WEBROOT

Smarter Cybersecurity®

2018 Webroot

MID-YEAR UPDATE

SEPTEMBER 2018

Introduction

One of the biggest security takeaways from the first half of 2018 is that we can never make our computer systems perfectly secure, and the underlying hardware can be just as susceptible to exploitable flaws as the software that runs on it. Two new vulnerabilities—Meltdown and Spectre—affected nearly every device with a CPU, making this one perhaps the worst first half ever in terms of computer security. While not the most severe we've ever seen, these vulnerabilities hit the entire ecosystem of computers due to flaws in how modern processors isolate private memory. Until they were fixed, they offered access to bad actors who could gain access to private data, such as login credentials. What's more, Meltdown and Spectre existed for two decades before being discovered, and there are certainly many other bugs lurking.

Here's the good news: our collective approach to Meltdown and Spectre revealed some positive trends in cooperation and communication. First, the vulnerabilities were discovered by white hat hackers. Google's Project Zero, as well as bug bounty programs from Microsoft and Apple, have been working. They incent people who discover vulnerabilities to communicate directly with the parties who can fix them, before going public with the information. Second, their existence was closely guarded, to allow time for OS manufacturers to develop fixes. Competing companies shared information and worked in tandem to find a software solution to a hardware problem, and that's a noteworthy trend.

The bad news: threat actors aren't standing still. They constantly evolve methods, techniques and evasion approaches, making other malware campaigns such as Emotet, TrickBot and Zeus Panda more persistent and harder to detect. They are pivoting from ransomware to cryptojacking. Increasingly sophisticated phishing attacks are stealing credentials, introducing malware, and doing reconnaissance. Phishing attacks are also becoming more targeted, as criminals find ever-more-valuable information stores.

The Webroot Threat Research Team has analyzed the data from our customer base during the first half of 2018. This mid-year threat report not only shows the stats, but also tells the story behind the headlines. The bottom line from our observations: it has never been more important to implement a robust, effective, multi-layered and continuously evolving security approach to keep valuable data and systems secure.

The Biggest Threats

Malware, ransomware, cryptojacking, and botnets continue to dominate the threat landscape; from January through June of 2018, a full 87% of the threats were malware (including ransomware) and cryptojacking, followed by 12% from botnets. We'll unpack each of these threats and share our observations on the story the numbers tell.

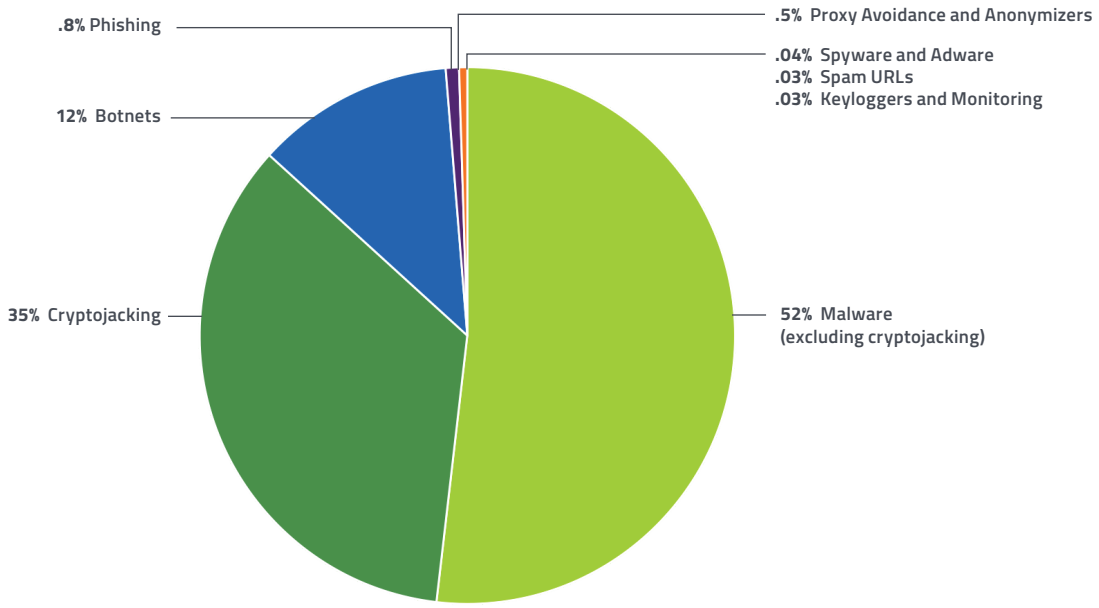

Figure 1: The current threat landscape

Ransomware Adopts a New Business Model

Last year, ransomware went on a rampage, causing panic for its victims. Many businesses scrambled to safeguard mission-critical data, often succumbing to demands to pay increasingly expensive ransoms via cryptocurrency, which skyrocketed in value itself. However, these days, the difficulty of pulling off a productive ransomware campaign, coupled with increasing use of good backups—including cloud backups that save previous versions—mean that today's ransomware authors are less able to scare users into paying ransoms to salvage their data.

The threat of ransomware is further reduced as more users turn to Windows 10; by mid-year, Webroot saw 75% of consumers and 40% of businesses had moved to this more secure operating system.

But ransomware has not gone away. Instead, it has become a more targeted business model for criminals who seek out unsecured Remote Desktop Protocol (RDP) connections as the attack vector. Using tools like Shodan, malicious actors scan for the many organizations that have left their environment wide open to infiltration by not creating adequate RDP settings. Less sophisticated cybercriminals can even go to the dark web and buy RDP access to already hacked machines. Once they access a given system, criminals can browse all data on the system or shared drives to assess its value, as well as deploy ransomware or other malware. If they succeed in disabling endpoint protection for even a few minutes, they know their malicious payloads will execute successfully.

Thanks to improperly configured RDP, the SamSam Ransomware group and their campaigns have made millions in cryptocurrency this year, and even made headline news when they shut down government sectors of Atlanta and Colorado, along with medical testing giant LabCorp. But there are now multiple viable choices for payloads in an RDP compromise. Because the criminal can see all the hardware installed, it's easy to determine if the installed CPU and GPU would deliver more profit mining cryptocurrency than if attackers simply deployed a ransomware infection.

Education can play a crucial role in protecting an organization from compromise. Too many IT departments leave default ports open and are lax about password policies, underscoring the reality that employees are the weakest link.

Training on how to configure the environment and establish a baseline of resilience is just as important for a company with 50 employees as for a multinational corporation.

Cryptomining Dethrones Ransomware as #1 Threat

Many criminals have moved on to easier, faster, and less-risky ways to benefit from cryptocurrency without using malware. Very profitable yet with a minimal criminal footprint, cryptomining works on any device—not just computers and phones, but even IoT devices like routers and TVs. Some website owners voluntarily participate in cryptomining, seeing it as an easy way to generate revenue to pay their server costs without bombarding site visitors with annoying banner and sidebar ads. However, others carry out cryptomining without letting the visitor know.

In either case, it may be largely invisible to the end user, who likely won't notice a small spike in their electric bill. But for an organization, power bills can skyrocket, especially when criminals employ scaling, i.e., keeping the drain on the CPU minimal when a keyboard or mouse is being used but scaling up to 100% at other times.

With energy use for mining doubling every six months, cryptomining will account for an estimated 3% of the world's electricity consumption by 2020.

Bitcoin is the biggest culprit when it comes to energy usage, and it requires the criminal to take steps to launder the payout and obfuscate the trail that inevitably leads back to them. For this reason, the most common type of cryptocoin mined is Monero, since it runs on any consumer-grade hardware, and has an anonymous blockchain so there is no need to launder the ill-gotten profits.

The Malware Evolution

Malware rounds out the top three threats seen in the first half of 2018. While still prevalent (an average of 1% of the traffic seen in the first six months of 2018, down from 2% in 2017), malware continues to decline.

This 50% drop is largely because there are easier ways to profit from remote systems than by deploying malware. It only takes a small number of people to view a website that hosts cryptojacking JavaScript for a bad actor to not just break even, but make a quick profit.

Botnets are the most common delivery method for malware, and Emotet wins the prize for most prevalent and persistent botnet we've seen. Its payloads are delivered at an impressive pace, showing that threat actors have automated multiple steps in their campaign operations. Emotet aspires to increase the number of zombies in its spam botnet, with a concentration on credential-gathering. It is so popular and effective, several major malware campaigns use Emotet as a delivery vector.

The threat actors behind Emotet now have the option to create additional layers within their botnet, ultimately increasing its resiliency. They have recently developed a Universal Plug and Play (UPnP) module that allows Emotet to turn victims' routers into potential proxy nodes for their command and control infrastructure. Most residential routers—which are Linux-based and have no antivirus—are viewed by their owners as black boxes, so proper setup is not a priority, and no one will notice when a criminal exploits convenient UPnP to plug IoT devices into their router.

When we look at the other primary malware families, we see more evidence that criminals are making their malware more resilient, harder to detect and longer-lasting, and that we are in a constantly shifting battlefield where threat actors change their tactics in response to security defenses. Trickbot has started adding Tor servers to its level 1 command and control infrastructure to ensure that the servers used to distribute the attack modules and web injections remain active for a longer period of time. Zeus Panda (Panda Banker) remains prevalent and, in the last few months, has begun to target more regions of the world. Across the board, threat actors have made changes to internal protection mechanisms to ensure their payloads remain difficult to reverse-engineer and detect.

Phishing: the Unrelenting Attack

Phishing and targeted social engineering attacks are all on the rise: Webroot saw phishing attempts increase by more than 60% from January to June.

Phishing continues to be an effective method of breaking into corporate networks. All it takes is for one person to be tricked, and the threat actor can obtain credentials and perpetrate an RDP attack as discussed in the Ransomware section.

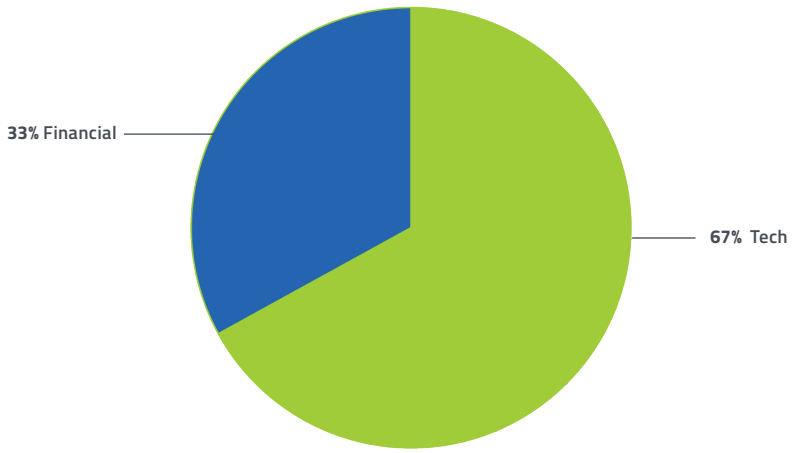

Figure 2: Websites most impersonated by phishing in H1 2018

Bad actors continue to shift and fine-tune their targets as they learn which attacks are the most successful and lucrative. While Google has been a primary target for the past three years, Dropbox (at 17% of the attacks) overtook Google (at 15%) in the first half of 2018.

When a threat actor breaks into someone's Gmail account, the potential reward may be limited to just one person's data. However, with Dropbox, the reward could be much greater: consumer and business users store tax, financial, personal, and business information in Dropbox. With the increasing prevalence of corporate Dropbox accounts, the payoff grows exponentially. Gaining access to a corporate Dropbox account could also expose cryptokeys, unlocking a massive amount of mission-critical and highly sensitive data.

Using endpoint security products like Webroot SecureAnywhere® protection, which is fed by the Webroot BrightCloud® Real-Time Anti-Phishing Service, plays a vital role in thwarting such attacks before they can do damage, but the human element still needs to be addressed. Fortunately, the evidence is mounting that end user cybersecurity education and phishing simulations, like those available in Webroot® Security Awareness Training, significantly improve the chances that employees will successfully avoid phishing attacks.

Web-based Threats

We have seen tens of millions of malicious URLs in the first half of 2018, spread out across four broad categories: 87% were malware, cryptojacking and ransomware; 12% botnets; <1% phishing and other frauds; and <1% proxy avoidance and anonymizers. The remaining 0.2% included spam URLs, spyware and adware, and keyloggers and monitoring.

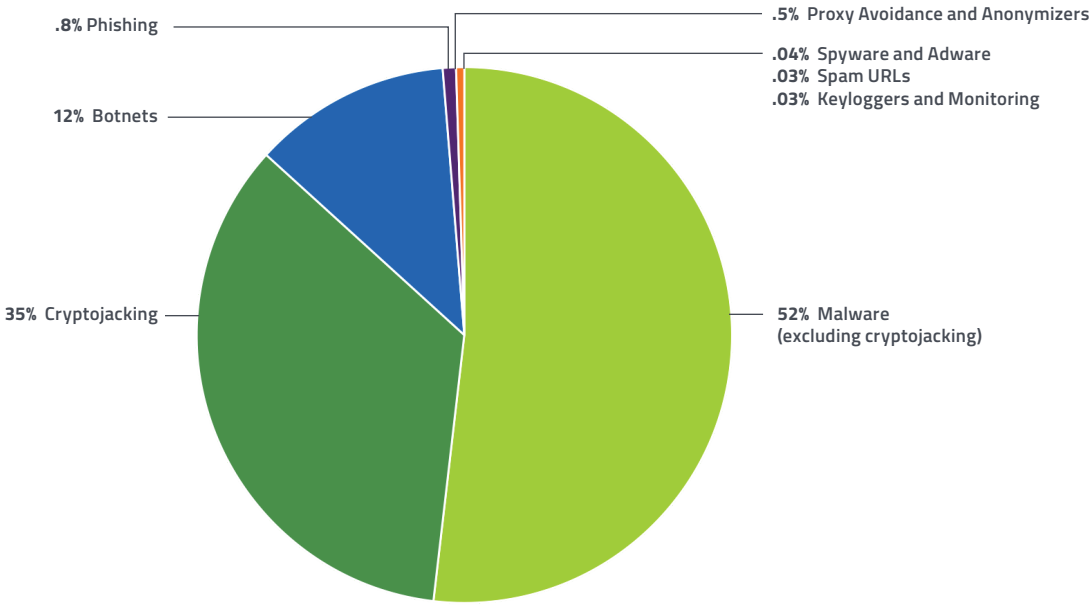

Figure 3: Top web-based threats

Webroot SecureAnywhere® DNS Protection encounters new phishing domains and botnets daily. Results from DNS Protection customers from April to June 2018 showed hundreds of thousands of encounters with risk categories (which were blocked by the product.)

Approximately 0.5% of traffic we saw via DNS Protection was malicious.

A deeper dive into web-based threats confirms that cryptomining and cryptojacking are becoming more commonplace. Of the many millions of URL requests we see per day, customers visited sites with cryptomining scripts approximately 3% of the time, and roughly one-fifth of those were visits to coinhive.com and its subdomains (the nodes to which cryptomining relays go). It's important to note that the creators of Coinhive claim to have developed the mining script as a legitimate way for website owners to monetize their sites without having to serve ads; for its part, Coinhive takes 30% of the money collected. Sites that use the Coinhive script intentionally—primarily pornography, torrent, and streaming sites—may or may not inform their visitors that they are actively mining. While Coinhive has tried many times to implement a mandatory opt-in script so users would have to knowingly agree to allow the use of their CPU power, the overwhelming majority of hosted Coinhive scripts do not require any opt-in. Other sites may have been modified by malicious users to perform cryptomining without the site owner's knowledge, sending the redirects to Coinhive to mine Monero. In those cases, the counts are much lower than the principal domains listed below, since the activity would be discovered and removed.

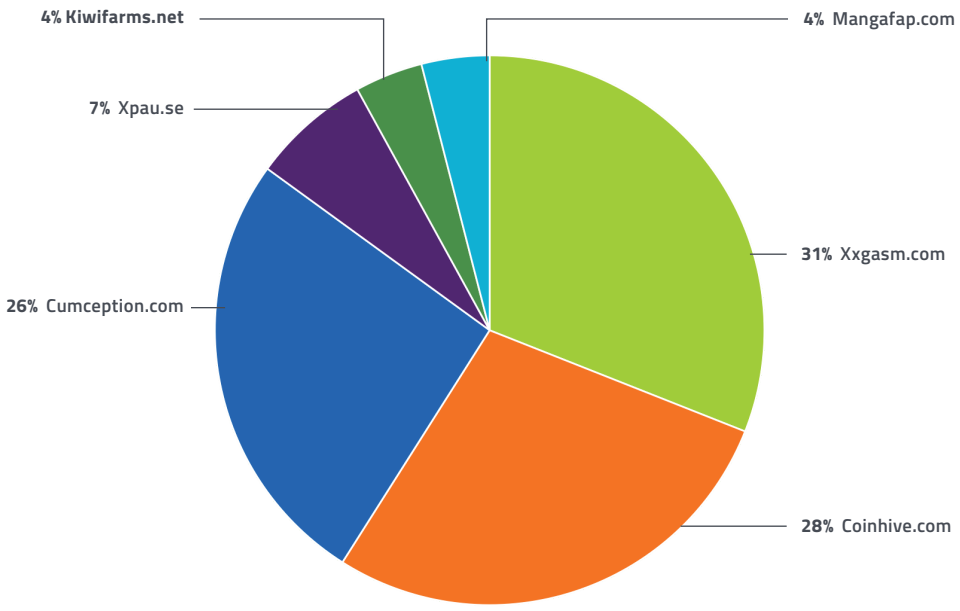

Figure 4: Top cryptomining domains

Security Awareness Training: a Force Multiplier

One positive outcome of the large number of cybersecurity threats we've seen in 2018 is the extent to which employee security awareness is becoming a key ingredient in many organizations' security strategy.

93% of breaches are initiated by phishing, and 22% of employees have clicked at least one phishing link in the last year.[1]

From: "microsoft@helpdesk-notification.com" <microsoft@helpdesk-notification.com>
Date: Wednesday, September 12, 2018 at 4:07 PM
To: <Recipient>
Subject: Your Microsoft Account Password Has Been Changed

Microsoft account

Your password changed

The password for the Microsoft account <recipient email> was just changed.

If it was you, then you can safely ignore this email.

If this wasn't you, your account has been compromised. Please follow these steps:

1. Reset your password.
2. Learn how to make your account more secure.

To opt out or change where you receive security notifications, click here.

Thanks,
The Microsoft account team

Training that focuses on the key indicators that an email or link is a phishing attempt is key to reducing risk. Additionally, security awareness training to protect employees and data also helps businesses avoid fines and ensure compliance with SEC, FINRA, HIPAA, GDPR and other regulations.

[1] Verizon. "2018 Data Breach Investigations Report." (April 2018)

To ensure success, training must be ongoing throughout an employee's tenure with the company. As the next graph shows, results from our Webroot® Security Awareness Training customer base in H1 2018 underscore the necessity of continuous reinforcement:

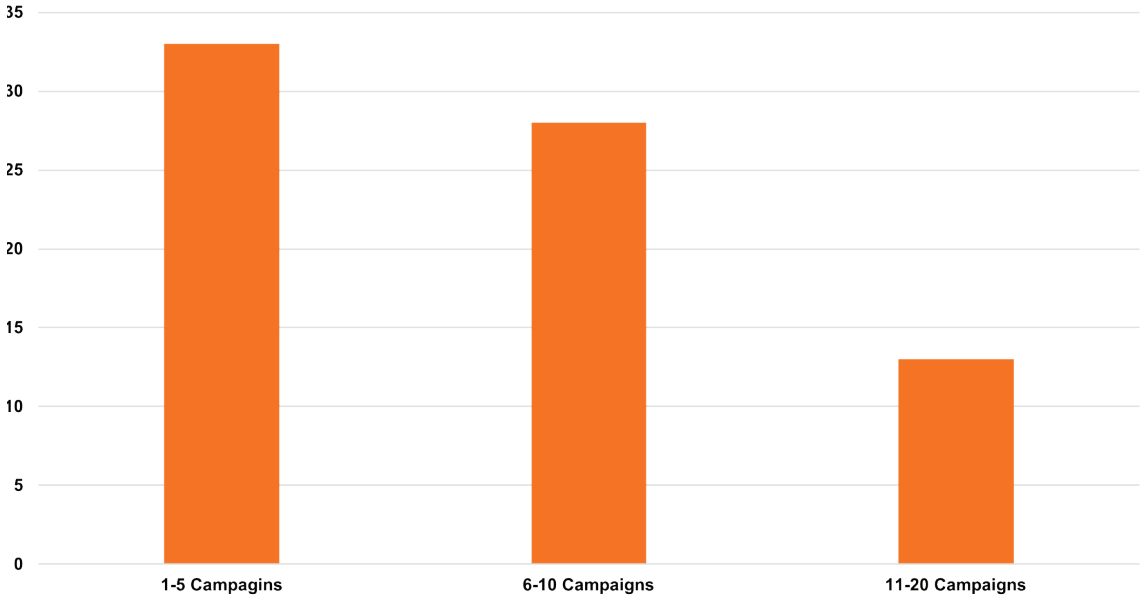

Figure 5: The more training campaigns you run, the more the phishing email click-through rate drops.

In our own testing, we see that risk is reduced proportionally; i.e., the more security awareness training is conducted, the better employees are at spotting and avoiding risks.

1) Companies that ran between 1-5 campaigns saw a 33% phishing click-through rate.

2) 6-10 campaigns dropped the rate to 28%.

3) 11 or more campaigns reduced the rate to 13%.

Additionally, phishing simulations and campaigns are most effective when the content is current and relevant.

Conclusion

This mid-year update to our annual threat report shines a light on the trends and changes seen by the Webroot threat research team, as experienced by our millions of customers. In the first half of 2018, we've seen a threat landscape that continues to expand as malware writers adapt new techniques and procedures to continually avoid detection, increase infection rates, and expand their target markets.

Key Takeaways:

» Ransomware attacks moved beyond brute force spam and phishing attacks, taking advantage of RDP vulnerabilities to conduct reconnaissance and find the most valuable targets.

» We've seen a massive move to cryptomining and cryptojacking to line the pockets of criminals at the expense of end users and organizations.

» Phishing continues to accelerate, shifting its primary target to Dropbox.

» Businesses are beginning to realize the necessity of security awareness training programs to educate end users on how to spot and avoid phishing emails and other risks.

As we move through the second half of 2018, we anticipate that threat actors will continue to adopt new techniques in an effort to stay one step ahead of defenders. It's a constant chase; as soon as one avenue is closed off, they look for another—whether it's RDP, UPnP, or another as-yet-unknown vulnerability that opens new doors. We anticipate expansion of targets as cybercriminals aim at new geographies around the world. The last half of 2018 will likely see many more instances of cryptojacking, as threat actors obfuscate their intent and may even circumvent Coinhive altogether.

Security isn't perfect, and threat actors don't stand still. It's worth their time and effort to continuously seek new, innovative ways to gain wealth and, for some, achieve a kind of notoriety.

The best and only way to withstand evolving threats is to employ a layered approach: proven security technology that covers all threat vectors and is constantly kept up to date, coupled with sophisticated, ongoing end user awareness training.

The Mid-year Update is an extension of the annual Webroot Threat Report, which examines emerging threats and cybercrime trends from the previous year, and shares perspectives and predictions for the future. To read the annual Webroot Threat Report, visit webroot.com/2018ThreatReport

About Webroot

Webroot was the first to harness the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide the number one security solution for managed service providers and small businesses, who rely on Webroot for endpoint protection, network protection, and security awareness training. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Headquartered in Colorado, Webroot operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity® solutions at webroot.com.

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