

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

WEBROOT, INC. and	)	
OPEN TEXT, INC.,	)	
	)	
Plaintiffs,	)	
v.	)	Civil Action No. 6:22-cv-00239
	)	
TREND MICRO INC.,	)	JURY TRIAL DEMANDED
	)	
Defendant.	)	
_____	)	

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiffs Webroot, Inc. (“Webroot”) and Open Text, Inc. (“OpenText”) (collectively “Plaintiffs”) allege against Trend Micro Inc. (“Trend Micro” or “Defendant”) the following:

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

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

82. 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.

83. 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.)

84. 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.)

85. 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.

86. 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 systems 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.)

87. 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 techniques 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.)

88. 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.)

89. 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.)

90. 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.)

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 (DC 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.*