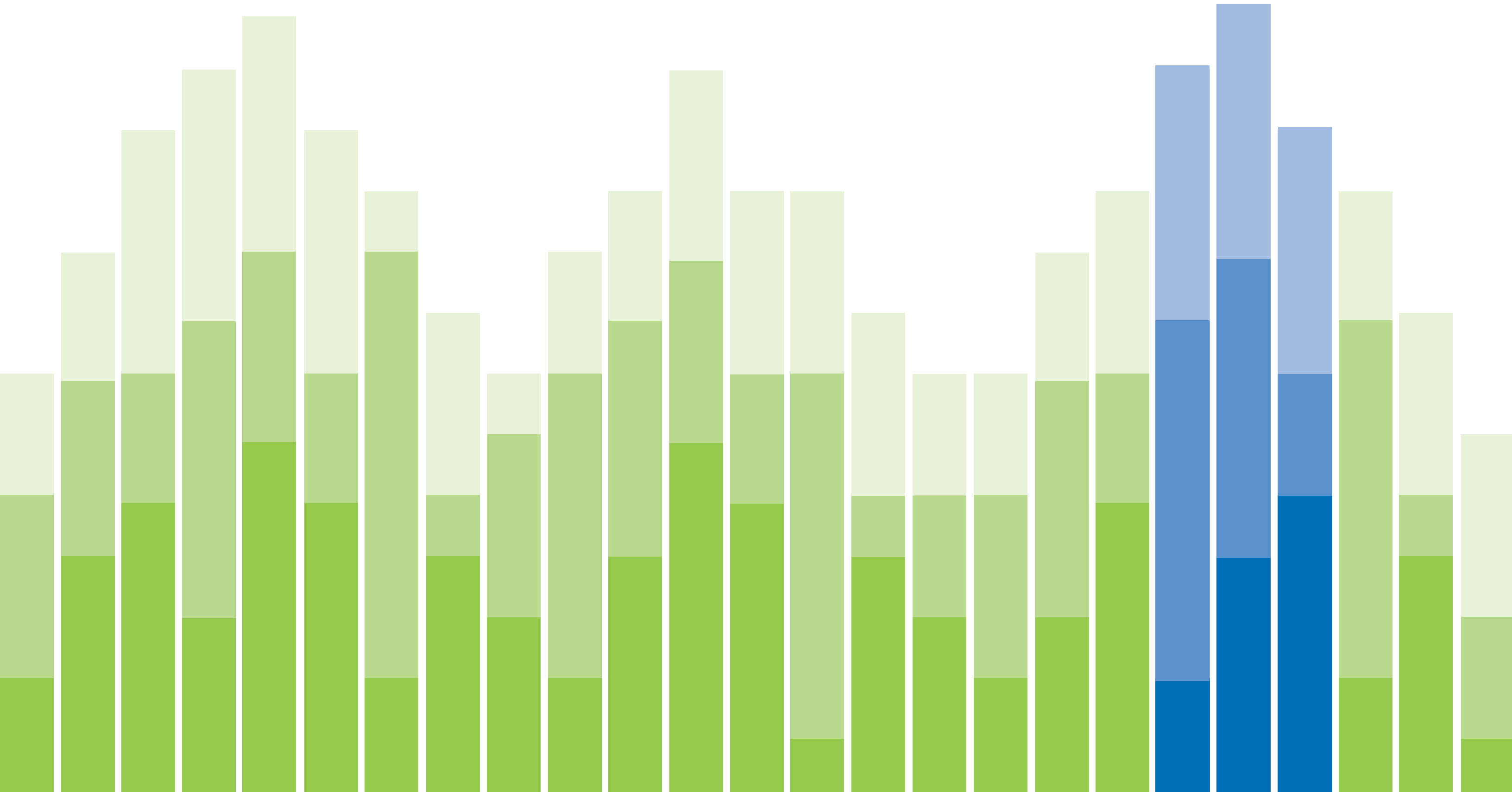
WEBROOT®
Smarter Cybersecurity™

DECEMBER 2017

QUARTERLY THREAT TRENDS

Webroot BrightCloud® Threat Intelligence: A Window Into the Future



Who wouldn't want the ability to see what will happen in the future? Nowhere is this yearning greater than in the world of cybersecurity, where even a small glimpse of future threats could prevent a disastrous and costly breach. The security industry is looking to move beyond reactive mode and be proactive, automating the response to threats and preventing attacks before they happen. This edition of the Quarterly Threat Trends report shows ways in which Webroot BrightCloud Threat Intelligence Services can actually bring you these desired predictive capabilities, helping you avoid threats and potential breaches. First, let's take a look at some predictions for 2018 from Webroot experts.

Looking into the Future

As threat intelligence gets smarter, it can detect an impending attack and stop it even before the target becomes aware of its existence. We saw a recent example of exactly that behavior in late November 2017, when a ransomware attack based on a variant of NotPetya hit the news. Webroot was able to quickly determine that none of its customers had been affected. Machine-learning and cloud-based analytics recognized similarities to the existing threat, predicted the presence of malware, and stopped it at the network perimeter before it could infect any endpoints.

Leveraging BrightCloud predictive capabilities, the Webroot team is anticipating security events we might see in the near future. Some of their predictions:

Gary Hayslip, Webroot Chief Information Security Officer:

» **Artificial Intelligence: Not Just for the Good Guys**
We anticipate seeing malware that uses artificial intelligence (AI) to get past anti-malware software. A recent demonstration at DefCon shows an instance of malware writers using open-source AI available on GitHub. They were able to create malware variants that got past antivirus solutions 16% of the time. As with any technology, it comes down to who is reviewing the data, and who has the better models.

In this regard, Webroot is in a very strong position, having spent more than a decade perfecting its models and sourcing a massive amount of real-world information on a continuous basis. We continually conduct cutting-edge research and incorporate learning into the security platform of services for partners, so they have the tools to be effective in reducing risk exposure and protecting their customers.

» **Destructive Ransomware**
We expect that soon, we will see ransomware intended to destroy, rather than encrypt. Phishing attacks are by far the most common vector for ransomware, and it becomes even more important to stop the attacks from carrying out their intended mission.

The BrightCloud Real-Time Anti-Phishing Service blocks access to pages or URLs that are implicated in phishing attacks, inspecting all indicators of compromise in a coordinated fashion to find all indications of potential malicious activity. In addition, BrightCloud Streaming Malware Detection blocks malicious files at the perimeter, upstream from other technologies.

David Kennerley, Webroot Director of Threat Research:

» **Ransomware as a Vector for Secondary Infections**
Ransomware writers are getting better at covering their tracks while carrying out more targeted attacks. This is especially true of ransomware that is being served up from malicious URLs, and coming in via phishing attacks. Such attacks may be targeted at specific vulnerabilities the hackers feel are likely to exist at a given company, based on its application portfolio, the size of the network, and other factors that the hackers can discern. Once inside, the ransomware could then make decisions as to what payloads to launch for a secondary infection, based on what it has learned from previous infections and successful attack models.

Nick Emanuel, Webroot Director of Product:

» **The Lure of Embedded Links**
We will continue to see phishing and spear phishing threats that increasingly rely on embedded links. With new GDPR regulations coming soon and Britain leaving the E.U., we expect to see companies targeted with phishing and spear phishing attacks that specifically message these topics. Traditional threat intelligence products are inadequate on two levels: they rely on static phishing lists, which are too slow to keep up with the pace of today's attacks and easily miss phishing sites that come and go in the blink of an eye. In addition, they look at indicators of compromise in isolation, without the contextual analysis that would allow them to connect the dots and predict a real attack.

Webroot BrightCloud Threat Intelligence Service not only provides the Real-Time Anti-Phishing Service, but its rich machine learning models and contextual analysis bring together disparate indicators of compromise that, taken as a whole, paint a very different picture of a threat. As more and more phishing attacks rely on embedded links, BrightCloud provides multiple levels of protection.

Essential Ingredients for Predictive Threat Intelligence

The promise of threat intelligence to predict future events has been around for years, but in many cases it has fallen short. The reason is simple: threat intelligence, in and of itself, is not enough to foretell what will happen. All too often it is poorly-sourced, the machine-learning supporting it is not robust, data is outdated, and indicators of risk are viewed in isolation. To be truly useful as a predictive tool, threat intelligence must:

- Be built on the right foundation, with insight based on analyzing behavior over time
- Use appropriate (and sufficient) sources
- Employ effective machine learning, constantly improving its predictive capabilities
- See the "big picture" through contextual analysis

How Webroot BrightCloud Threat Intelligence Is Uniquely Predictive

Webroot BrightCloud Threat Intelligence provides a unique window into the future, due to its platform, sources, machine learning, and contextual analysis.

Platform

First, Webroot is an advanced, cloud-based security platform that provides threat intelligence on URLs, IPs, files, and mobile applications. For more than 10 years, the platform has been effectively using machine learning, massive cloud-based scale, and automation to ensure lightning-fast processing. A globally-distributed database ensures speed and depth of processing. The numbers speak for themselves: Webroot BrightCloud Threat Intelligence Services continuously classify and score 95% of the internet, as well as monitor the entire IPv4 space and the in-use IPv6 space.

Sources

Second, the sources for BrightCloud are both broad and deep, drawing from real-world products and people interacting with their systems and their networks, rather than merely relying on crawlers, honeypots, or passive sensors waiting for something to happen. Webroot relies on more than 40 million sensors and 30 million connected endpoints around the world to power threat intelligence. Over the past 10 years, Webroot has categorized more than 27 billion URLs, and more than 600 million domains.

The input vector size for each is massive: BrightCloud has the capacity to capture more than one million characteristics of a single web page.

BrightCloud has classified and categorized more than four billion IP addresses, more than 55 million mobile apps, and more than 13 billion file behavior records. What's more, this massive amount of data is continually analyzed in real time. Webroot classifies URLs at a rate of 5,000 per second, finding 25,000 new malicious URLs each day. When combined with the 100,000 new malicious IP addresses and 6,000 new phishing sites discovered daily, there's no question that Webroot is the leading provider of threat intelligence to the Networking and Information Security industries.

Effective Machine Learning

Third, machine learning is an integral component of the threat intelligence platform because it enables a high detection rate over time, even in spite of the ever-changing nature of threats. Machine Learning from Webroot is a distributed system that incorporates big data constructs, such as the Hadoop file system, to automatically classify approximately one million undetermined file executables per day and determine whether each one is benign or malicious. Machine learning also fully automates the detection of zero-day phishing sites. It incorporates a variety of classification techniques working in parallel including Maximum Entropy Discrimination (MED), active learning, and active feedback.

The Webroot self-learning platform incorporates continuous inputs to quickly and accurately identify previously-unknown threats. For example, when a file first begins to traverse the network, Webroot pulls data points even before the file lands on a user's hard disk. Based on information such as strings, authors, URLs, and embedded IPs, the model starts to develop an opinion. The reputation score is derived instantly, even based on a small amount of information, which enables customers to set thresholds and block or allow everything below or above a given score. This means the software can predict that a file is malware and stop it in its tracks. At the same time, it learns from the results of this reputation decision, perfecting its algorithms to make decisions with greater precision the next time.

While many threat intelligence vendors claim to employ machine learning, they universally lack the years of continuous learning that has fine-tuned the Webroot machine-learning engine. Webroot's algorithms and mathematical models are unique and protected by multiple patents. None can compare to Webroot's more than 80 patents (with an average of 8-10 filed each year) for optimization of machine-learning technology.

Contextual Analysis

Fourth, and critically important, contextual analysis weaves the strands of intelligence together, revealing the big picture. Instead of looking at URLs, IPs, files, and mobile apps in isolation, contextual analysis from Webroot does predictive risk scoring by correlating previously-disparate data derived from real-world endpoints. Using a "guilt-by-association" model, the contextual database correlates URLs, IPs, files, and mobile apps that seem to be benign, but are tied to other locations or assets that have exhibited malicious activity.

Take, for example, a URL that has a reputation of serving malware. If a new, never-before-seen file is associated with that URL, it has a higher likelihood of being malicious than an unknown file only associated with benign sites.

Another example is a phishing attack that appears to come from the HR department. A competing threat intelligence solution might identify the source IP address as benign based on their latest information. However, Webroot can see that it was previously malicious, then turned benign, and has once again become threatening. It can also spot internal links to URLs that have exhibited malicious activity, and can assume the email is malicious.

What it Means to You and Your Customers

With Webroot, you gain the ability to see patterns as they emerge, automatically take action, and understand why decisions were made.

See Patterns as They Emerge

The Webroot platform is structured to organize massive amounts of information, sift through it, and find the signal in all the noise – to predict the most dangerous and difficult-to-detect zero-day threats. Unlike other threat intelligence services that rely on narrow data sets that are too small to show patterns, Webroot leverages broad and varied data sources for accurate, consistent, and dependable threat detection.

Machine learning, done right, has been proven to predict a future outcome. In the case of BrightCloud, machine learning and contextual analysis drive actionable threat intelligence that can predict the behaviors of unknown objects and find previously unidentified threats. BrightCloud assesses internet objects based on their history and relationship to known malicious objects, assigning a score that indicates the likelihood that an object will attack in the future. Webroot's long history in the market has led to a stronger coverage model and the ability to track changes to objects over time. In addition, Webroot staffs dedicated teams of data scientists and threat researchers who specialize in security and leverage their years of experience to continuously enhance the ability to predict.

Automatically Take Action

The predictive reputation score generated by Webroot advanced contextual analysis gives customers the ability to make decisions and take action automatically. Webroot has built a global reach and an interconnected infrastructure, so that if any one machine sees a threat, all systems will be protected within five minutes. This is vitally important in a world where phishing sites go up and down in the span of less than a day.

Trust the Reputation Scores

Webroot sees very low false-positive rates, which increases the reliability of the prediction, as does the solid track record built up over 10 years. This allows Webroot to look back over time and demonstrate exactly when an IP turned from bad, to good, to bad again. In fact, it is this reputation score that elevates Webroot BrightCloud Threat Intelligence Services to the role of trusted advisor: customers are confident taking action based on the reputation score and active threat status.

Webroot also provides full transparency for maximum trust in its predictive results. BrightCloud Contextual Threat Insights show clearly why decisions were made. Threat insights answer the questions “Why did BrightCloud determine that a particular IP, URL, file, or mobile app is malicious, how long has it been a threat, and what type of malicious activity was it involved in?” This allows the service to provide insights into the threats and exposes possible factors used by BrightCloud in its determination. This not only instills trust in the determinations, it also helps Security Operations teams understand the severity of threats and prioritize their incident response or investigations accordingly.

Conclusion

In cybersecurity, the only thing constant is change. Criminals are getting smarter and more sophisticated, so we must work smarter to stay ahead of them. The ability to accurately predict what could happen, at the moment of greatest impact, is the best and smartest way to ensure robust security. Threat intelligence alone cannot perform all these tasks. Only when it meets the stringent requirements for platform, broad sources of intelligence, machine learning, and contextual analysis can it hope to open a window into the future.

Webroot is the trusted provider of operational threat intelligence to leading network and information security providers. For the past 10 years, Webroot has been investing in continuous improvements to its self-learning platform, drawing on an ever-broader set of intelligence sources, and using contextual analysis to see the big picture. BrightCloud is the result of these ongoing efforts, and provides the speed, scale, scope, and trustworthiness to stay ahead of the attacks and deliver highly actionable, timely, and predictive threat intelligence.

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