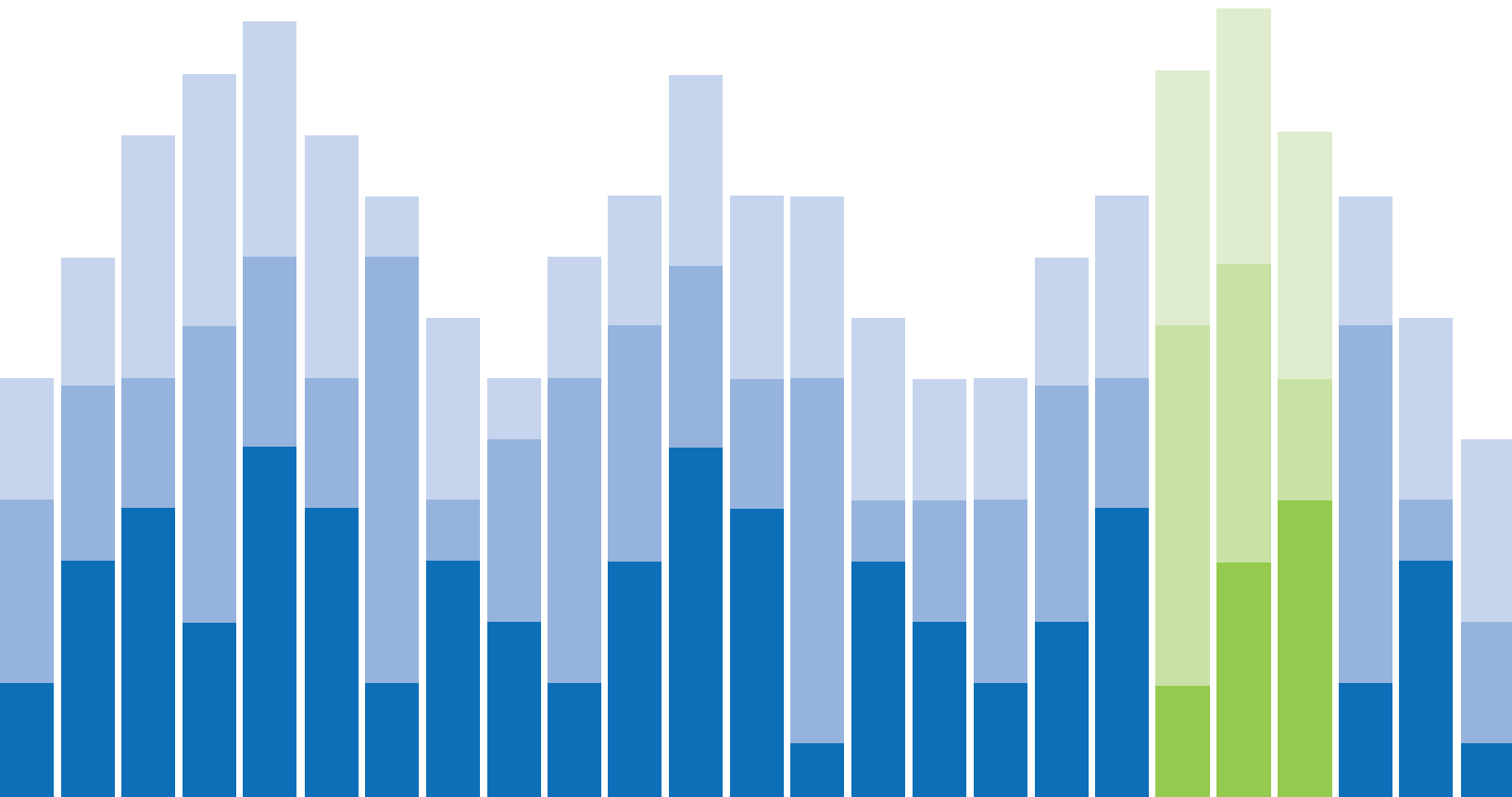
WEBROOT®
Smarter Cybersecurity™

QUARTERLY THREAT TRENDS

June 2017



Webroot Malware detection trends: Stopping Threats at the Network Edge

Organizations are being overwhelmed by malware and potentially unwanted applications (PUAs) such as spyware and adware. While malware and PUAs have been top-of-mind for organizations for years, 2017 brings a significant increase in the level of concern. Even though organizations continue to invest more and more of their IT budgets in security technologies, more attacks are succeeding. In particular, the popularity of ransomware has rapidly increased and it's causing major operational problems and damage to organizations' reputations.

First-generation antimalware technologies, such as signature-based antivirus software, are not effective at detecting and stopping current malware and PUAs on endpoints or networks. Sandboxing, endpoint protection suites, and other newer antimalware techniques offer much stronger malware and PUA detection capabilities. Unfortunately, these technologies are resource-intensive, queueing files for analysis and monitoring each file's behavior during execution, so they can introduce unacceptable latency that disrupts operations.

This report takes a closer look at the current state of malware and PUAs, and explains in more detail why traditional antivirus software and other antimalware technologies alone are not sufficient to protect organizations. The report then proposes a new machine learning-based technology that combats the challenges of zero-day, polymorphic, and highly targeted malware: Webroot BrightCloud® Streaming Malware Detection. Streaming Malware Detection blocks malicious files in transit at the network edge, without needing to download the entire file, and effectively complements existing antimalware solutions.

Today's Malware and PUAs

Malware and PUAs reach users through many mechanisms, including email, instant messaging, and drive-by downloads, where visiting a malicious website causes malware or PUA files to be transferred from the web server to the victim's computer. More than 85% of malware infections are occurring via web browsing. Basic internet use is a high-risk activity for every organization, regardless of size or sector, according to Webroot research.

Today's malware and PUAs have a staggering variety of purposes. Perhaps the most common among these is to extort money, which is illustrated best by headline-worthy ransomware families. Ransomware is a form of malware that takes control of a computer or its files and demands a ransom payment to relinquish control. In May 2017, the WannaCry ransomware infected computers all over the world and caused serious disruptions for hospitals and many other organizations. Webroot research shows that over 60% of companies have already been affected by ransomware, with the financial and retail sectors being hit the hardest.

Another common purpose for malware and PUAs is to gain remote access to and control over a computer. Attackers typically achieve this by installing new executables or overwriting old executables. Their purpose may be to steal sensitive data from the computer (including passwords typed on the keyboard by the user), to use the computer to attack other computers, or any number of other tasks as directed by the attacker.

The characteristics of malware and PUA files have changed a great deal over the years. While attackers used to deliver a single malicious file to thousands or millions of users, they now often deliver a unique malicious file to each user. The most successful modern malware and PUA files are polymorphic, automatically generated via tools that produce vast numbers of unique, single-use files. By delivering each malicious file to only one user or a small number of users, it's difficult or impossible for signature-based antivirus technologies to identify these zero-day files as malicious. Another significant change in malware and PUAs is that today's attackers usually intend for them to be short-lived, hosting their files on malicious websites that only exist for a few hours each. These techniques further hamper efforts to detect and stop malware and PUA files.

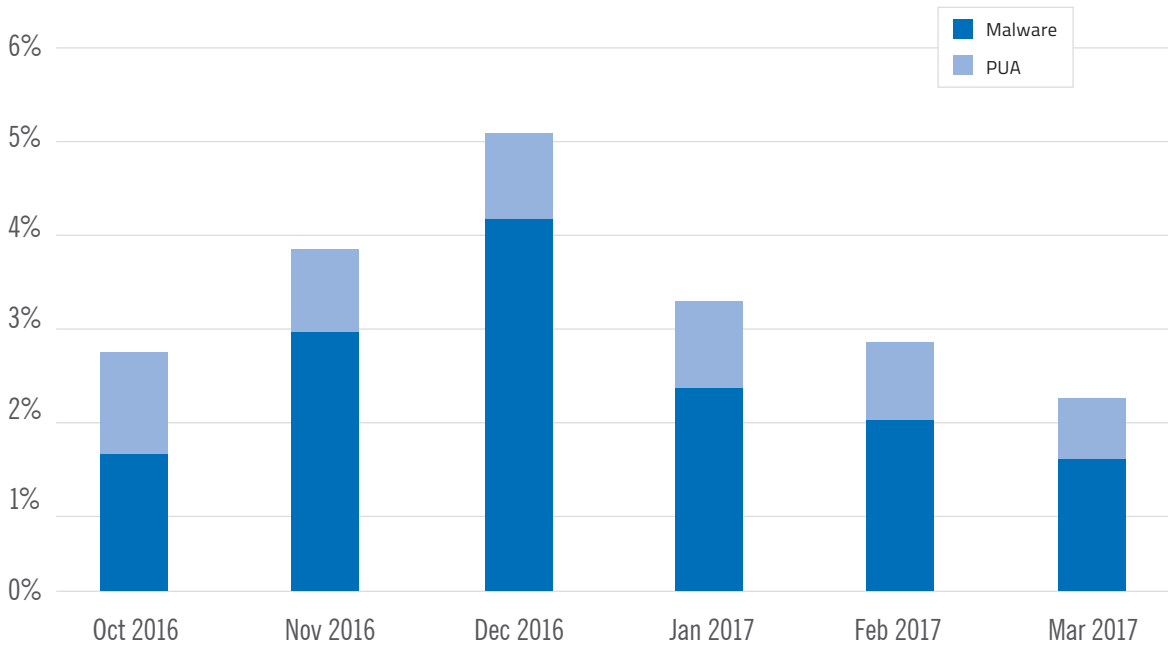


Figure 1: Percentage of Malware and PUA Files Among All Files

To help organizations fight back, Webroot continually expands and refines its Webroot® Threat Intelligence Platform, which automatically collects and analyzes data related to new files (unique files that have never been seen before) to identify trends. Figure 1 shows the percentages of all new files that Webroot identified as malware and PUAs from October 2016 through March 2017. Other than a spike in December, which is likely related to taking advantage of the increase in online shopping around the holidays, there is not a great deal of variation in the total percentage of new files that are malware or PUAs—between 2 to 4%.

A more noticeable trend in new files is the long-term change in the percentage that are PUAs. In 2014, it was 11.6%, but shrank to 7.2% in 2015. By 2016, this number had dwindled to 2.2%, and Figure 1 reflects a recent share of only about 1%. The most likely explanation for the large decrease in PUAs is that many organizations were not aware a few years ago of the malicious nature of many PUAs, which are often a gateway for subsequent malware infections. As awareness has spread, organizations have increased their efforts to detect and stop PUAs, so they have become less attractive for attackers to use.

While PUAs have been decreasing in popularity, the number of new unique files seen each year has been increasing. Figure 2 shows there was an 18% increase from 2014 to 2015, and a 15% increase from 2015 to 2016. Based on early 2017 numbers, estimates are there will be another 10 to 20% increase from 2016 to 2017. So the drop in the percentage of PUAs among new files is somewhat offset by the simultaneous increase in the total number of new files (benign, malware, and PUAs) being seen each year.

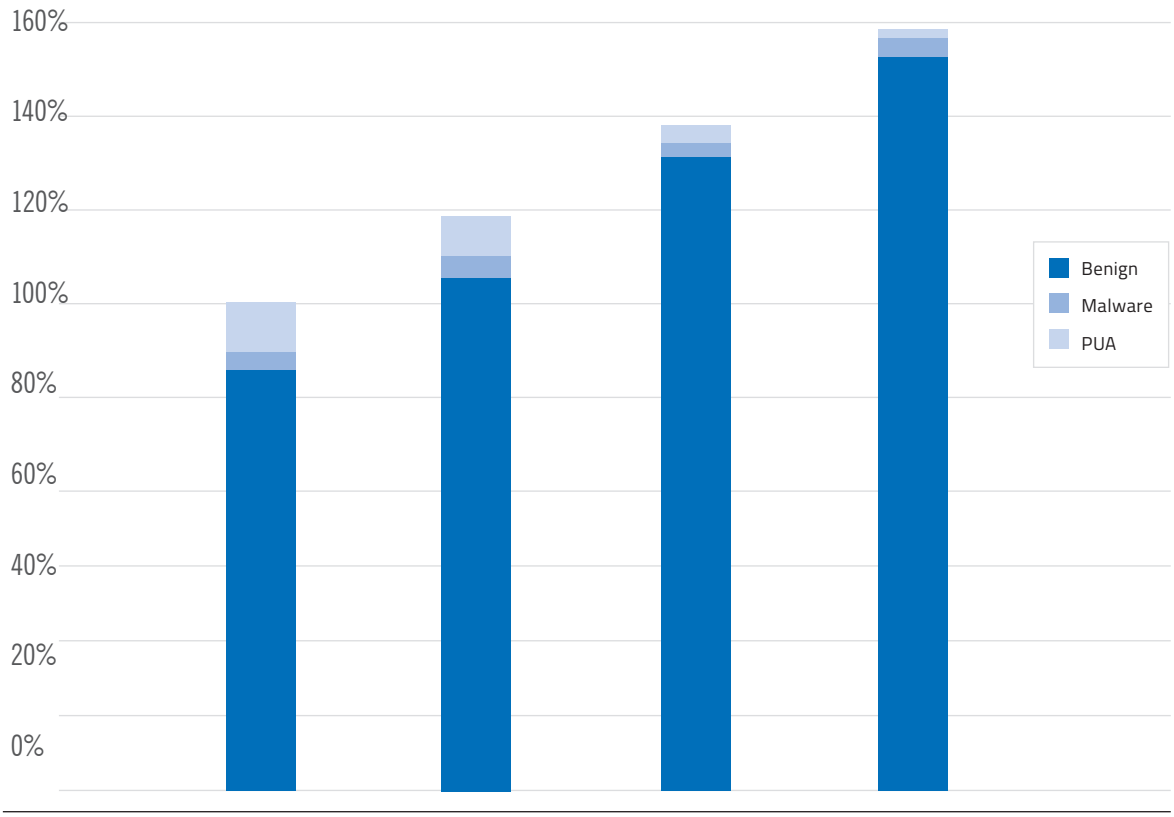


Figure 2: Number of New Unique Files Seen Each Year

Another noteworthy statistic identified by the Webroot Threat Research team involves the number of PCs with each new malware or PUA file. As Table 1 shows, from October 2016 through March 2017 over 95% of new malware and PUA files were only observed on a single PC. Approximately 0.4% of new malware and PUA files were seen on more than 10 PCs. This emphasizes how unique and rare malware and PUA files are today. It also indicates how effective Webroot is at stopping attempts to download new threats. Table 1 only reflects successful downloads of malware and PUA files to PCs and does not include blocked attempts. On average, Webroot detected and stopped almost 2000 download attempts for each new malware or PUA file, with a median of 4 times and a maximum of over 750,000 attempts.

Number of PCs	Percentage
1	95.38%
2-10	4.16%
11-100	0.41%
101-500	0.04%
501-1000	< 0.01%
Over 1000	< 0.01%

Table 1: Number of PCs with Each New Malware or PUA File

Yet another important observation from Webroot Threat Intelligence data involves the number of domains hosting each new malware or PUA file. About 90% of these files were only available from a single domain each. There were cases, however, where many domains had the same file—at the extreme, nearly 3000 domains. Webroot also analyzed the domains hosting malware and PUA files. The number of unique malware and PUA files hosted per domain averaged nearly 4300, with a maximum of over 11 million—but the median value was only 1. Over 50% of unique malware and PUA files were only hosted by a single domain each, and over two-thirds were hosted on only one or two domains each. A related statistic is approximately one-fifth of malware and PUA files were being hosted by domains in benign categories.

Although blocking a number of malicious domains may stop a considerable percentage of malware and PUA files, it won't stop the rest of those files from reaching their victims. There are far too many unique instances of malware and PUA files across countless domains, with many of these files and their hosting by domains being short-lived and constantly changing, to make blocking malicious files by domain effective.

Established Technologies for Stopping Malware & PUAs

There are many established technologies for stopping malware and PUAs, including traditional signature-based antimalware software and sandboxing technologies. Signature-based techniques are mostly ineffective against current malware and PUA threats because of their inability to detect threats that haven't been seen before. A vendor of signature-based protection software could not possibly keep up with the sheer volume of malware and PUA files and the speed and frequency they are deployed. There are significant delays in publishing signatures because of the effort needed to collect and analyze files, and then create, test, and distribute signatures to customers, who in turn must distribute the signatures to their endpoints. Considering the short-lived and single-use nature of most malware and PUAs today, signatures often wouldn't be available to protect endpoints until well after the corresponding threats had already done their damage, if signatures ever became available at all.

Sandboxing technologies are designed to examine and analyze new files in an isolated sandbox environment to determine if the files have malicious intent. This makes them much more effective against unknown malware and PUAs than signature-based technologies. Unfortunately, the types of file analysis done in a sandbox take a lot of time and resources, with one of the most popular being able to handle only around 11 files per minute. The analysis can't start until the entire file has been received and copied to the sandbox. The analysis itself requires extensive hardware resources and delays delivery of benign files to their recipients. Multiply this by the sheer volume of files to process and major latency can occur with sandboxing, to the point of disrupting operations.

Another issue with sandboxing technologies is that malware and PUA authors are developing and using techniques to avoid sandbox detection. For example, executable files may be hidden or may be launched after a long delay. Executable files could also masquerade as authorized system files. Malware and PUAs that can evade detection by sandboxing is becoming a major concern; according to a 2015 report by Dr. Christopher Kruegel, the frequency of sandbox-evading malware had increased by over 2000% in just one year.

The Webroot Threat Intelligence Platform has avoided the shortcomings of other methods for detecting and stopping malware and PUAs. In the real world, Webroot has proven extremely fast at identifying new malware and PUA files. Figure 3 shows three time ranges for identification: within one hour, within 12 hours, and over 12 hours. From October 2016 through March 2017, Webroot identified approximately 96% of new malware and PUA file threats within 12 hours of their first appearance. In the majority of cases, identification of these files happened in less than one hour.

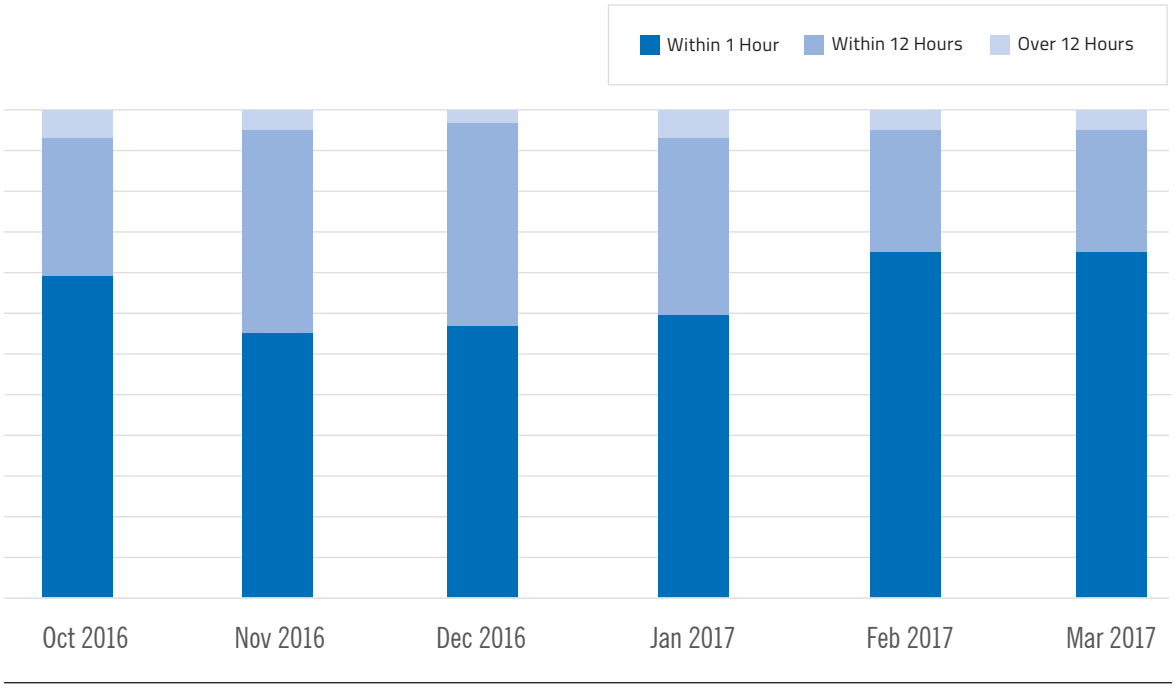


Figure 3: Webroot's Speed at Identifying Just-Released Malware and PUA Files

Webroot BrightCloud® Streaming Malware Detection

New advances in machine learning from Webroot have enabled the company to develop new malware detection capabilities to identify traditional, zero-day, and polymorphic malware, even malware that avoid being detected by sandboxing techniques. Webroot has evolved its own technologies to complement existing malware detection products by addressing their major drawbacks: resource consumption, latency, and dependence on signatures.

Webroot has a new patent-pending technology called Webroot BrightCloud® Streaming Malware Detection, which is significantly faster than signature-based and sandboxing techniques, and is available for other vendors to integrate into their security solutions. Streaming Malware Detection works as a network-based pre-filter that reduces the number of sandboxes, endpoint protection suites, and other tools to analyze. The combination of a sandboxing technology or endpoint protection suite and an Streaming Malware Detection-enabled technology helps improve file delivery times while enabling organizations to maximize the return on investment for their existing security technologies.

Figure 4 illustrates the basic architecture. Files attempting to reach hosts within the organization enter the Streaming Malware Detection-enabled solution, which is located in a dedicated appliance at the edge of the network. Streaming Malware Detection analyzes each file and chooses one of the following actions:

» **Allow**. Streaming Malware Detection recognizes the file as known-benign or otherwise determines it poses no threat to the organization. There is no need to send the file to the sandbox for further evaluation, so the solution passes the file on to its destination.

» **Block.** Streaming Malware Detection has determined that the file is malicious (malware or PUA), so it does not permit it to go any further.

» **Investigate.** Streaming Malware Detection cannot determine if the file is benign or malicious, so it sends it to the sandbox or other investigative solution for further analysis and decision making.

Through this architecture, Streaming Malware Detection takes a large burden off sandboxing technologies, as well as other security controls like traditional signature-based antivirus software and endpoint protection suites that are also looking for malware and PUAs. This architecture avoids slowing down network traffic by analyzing files as they stream through the network. The Streaming Malware Detection architecture is also self-contained, enabling determinations to be made locally by the network device. There is no need to constantly access resources in the cloud or elsewhere outside the organization's networks in order to make determinations.

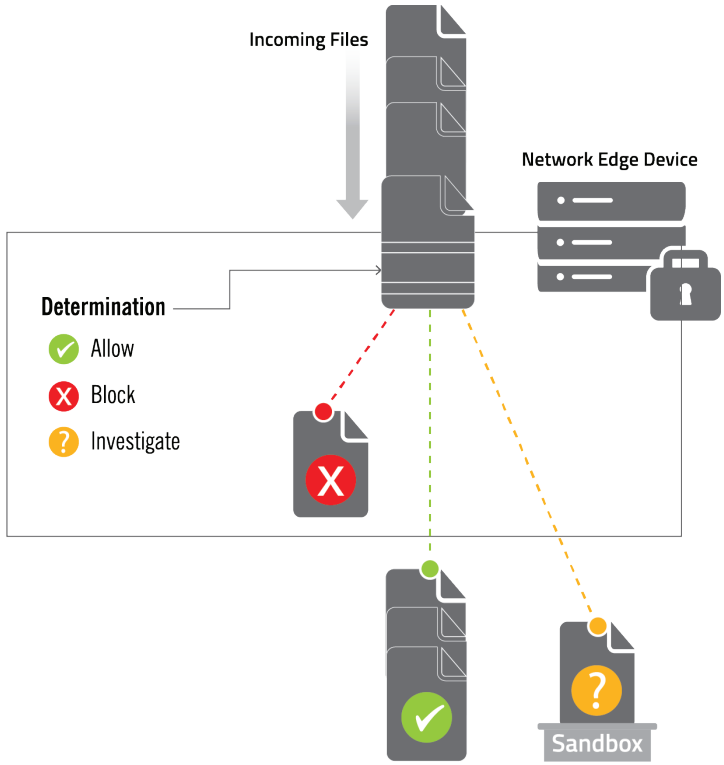


Figure 3: Webroot's Speed at Identifying Just-Released Malware and PUA Files

Streaming Malware Detection minimizes latency by performing file stream monitoring, which means it can start analyzing parts of the file as it enters the network. Other security technologies can't begin analyzing a file for malware or PUAs until they receive the entire file. Streaming Malware Detection monitors and parses network packet streams, looking at the small piece of a Windows Portable Executable (PE) file contained in each packet. This allows Streaming Malware Detection to start its analysis sooner, and, in many cases, the solution can determine how the file should be handled based on analyzing just a portion of it.

Streaming Malware Detection assesses risk using advanced machine learning techniques. Webroot continuously trains and updates its machine learning models to improve accuracy and efficiency, including minimizing false positives. The updates take into account information on the latest threats and vulnerabilities from the Webroot® Threat Intelligence Platform, the Webroot Threat Research team, and carefully screened third-party sources. Webroot provides a daily download of the latest Streaming Malware Detection machine learning model, with the update process designed to minimize any latency in file stream monitoring. During use, the machine learning model on each enabled device takes into account millions of individually weighted factors to develop a risk score for each file it analyzes. These scores translate into the Allow, Block, and Investigate actions.

In initial internal testing, Webroot BrightCloud Streaming Malware Detection has shown it operates 30 to 40 times faster than signature-based solutions, and over 500 times faster than sandboxing technologies analyzing the same files. This is how Streaming Malware Detection reduces the queue of files requiring sandbox evaluation or evaluation by signature-based software without introducing additional latency into the processes.

Conclusion

The most significant findings from recent analysis performed by the Webroot® Threat Intelligence Platform and the Webroot Threat Research team are:

» Between 2 to 4% of all new files are malware or PUAs. The number of new files seen each year has been increasing at least 15% a year the past few years.

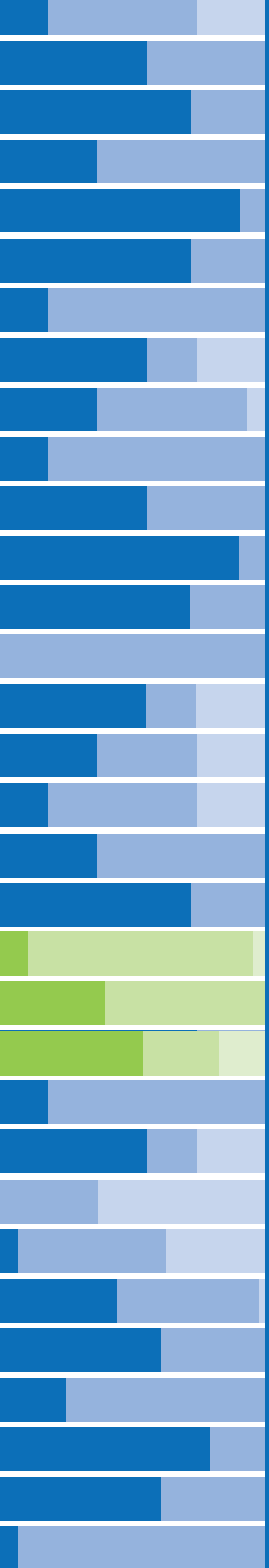
» Over 95% of new malware and PUA files were only observed on a single PC. Webroot detected and stopped nearly 2000 download attempts on average for each new malware and PUA file.

» In most cases (approximately 90%), each new malware or PUA file is only available from one domain, although some files have been seen on thousands of domains. Most domains that host malware and PUA files only have one of them, but one domain was found to host over 11 million such files. Also, approximately 19% of malware and PUA files were hosted by domains considered benign.

» Between October 2016 and March 2017, Webroot threat intelligence identified approximately 96% of new malware and PUA files within 12 hours of their first appearance, and in the majority of cases identification occurred within the first hour.

These findings underscore the need for effective technologies to detect and stop malware and PUAs. Although sandboxing, endpoint protection, and traditional signature-based antivirus technologies have benefits, their resource consumption, added latency, and dependence on frequent updates make them unacceptable when used on their own. Webroot recommends deploying Streaming Malware Detection-enabled filtering technologies at the network perimeter. Streaming Malware Detection will greatly reduce the workload of the detection technologies behind it by rapidly identifying most malicious and benign files without adding overhead. This passes on just the toughest cases for the other detection technologies to analyze. The solution's use of file stream monitoring, machine learning, and constant feed of threat intelligence enables it to work hundreds of times faster than sandboxing, minimizing latency and optimizing resource consumption for the Streaming Malware Detection/sandbox combination.

For more information on Streaming Malware Detection, visit webroot.com/brightcloud



About Webroot

Webroot delivers network and endpoint security and threat intelligence services to protect businesses and individuals around the globe. Our smarter approach harnesses the power of cloud-based collective threat intelligence derived from millions of real-world devices to stop threats in real time and help secure the connected world. Our award-winning SecureAnywhere® endpoint solutions, BrightCloud® Threat Intelligence Services, and FlowScape® network behavioral analytics protect millions of devices across businesses, home users, and the Internet of Things. Trusted and integrated by market-leading companies, including Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more, Webroot is headquartered in Colorado and operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity™ solutions at www.webroot.com.

385 Interlocken Crescent Suite 800 Broomfield, Colorado 800.870.8102 webroot.com