1002
Page 208 of 347

Concept Modifiers: None

Filters: None

2 **2021-12-16 15:04 UTC | 977,509 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Same as Query 1

Concept Modifiers: None

Filters (1):
Title+Abstract+Body/Description+Related Terms limited to: vector

3 **2021-12-16 15:04 UTC | ~976,337 results from**

De-Dup: Extended Family Numbers (PAT only) | **Cut-off:** None | **Sort:** Relevance

Main Concept: Same as Query 1

Concept Modifiers: None

Filters: Same as Query 2

4 **2021-12-16 15:04 UTC | ~824,018 results from**

De-Dup: Extended Family Numbers (PAT only) | **Cut-off:** None | **Sort:** Relevance

Main Concept: Same as Query 1

Concept Modifiers: None

Filters (2):
Title+Abstract+Body/Description+Related Terms limited to: vector
Title+Abstract+Body/Description+Related Terms limited to: svm; clustering; neural; bayes; bayesian; "decision tree"; "support vector"

5 **2021-12-16 15:05 UTC | ~15,442 results from**

De-Dup: Extended Family Numbers (PAT only) | **Cut-off:** None | **Sort:** Relevance

Main Concept: Same as Query 1

Concept Modifiers: None

Filters (3):
Title+Abstract+Body/Description+Related Terms limited to: vector
Title+Abstract+Body/Description+Related Terms limited to: svm; clustering; neural; bayes; bayesian; "decision tree"; "support vector"
Title+Abstract+Body/Description+Related Terms limited to: antivirus; malware

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L141	30	(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	ON	2021/12/14 06:48 AM
L142	14	L135 and benign	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2021/12/14 06:49 AM
L143	6	(antivirus malware) and (@ad<"20150512" @prad<"20150512") and ((support adj vector) (machine adj learning)) and (exclu$4 ignor$4 filter$4 (turn$4 adj off)) near2 (feature outlier data point) with (range threshold)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2021/12/14 06:49 AM
L144	61	(machine ADJ learning) AND (feature ADJ vector) AND (exclu$4 (turn$4 ADJ off) omit$4 omission ignor$4) near2 (feature (data ADJ point)) WITH (range threshold deviat$4 outlier)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2021/12/14 06:53 AM
L145	11	(@ad<"20150512" @prad<"20150512") AND (machine ADJ learning) AND (feature ADJ vector) AND (exclu$4 (turn$4 ADJ off) omit$4 omission ignor$4) near2 (feature (data ADJ point)) WITH (range threshold deviat$4 outlier)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2021/12/14 06:54 AM
L146	10129	bayes$3 SAME (SVM (support ADJ vector)) SAME (decision ADJ tree) SAME cluster$4	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO,	OR	ON	ON	2021/12/16 08:48 AM

			RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L147	8795	bayes$3 SAME (SVM (support ADJ vector)) SAME (decision ADJ tree) SAME clustering	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2021/12/16 08:48 AM
L148	6913	bayes$3 SAME (SVM (support ADJ vector)) SAME (decision ADJ tree) SAME clustering SAME (machine ADJ learn$4)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2021/12/16 08:49 AM
L149	759	bayes$3 SAME (SVM (support ADJ vector)) SAME (decision ADJ tree) SAME clustering SAME (machine ADJ learn$4) AND (virus)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2021/12/16 08:49 AM
L150	132	bayes$3 SAME (SVM (support ADJ vector)) SAME (decision ADJ tree) SAME clustering	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU,	OR	ON	ON	2021/12/16 08:49 AM

		SAME (machine ADJ learn$4) AND (malware)	CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L151	1	bayes$3 SAME (SVM (support ADJ vector)) SAME (decision ADJ tree) SAME clustering SAME (machine ADJ learn$4) AND (malware) AND (prevent prohibit$4) near3 (execut$4)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2021/12/16 08:49 AM
L152	22	(@ad<"20150512" @prad<"20150512") AND bayes$3 SAME (SVM (support ADJ vector)) SAME (decision ADJ tree) SAME clustering SAME (machine ADJ learn$4) AND (malware)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2021/12/16 08:50 AM
L153	14	L135 and benign	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2021/12/16 09:37 AM
L154	123	((("Schmidtler") near3 ("Mauritius"))).INV. ((("Dalal") near3 ("Gaurav"))).INV. ((("Yoosoofmiya") near3 ("Reza"))).INV.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2021/12/16 09:37 AM
L155	25	((EP-2182458-A1).did. AND FPRS.dbnm.) OR	(US-PGPUB; USPAT; USOCR; FIT (AP, AT,	OR	ON	ON	2021/12/16 09:37 AM

		((US-20110172504-A1 OR US-20110154490-A1 OR US-20100293273-A1 OR US-20060037080-A1 OR US-20060026675-A1 OR US-20170262633-A1 OR US-20100082642-A1 OR US-20180365573-A1 OR US-20120079596-A1 OR US-20090274376-A1 OR US-20090013405-A1 OR US-20160021174-A1 OR US-20120227105-A1 OR US-20140310517-A1 OR US-20160156646-A1 OR US-20130291111-A1 OR US-20090300765-A1 OR US-20160225017-A1 OR US-20150213365-A1).did. AND PGPB.dbnm.) OR ((US-10116688-B1 OR US-8161548-B1 OR US-9197663-B1 OR US-8510836-B1 OR US-9465940-B1).did. AND USPT.dbnm.)	AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L156	51	("10116688"|"20060026675"|"20060037080"|"20090013405"|"20090274376"|"20090300765"|"20100082642"|"20100293273"|"20110154490"|"20110172504"|"20120227105"|"20130291111"|"20140310517"|"20160021174"|"20160156646"|"20170262633"|"20180365573"|"8161548"|"8510836").PN.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2021/12/16 09:38 AM
L157	6	L155 NOT 156	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV,	OR	ON	ON	2021/12/16 09:38 AM

			MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				

PE2E SEARCH - Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
N143	10	N141 and (((turn$4 adj off) disregard$4 exclu$4 ignor$4) near2 (feature)).clm. and classifier.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2021/12/14 06:50 AM
N144	10	N141 and (((turn$4 adj off) disregard$4 exclu$4 ignor$4) near2 (feature)).clm. and classifier.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2021/12/14 06:50 AM
N145	10	N66 and (((turn$4 adj off) disregard$4 exclu$4 ignor$4) near2 (feature)).clm. and classifier.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2021/12/14 06:50 AM
N146	10	N66 and (((turn$4 adj off) disregard$4 exclu$4 ignor$4) near2 (feature)).clm. and classifier.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2021/12/16 09:53 AM
N147	10	N141 and (((turn$4 adj off) disregard$4 exclu$4 ignor$4) near2 (feature)).clm. and classifier.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2021/12/16 09:53 AM
N148	10	N141 and (((turn$4 adj off) disregard$4 exclu$4 ignor$4) near2 (feature)).clm. and classifier.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2021/12/16 09:53 AM

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 16/791,649	Filing Date 02/14/2020	☐ 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 $100 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $460 =	
☐ 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	02/08/2022	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 45	Minus	** 50	= 0		x $100 =	0
	Independent (37 CFR 1.16(h))	* 5	Minus	*** 5	= 0		x $480 =	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.	SLIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/Theresa OKON/
*** 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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
REPLY TO OFFICE ACTION DATED 12/21/2021	Atty. Docket No. **OPEN7950-1**

First Named Inventor **Mauritius Schmidtler**	
Application Number **16/791,649**	Date Filed **February 14, 2020**
Title **AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS**	
Group Art Unit **2493**	Examiner **Michael J. Simitoski**
Confirmation Number: **2519**	

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 8, 2022.**

By: *Margarita Marquez*
Margarita Marquez

This paper is submitted in response to the Official Action mailed on December 21, 2021 and the Examiner Interview conducted February 8, 2022. Please reconsider the above-identified application in view of the following amendments and remarks.

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

Remarks/Arguments begin on page 10 of this paper.

AMENDMENTS TO THE CLAIMS:

Please amend the claims as set forth in the following listing. This listing of claims will replace all prior versions, and listings, of claims in the present application:

1. (Canceled)

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

identifying, by a knowledge module, static data points that may be indicative of either a harmful or benign executable file;

associating, by the knowledge module, the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting, by the knowledge module, a plurality of static data points from the identified executable file;

generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off ~~based on information associated with one or more of the plurality of extracted static data points~~ based at least in part on evaluation of whether a value of one of the plurality of static data points is within a predetermined range; and

providing the generated feature vector to one or more support vector machines to build a probabilistic model that indicates whether the executable file fits into one of the categories of files.

3. (Previously Presented) The computer-implemented method according to claim 2, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

4. (Previously Presented) The computer-implemented method according to claim 2, wherein the one or more support vector machines builds the probabilistic model by performing data analysis and pattern recognition on the one or more feature vectors.

5. (Previously Presented) The computer-implemented method according to claim 2, wherein the probabilistic model indicates whether the executable file is harmful.

6. (Previously Presented) The computer-implemented method according to claim 2, wherein the executable file is identified in response to a detected condition.

7. (Previously Presented) The computer-implemented method according to claim 6, wherein the detected condition is user request for a file download.

8. (Previously Presented) The computer-implemented method according to claim 6, wherein the detected condition is the detection of a new file attempting to execute.

9. (Previously Presented) The computer-implemented method according to claim 2, wherein the plurality of static data points represent predefined character strings in the executable file.

10. (Canceled)

11. (Previously Presented) The computer-implemented method according to claim 2, wherein a determination of whether the executable file is harmful is used to retrain the classifier.

12. (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:

identifying static data points that may be indicative of either a harmful or benign executable file;

associating the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting a plurality of static data points from the identified executable file; and

generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off ~~based on information associated with one or more of~~

~~the plurality of extracted static data points~~ based at least in part on evaluation of whether a value of one of the plurality of static data points is within a predetermined range; and

providing the generated feature vector to one or more support vector machines to build a probabilistic model that indicates whether the executable file fits into one of the categories of files.

13. (Previously Presented) The system according to claim 12, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

14. (Previously Presented) The system according to claim 12, wherein the one or more support vector machines builds the probabilistic model by performing data analysis and pattern recognition on the one or more feature vectors.

15. (Previously Presented) The system according to claim 12, wherein the probabilistic model indicates whether the executable file is harmful.

16. (Previously Presented) The system according to claim 12, wherein the plurality of static data points represent predefined character strings in the executable file.

17. (Canceled).

18. (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:

identifying static data points that may be indicative of either a harmful or benign executable file;

associating the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting a plurality of static data points from the identified executable file;

generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off based ~~on information associated with one or more of the plurality~~

~~of extracted static data points~~ at least in part on evaluation of whether a value of one of the plurality of static data points is within a predetermined range; and

providing the generated feature vector to one or more support vector machines to build a probabilistic model that indicates whether the executable file fits into one of the categories of files.

19. (Previously Presented) The computer-readable storage device according to claim 18, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

20. (Previously Presented) The computer-readable storage device according to claim 18, wherein the plurality of static data points represent predefined character strings in the executable file.

21. (Canceled)

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

identifying static data points that may be indicative of either a harmful or benign executable file;

associating the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting a plurality of static data points from the executable file;

generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off ~~based on information associated with one or more of the plurality of extracted static data points~~ based at least in part on evaluation of whether a value of one of the plurality of static data points is within a predetermined range; and

evaluating the feature vector using a machine learning model to determine whether the executable file fits into one of the categories of files.

23. (Previously Presented) The computer-implemented method according to claim 22, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

24. (Previously Presented) The computer-implemented method according to claim 22, wherein the machine learning model comprises an artificial neural network.

25. (Previously Presented) The computer-implemented method according to claim 22, wherein the machine learning model comprises a support vector machine.

26. (Previously Presented) The computer-implemented method according to claim 22, wherein the machine learning model comprises a machine learning decision tree.

27. (Previously Presented) The computer-implemented method according to claim 22, wherein the machine learning model comprises a Bayesian network.

28. (Previously Presented) The computer-implemented method according to claim 22, wherein evaluating the feature vector using the machine learning model comprises evaluating the feature vector using support vector processing.

29. (Previously Presented) The computer-implemented method according to claim 22, wherein the machine learning model comprises a clustering model.

30. (Previously Presented) The computer-implemented method according to claim 22, wherein the executable file is identified in response to a detected condition.

31. (Previously Presented) The computer-implemented method according to claim 30, wherein the detected condition is user request for a file download.

32. (Previously Presented) The computer-implemented method according to claim 30, wherein the detected condition is the detection of a new file attempting to execute.

33. (Previously Presented) The computer-implemented method according to claim 22, wherein the plurality of static data points represent predefined character strings in the executable file.

34. (Canceled)

35. (Previously Presented) The computer-implemented method according to claim 22, wherein a determination of whether the executable file is harmful is used to retrain the classifier.

36. (Previously Presented) The computer-implemented method according to claim 22, further comprising preventing execution of the executable file based on classifying the executable file as harmful.

37. (Currently Amended) A computer-readable storage device containing instructions, that when executed on a processor, cause the processor to execute a process comprising:

identifying static data points that may be indicative of either a harmful or benign executable file;

associating the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting a plurality of static data points from the executable file;

generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off ~~based on information associated with one or more of the plurality of extracted static data points~~ based at least in part on evaluation of whether a value of one of the plurality of static data points is within a predetermined range; and

evaluating the feature vector using a machine learning model to determine whether the executable file fits into one of the categories of files.

38. (Previously Presented) The computer-readable storage device according to claim 37, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

39. (Previously Presented) The computer-readable storage device according to claim 37, wherein the machine learning model comprises an artificial neural network.

40. (Previously Presented) The computer-readable storage device according to claim 37, wherein the machine learning model comprises a support vector machine.

41. (Previously Presented) The computer-readable storage device according to claim 37, wherein the machine learning model comprises a machine learning decision tree.

42. (Previously Presented) The computer-readable storage device according to claim 37, wherein the machine learning model comprises a Bayesian network.

43. (Previously Presented) The computer-readable storage device according to claim 37, wherein evaluating the feature vector using the machine learning model comprises evaluating the feature vector using support vector processing.

44. (Previously Presented) The computer-readable storage device according to claim 37, wherein the machine learning model comprises a clustering model.

45. (Previously Presented) The computer-readable storage device according to claim 37, wherein the executable file is identified in response to a detected condition.

46. (Previously Presented) The computer-readable storage device according to claim 45, wherein the detected condition is user request for a file download.

47. (Previously Presented) The computer-readable storage device according to claim 45, wherein the detected condition is the detection of a new file attempting to execute.

48. (Previously Presented) The computer-readable storage device according to claim 37, wherein the plurality of static data points represent predefined character strings in the executable file.

49. (Canceled)

50. (Previously Presented) The computer-readable storage device according to claim 37, wherein a determination of whether the executable file is harmful is used to retrain the classifier.

51. (Previously Presented) The computer-readable storage device according to claim 37, further comprising preventing execution of the executable file based on classifying the executable file as harmful.

REMARKS

Applicant appreciates the time taken by the Examiner to review Applicant's present application. This application has been carefully reviewed in light of the Official Action mailed on December 21, 2021 ("Office Action") and the Examiner Interview held on February 8, 2022. Applicant does not acquiesce to the Examiner's rejections, claim interpretations or other statements in the Office Action. However, in order to expedite prosecution Applicant has amended claims 2, 12, 18, 22, and 37 and canceled claims 10, 17, 21, 34, and 49. Claim 1 was previously canceled. Thus, claims 2-9, 11-16, 18-20, 22-33, 35-48, 50, and 51 are pending, with claims 2, 12, 18, 22, and 37 being independent. No new matter has been added. Applicant respectfully requests reconsideration and favorable action in this case.

Interview Summary

Pursuant to a proposed amendment submitted to the Examiner, a telephonic interview was conducted on February 8, 2022, between Examiner Simitoski and Attorney Adair. During the interview, the proposed amendment was discussed. The examiner indicated that the proposed amendment would overcome the rejection under 35 U.S.C. § 103.

Applicant appreciates the time and effort taken by Examiner Simitoski to review Applicant's present application and to discuss the proposed amendment.

Claim Objections

Claim 49 stands currently objected to because of alleged informalities. Applicant appreciates the examiner pointing out the informality in claim 49. Claim 49, however, is canceled, rendering the objection moot.

Rejections under 35 U.S.C. § 103

Claims 2-5, 9, 11-16, 18-20, 22-28, 33, 35, 37-43, 48 and 50 stand rejected as obvious over *Detection of Malicious Code by Applying Machine Learning Classifiers on Static Features: A State-of-the-Art Survey* ("Shabtai") in view of U.S. Publication No. 2010/0082642 ("Forman").

Claims 6-8, 30-32, 36, 45-47 and 51 stand rejected as obvious over Shabtai and Forman, as applied to Claim 1 above, in view of U.S. Publication No. 2010/0293273 ("Basarrate").

Claims 29 and 44 stand rejected as obvious over Shabtai and Forman, as applied to Claim 1 above, in view of U.S. Publication No. 2015/0213365 ("Ideses").

The Examiner indicated that claims 10, 17, 21, 34 and 49, which recited "wherein the one or more features of the feature vector are selectively turned on or off based at least in part on evaluation of whether a value of one of the plurality of extracted static data points is within a predetermined range," included allowable subject matter. Accordingly, to expedite prosecution, the independent claims are amended herein to recite "wherein one or more features of the feature vector are selectively turned on or off based at least in part on evaluation of whether a value of one of the plurality of static data points is within a predetermined range," which is consistent with the proposed amendment discussed during the Examiner Interview. Applicant therefore requests withdrawal of the rejection and allowance of the claims.

Allowable Subject Matter

Applicant appreciates the Examiner's acknowledgement that claims 10, 17, 21, 34 and 49 include allowable subject matter.

Conclusion

Applicant has now made an earnest attempt to place this case in condition for allowance. Other than as explicitly set forth above, this reply does not include an acquiescence to statements, assertions, assumptions, conclusions, or any combination thereof in the Office Action. For the foregoing reasons and for other reasons clearly apparent, Applicant respectfully requests full allowance of the pending claims. The Examiner is invited to telephone the undersigned at the number listed below for prompt action in the event any issues remain.

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
Attorneys for Applicant

/John L. Adair/

John L. Adair
Reg. No. 48,828

Date: February 8, 2022

1301 W. 25th Street, Suite 408
Austin, TX 78705
Tel. (512) 637-9220
Fax. (512) 371-9088

Electronic Acknowledgement Receipt

EFS ID:	44945412
Application Number:	16791649
International Application Number:	
Confirmation Number:	2519
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/Margarita Marquez
Filer Authorized By:	John L. Adair
Attorney Docket Number:	OPEN7950-1
Receipt Date:	08-FEB-2022
Filing Date:	14-FEB-2020
Time Stamp:	15:58:57
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		OPEN7950-1_ROA_02-08-2022.pdf	59793 09acf8ceb8664cb749f460db8833cdcc42b5eefb	yes	12

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	9
	Applicant Arguments/Remarks Made in an Amendment	10	12
Warnings:			
Information:			
	Total Files Size (in bytes):	59793	

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.
16/791,649	02/14/2020	Mauritius Schmidtler	OPEN7950-1	2519

109422 7590 02/14/2022

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

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2493	

NOTIFICATION DATE	DELIVERY MODE
02/14/2022	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):

USPTOMAIL@SPRINKLELAW.COM

Applicant-Initiated Interview Summary	**Application No.** 16/791,649	**Applicant(s)** Schmidtler et al.		
	Examiner MICHAEL J SIMITOSKI	**Art Unit** 2493	**AIA (First Inventor to File) Status** Yes	**Page** 1 of 1

All Participants (applicant, applicants representative, PTO personnel)	**Title**	**Type**
MICHAEL J SIMITOSKI	Primary Examiner	Telephonic
John Adair, 48,828	Attorney of Record	

Date of Interview: 08 February 2022

Issues Discussed:

35 U.S.C. 103

Applicant contacted the Examiner to discuss the attached proposed amendment to claim 2 (and similar amendments to the remaining independent claims). The Examiner agreed that the amendment would overcome the rejection of record.

☑ Attachment

/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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
PROPOSED AMENDMENT	Atty. Docket No. **OPEN7950-1**

First Named Inventor **Mauritius Schmidtler**	
Application Number **16/791,649**	Date Filed **February 14, 2020**
Title **AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS**	
Group Art Unit **2493**	Examiner **Michael J. Simitoski**
Confirmation Number: **2519**	

Examiner Simitoski,

Please find attached a proposed amendment in the above-referenced case.

Respectfully submitted,

Sprinkle IP Law Group
Attorneys for Applicant

/John L. Adair/

John L. Adair
Reg. No. 48,828

Date: February 1, 2022

1301 W. 25th Street, Suite 408
Austin, TX 78705
Tel. (512) 637-9220
Fax. (512) 371-9088

AMENDMENTS TO THE CLAIMS:

Please amend the claims as set forth in the following listing. This listing of claims will replace all prior versions, and listings, of claims in the present application:

1. (Canceled)

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

identifying, by a knowledge module, static data points that may be indicative of either a harmful or benign executable file;

associating, by the knowledge module, the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting, by the knowledge module, a plurality of static data points from the identified executable file;

generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off ~~based on information associated with one or more of the plurality of extracted static data points~~ based at least in part on evaluation of whether a value of one of the plurality of static data points is within a predetermined range; and

providing the generated feature vector to one or more support vector machines to build a probabilistic model that indicates whether the executable file fits into one of the categories of files.

3. (Previously Presented) The computer-implemented method according to claim 2, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

4. (Previously Presented) The computer-implemented method according to claim 2, wherein the one or more support vector machines builds the probabilistic model by performing data analysis and pattern recognition on the one or more feature vectors.

5. (Previously Presented) The computer-implemented method according to claim 2, wherein the probabilistic model indicates whether the executable file is harmful.

6. (Previously Presented) The computer-implemented method according to claim 2, wherein the executable file is identified in response to a detected condition.

7. (Previously Presented) The computer-implemented method according to claim 6, wherein the detected condition is user request for a file download.

8. (Previously Presented) The computer-implemented method according to claim 6, wherein the detected condition is the detection of a new file attempting to execute.

9. (Previously Presented) The computer-implemented method according to claim 2, wherein the plurality of static data points represent predefined character strings in the executable file.

10. (Canceled)

11. (Previously Presented) The computer-implemented method according to claim 2, wherein a determination of whether the executable file is harmful is used to retrain the classifier.

12. (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:

identifying static data points that may be indicative of either a harmful or benign executable file;

associating the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting a plurality of static data points from the identified executable file; and

generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off ~~based on information associated with one or more of~~

~~the plurality of extracted static data points~~ based at least in part on evaluation of whether a value of one of the plurality of static data points is within a predetermined range; and

providing the generated feature vector to one or more support vector machines to build a probabilistic model that indicates whether the executable file fits into one of the categories of files.

13. (Previously Presented) The system according to claim 12, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

14. (Previously Presented) The system according to claim 12, wherein the one or more support vector machines builds the probabilistic model by performing data analysis and pattern recognition on the one or more feature vectors.

15. (Previously Presented) The system according to claim 12, wherein the probabilistic model indicates whether the executable file is harmful.

16. (Previously Presented) The system according to claim 12, wherein the plurality of static data points represent predefined character strings in the executable file.

17. (Canceled).

18. (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:

identifying static data points that may be indicative of either a harmful or benign executable file;

associating the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting a plurality of static data points from the identified executable file;

generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off based ~~on information associated with one or more of the plurality~~

~~of extracted static data points~~ at least in part on evaluation of whether a value of one of the plurality of static data points is within a predetermined range; and

providing the generated feature vector to one or more support vector machines to build a probabilistic model that indicates whether the executable file fits into one of the categories of files.

19. (Previously Presented) The computer-readable storage device according to claim 18, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

20. (Previously Presented) The computer-readable storage device according to claim 18, wherein the plurality of static data points represent predefined character strings in the executable file.

21. (Canceled)

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

identifying static data points that may be indicative of either a harmful or benign executable file;

associating the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting a plurality of static data points from the executable file;

generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off ~~based on information associated with one or more of the plurality of extracted static data points~~ based at least in part on evaluation of whether a value of one of the plurality of static data points is within a predetermined range; and

evaluating the feature vector using a machine learning model to determine whether the executable file fits into one of the categories of files.

23. (Previously Presented) The computer-implemented method according to claim 22, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

24. (Previously Presented) The computer-implemented method according to claim 22, wherein the machine learning model comprises an artificial neural network.

25. (Previously Presented) The computer-implemented method according to claim 22, wherein the machine learning model comprises a support vector machine.

26. (Previously Presented) The computer-implemented method according to claim 22, wherein the machine learning model comprises a machine learning decision tree.

27. (Previously Presented) The computer-implemented method according to claim 22, wherein the machine learning model comprises a Bayesian network.

28. (Previously Presented) The computer-implemented method according to claim 22, wherein evaluating the feature vector using the machine learning model comprises evaluating the feature vector using support vector processing.

29. (Previously Presented) The computer-implemented method according to claim 22, wherein the machine learning model comprises a clustering model.

30. (Previously Presented) The computer-implemented method according to claim 22, wherein the executable file is identified in response to a detected condition.

31. (Previously Presented) The computer-implemented method according to claim 30, wherein the detected condition is user request for a file download.

32. (Previously Presented) The computer-implemented method according to claim 30, wherein the detected condition is the detection of a new file attempting to execute.

33. (Previously Presented) The computer-implemented method according to claim 22, wherein the plurality of static data points represent predefined character strings in the executable file.

34. (Canceled)

35. (Previously Presented) The computer-implemented method according to claim 22, wherein a determination of whether the executable file is harmful is used to retrain the classifier.

36. (Previously Presented) The computer-implemented method according to claim 22, further comprising preventing execution of the executable file based on classifying the executable file as harmful.

37. (Currently Amended) A computer-readable storage device containing instructions, that when executed on a processor, cause the processor to execute a process comprising:

identifying static data points that may be indicative of either a harmful or benign executable file;

associating the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting a plurality of static data points from the executable file;

generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off ~~based on information associated with one or more of the plurality of extracted static data points~~ based at least in part on evaluation of whether a value of one of the plurality of static data points is within a predetermined range; and

evaluating the feature vector using a machine learning model to determine whether the executable file fits into one of the categories of files.

38. (Previously Presented) The computer-readable storage device according to claim 37, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

39. (Previously Presented) The computer-readable storage device according to claim 37, wherein the machine learning model comprises an artificial neural network.

40. (Previously Presented) The computer-readable storage device according to claim 37, wherein the machine learning model comprises a support vector machine.

41. (Previously Presented) The computer-readable storage device according to claim 37, wherein the machine learning model comprises a machine learning decision tree.

42. (Previously Presented) The computer-readable storage device according to claim 37, wherein the machine learning model comprises a Bayesian network.

43. (Previously Presented) The computer-readable storage device according to claim 37, wherein evaluating the feature vector using the machine learning model comprises evaluating the feature vector using support vector processing.

44. (Previously Presented) The computer-readable storage device according to claim 37, wherein the machine learning model comprises a clustering model.

45. (Previously Presented) The computer-readable storage device according to claim 37, wherein the executable file is identified in response to a detected condition.

46. (Previously Presented) The computer-readable storage device according to claim 45, wherein the detected condition is user request for a file download.

47. (Previously Presented) The computer-readable storage device according to claim 45, wherein the detected condition is the detection of a new file attempting to execute.

48. (Previously Presented) The computer-readable storage device according to claim 37, wherein the plurality of static data points represent predefined character strings in the executable file.

49. (Canceled)

50. (Previously Presented) The computer-readable storage device according to claim 37, wherein a determination of whether the executable file is harmful is used to retrain the classifier.

51. (Previously Presented) The computer-readable storage device according to claim 37, further comprising preventing execution of the executable file based on classifying the executable file as harmful.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
Interview Summary	Atty. Docket No. **OPEN7950-1**

First Named Inventor **Mauritius Schmidtler**	
Application Number **16/791,649**	Date Filed **February 14, 2020**
Title **AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS**	
Group Art Unit **2493**	Examiner **Michael J. Simitoski**
Confirmation Number: **2519**	

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 **March 14, 2022.**

By: */Margarita Marquez/*
Margarita Marquez

This paper is submitted in response to the Examiner's Applicant-Initiated Interview Summary mailed February 14, 2022.

Pursuant to a proposed amendment submitted to the Examiner, a telephonic interview was conducted on February 8, 2022, between Examiner Simitoski and Attorney Adair. During the interview, the proposed amendment was discussed. The examiner indicated that the proposed amendment would overcome the rejection under 35 U.S.C. § 103.

Applicant appreciates the time and effort taken by Examiner Simitoski to review Applicant's present application and to discuss the proposed amendment.

Respectfully submitted,

Sprinkle IP Law Group
Attorneys for Applicant

/John L. Adair/

John L. Adair
Reg. No. 48,828

Date: March 14, 2022

1301 W. 25th Street, Suite 408
Austin, TX 78705
Tel. (512) 637-9220
Fax. (512) 371-9088

Electronic Acknowledgement Receipt

EFS ID:	45223878
Application Number:	16791649
International Application Number:	
Confirmation Number:	2519
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/Margarita Marquez
Filer Authorized By:	John L. Adair
Attorney Docket Number:	OPEN7950-1
Receipt Date:	14-MAR-2022
Filing Date:	14-FEB-2020
Time Stamp:	18:22:35
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	Applicant summary of interview with examiner	OPEN7950-1_Reply_IS_03-14-2022.pdf	21798 a13953472cd4bd41deffb29b9fb39e18fbf32ba1	no	2

Warnings:

Information:	
Total Files Size (in bytes):	21798

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.

TRANSMITTAL OF PAYMENT OF ISSUE FEE (Undiscounted) 37 C.F.R. 1.311	Docket No. OPEN7950-1

First Named Inventor **Mauritius Schmidtler**				
Application No.	Filing Date	Examiner	Group Art Unit	Confirmation No.
16/791,649	**02/14/2020**	**Michael J. Simitoski**	**2493**	**2519**

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: $1,200
- ☐ Amendment Under 1.312
- ☒ Comments on Reasons for 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.

/John L. Adair/

John L. Adair
Reg. No. 48,828

Customer No. 109422
Sprinkle IP Law Group
1301 W. 25th Street, Suite 400
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 and items referenced herein are being deposited electronically with the U.S. Patent and Trademark Office using the United States Patent and Trademark Office's EFS-Web system on April 15, 2022.

/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 04/15/2022
Sprinkle IP Law Group/OPEN
1301 W. 25th Street, Suite 400
Austin, TX 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.

Shenise Ramdeen	(Typed or printed name)
/Shenise Ramdeen/	(Signature)
April 15, 2022	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/791,649	02/14/2020	Mauritius Schmidtler	OPEN7950-1	2519

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	$1200	$0.00	$0.00	$1200	07/15/2022

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/AIA/122 or PTO/SB/122) attached.

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

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

1 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	(B) RESIDENCE: (CITY and STATE OR COUNTRY)
Webroot Inc.	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 /John L. Adair/ Date April 15, 2022

Typed or printed name John L. Adair Registration No. 48,828

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
Comments on Statement of Reasons for Allowance	Atty. Docket No. **OPEN7950-1**

First Named Inventor **Mauritius Schmidtler**	
Application Number **16/791,649**	Date Filed **February 14, 2020**
Title **AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS**	
Group Art Unit **2493**	Examiner **Michael J. Simitoski**
Confirmation Number **2519**	

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

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 **April 15, 2022.**

/Shenise Ramdeen/
Shenise Ramdeen

Dear Sir:

Applicant appreciates the Examiner's allowance of Claims 2-9, 11-16, 18-20, 22-33, 35-48, and 50-51 of United States Patent Application No. 16/791,649. 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 or identify any particular element of the claims as a reason for allowance 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
Attorneys for Applicant

/John L. Adair/

John L. Adair
Reg. No. 48,828

Date: April 15, 2022
1301 W. 25th Street, Suite 400
Austin, TX 78705
Tel. (512) 637-9220
Fax. (512) 371-9088

Electronic Patent Application Fee Transmittal

Application Number:	16791649
Filing Date:	14-Feb-2020
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:	OPEN7950-1

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	1200	1200

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**1200**

Electronic Acknowledgement Receipt

EFS ID:	45488901
Application Number:	16791649
International Application Number:	
Confirmation Number:	2519
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:	OPEN7950-1
Receipt Date:	15-APR-2022
Filing Date:	14-FEB-2020
Time Stamp:	17:55:14
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$1200
RAM confirmation Number	E20224EH55392654
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	Transmittal Letter	OPEN7950-1_IssueFeeTrans04-15-22.pdf	18660 a0036375f020270599591cac43bd317b65278fa1	no	1
Warnings:					
Information:					
2	Issue Fee Payment (PTO-85B)	OPEN7950-1_PTOL-8504-15-22.pdf	182411 fd8ed25e29d790a4d4705c56029007cdcc38e240	no	1
Warnings:					
Information:					
3	Post Allowance Communication - Incoming	OPEN7950-1_Comments04-15-22.pdf	20180 ef0aafd416eeaf4c25f9fd516895f3f7a8abdf90	no	1
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	37937 8f40dbd945b6b82d63ae67f46be3aa098e1ebf4f	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	259188		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

109422 7590 04/15/2022
Sprinkle IP Law Group/OPEN
1301 W. 25th Street, Suite 400
Austin, TX 78705

EXAMINER
SIMITOSKI, MICHAEL J

ART UNIT	PAPER NUMBER
2493	

DATE MAILED: 04/15/2022

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/791,649	02/14/2020	Mauritius Schmidtler	OPEN7950-1	2519

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	$1200	$0.00	$0.00	$1200	07/15/2022

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. 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)

109422 7590 04/15/2022
Sprinkle IP Law Group/OPEN
1301 W. 25th Street, Suite 400
Austin, TX 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.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/791,649	02/14/2020	Mauritius Schmidtler	OPEN7950-1	2519

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	$1200	$0.00	$0.00	$1200	07/15/2022

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/AIA/122 or PTO/SB/122) attached.

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

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

1 _____
2 _____
3 _____

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

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document 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. 1002
Page 254 of 347

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.
16/791,649	02/14/2020	Mauritius Schmidtler	OPEN7950-1	2519

109422 7590 04/15/2022

Sprinkle IP Law Group/OPEN
1301 W. 25th Street, Suite 400
Austin, TX 78705

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2493	

DATE MAILED: 04/15/2022

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. 16/791,649	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 reply dated 2/8/2022.
   ☐ 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. _____.
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: 2-9,11-16,18-20,22-33,35-48 and 50-51

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 2/8/2022 was received and considered.

3. Claims 2-9, 11-16, 18-20, 22-33, 35-48 and 50-51 are pending.

Terminal Disclaimer

4. The terminal disclaimer filed on 8/11/2021 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of **10,599,844** has been reviewed and is accepted. The terminal disclaimer has been recorded.

Allowable Subject Matter

5. Claims 2-9, 11-16, 18-20, 22-33, 35-48 and 50-51 are allowed.

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

a. Note application 14/709,875 for previous search and prosecution histories.

b. The Forman reference teaches, in the same field of endeavor as the claimed invention, selectively turning on/off one or more features of a generated feature vector based on the number of classifiers associated with the features for the benefit of efficiency. However, the prior art, either alone or in a reasonable combination, fails to teach selectively turning on/off one or more features of the generated feature vector based at least in part on evaluation of whether a value of one of the plurality of static data points is within a predetermined range, as recited within the framework of claimed invention 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 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 published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: https://patentcenter.uspto.gov. Visit https://www.uspto.gov/patents/apply/patent-center for more information about Patent Center and https://www.uspto.gov/patents/docx for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Michael Simitoski/
Primary Examiner, Art Unit 2493

April 5, 2022

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/791,649	Schmidtler et al.
	Examiner	Art Unit
	MICHAEL J SIMITOSKI	2493

CPC - Searched*		
Symbol	Date	Examiner
G06F 21/51,53,562,56,565,566; 2221/033; 8/53 | G06N 20/00,10 | H04L 63/145	04/05/2022	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.

Search Notes		
Search Notes	Date	Examiner
EAST, NPL and inventor search performed (see EAST and NPL search histories, attached and/or previously made of record)	04/05/2022	MJS
Consulted Common Citation Document and Global Dossier for related/family applications and prosecution histories	04/05/2022	MJS

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
G06F	21/51,53,562,56,565,566; 2221/033; 8/53	04/05/2022	MJS
G06N	20/00,10	04/05/2022	MJS
H04L	63/145	04/05/2022	MJS

/Michael Simitoski/ Primary Examiner, Art Unit 2493	

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/791,649	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
G06N	/	20	/	10		I	2019-01-01
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)	45	
/Michael Simitoski/ Primary Examiner, Art Unit 2493	06 April 2022	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

U.S. Patent and Trademark Office

Part of Paper No.: 20220405

Sophos Ex. 1002
Page 262 of 347

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/791,649	Schmidtler et al.
	Examiner	**Art Unit**
	MICHAEL J SIMITOSKI	2493

INTERNATIONAL CLASSIFICATION				
CLAIMED				
G06F	/	21	/	56
G06N	/	5	/	04

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)	45	
/Michael Simitoski/ Primary Examiner, Art Unit 2493	06 April 2022	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

U.S. Patent and Trademark Office

Part of Paper No.: 20220405

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/791,649	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		10	16	19	24	28	32	37	41	46				
1	2	9	11	17	20	25	29	33	38	42	47				
2	3	10	12		21	26	30	34	39	43	48				
3	4	11	13	18	22	27	31	35	40		49				
4	5	12	14	19	23	28	32	36	41	44	50				
5	6	13	15	20	24	29	33	37	42	45	51				
6	7	14	16	21	25		34	38	43						
7	8		17	22	26	30	35	39	44						
8	9	15	18	23	27	31	36	40	45						

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	45	
/Michael Simitoski/ Primary Examiner, Art Unit 2493	06 April 2022	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

U.S. Patent and Trademark Office

Part of Paper No.: 20220405

CCD view for US202016791649

#	CC	Cat.	Citation details
1	*US*		**Application N° US202016791649** (US16791649) - 14 February 2020
2	*US*		**Application N° US201514709875** (US14709875) - 12 May 2015
			National Search Report
			US9465940 B1 (CYLANCE INC [US]) - 11 October 2016
			US2007240220 A1 (TUVELL GEORGE, , et al) - 11 October 2007
			US2012079596 A1 (THOMAS RALPH [US], et al) - 29 March 2012
			US9197663 B1 (BIT9 INC [US]) - 24 November 2015
			US8719924 B1 (WILLIAMSON MATTHEW [US], et al) - 6 May 2014
			US2014165203 A1 (SOURCEFIRE INC [US]) - 12 June 2014
			US2010192222 A1 (MICROSOFT CORP [US]) - 29 July 2010
		X	US8709924 B2 (HANAWA HIROJI [US], et al) - 29 April 2014 * claim 1 | column 1 lines 57 - 67] | column 2 lines 37 - 40] | column 3 lines 1 - 6] abstract | column 6 lines 4 - 26] Fig. 1 | column 3 lines 1
		Y	US2007240220 A1 (TUVELL GEORGE, , et al) - 11 October 2007 * [0104] | [0161] | [0336] Fig. 9 | [0162] | abs | [0163] Fig. 7 | [0323], [0336] Fig. 9 | [0323] | abstract | [0009] | [0011] | claim 4 | claim
		Y	US9197663 B1 (BIT9 INC [US]) - 24 November 2015 * column 2 lines 17 - 20 and 47 - 52] | column 3 lines 26 - 30] | column 20 lines 44 - 61] | abstract | column 4 line 64 column 5 line 3] | col
		Y	US2012079596 A1 (THOMAS RALPH [US], et al) - 29 March 2012 * [0239] | [0175], [0225] and [0272] | [0038], [0175], [0225] and [0272] | table 4] and [0257] | [0250] | table 4] | Fig. 8] | [0250], [0251
		A	US8719924 B1 (WILLIAMSON MATTHEW [US], et al) - 6 May 2014
		A	US2014165203 A1 (SOURCEFIRE INC [US]) - 12 June 2014
		A	US9465940 B1 (CYLANCE INC [US]) - 11 October 2016
		A	US2010192222 A1 (MICROSOFT CORP [US]) - 29 July 2010
			US8510836 B1 (NACHENBERG CAREY S [US], et al) - 13 August 2013
			US8719924 B1 (WILLIAMSON MATTHEW [US], et al) - 6 May 2014
			US9197663 B1 (BIT9 INC [US]) - 24 November 2015
			US9465940 B1 (CYLANCE INC [US]) - 11 October 2016
			US2007240220 A1 (TUVELL GEORGE, , et al) - 11 October 2007
			US2009013405 A1 (MESSAGELABS LTD [GB]) - 8 January 2009
			US2009274376 A1 (YAHOO INC [US]) - 5 November 2009
			US2009300765 A1 (DEUTSCHE TELEKOM AG [DE]) - 3 December 2009
			US20100082642 A1 (Forman George, , et al) - 1 April 2010
			US2010192222 A1 (MICROSOFT CORP [US]) - 29 July 2010
			US2012079596 A1 (THOMAS RALPH [US], et al) - 29 March 2012
			US2012227105 A1 (FRIEDRICHS OLIVER [US], et al) - 6 September 2012
			US2013291111 A1 (ZHOU HONGYI [CN], et al) - 31 October 2013
			US2014165203 A1 (SOURCEFIRE INC [US]) - 12 June 2014
			US2014310517 A1 (IBM [US]) - 16 October 2014
			US20160021174 A1 (TELEFONICA DIGITAL ESPANA SLU [ES]) - 21 January 2016
			US2016156646 A1 (HEWLETT PACKARD DEVELOPMENT CO [US]) - 2 June 2016
			US2017262633 A1 (BLUVECTOR INC [US]) - 14 September 2017
			US2018365573 A1 (INTEL CORP [US]) - 20 December 2018
			Detection of malicious code by applying machine learning classifiers on static features: A state-of-the-art survey Authors: Shabtai A, Moskovitch R, Elovici Y, Glezer C Publication data: Information Security Technical Report, 20090201 Elsevier Advanced Technology, AMSTERDAM, NL Source info: Vol: 14, Nr: 1, Page(s): 16 - 29

Sophos Ex. 1002
Page 265 of 347

#	CC	Cat.	Citation details
			Detection of malicious code by applying machine learning classifiers on static features: A state-of-the-art survey Authors: Shabtai A, Moskovitch R, Elovici Y, Glezer C Publication data: Information Security Technical Report, 20090201 Elsevier Advanced Technology, AMSTERDAM, NL Source info: Vol: 14, Nr: 1, Page(s): 16 - 29
			Non-patent literature - Bost, Raphael, et al. "Machine learning classification over encrypted data." NDSS. vol. 4324. 2015. (Year: 2015).
			Non-patent literature - Choi, Junho, et al. "Efficient malicious code detection using n-gram analysis and SVM." 2011 14th International Conference on Network-Based
			Non-patent literature - Devi, Dhruwajita, and Sukumar Nandi. "Detection of packed malware." Proceedings of the First International Conference on Security of Intern
			Non-patent literature - Dube, Thomas, et al. "Malware target recognition via static heuristics." Computers & Security 31.1 (2012): 137-147. (Year: 2012).
			Non-patent literature - Merkel, Ronny, et al. "Statistical detection of malicious pe-executables for fast offline analysis." IFIP International Conference on Communicati
			Non-patent literature - Singla, Sanjam, et al. "A Novel Approach to Malware Detection using Static Classification." International Journal of Computer Science and Info
			Non-patent literature - Tabish, S. Momina, M. Zubair Shafiq, and Muddassar Farooq. "Malware detection using statistical analysis of byte-level file content." Proceedin
			Non-patent literature - Treadwell, Scott, and Mian Zhou. "A heuristic approach for detection of obfuscated malware." 2009 IEEE International Conference on Intelliger
			Applicant
			Non-patent literature - International Patent Application No. PCT/US2016/032090, International Search Report and Written Opinion dated Jul. 29, 2016, 13 pages.
			Non-patent literature - Perdisci et al. (2008) Pattern Recognition Letters 29:1941-1946 "Classification of packed executables for accurate computer virus detection".
			Non-patent literature - Perdisci et al. (2008) IEEE. Annual Computer Security Applications Conference 301-310 "McBoost: Boosting Scalability in Malware Collection a
			Non-patent literature - Khan, Hassan et al., "Determining Malicious Executable Distinguishing Attributes and Low-Complexity Detection", J. Comput Virol, 7.2 (2011),
			Non-patent literature - Kolter, J. Zico et al., "Learning to Detect and Classift Malicious Executables in the Wild", Journal of Machine Learning Research 7 (2006), pp. 2
			Non-patent literature - International Patent Application No. PCT/US2016/032090, International Preliminary Report on Patentability dated Nov. 14, 2017, 7 pages.
3	WO		**Application N° WO2016US32090** (WOUS2016/032090) - 12 May 2016
			International Search Report
		A	US2010192222 A1 (MICROSOFT CORP [US]) - 29 July 2010 * sentences 3 - 6, paragraph [0019] * * sentences 9 - 11, paragraph [0032] *
		X I	***Classification of packed executables for accurate computer virus detection*** Authors: Perdisci R, Lanzi A, Lee W Publication data: PATTERN RECOGNITION LETTERS, 20081015 ELSEVIER, AMSTERDAM, NL Source info: Vol: 29, Nr: 14, Page(s): 1941 - 1946 * page 1942, column left, lines 10 - 14, 41 - 42, 51 - 53; figure 1 * * page 1943, column left, lines 9 - 14 * * section 4 "Experiments"; page 1944, column right, lines 6 - 9, 24, 25, 28 * * page 1945; table 1 *
		A	***McBoost: Boosting Scalability in Malware Collection and Analysis Using Statistical Classification of Executables*** Authors: Roberto Perdisci, Andrea Lanzi, Wenke Lee Publication data: Computer Security Applications Conference, 2008. ACSAC 2008. Annual, 20081208 IEEE, Piscataway, NJ, USA Source info: Page(s): 301 - 310 * page 304, column left *

Search History

Report Run Date: 2022-04-05 UTC
Searches: 6
Markers: 0

Sophos Ex. 1002
Page 267 of 347

Search #	Timestamp	Results	Page
1	2022-04-05 10:21 UTC	~2,251,723	3
2	2022-04-05 10:21 UTC	~1,050,892	4
3	2022-04-05 10:22 UTC	~889,867	4
4	2022-04-05 10:22 UTC	~16,872	4
5	2022-04-05 10:22 UTC	~18,682	4
6	2022-04-05 10:23 UTC	~2593	5

Content: Patents + NPL (187)

US Patents | US Designs | US Applications | EPO Patents | EPO Applications | China Patents | China Applications | Japan Patents | Japan Applications | Korea Patents | Korea Applications | WIPO Applications | Argentina Patents | Argentina Applications | Brazil Patents | Brazil Applications | Canada Patents | Canada Applications | Chile Patents | Chile Applications | Colombia Applications | Costa Rica Applications | Cuba Patents | Cuba Applications | Dominican Republic Applications | Ecuador Patents | Ecuador Applications | El Salvador Applications | Guatemala Applications | Honduras Applications | Mexico Patents | Mexico Applications | Nicaragua Patents | Panama Applications | Peru Applications | Trinidad & Tobago Patents | Uruguay Applications | Austria Patents | Austria Applications | Belarus Patents | Belgium Patents | Belgium Applications | Bosnia & Herzegovina Patents | Bosnia & Herzegovina Applications | Bulgaria Patents | Bulgaria Applications | Croatia Patents | Croatia Applications | Czech Republic Patents | Czech Republic Applications | Czechoslovakia Patents | Czechoslovakia Applications | Denmark Patents | Denmark Applications | Estonia Patents | Estonia Applications | EUIPO Patents | Finland Patents | Finland Applications | France Patents | France Applications | Germany Patents | Germany Applications | Great Britain Patents | Great Britain Applications | Greece Patents | Greece Applications | Hungary Patents | Hungary Applications | Iceland Patents | Iceland Applications | Ireland Patents | Ireland Applications | Italy Patents | Italy Applications | Latvia Patents | Latvia Applications | Lithuania Patents | Lithuania Applications | Luxembourg Patents | Malta Patents | Monaco Patents | Montenegro Patents | Montenegro Applications | Netherlands Patents | Netherlands Applications | Norway Patents | Norway Applications | Poland Patents | Poland Applications | Portugal Patents | Portugal Applications | Republic of Moldova Patents | Republic of Moldova Applications | Romania Patents | Romania Applications | San Marino Patents | San Marino Applications | Serbia Patents | Serbia Applications | Slovakia Patents | Slovakia Applications | Slovenia Patents | Spain Patents | Spain Applications | Sweden Patents | Sweden Applications | Switzerland Patents | Switzerland Applications | Ukraine Patents | Yugoslavia/Serbia and Montenegro Patents | Yugoslavia/Serbia and Montenegro Applications | Armenia Patents | Australia Patents | Australia Applications | Cyprus Patents | Gulf Cooperation Council Patents | Hong Kong Patents | India Patents | India Applications | Indonesia Patents | Indonesia Applications | Israel Applications | Jordan Patents | Kyrgyzstan Patents | Macao Applications | Malaysia Patents | Mongolia Patents | New Zealand Patents | Philippines Patents | Philippines Applications | Saudi Arabia Patents | Singapore Patents | Singapore Applications | Taiwan Patents | Taiwan Applications | Tajikistan Patents | Tajikistan Applications | Thailand Applications | Uzbekistan Patents | Vietnam Patents | Algeria Patents | ARIPO Patents | ARIPO Applications | Egypt Patents | Kenya Patents | Malawi Patents | Morocco Patents | Morocco Applications | OAPI Patents | South Africa Patents | Tunisia Applications | Zambia Patents | Zimbabwe Patents | EAPO Patents | EAPO Applications | Georgia Patents | Georgia Applications | Kazakhstan Patents | Kazakhstan Applications | Russia Patents | Russia Applications | Turkey Patents | Turkey Applications | IEEE Xplore Publications: IEEE Periodicals | IEEE Xplore Publications: IEEE Conferences | IEEE Xplore Publications: IEEE Standards | IEEE Xplore Publications: IEEE Early Access | IEEE Xplore Publications: SMPTE Periodicals | IEEE Xplore Publications: SMPTE Conferences | IEEE Xplore Publications: SMPTE Standards | IEEE Xplore Publications: MIT Press eBooks | IEEE Xplore Publications: Wiley-IEEE eBooks | IEEE Xplore Publications: IBM Periodicals | IEEE Xplore Publications: URSI Periodicals | IEEE Xplore Publications: VDE Conferences | IEEE Xplore Publications: Periodicals from China | IP.com Prior Art Database: The IP.com Journal | IP.com Prior Art Database: Internet Society RFC | IP.com Prior Art Database: IBM TDB Archive | IP.com Prior Art Database: Legacy Journals | IP.com Prior Art Database: Software Patent Institute | OnePetro.org: Periodicals at OnePetro.org | OnePetro.org: Conferences at OnePetro.org | Other Literature: IBM Redbooks | Other Literature: PubMed Central | Other Literature: arXiv.org

1 **2022-04-05 10:21 UTC | ~2,251,723 results from**

De-Dup: Simple Family Numbers (PAT only) | **Cut-off:** None | **Sort:** Relevance

Main Concept: Text
machine learning ignore features

Sophos Ex. 1002
Page 269 of 347

Concept Modifiers: None

Filters: None

2 **2022-04-05 10:21 UTC | ~1,050,892 results from**

De-Dup: Simple Family Numbers (PAT only) | **Cut-off:** None | **Sort:** Relevance

Main Concept: Same as Search 1

Concept Modifiers: None

Filters (1):
Title+Abstract+Body/Description+Related Terms limited to: vector

3 **2022-04-05 10:22 UTC | ~889,867 results from**

De-Dup: Simple Family Numbers (PAT only) | **Cut-off:** None | **Sort:** Relevance

Main Concept: Same as Search 1

Concept Modifiers: None

Filters (2):
Title+Abstract+Body/Description+Related Terms limited to: vector
Title+Abstract+Body/Description+Related Terms limited to: svm; clustering; neural; bayes; bayesian; "decision tree"; "support vector"

4 **2022-04-05 10:22 UTC | ~16,872 results from**

De-Dup: Simple Family Numbers (PAT only) | **Cut-off:** None | **Sort:** Relevance

Main Concept: Same as Search 1

Concept Modifiers: None

Filters (3):
Title+Abstract+Body/Description+Related Terms limited to: vector
Title+Abstract+Body/Description+Related Terms limited to: svm; clustering; neural; bayes; bayesian; "decision tree"; "support vector"
Title+Abstract+Body/Description+Related Terms limited to: antivirus; malware

5 **2022-04-05 10:22 UTC | ~18,682 results from**

De-Dup: Simple Family Numbers (PAT only) | **Cut-off:** None | **Sort:** Relevance

Main Concept: Text
machine learning ignore feature range

Concept Modifiers: None

Filters: Same as Search 4

Sophos Ex. 1002
Page 270 of 347

6 **2022-04-05 10:23 UTC | ~2593 results from**

De-Dup: Simple Family Numbers (PAT only) | **Cut-off:** None | **Sort:** Relevance

Main Concept: Text
machine learning ignore feature range outlier

Concept Modifiers: None

Filters: Same as Search 4

Sophos Ex. 1002
Page 271 of 347

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L158	126	((("Schmidtler") near3 ("Mauritius"))).INV. ((("Dalal") near3 ("Gaurav"))).INV. ((("Yoosoofmiya") near3 ("Reza"))).INV.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/04/05 06:19 AM
L159	22	(@ad<"20150512" @prad<"20150512") AND bayes$3 SAME (SVM (support ADJ vector)) SAME (decision ADJ tree) SAME clustering SAME (machine ADJ learn$4) AND (malware)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/04/05 06:19 AM
L160	11	(@ad<"20150512" @prad<"20150512") AND (machine ADJ learning) AND (feature ADJ vector) AND (exclu$4 (turn$4 ADJ off) omit$4 omission ignor$4) near2 (feature (data ADJ point)) WITH (range threshold deviat$4 outlier)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/04/05 06:19 AM

PE2E SEARCH - Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
N149	10	N141 and (((turn$4 adj off) disregard$4 exclu$4 ignor$4) near2 (feature)).clm. and classifier.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/05 06:20 AM

Bibliographic Data

Application No: 16/791,649

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.
02/14/2020	726	2493	OPEN7950-1
RULE			

APPLICANTS

Webroot Inc., Broomfield, CO,

INVENTORS

Mauritius Schmidtler, Escondido, CA, UNITED STATES

Gaurav Dalal, San Jose, CA, UNITED STATES

Reza Yoosoofmiya, San Diego, CA, UNITED STATES

CONTINUING DATA

This application is a CON of 14709875 05/12/2015 PAT 10599844

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

03/02/2020

STATE OR COUNTRY

UNITED STATES

ADDRESS

Sprinkle IP Law Group/OPEN
1301 W. 25th Street, Suite 400
Austin, TX 78705
UNITED STATES

FILING FEE RECEIVED

$1,720

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.
16/791,649	05/24/2022	11341239	OPEN7950-1	2519

109422 7590 05/04/2022

Sprinkle IP Law Group/OPEN
1301 W. 25th Street, Suite 400
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 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

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

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

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Patents Stakeholder Experience (OPSE), Stakeholder Support Division (SSD) at (571)-272-4200.

INVENTOR(s) (Please see PAIR WEB site http://pair.uspto.gov for additional inventors):

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

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Webroot Inc., Broomfield, CO;

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

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 16/791,649	Filing Date 02/14/2020	☐ 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 $100 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $460 =	
☐ 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	05/10/2022	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 59	Minus	** 50	= 9		x $100 =	900
	Independent (37 CFR 1.16(h))	* 6	Minus	*** 5	= 1		x $480 =	480
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	1380

		(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".	/DORIS M KING/
*** 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.

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	16791649	Filing Date	2020-02-14	Docket Number (if applicable)	OPEN7950-1	Art Unit	2493
First Named Inventor	Mauritius Schmidtler			Examiner Name	Michael J. Simitoski		

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 503183

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	/John L. Adair/	Date (YYYY-MM-DD)	2022-05-10
Name	John L. Adair	Registration Number	48828

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
SUPPLEMENTAL AMENDMENT	Atty. Docket No. (Opt.) **OPEN7950-1**

First Named Inventor **Mauritius Schmidtler**	
Application Number **16/791,649**	Date Filed **February 14, 2020**
Title **AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS**	
Group Art Unit **2493**	Examiner **Michael J. Simitoski**
Confirmation Number **2519**	

Mail Stop: Issue Fee

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

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 **May 10, 2022.**

/Shenise Ramdeen/
Shenise Ramdeen

Applicant files this Supplemental Amendment concurrently with a Request for Continued Examination and a Petition to Withdraw from Issue. Please amend the above-identified application as follows.

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows:

1. (Canceled)

2. (Previously Presented) A computer-implemented method comprising:

identifying, by a knowledge module, static data points that may be indicative of either a harmful or benign executable file;

associating, by the knowledge module, the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting, by the knowledge module, a plurality of static data points from the identified executable file;

generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off based at least in part on evaluation of whether a value of one of the plurality of static data points is within a predetermined range; and

providing the generated feature vector to one or more support vector machines to build a probabilistic model that indicates whether the executable file fits into one of the categories of files.

3. (Previously Presented) The computer-implemented method according to claim 2, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

4. (Previously Presented) The computer-implemented method according to claim 2, wherein the one or more support vector machines builds the probabilistic model by performing data analysis and pattern recognition on the one or more feature vectors.

5. (Previously Presented) The computer-implemented method according to claim 2, wherein the probabilistic model indicates whether the executable file is harmful.

6. (Previously Presented) The computer-implemented method according to claim 2, wherein the executable file is identified in response to a detected condition.

7. (Previously Presented) The computer-implemented method according to claim 6, wherein the detected condition is user request for a file download.

8. (Previously Presented) The computer-implemented method according to claim 6, wherein the detected condition is the detection of a new file attempting to execute.

9. (Previously Presented) The computer-implemented method according to claim 2, wherein the plurality of static data points represent predefined character strings in the executable file.

10. (Canceled)

11. (Previously Presented) The computer-implemented method according to claim 2, wherein a determination of whether the executable file is harmful is used to retrain the classifier.

12. (Previously Presented) A system comprising:

at least one memory; and

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

identifying static data points that may be indicative of either a harmful or benign executable file;

associating the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting a plurality of static data points from the identified executable file; and

generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off based at least in part on evaluation of whether a value of one of the plurality of static data points is within a predetermined range; and

providing the generated feature vector to one or more support vector machines to build a probabilistic model that indicates whether the executable file fits into one of the categories of files.

13. (Previously Presented) The system according to claim 12, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

14. (Previously Presented) The system according to claim 12, wherein the one or more support vector machines builds the probabilistic model by performing data analysis and pattern recognition on the one or more feature vectors.

15. (Previously Presented) The system according to claim 12, wherein the probabilistic model indicates whether the executable file is harmful.

16. (Previously Presented) The system according to claim 12, wherein the plurality of static data points represent predefined character strings in the executable file.

17. (Canceled).

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

identifying static data points that may be indicative of either a harmful or benign executable file;

associating the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting a plurality of static data points from the identified executable file;

generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off based at least in part on evaluation of whether a value of one of the plurality of static data points is within a predetermined range; and

providing the generated feature vector to one or more support vector machines to build a probabilistic model that indicates whether the executable file fits into one of the categories of files.

19. (Previously Presented) The computer-readable storage device according to claim 18, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

20. (Previously Presented) The computer-readable storage device according to claim 18, wherein the plurality of static data points represent predefined character strings in the executable file.

21. (Canceled)

22. (Previously Presented) A computer-implemented method comprising:

identifying static data points that may be indicative of either a harmful or benign executable file;

associating the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting a plurality of static data points from the executable file;

generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off based at least in part on evaluation of whether a value of one of the plurality of static data points is within a predetermined range; and

evaluating the feature vector using a machine learning model to determine whether the executable file fits into one of the categories of files.

23. (Previously Presented) The computer-implemented method according to claim 22, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

24. (Previously Presented) The computer-implemented method according to claim 22, wherein the machine learning model comprises an artificial neural network.

25. (Previously Presented) The computer-implemented method according to claim 22, wherein the machine learning model comprises a support vector machine.

26. (Previously Presented) The computer-implemented method according to claim 22, wherein the machine learning model comprises a machine learning decision tree.

27. (Previously Presented) The computer-implemented method according to claim 22, wherein the machine learning model comprises a Bayesian network.

28. (Previously Presented) The computer-implemented method according to claim 22, wherein evaluating the feature vector using the machine learning model comprises evaluating the feature vector using support vector processing.

29. (Previously Presented) The computer-implemented method according to claim 22, wherein the machine learning model comprises a clustering model.

30. (Previously Presented) The computer-implemented method according to claim 22, wherein the executable file is identified in response to a detected condition.

31. (Previously Presented) The computer-implemented method according to claim 30, wherein the detected condition is user request for a file download.

32. (Previously Presented) The computer-implemented method according to claim 30, wherein the detected condition is the detection of a new file attempting to execute.

33. (Previously Presented) The computer-implemented method according to claim 22, wherein the plurality of static data points represent predefined character strings in the executable file.

34. (Canceled)

35. (Previously Presented) The computer-implemented method according to claim 22, wherein a determination of whether the executable file is harmful is used to retrain the classifier.

36. (Previously Presented) The computer-implemented method according to claim 22, further comprising preventing execution of the executable file based on classifying the executable file as harmful.

37. (Previously Presented) A computer-readable storage device containing instructions, that when executed on a processor, cause the processor to execute a process comprising:

identifying static data points that may be indicative of either a harmful or benign executable file;

associating the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;

identifying an executable file to be evaluated;

extracting a plurality of static data points from the executable file;

generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off based at least in part on evaluation of whether a value of one of the plurality of static data points is within a predetermined range; and

evaluating the feature vector using a machine learning model to determine whether the executable file fits into one of the categories of files.

38. (Previously Presented) The computer-readable storage device according to claim 37, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

39. (Previously Presented) The computer-readable storage device according to claim 37, wherein the machine learning model comprises an artificial neural network.

40. (Previously Presented) The computer-readable storage device according to claim 37, wherein the machine learning model comprises a support vector machine.

41. (Previously Presented) The computer-readable storage device according to claim 37, wherein the machine learning model comprises a machine learning decision tree.

42. (Previously Presented) The computer-readable storage device according to claim 37, wherein the machine learning model comprises a Bayesian network.

43. (Previously Presented) The computer-readable storage device according to claim 37, wherein evaluating the feature vector using the machine learning model comprises evaluating the feature vector using support vector processing.

44. (Previously Presented) The computer-readable storage device according to claim 37, wherein the machine learning model comprises a clustering model.

45. (Previously Presented) The computer-readable storage device according to claim 37, wherein the executable file is identified in response to a detected condition.

46. (Previously Presented) The computer-readable storage device according to claim 45, wherein the detected condition is user request for a file download.

47. (Previously Presented) The computer-readable storage device according to claim 45, wherein the detected condition is the detection of a new file attempting to execute.

48. (Previously Presented) The computer-readable storage device according to claim 37, wherein the plurality of static data points represent predefined character strings in the executable file.

49. (Canceled)

50. (Previously Presented) The computer-readable storage device according to claim 37, wherein a determination of whether the executable file is harmful is used to retrain the classifier.

51. (Currently Amended) The computer-readable storage device according to claim 37, ~~further comprising~~ wherein the process further comprises preventing execution of the executable file based on classifying the executable file as harmful.

52. (New) A system comprising:

at least one memory;

at least one processor configured to perform operation of:

identifying static data points that may be indicative of either a harmful or benign executable file; and

associating the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files; and

at least one processor configured to perform operation of:

identifying an executable file to be evaluated;

extracting a plurality of static data points from the executable file;

generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off based at least in part on evaluation of whether a value of one of the plurality of static data points is within a predetermined range; and

evaluating the feature vector using a machine learning model to determine whether the executable file fits into one of the categories of files.

53. (New) The system according to claim 52, wherein the plurality of static data points are extracted without decrypting or unpacking the executable file.

54. (New) The system according to claim 52, wherein the machine learning model comprises an artificial neural network.

55. (New) The system according to claim 52, wherein the machine learning model comprises a support vector machine.

56. (New) The system according to claim 52, wherein the machine learning model comprises a machine learning decision tree.

57. (New) The system according to claim 52, wherein the machine learning model comprises a Bayesian network.

58. (New) The system according to claim 52, wherein evaluating the feature vector using the machine learning model comprises evaluating the feature vector using support vector processing.

59. (New) The system according to claim 52, wherein the machine learning model comprises a clustering model.

60. (New) The system according to claim 52, wherein the executable file is identified in response to a detected condition.

61. (New) The system according to claim 60, wherein the detected condition is user request for a file download.

62. (New) The system according to claim 60, wherein the detected condition is the detection of a new file attempting to execute.

63. (New) The system according to claim 52, wherein the plurality of static data points represent predefined character strings in the executable file.

64. (New) The system according to claim 52, wherein a determination of whether the executable file is harmful is used to retrain the classifier.

65. (New) The system according to claim 52, further comprising at least one processor configured to perform operation of:

preventing execution of the executable file based on classifying the executable file as harmful.

REMARKS

Applicant appreciates the time taken by the Examiner to review Applicant's present application. Claims 2-9, 11-16, 18-20, 22-33, 35-48, and 50-65 are pending, with claims 2, 12, 18, 22, 37, and 52 being independent. Claim 51 has been amended. Claims 52-65 have been added. No new subject matter has been added.

Amendments to the Claims

Applicant appreciates the Examiner's prior allowance of claims 2-9, 11-16, 18-20, 22-33, 35-48, and 50-51. *See,* Notice of Allowance mailed April 15, 2022. New claims 52-65 are a set of "system" claims that corresponds to the previously allowed computer-implemented method claims 22-33 and 35-36 and computer-readable storage device claims 37-48 and 50-51. As such, claims 52-65 incorporate subject matter previously found to be allowable. Applicant therefore submits that claims 52-65 are similarly allowable.

Claim 51 is amended to recite "wherein the process further comprises . . ." Antecedent basis for "the process" is provided by claim 37, which recites "instructions, that when executed on a processor, cause the processor to execute a process . . ."

Conclusion

Applicant has made an earnest attempt to place this case in condition for allowance. Applicant respectfully requests full allowance of the pending claims. The Examiner is invited to telephone the undersigned at the number listed below for prompt action in the event any issues remain.

The Commissioner is hereby authorized to charge any deficiencies or credit any overpayment to Deposit Account No. 50-3183.

* * *

Respectfully submitted,

Sprinkle IP Law Group

/John L. Adair/

John L. Adair
Reg. No. 48,828

Dated: May 10, 2022

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. 512-637-9220
Fax. 512-371-9088

Electronic Patent Application Fee Transmittal

Application Number:	16791649
Filing Date:	14-Feb-2020
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:	OPEN7950-1

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($)
Miscellaneous:				
RCE- 2ND AND SUBSEQUENT REQUEST	1820	1	2000	2000
		Total in USD ($)		**2000**

Electronic Acknowledgement Receipt

EFS ID:	45680632
Application Number:	16791649
International Application Number:	
Confirmation Number:	2519
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:	OPEN7950-1
Receipt Date:	10-MAY-2022
Filing Date:	14-FEB-2020
Time Stamp:	17:45:10
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$2000
RAM confirmation Number	E202250H45334357
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	Request for Continued Examination (RCE)	OPEN7950-1_RCE05-10-22.pdf	39579 d4e3f05af000fdac9635e8ab23869a19c3f9a4ff	no	3
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
2		OPEN7950-1_SupplementalAmendment05-10-22.pdf	55689 a17b59cac19749cdcdc61245a7e6fa9a428308ec	yes	12

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment Submitted/Entered with Filing of Continued Prosecution Application (CPA)/Request for Continued Examination(RCE)	1	1
Claims	2	10
Applicant Arguments/Remarks Made in an Amendment	11	12

Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	38157 c257ec791f3e73c563dbd15089fa9244ca05cb10	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	133425		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

Electronic Patent Application Fee Transmittal

Application Number:	16791649
Filing Date:	14-Feb-2020
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:	OPEN7950-1

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:				
CLAIMS IN EXCESS OF 20	1202	13	100	1300
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**1300**

Electronic Acknowledgement Receipt

EFS ID:	45680670
Application Number:	16791649
International Application Number:	
Confirmation Number:	2519
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:	OPEN7950-1
Receipt Date:	10-MAY-2022
Filing Date:	14-FEB-2020
Time Stamp:	17:47:20
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$1300
RAM confirmation Number	E202250H47394398
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	Fee Worksheet (SB06)	fee-info.pdf	37980 7d0e03298cb8b0734c181c649aca127224b03a5b	no	2

Warnings:

Information:

Total Files Size (in bytes):	37980

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.

Doc Code: PET.AUTO Document Description: Petition automatically granted by EFS-Web	PTO/SB/140 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**PETITION TO WITHDRAW AN APPLICATION FROM ISSUE AFTER PAYMENT OF THE ISSUE FEE UNDER 37 CFR 1.313(c)**
Application Number	16791649
Filing Date	14-Feb-2020
First Named Inventor	Mauritius Schmidtler
Art Unit	2493
Examiner Name	
Attorney Docket Number	OPEN7950-1
Title	AUTOMATIC THREAT DETECTION OF EXECUTABLE FILES BASED ON STATIC DATA ANALYSIS

An application may be withdrawn from issue for further action upon petition by the applicant. To request that the Office withdraw an application from issue, applicant must file a petition under this section including the fee set forth in § 1.17(h) and a showing of good and sufficient reasons why withdrawal of the application from issue is necessary.

APPLICANT HEREBY PETITIONS TO WITHDRAW THIS APPLICATION FROM ISSUE UNDER 37 CFR 1.313(c).

A grantable petition requires the following items:
(1) Petition fee; and
(2) One of the following reasons:
(a) Unpatentability of one or more claims, which must be accompanied by an unequivocal statement that one or more claims are unpatentable, an amendment to such claim or claims, and an explanation as to how the amendment causes such claim or claims to be patentable;
(b) Consideration of a request for continued examination in compliance with § 1.114 (for a utility or plant application only); or
(c) Express abandonment of the application. Such express abandonment may be in favor of a continuing application, but not a CPA under 37 CFR 1.53(d).

Petition Fee

○	Small Entity
○	Micro Entity
◉	Regular Undiscounted

Reason for withdrawal from issue

◯ One or more claims are unpatentable ◉ Consideration of a request for continued examination (RCE) (List of Required Documents and Fees) ◯ Applicant hereby expressly abandons the instant application (any attorney/agent signing for this reason must have power of attorney pursuant to 37 CFR 1.32(b)).
RCE request,submission, and fee. ☒ I certify, in accordance with 37 CFR 1.4(d)(4) that : The RCE request ,submission, and fee have already been filed in the above-identified application on 2022.05.10 ☐ Are attached.
THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES I certify, in accordance with 37 CFR 1.4(d)(4) that I am: ◉ An attorney or agent registered to practice before the Patent and Trademark Office who has been given power of attorney in this application. ◯ An attorney or agent registered to practice before the Patent and Trademark Office, acting in a representative capacity. ◯ A sole inventor ◯ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application ◯ A joint inventor; all of whom are signing this e-petition

Signature	/John Adair/
Name	John Adair
Registration Number	48828

Electronic Patent Application Fee Transmittal

Application Number:	16791649
Filing Date:	14-Feb-2020
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
Attorney Docket Number:	OPEN7950-1

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
PETITION FEE- 37 CFR 1.17(H) (GROUP III)	1464	1	140	140
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**140**

UNITED STATES PATENT AND TRADEMARK OFFICE

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

Decision Date : May 10, 2022

In re Application of :

Mauritius Schmidtler

DECISION ON PETITION

UNDER CFR 1.313(c)(2)

Application No : 16791649

Filed : 14-Feb-2020

Attorney Docket No : OPEN7950-1

This is an electronic decision on the petition under 37 CFR 1.313(c)(2), filed May 10, 2022 , to withdraw the above-identified application from issue after payment of the issue fee.

The petition is **GRANTED.**

The above-identified application is withdrawn from issue for consideration of a submission under 37 CFR 1.114 (request for continued examination). See 37 CFR 1.313(c)(2).

Petitioner is advised that the issue fee paid in this application cannot be refunded. If, however, this application is again allowed, petitioner may request that it be applied towards the issue fee required by the new Notice of Allowance.

Telephone inquiries concerning this decision should be directed to the Patent Electronic Business Center (EBC) at 866-217-9197.

This application file is being referred to Technology Center AU 2493 for processing of the request for continuing examination under 37 CFR 1.114 .

Office of Petitions

Electronic Acknowledgement Receipt

EFS ID:	45680797
Application Number:	16791649
International Application Number:	
Confirmation Number:	2519
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
Filer Authorized By:	
Attorney Docket Number:	OPEN7950-1
Receipt Date:	10-MAY-2022
Filing Date:	14-FEB-2020
Time Stamp:	17:58:11
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$140
RAM confirmation Number	E202250H58064550
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	ePetition Request Form	petition-request.pdf	40076 8b425b6a6f82a5b89e02473556192d77f5878380	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	38212 b45510cc6a3fc6bc9c2667b3a32a484cbd86f50d	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	78288		

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

Office of the Chief Financial Officer

Document Code:WFEE

User :69169

Sale Accounting Date:05/18/2022

Sale Item Reference Number	Effective Date
16791649	05/10/2022

Document Number	Fee Code	Fee Code Description	Amount Paid	Payment Method
I20225HM29552611	1201	INDEPENDENT CLAIMS IN EXCESS OF 3	$480.00	Deposit Account

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

109422 7590 06/15/2022

Sprinkle IP Law Group/OPEN
1301 W. 25th Street, Suite 400
Austin, TX 78705

EXAMINER
SIMITOSKI, MICHAEL J

ART UNIT	PAPER NUMBER
2493	

DATE MAILED: 06/15/2022

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/791,649	02/14/2020	Mauritius Schmidtler	OPEN7950-1	2519

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	$1200	$0.00	$1200.00	$0	09/15/2022

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. 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)

109422 7590 06/15/2022
Sprinkle IP Law Group/OPEN
1301 W. 25th Street, Suite 400
Austin, TX 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.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/791,649	02/14/2020	Mauritius Schmidtler	OPEN7950-1	2519

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	$1200	$0.00	$1200.00	$0	09/15/2022

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/AIA/122 or PTO/SB/122) attached.

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

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

1 _____
2 _____
3 _____

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

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document 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. 1002
Page 309 of 347

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.
16/791,649	02/14/2020	Mauritius Schmidtler	OPEN7950-1	2519

109422 7590 06/15/2022

Sprinkle IP Law Group/OPEN
1301 W. 25th Street, Suite 400
Austin, TX 78705

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2493	

DATE MAILED: 06/15/2022

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. 16/791,649	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 reply dated 2/8/2022.
   ☐ 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. _____.
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: 2-9,11-16,18-20,22-33,35-48 and 50-51

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 5/10/2022 was received and considered.

3. Claims 2-9, 11-16, 18-20, 22-33, 35-48 and 50-65 are pending.

Terminal Disclaimer

4. The terminal disclaimer filed on 8/11/2021 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of **10,599,844** has been reviewed and is accepted. The terminal disclaimer has been recorded.

Allowable Subject Matter

5. Claims 2-9, 11-16, 18-20, 22-33, 35-48 and 50-65 are allowed.

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

a. Note application 14/709,875 for previous search and prosecution histories.

b. The Forman reference teaches, in the same field of endeavor as the claimed invention, selectively turning on/off one or more features of a generated feature vector based on the number of classifiers associated with the features for the benefit of efficiency. However, the prior art, either alone or in a reasonable combination, fails to teach selectively turning on/off one or more features of the generated feature vector based at least in part on evaluation of whether a value of one of the plurality of static data points is within a predetermined range, as recited within the framework of claimed invention 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 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 published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: https://patentcenter.uspto.gov. Visit https://www.uspto.gov/patents/apply/patent-center for more information about Patent Center and https://www.uspto.gov/patents/docx for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Michael Simitoski/
Primary Examiner, Art Unit 2493

June 6, 2022

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/791,649	Schmidtler et al.
	Examiner	Art Unit
	MICHAEL J SIMITOSKI	2493

CPC - Searched*		
Symbol	Date	Examiner
G06F 21/51,53,562,56,565,566; 2221/033; 8/53 | G06N 20/00,10 | H04L 63/145	06/06/2022	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.

Search Notes		
Search Notes	Date	Examiner
EAST, NPL and inventor search performed (see EAST and NPL search histories, attached and/or previously made of record)	06/06/2022	MJS
Consulted Common Citation Document and Global Dossier for related/family applications and prosecution histories	06/06/2022	MJS

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
G06F	21/51,53,562,56,565,566; 2221/033; 8/53	06/06/2022	MJS
G06N	20/00,10	06/06/2022	MJS
H04L	63/145	06/06/2022	MJS

/Michael Simitoski/ Primary Examiner, Art Unit 2493	

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/791,649	Schmidtler et al.
	Examiner	**Art Unit**
	MICHAEL J SIMITOSKI	2493

CPC								
Symbol							**Type**	**Version**
G06F	/	21	/	565			F	2013-01-01
G06F	/	21	/	562			I	2013-01-01
G06N	/	20	/	10			I	2019-01-01
G06N	/	20	/	00			I	2019-01-01
G06F	/	2221	/	033			A	2013-01-01
G06F	/	8	/	53			A	2013-01-01

CPC Combination Sets									
Symbol							**Type**	**Set**	**Ranking**	**Version**
	/		/							

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	59	
/Michael Simitoski/ Primary Examiner, Art Unit 2493	06 June 2022	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

U.S. Patent and Trademark Office — Part of Paper No.: 20220606

Sophos Ex. 1002
Page 317 of 347

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/791,649	Schmidtler et al.
	Examiner	**Art Unit**
	MICHAEL J SIMITOSKI	2493

INTERNATIONAL CLASSIFICATION				
CLAIMED				
G06F	/	21	/	56
G06N	/	5	/	04

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)	59	
/Michael Simitoski/ Primary Examiner, Art Unit 2493	06 June 2022	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

U.S. Patent and Trademark Office

Part of Paper No.: 20220606

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/791,649	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		10	16	19	24	28	32	37	41	46	49	55	58	64
1	2	9	11	17	20	25	29	33	38	42	47	50	56	59	65
2	3	10	12		21	26	30	34	39	43	48	51	57		
3	4	11	13	18	22	27	31	35	40		49	52	58		
4	5	12	14	19	23	28	32	36	41	44	50	53	59		
5	6	13	15	20	24	29	33	37	42	45	51	54	60		
6	7	14	16	21	25		34	38	43	46	52	55	61		
7	8		17	22	26	30	35	39	44	47	53	56	62		
8	9	15	18	23	27	31	36	40	45	48	54	57	63		

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 59	
/Michael Simitoski/ Primary Examiner, Art Unit 2493 (Primary Examiner)	06 June 2022 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 3

U.S. Patent and Trademark Office

Part of Paper No.: 20220606

Bibliographic Data

Application No: 16/791,649

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.
02/14/2020	726	2493	OPEN7950-1
RULE			

APPLICANTS

Webroot Inc., Broomfield, CO,

INVENTORS

Mauritius Schmidtler, Escondido, CA, UNITED STATES

Gaurav Dalal, San Jose, CA, UNITED STATES

Reza Yoosoofmiya, San Diego, CA, UNITED STATES

CONTINUING DATA

This application is a CON of 14709875 05/12/2015 PAT 10599844

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

03/02/2020

STATE OR COUNTRY

UNITED STATES

ADDRESS

Sprinkle IP Law Group/OPEN
1301 W. 25th Street, Suite 400
Austin, TX 78705
UNITED STATES

FILING FEE RECEIVED

$1,720

CCD view for US202016791649

#	CC	Cat.	Citation details
1	*US*		**Application N° US202016791649** (US16791649) - 14 February 2020
2	*US*		**Application N° US201514709875** (US14709875) - 12 May 2015
			National Search Report
			US9465940 B1 (CYLANCE INC [US]) - 11 October 2016
			US2007240220 A1 (TUVELL GEORGE, , et al) - 11 October 2007
			US2012079596 A1 (THOMAS RALPH [US], et al) - 29 March 2012
			US9197663 B1 (BIT9 INC [US]) - 24 November 2015
			US8719924 B1 (WILLIAMSON MATTHEW [US], et al) - 6 May 2014
			US2014165203 A1 (SOURCEFIRE INC [US]) - 12 June 2014
			US2010192222 A1 (MICROSOFT CORP [US]) - 29 July 2010
		X	US8709924 B2 (HANAWA HIROJI [US], et al) - 29 April 2014 * claim 1 ¦ column 1 lines 57 - 67] ¦ column 2 lines 37 - 40] ¦ column 3 lines 1 - 6] abstract ¦ column 6 lines 4 - 26] Fig. 1 ¦ column 3 lines 1
		Y	US2007240220 A1 (TUVELL GEORGE, , et al) - 11 October 2007 * [0104] ¦ [0161] ¦ [0336] Fig. 9 ¦ [0162] ¦ abs ¦ [0163] Fig. 7 ¦ [0323], [0336] Fig. 9 ¦ [0323] ¦ abstract ¦ [0009] ¦ [0011] ¦ claim 4 ¦ claim
		Y	US9197663 B1 (BIT9 INC [US]) - 24 November 2015 * column 2 lines 17 - 20 and 47 - 52] ¦ column 3 lines 26 - 30] ¦ column 20 lines 44 - 61] ¦ abstract ¦ column 4 line 64 column 5 line 3] ¦ col
		Y	US2012079596 A1 (THOMAS RALPH [US], et al) - 29 March 2012 * [0239] ¦ [0175], [0225] and [0272] ¦ [0038], [0175], [0225] and [0272] ¦ table 4] and [0257] ¦ [0250] ¦ table 4] ¦ Fig. 8] ¦ [0250], [0251
		A	US8719924 B1 (WILLIAMSON MATTHEW [US], et al) - 6 May 2014
		A	US2014165203 A1 (SOURCEFIRE INC [US]) - 12 June 2014
		A	US9465940 B1 (CYLANCE INC [US]) - 11 October 2016
		A	US2010192222 A1 (MICROSOFT CORP [US]) - 29 July 2010
			US8510836 B1 (NACHENBERG CAREY S [US], et al) - 13 August 2013
			US8719924 B1 (WILLIAMSON MATTHEW [US], et al) - 6 May 2014
			US9197663 B1 (BIT9 INC [US]) - 24 November 2015
			US9465940 B1 (CYLANCE INC [US]) - 11 October 2016
			US2007240220 A1 (TUVELL GEORGE, , et al) - 11 October 2007
			US2009013405 A1 (MESSAGELABS LTD [GB]) - 8 January 2009
			US2009274376 A1 (YAHOO INC [US]) - 5 November 2009
			US2009300765 A1 (DEUTSCHE TELEKOM AG [DE]) - 3 December 2009
			US20100082642 A1 (Forman George, , et al) - 1 April 2010
			US2010192222 A1 (MICROSOFT CORP [US]) - 29 July 2010
			US2012079596 A1 (THOMAS RALPH [US], et al) - 29 March 2012
			US2012227105 A1 (FRIEDRICHS OLIVER [US], et al) - 6 September 2012
			US2013291111 A1 (ZHOU HONGYI [CN], et al) - 31 October 2013
			US2014165203 A1 (SOURCEFIRE INC [US]) - 12 June 2014
			US2014310517 A1 (IBM [US]) - 16 October 2014
			US20160021174 A1 (TELEFONICA DIGITAL ESPANA SLU [ES]) - 21 January 2016
			US2016156646 A1 (HEWLETT PACKARD DEVELOPMENT CO [US]) - 2 June 2016
			US2017262633 A1 (BLUVECTOR INC [US]) - 14 September 2017
			US2018365573 A1 (INTEL CORP [US]) - 20 December 2018
			Detection of malicious code by applying machine learning classifiers on static features: A state-of-the-art survey Authors: Shabtai A, Moskovitch R, Elovici Y, Glezer C Publication data: Information Security Technical Report, 20090201 Elsevier Advanced Technology, AMSTERDAM, NL Source info: Vol: 14, Nr: 1, Page(s): 16 - 29

Sophos Ex. 1002
Page 321 of 347

#	CC	Cat.	Citation details
			Detection of malicious code by applying machine learning classifiers on static features: A state-of-the-art survey Authors: Shabtai A, Moskovitch R, Elovici Y, Glezer C Publication data: Information Security Technical Report, 20090201 Elsevier Advanced Technology, AMSTERDAM, NL Source info: Vol: 14, Nr: 1, Page(s): 16 - 29
			Non-patent literature - Bost, Raphael, et al. "Machine learning classification over encrypted data." NDSS. vol. 4324. 2015. (Year: 2015).
			Non-patent literature - Choi, Junho, et al. "Efficient malicious code detection using n-gram analysis and SVM." 2011 14th International Conference on Network-Based
			Non-patent literature - Devi, Dhruwajita, and Sukumar Nandi. "Detection of packed malware." Proceedings of the First International Conference on Security of Intern
			Non-patent literature - Dube, Thomas, et al. "Malware target recognition via static heuristics." Computers & Security 31.1 (2012): 137-147. (Year: 2012).
			Non-patent literature - Merkel, Ronny, et al. "Statistical detection of malicious pe-executables for fast offline analysis." IFIP International Conference on Communicati
			Non-patent literature - Singla, Sanjam, et al. "A Novel Approach to Malware Detection using Static Classification." International Journal of Computer Science and Info
			Non-patent literature - Tabish, S. Momina, M. Zubair Shafiq, and Muddassar Farooq. "Malware detection using statistical analysis of byte-level file content." Proceedin
			Non-patent literature - Treadwell, Scott, and Mian Zhou. "A heuristic approach for detection of obfuscated malware." 2009 IEEE International Conference on Intelliger
			Applicant
			Non-patent literature - International Patent Application No. PCT/US2016/032090, International Search Report and Written Opinion dated Jul. 29, 2016, 13 pages.
			Non-patent literature - Perdisci et al. (2008) Pattern Recognition Letters 29:1941-1946 "Classification of packed executables for accurate computer virus detection".
			Non-patent literature - Perdisci et al. (2008) IEEE. Annual Computer Security Applications Conference 301-310 "McBoost: Boosting Scalability in Malware Collection a
			Non-patent literature - Khan, Hassan et al., "Determining Malicious Executable Distinguishing Attributes and Low-Complexity Detection", J. Comput Virol, 7.2 (2011),
			Non-patent literature - Kolter, J. Zico et al., "Learning to Detect and Classift Malicious Executables in the Wild", Journal of Machine Learning Research 7 (2006), pp. 2
			Non-patent literature - International Patent Application No. PCT/US2016/032090, International Preliminary Report on Patentability dated Nov. 14, 2017, 7 pages.
3	WO		**Application N° WO2016US32090** (WOUS2016/032090) - 12 May 2016
			International Search Report
		A	US2010192222 A1 (MICROSOFT CORP [US]) - 29 July 2010 * sentences 3 - 6, paragraph [0019] * * sentences 9 - 11, paragraph [0032] *
		X I	***Classification of packed executables for accurate computer virus detection*** Authors: Perdisci R, Lanzi A, Lee W Publication data: PATTERN RECOGNITION LETTERS, 20081015 ELSEVIER, AMSTERDAM, NL Source info: Vol: 29, Nr: 14, Page(s): 1941 - 1946 * page 1942, column left, lines 10 - 14, 41 - 42, 51 - 53; figure 1 * * page 1943, column left, lines 9 - 14 * * section 4 "Experiments"; page 1944, column right, lines 6 - 9, 24, 25, 28 * * page 1945; table 1 *
		A	***McBoost: Boosting Scalability in Malware Collection and Analysis Using Statistical Classification of Executables*** Authors: Roberto Perdisci, Andrea Lanzi, Wenke Lee Publication data: Computer Security Applications Conference, 2008. ACSAC 2008. Annual, 20081208 IEEE, Piscataway, NJ, USA Source info: Page(s): 301 - 310 * page 304, column left *

Search History

Report Run Date: 2022-04-05 UTC
Searches: 6
Markers: 0

Sophos Ex. 1002
Page 323 of 347

Search #	Timestamp	Results	Page
1	2022-04-05 10:21 UTC	~2,251,723	3
2	2022-04-05 10:21 UTC	~1,050,892	4
3	2022-04-05 10:22 UTC	~889,867	4
4	2022-04-05 10:22 UTC	~16,872	4
5	2022-04-05 10:22 UTC	~18,682	4
6	2022-04-05 10:23 UTC	~2593	5

Content: Patents + NPL (187)

US Patents | US Designs | US Applications | EPO Patents | EPO Applications | China Patents | China Applications | Japan Patents | Japan Applications | Korea Patents | Korea Applications | WIPO Applications | Argentina Patents | Argentina Applications | Brazil Patents | Brazil Applications | Canada Patents | Canada Applications | Chile Patents | Chile Applications | Colombia Applications | Costa Rica Applications | Cuba Patents | Cuba Applications | Dominican Republic Applications | Ecuador Patents | Ecuador Applications | El Salvador Applications | Guatemala Applications | Honduras Applications | Mexico Patents | Mexico Applications | Nicaragua Patents | Panama Applications | Peru Applications | Trinidad & Tobago Patents | Uruguay Applications | Austria Patents | Austria Applications | Belarus Patents | Belgium Patents | Belgium Applications | Bosnia & Herzegovina Patents | Bosnia & Herzegovina Applications | Bulgaria Patents | Bulgaria Applications | Croatia Patents | Croatia Applications | Czech Republic Patents | Czech Republic Applications | Czechoslovakia Patents | Czechoslovakia Applications | Denmark Patents | Denmark Applications | Estonia Patents | Estonia Applications | EUIPO Patents | Finland Patents | Finland Applications | France Patents | France Applications | Germany Patents | Germany Applications | Great Britain Patents | Great Britain Applications | Greece Patents | Greece Applications | Hungary Patents | Hungary Applications | Iceland Patents | Iceland Applications | Ireland Patents | Ireland Applications | Italy Patents | Italy Applications | Latvia Patents | Latvia Applications | Lithuania Patents | Lithuania Applications | Luxembourg Patents | Malta Patents | Monaco Patents | Montenegro Patents | Montenegro Applications | Netherlands Patents | Netherlands Applications | Norway Patents | Norway Applications | Poland Patents | Poland Applications | Portugal Patents | Portugal Applications | Republic of Moldova Patents | Republic of Moldova Applications | Romania Patents | Romania Applications | San Marino Patents | San Marino Applications | Serbia Patents | Serbia Applications | Slovakia Patents | Slovakia Applications | Slovenia Patents | Spain Patents | Spain Applications | Sweden Patents | Sweden Applications | Switzerland Patents | Switzerland Applications | Ukraine Patents | Yugoslavia/Serbia and Montenegro Patents | Yugoslavia/Serbia and Montenegro Applications | Armenia Patents | Australia Patents | Australia Applications | Cyprus Patents | Gulf Cooperation Council Patents | Hong Kong Patents | India Patents | India Applications | Indonesia Patents | Indonesia Applications | Israel Applications | Jordan Patents | Kyrgyzstan Patents | Macao Applications | Malaysia Patents | Mongolia Patents | New Zealand Patents | Philippines Patents | Philippines Applications | Saudi Arabia Patents | Singapore Patents | Singapore Applications | Taiwan Patents | Taiwan Applications | Tajikistan Patents | Tajikistan Applications | Thailand Applications | Uzbekistan Patents | Vietnam Patents | Algeria Patents | ARIPO Patents | ARIPO Applications | Egypt Patents | Kenya Patents | Malawi Patents | Morocco Patents | Morocco Applications | OAPI Patents | South Africa Patents | Tunisia Applications | Zambia Patents | Zimbabwe Patents | EAPO Patents | EAPO Applications | Georgia Patents | Georgia Applications | Kazakhstan Patents | Kazakhstan Applications | Russia Patents | Russia Applications | Turkey Patents | Turkey Applications | IEEE Xplore Publications: IEEE Periodicals | IEEE Xplore Publications: IEEE Conferences | IEEE Xplore Publications: IEEE Standards | IEEE Xplore Publications: IEEE Early Access | IEEE Xplore Publications: SMPTE Periodicals | IEEE Xplore Publications: SMPTE Conferences | IEEE Xplore Publications: SMPTE Standards | IEEE Xplore Publications: MIT Press eBooks | IEEE Xplore Publications: Wiley-IEEE eBooks | IEEE Xplore Publications: IBM Periodicals | IEEE Xplore Publications: URSI Periodicals | IEEE Xplore Publications: VDE Conferences | IEEE Xplore Publications: Periodicals from China | IP.com Prior Art Database: The IP.com Journal | IP.com Prior Art Database: Internet Society RFC | IP.com Prior Art Database: IBM TDB Archive | IP.com Prior Art Database: Legacy Journals | IP.com Prior Art Database: Software Patent Institute | OnePetro.org: Periodicals at OnePetro.org | OnePetro.org: Conferences at OnePetro.org | Other Literature: IBM Redbooks | Other Literature: PubMed Central | Other Literature: arXiv.org

1 **2022-04-05 10:21 UTC | ~2,251,723 results from**

De-Dup: Simple Family Numbers (PAT only) | **Cut-off:** None | **Sort:** Relevance

Main Concept: Text
machine learning ignore features

Sophos Ex. 1002
Page 325 of 347

Concept Modifiers: None

Filters: None

2 **2022-04-05 10:21 UTC | ~1,050,892 results from**

De-Dup: Simple Family Numbers (PAT only) | **Cut-off:** None | **Sort:** Relevance

Main Concept: Same as Search 1

Concept Modifiers: None

Filters (1):
Title+Abstract+Body/Description+Related Terms limited to: vector

3 **2022-04-05 10:22 UTC | ~889,867 results from**

De-Dup: Simple Family Numbers (PAT only) | **Cut-off:** None | **Sort:** Relevance

Main Concept: Same as Search 1

Concept Modifiers: None

Filters (2):
Title+Abstract+Body/Description+Related Terms limited to: vector
Title+Abstract+Body/Description+Related Terms limited to: svm; clustering; neural; bayes; bayesian; "decision tree"; "support vector"

4 **2022-04-05 10:22 UTC | ~16,872 results from**

De-Dup: Simple Family Numbers (PAT only) | **Cut-off:** None | **Sort:** Relevance

Main Concept: Same as Search 1

Concept Modifiers: None

Filters (3):
Title+Abstract+Body/Description+Related Terms limited to: vector
Title+Abstract+Body/Description+Related Terms limited to: svm; clustering; neural; bayes; bayesian; "decision tree"; "support vector"
Title+Abstract+Body/Description+Related Terms limited to: antivirus; malware

5 **2022-04-05 10:22 UTC | ~18,682 results from**

De-Dup: Simple Family Numbers (PAT only) | **Cut-off:** None | **Sort:** Relevance

Main Concept: Text
machine learning ignore feature range

Concept Modifiers: None

Filters: Same as Search 4

Sophos Ex. 1002
Page 326 of 347

6 **2022-04-05 10:23 UTC | ~2593 results from**

De-Dup: Simple Family Numbers (PAT only) | **Cut-off:** None | **Sort:** Relevance

Main Concept: Text
machine learning ignore feature range outlier

Concept Modifiers: None

Filters: Same as Search 4

Sophos Ex. 1002
Page 327 of 347

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L158	126	((("Schmidtler") near3 ("Mauritius"))).INV. ((("Dalal") near3 ("Gaurav"))).INV. ((("Yoosoofmiya") near3 ("Reza"))).INV.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/04/05 06:19 AM
L159	22	(@ad<"20150512" @prad<"20150512") AND bayes$3 SAME (SVM (support ADJ vector)) SAME (decision ADJ tree) SAME clustering SAME (machine ADJ learn$4) AND (malware)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/04/05 06:19 AM
L160	11	(@ad<"20150512" @prad<"20150512") AND (machine ADJ learning) AND (feature ADJ vector) AND (exclu$4 (turn$4 ADJ off) omit$4 omission ignor$4) near2 (feature (data ADJ point)) WITH (range threshold deviat$4 outlier)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/04/05 06:19 AM

PE2E SEARCH - Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
N149	10	N141 and (((turn$4 adj off) disregard$4 exclu$4 ignor$4) near2 (feature)).clm. and classifier.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/05 06:20 AM
N150	49	(((turn$4 ADJ off) disregard$4 exclu$4 ignor$4) near2 (feature)).clm. AND classifier.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/05 06:33 AM
N151	0	(((turn$4 ADJ off)) near2 (feature)).clm. AND classifier.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/05 06:33 AM

N152	8	(((selectively)) near2 (feature)).clm. AND classifier.clm.	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/05 06:33 AM

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 06/15/2022
Sprinkle IP Law Group/OPEN
1301 W. 25th Street, Suite 400
Austin, TX 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.

Shenise Ramdeen	(Typed or printed name)
/Shenise Ramdeen/	(Signature)
June 21, 2022	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/791,649	02/14/2020	Mauritius Schmidtler	OPEN7950-1	2519

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	$1200	$0.00	$1200.00	$0	09/15/2022

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/AIA/122 or PTO/SB/122) attached.

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

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

1 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 /John L. Adair/ Date June 21, 2022

Typed or printed name John L. Adair Registration No. 48,828

Sophos Ex. 1002
Page 390 of 647

TRANSMITTAL OF PAYMENT OF ISSUE FEE (Undiscounted) 37 C.F.R. 1.311				Docket No. OPEN7950-1
First Named Inventor **Mauritius Schmidtler**				
Application No. **16/791,649**	Filing Date **02/14/2020**	Examiner **Michael J. Simitoski**	Group Art Unit **2493**	Confirmation No. **2519**
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: $1,200
- ☐ Amendment Under 1.312
- ☒ Comments on Statement of Reasons for 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.

/John L. Adair/

John L. Adair
Reg. No. 48,828

Customer No. 109422
Sprinkle IP Law Group
1301 W. 25th Street, Suite 400
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 and items referenced herein are being deposited electronically with the U.S. Patent and Trademark Office using the United States Patent and Trademark Office's EFS-Web system on June 21, 2022.

/Shenise Ramdeen/
Shenise Ramdeen

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
Comments on Statement of Reasons for Allowance	Atty. Docket No. **OPEN7950-1**

First Named Inventor **Mauritius Schmidtler**	
Application Number **16/791,649**	Date Filed **February 14, 2020**
Title **Automatic Threat Detection Of Executable Files Based On Static Data Analysis**	
Group Art Unit **2493**	Examiner **Michael J. Simitoski**
Confirmation Number **2519**	

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 **June 21, 2022.**

/Shenise Ramdeen/
Shenise Ramdeen

Applicant appreciates the allowance of Claims 2-9, 11-16, 18-20, 22-33, 35-48 and 50-65 of United States Patent Application No. 16/791,649. Applicant submits that 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 that 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 that such limitations or interpretations (i) are inconsistent with the claim language, specification, or prior prosecution history; or (ii) identify any particular element of the claims as a reason for allowance in this case. Furthermore, Applicant does not acquiesce any characterization of the references.

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
Attorneys for Applicant

/John L. Adair/

John L. Adair
Reg. No. 48,828

Date: June 21, 2022

1301 W. 25th Street, Suite 400
Austin, TX 78705
Tel. (512) 637-9220
Fax. (512) 371-9088

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 06/15/2022
Sprinkle IP Law Group/OPEN
1301 W. 25th Street, Suite 400
Austin, TX 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.

Shenise Ramdeen	(Typed or printed name)
/Shenise Ramdeen/	(Signature)
June 21, 2022	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/791,649	02/14/2020	Mauritius Schmidtler	OPEN7950-1	2519

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	$1200	$0.00	$1200.00	$0	09/15/2022

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/AIA/122 or PTO/SB/122) attached.

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

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

1 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	(B) RESIDENCE: (CITY and STATE OR COUNTRY)
Webroot Inc.	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 /John L. Adair/ Date June 21, 2022

Typed or printed name John L. Adair Registration No. 48,828

Electronic Acknowledgement Receipt

EFS ID:	46009714
Application Number:	16791649
International Application Number:	
Confirmation Number:	2519
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:	OPEN7950-1
Receipt Date:	21-JUN-2022
Filing Date:	14-FEB-2020
Time Stamp:	17:45:15
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	OPEN7950-1_IssueFeeTrans06-21-22.pdf	18727 ebe257eb97a577d4225a8715f7fe86f8e46070d7	no	1

Warnings:

Information:					
2	Post Allowance Communication - Incoming	OPEN7950-1_Comments06-21-22.pdf	21612 61cd5252fb18890f2473677a35c3199715439c4a	no	2
Warnings:					
Information:					
3	Issue Fee Payment (PTO-85B)	OPEN7950-1_PTOL-85B06-21-22.pdf	183248 3b194a1ae215fe97e4412596536c840a11b79542	no	1
Warnings:					
Information:					
			Total Files Size (in bytes):	223587	

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

Office of the Chief Financial Officer

Document Code:WFEE

User :C44690

Sale Adjustment Accounting Date:06/22/2022

Effective Date	Sale Accounting Date	Sale Item Reference Number
04/15/2022	06/22/2022	16791649

Document Number	Fee Code	Fee Code Description	Amount Paid	Payment Method
I20226LG07240829	1501	UTILITY APPL ISSUE FEE	$1,200.00	DA

United States Patent and Trademark Office

Office of the Chief Financial Officer

Document Code:WFEE

User :C44690

Refund Accounting Date:06/22/2022

Effective Date	Sale Item Reference Number	Refund Total
04/15/2022	16791649	$1,200.00

Document Number	Fee Code	Fee Code Description	Amount Paid	Payment Method	Account Number
I20226LG07240829	1501	UTILITY APPL ISSUE FEE	$1,200.00	DA	503183

United States Patent and Trademark Office

Office of the Chief Financial Officer

Document Code:WFEE

User :C44690

Sale Accounting Date:06/22/2022

Sale Item Reference Number	Effective Date
16791649	06/21/2022

Document Number	Fee Code	Fee Code Description	Amount Paid	Payment Method
I20226LG10060915	1501	UTILITY APPL ISSUE FEE	$1,200.00	Deposit Account

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.
16/791,649	08/09/2022	11409869	OPEN7950-1	2519

109422 7590 07/20/2022

Sprinkle IP Law Group/OPEN
1301 W. 25th Street, Suite 400
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 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

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

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

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Patents Stakeholder Experience (OPSE), Stakeholder Support Division (SSD) at (571)-272-4200.

INVENTOR(s) (Please see PAIR WEB site http://pair.uspto.gov for additional inventors):

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

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Webroot Inc., Broomfield, CO;

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

AO 120 (Rev. 08/10)

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

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

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

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

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

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above---entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☑ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
8/31/2022		
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 11,409,869	8/9/2022	Webroot, Inc.
2 8,719,932	5/6/2014	Webroot, Inc.
3 8,201,243	6/12/2012	Webroot, Inc.
4 8,181,244	5/15/2012	Webroot, Inc.
5 8,856,505	10/7/2014	Webroot, Inc.

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

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

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

AO 120 (Rev. 08/10)

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

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

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

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:22-cv-00240	3/4/2022	Western District of Texas, Waco Division

PLAINTIFF	DEFENDANT
Webroot, Inc. and OpenText Inc.	Sophos Ltd.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above---entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY
9/8/2022	☑ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 11,409,869	8/9/2022	Webroot, Inc.
2		
3		
4		
5		

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

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

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

AO 120 (Rev. 08/10)

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

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

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

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

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

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1			
2			
3			
4			
5			

In the above---entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED 9/7/2022

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

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

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

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

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

AO 120 (Rev. 08/10)

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

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

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

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:22-cv-00243	3/4/2022	Western District of Texas, Waco Division

PLAINTIFF	DEFENDANT
Webroot, Inc. and OpenText Inc.	AO Kaspersky Lab

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1			
2			
3			
4			
5			

In the above---entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY
9/1/2022	☑ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	11,409,869	8/9/2022	Webroot, Inc.
2			
3			
4			
5			

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

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

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

AO 120 (Rev. 08/10)

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

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

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

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:22-cv-00342	3/31/2022	Western District of Texas, Waco Division

PLAINTIFF	DEFENDANT
Webroot, Inc. and OpenText Inc.	ForcePoint LLC

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above---entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY
9/8/2022	☑ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 11,409,869	8/9/2022	Webroot, Inc.
2		
3		
4		
5		

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

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

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

AO 120 (Rev. 08/10)

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

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court WESTERN DISTRICT OF TEXAS on the following

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

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:22-cv-00240	10/27/2022	WESTERN DISTRICT OF TEXAS

PLAINTIFF	DEFENDANT
WEBROOT, INC. and OPEN TEXT, INC.	SOPHOS LTD.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,418,250	4/9/2013	Webroot, Inc.
2	8,726,389	5/13/2014	Webroot, Inc.
3	9,578,045	2/21/2017	Webroot, Inc.
4	10,257,224	4/9/2019	Webroot, Inc.
5	10,284,591	5/7/2019	Webroot, Inc.

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading		
	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	10,499,844	12/10/2019	Webroot, Inc.
2	9,413,721	8/9/2016	Webroot, Inc.
3	11,409,869	8/9/2022	Webroot, Inc.
4			
5			

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

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

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

AO 120 (Rev. 08/10)

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

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court WESTERN DISTRICT OF TEXAS on the following

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

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:22-cv-00243	10/27/2022	WESTERN DISTRICT OF TEXAS

PLAINTIFF	DEFENDANT
WEBROOT, INC. and OPEN TEXT, INC.	AO KASPERSKY LAB

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,418,250	4/9/2013	Webroot, Inc.
2	8,726,389	5/13/2014	Webroot, Inc.
3	9,578,045	2/21/2017	Webroot, Inc.
4	10,257,224	4/9/2019	Webroot, Inc.
5	10,284,591	5/7/2019	Webroot, Inc.

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 10,499,844	12/10/2019	Webroot, Inc.
2 11,409,869	08/09/2022	Webroot, Inc.
3		
4		
5		

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

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

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