Skybox Security

VULNERABILITY AND THREAT TRENDS

2018 Mid-Year Update

Analysis of current vulnerabilities, exploits and threats in play

SKYBOX® SECURITY

Contents

EXECUTIVE SUMMARY

To deal with vulnerabilities old and new in your organization, it's vital to understand the role they play in the current threat landscape. This report examines new vulnerabilities published in 2018, newly developed exploits, new exploit-based malware and attacks, current threat tactics and more. Such insight gives context to the thousands of vulnerabilities.

This report examines trends in vulnerabilities, exploits and threats in order to better align your security strategy with the current threat landscape. Incorporating such intelligence to vulnerability management programs begins to put vulnerabilities in risk-based context and helps to focus remediation on vulnerabilities most likely to be used in an attack.

This is an update to a report published in January 2018 to reflect mid-year trends. All statistics for 2018 reflect data from the first half of the year — January 1, 2018 through June 30, 2018.

Key Findings

The Year of Cryptominers

If 2017 was the year of ransomware, 2018 looks likely to go down as the year of cryptominers. Malicious cryptomining made up nearly a third of attacks in the first half of 2018 — a statistic held by ransomware in the last half of 2017. Cryptomining malware is often able to run undetected, making money for attackers all the while, and goes directly to the source (i.e., where and how the money is produced) to make a profit rather than extorting individual victims. Cybercriminals seem all too happy to leverage these benefits.

Ransomware Loses Ground But Still a Threat

Cybercriminals by and large seem to be gravitating toward cryptominers for their profit-making machine of choice. As would-be victims get wise to ransomware tactics, defenses have become better. Proper backup systems and decryption programs have thwarted ransomware threats in many industries. However, as evidenced by attacks on healthcare and municipal organizations in the first half of 2018, ransomware remains a major concern, especially in vulnerable sectors. Successful attacks like WannaCry also remain a nuisance, hitting industrial giant Boeing a full ten months after the original outbreak.

Internet and Mobile Vulnerabilities Hold Strong Majority

Internet and mobile vulnerabilities make up nearly a third of all vulnerabilities; in contrast, vulnerabilities in server and desktop operating systems make up 14 percent and those in desktop applications account for just seven percent. This reflects the larger trend of software moving away from on-premise installations to the SaaS model. Unfortunately for security teams, they have less control over internet and mobile applications, potentially introducing a great deal of risk to their attack surface.

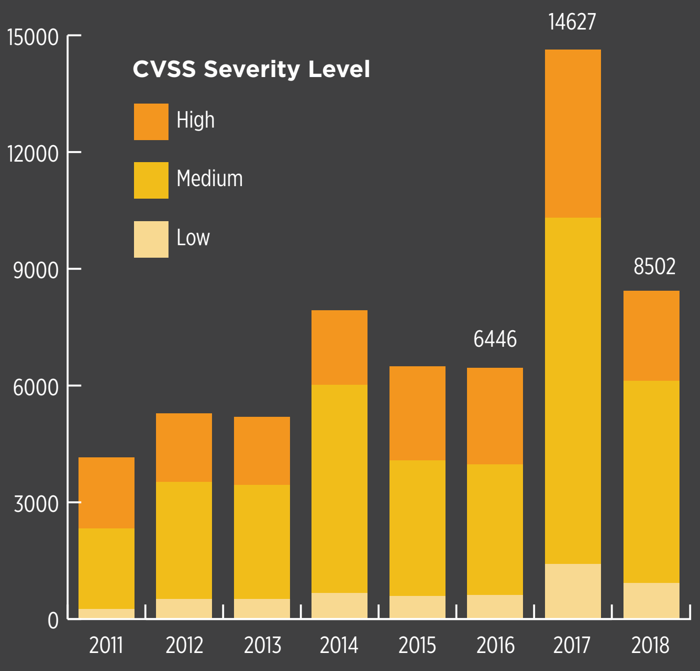
VULNERABILITIES AND EXPLOITS

The Vulnerability Flood Remains

In *The Vulnerability Flood* section of our January report, we noted the huge spike in the number of CVEs published. A total of 14,646 new CVEs were published by the end of 2017 representing a 127-percent jump over the previous year. This spike was due, in part, to increased resources in the MITRE organization and the National Vulnerability Database (NVD) which publishes CVEs, as well as an increase in vendor and third-party vulnerability research.

2018 shows no sign of slowing down. At the end of June, 8,502 CVEs had been published by NVD since the beginning of the year, already exceeding figures for all of 2016 and putting 2018 on track to exceed the record-breaking stats of 2017.

CVEs by Year



Source: https://nvd.nist.gov/vuln-metrics/visualizations/cvss-severity-distribution-over-time

In order to deal with the influx in vulnerabilities, organizations will need better prioritization mechanisms than simply base or temporal scores of the Common Vulnerability Scoring System (CVSS). To illustrate this issue, take for example CVE–2017–0147, a medium–severity (CVSS 5.3) information disclosure vulnerability in Microsoft's SMB protocol. This vulnerability, however, was used in the infamous NSA EternalBlue and EternalRomance exploits and used in the 2017 WannaCry attack. Clearly, CVSS doesn't always align with reality.

Additionally, CVSS doesn't reflect the risk posed in a unique network where certain critical vulnerabilities might be sufficiently protected by a combination of network topology and security controls, while a medium–severity vulnerability sits exposed to potential attack. Abiding by CVSS prioritization in this instance would incorrectly reflect the risk of such issues.

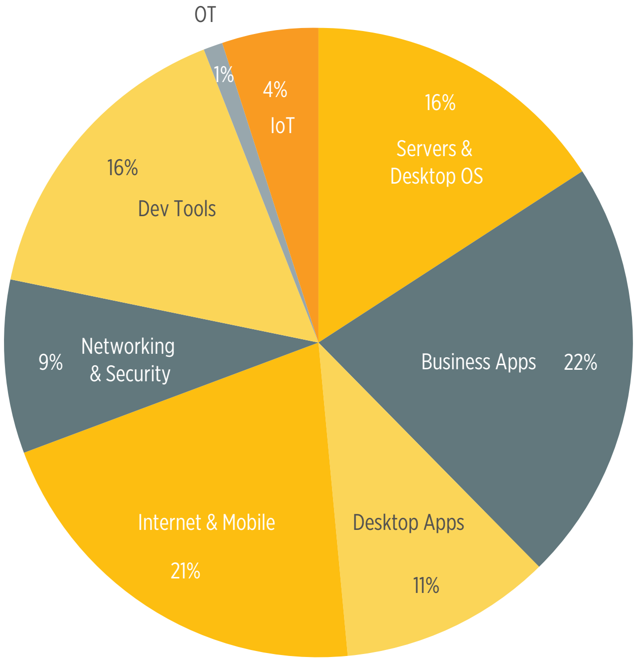
Vulnerabilities by Category

When analyzing vulnerabilities by the type of systems on which they exist, internet and mobile vulnerabilities account for the majority. As can be seen in the chart below, internet and mobile vulnerabilities make up 29 percent of vulnerabilities published in the first half of 2018, followed by business application and development tools with 19 and 17 percent, respectively. The internet and mobile category of vulnerabilities includes those found in mobile operating systems such as Google Android or Apple iOS; browsers like Google Chrome, Microsoft Edge, Mozilla Firefox and Apple Safari; and some internet applications like Adobe Flash and content management systems such as WordPress.

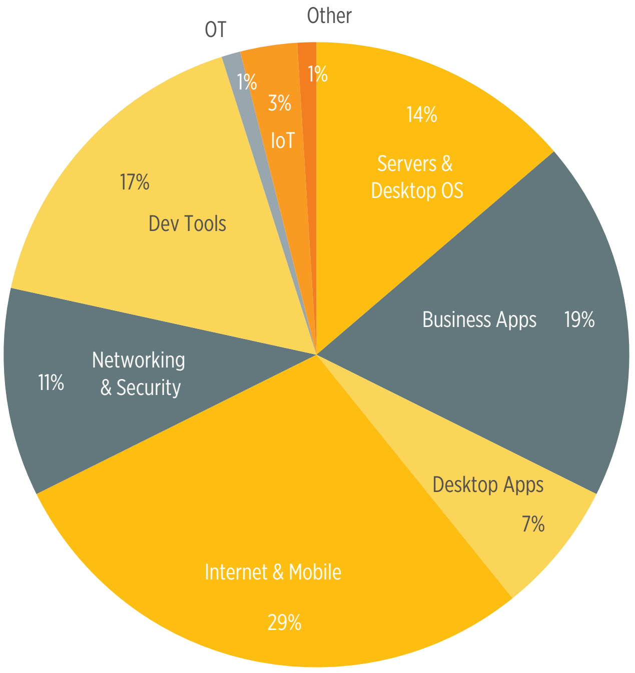
Comparing the second half of 2017 to the first half of 2018, internet and mobile vulnerabilities saw an 8 percent jump. During the same period, vulnerabilities in desktop applications fell 4 percentage points to just 7 percent of new vulnerabilities in the first half of 2018. These statistics highlight the shift from on–premise applications to internet and mobile application uses, as does a Microsoft prediction for its 2019 fiscal year: the tech giant estimated that two thirds of its business Office customers would be using Office 365.[1] And the more ubiquitous internet and mobile technology becomes, the more vulnerabilities will be discovered.

[1] Jha, Rajesh. Transcript from conference call at 2018 Deutsche Bank Technology Conference, Las Vegas. June 27, 2018. https://view.officeapps.live.com/op/view.aspx?src=https://c.s-microsoft.com/en-us/CMSFiles/JhaDB.docx?version=1cf04245-5f77-8460-1caf-eafa7764dfe0

Vulnerabilities Breakdown, Second Half of 2017



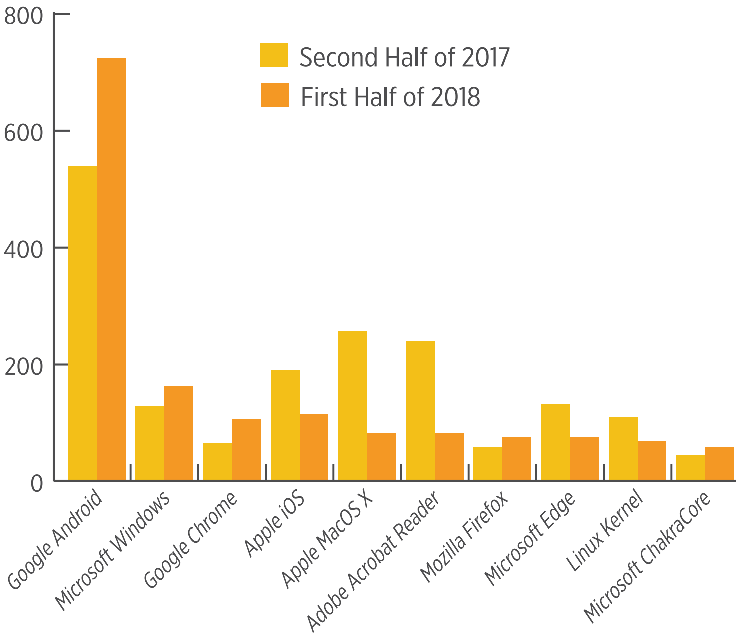
Vulnerabilities Breakdown, First Half of 2018



Top 10 Most Vulnerable Products

The top 10 products in the chart below made up for a fifth of newly published vulnerabilities — a combined total of 1,645 vulnerabilities — in the first half of 2018, while the remaining 990 products tracked by the Skybox® Research Lab were responsible for a combined total of 6,857 vulnerabilities. Tech giants including Google, Microsoft and Apple dominated the list in the first half of 2018. Smaller, open source applications do sometimes make the top ten; ImageMagick ranked fourth on the list for the second half of 2017 but fell to a slot in the thirties for the first half of 2018.

Vulnerabilities by Product



Google Android tallied 731 vulnerabilities in the first half of 2018 — nearly 200 more than in the second half of the previous year, accounting for 11 percent of all newly published vulnerabilities. Others in the top 10 list saw somewhat consistent vulnerability tallies between the second half of 2017 and first half of 2018; Linux Kernel, Microsoft Edge, Adobe Acrobat/Reader, Apple MacOS X and Apple iOS actually saw a decline.

WHY DOES Google Have SO MANY Vulnerabilities?

1 Mobile malware has increased overall. Google Android has proved more accessible than Apple iOS to malware developers, making for an easier target.

2 On top of the ubiquity of mobile devices themselves, Android is the market leader worldwide. More potential targets offer a better return on investment to exploit developers, who may be hunting for vulnerabilities on their own.

3 Google's bug bounty program for Android vulnerabilities is extremely active. In 2017, Google paid out nearly $3 million total for newly discovered vulnerabilities, in one instance paying $112,500 for a Pixel phone exploit alone.[2] Google also credits their bounty hunters, perhaps attracting more security researchers looking for fame and not just fortune.

4 Cryptocurrency malware has seen a 70 percent increase in the first half of 2018 over the second half of 2017, many of which target the popular Google Play store.

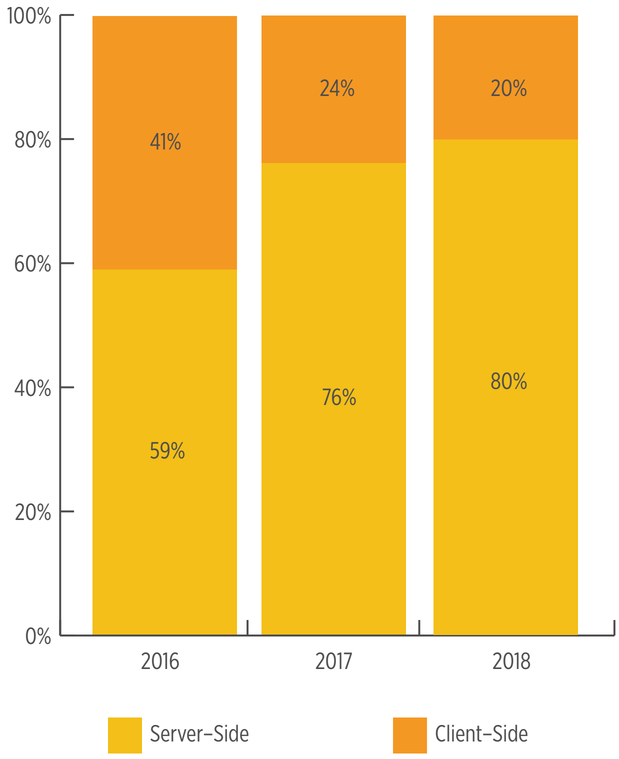
5 Mobile devices are increasingly connected to organizational networks, expanding their attack surface. However, due to "bring your own device" policies, IT departments have less control over mobile devices _ their OS upgrades, installed applications and links users choose to click.

[2] Tech Crunch. Google's bug bounty programs paid out almost $3M in 2017. June 27, 2018. https://techcrunch.com/2018/02/07/googles-bug-bounty-programs-paid-out-almost-3m-in-2017/

Server–Side Vulnerabilities Continues to Rise

The trend of server–side exploits dominating exploits in the wild has continued. In 2016, server–side vulnerabilities accounted for 59 percent of exploits in the wild; by mid–2018, that figure has risen to 80 percent. This trend is likely in part due to the decline of exploit kits leveraging client–side vulnerabilities, and the shift to server–side attacks like the Drupalgeddons, or attacks on network device like Cisco ASA.

Vulnerabilities Exploited in the Wild



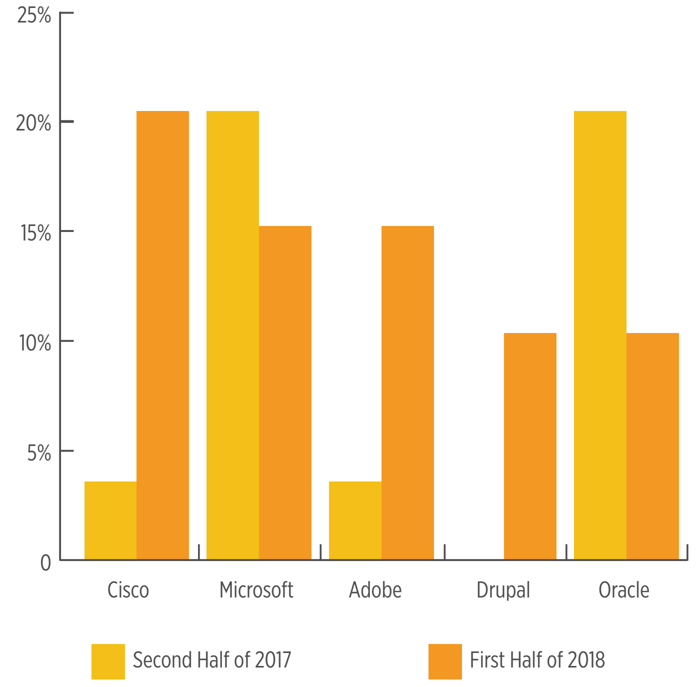
Most Exploited Vendors

Focusing in on exploits in the wild used in targeted as well as distributed attacks, Cisco shares the undesirable award for most exploited vendor in the first half of 2018, accounting for 21 percent of all exploits. In that time period, Cisco saw major exploits of Cisco Smart Install and Cisco ASA vulnerabilities as well as the VPNFilter malware which affected hundreds of thousands of Cisco routers worldwide.

Oracle, who held the first–place slot in the second half of 2017 with 21 percent of exploits, is now "only" in the fourth place with 11 percent of exploits in the first half of 2018.

Drupal was a surprise addition to the list, tying with Oracle for fourth place. In March, the Drupalgeddon2 attack exploiting CVE–2018–7600 put websites at risk worldwide and was leveraged by the Monero cryptominer and Muhstik botnet. Within a month, Dupralgeddon3 exploited security holes in Drupal versions 6 through 8 (CVE–2018–7602), allowing attackers to take full control of Drupal customer sites.

Most Exploited Vendors



THREATS

Web Browsers on the Rise ... Again

In Browser-based cyberthreats are still one of the biggest concerns facing cybersecurity professionals today. It's critical for organizations to implement effective protections from these hard-to-detect attacks.

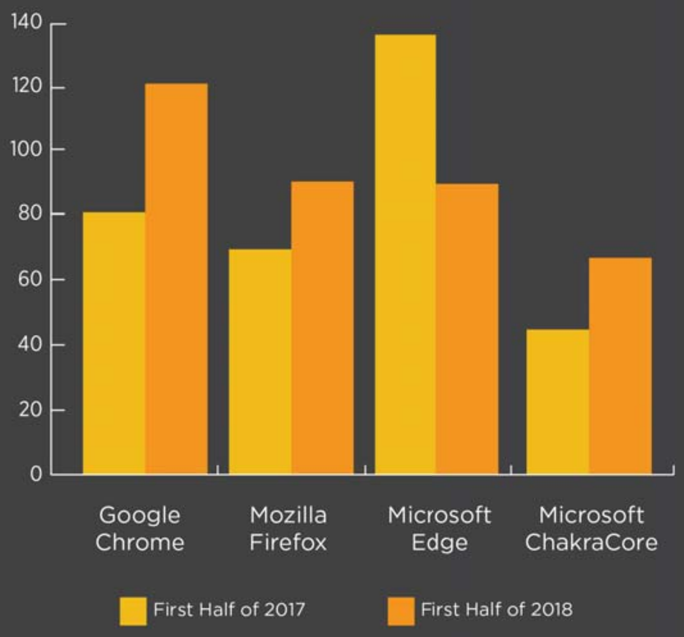
Out of the top 10 vulnerable products four are web browsers. With the exception of Microsoft Edge, all other web browsers saw an increase in the number of vulnerabilities in the first half of 2018 when compared with the second half of 2017.

Browsers are considered the most prone to malicious attacks from all other software in use. The reason is simple — web browsers constantly interact with websites and applications that cybercriminals have infected with malware (e.g., watering hole attack, malvertizing, adware, cryptominers).

Although browsers heavily use third-party plugins such as Javascript, Flash Player and ActiveX, these plugins will often have flaws attackers exploit to get access to systems. Online attackers use available vulnerabilities in browsers and their additional features to get access to the operating system, retrieve private data (banking Trojans), deny access to system files (ransomware) or install malicious software (cryptominers).

Web threats specifically designed to leverage browser-based vulnerabilities are on the rise not only because browsers are strategically desirable for attacks, but because such threats are extremely difficult to detect. Cryptominers, for example, can be active as long as the web session is active. Not all cryptominers need to install files, making it harder to detect. "File-less" malware is becoming a more popular obfuscation technique, as most malware detection and prevention technologies examine files such as downloads or attachments. If browser-based threats don't install files, conventional security controls have nothing to analyze. Unless organizations implement advanced tools that don't rely on file analysis, browser-based attacks will likely go undetected.

Top Vulnerable Browsers



Browser-Based Vulnerabilities AND THE Decline of Exploit Kits

In 2017, many exploit kits used mostly vulnerabilities in web browsers and similar applications. Continuing a trend since 2016, exploit kits have largely taken a backseat to other attack methods, though they're not entirely dead; the first half of 2018 saw multiple Adobe Flash zero-day vulnerabilities used in exploit kit attacks. But as use of vulnerability-plagued Flash is at an all-time low, attackers are looking to exploit other technology with a larger user base as these represent potential victims.

The exploit kits that are still around have shifted to using social engineering tools more than zero-day vulnerabilities. Financially motivated threat actors, though, have turned to cryptominers to target servers and harness their compute power to generate cryptocurrency.

Nation-State Threats

While much attention is given to the works of cybercriminals (ransomware, cryptominers), nation-state threat actors are still very active. Major cyber conflicts in the first half of 2018 include the VPNFilter malware and an Adobe Flash exploit.

VPNFilter

VPNFilter is a modular, multi-stage malware. Since 2016, when the malware was initially introduced, it has compromised more than 500,000 home and small office routers and NAS boxes. Infection of such a large scale could allow the malware's creators to utilize the affected nodes as a private VPN, making the trace back to the origin of a targeted attack very difficult.

The FBI hints to readers in its post that the VPNFilter malware attack could be the work of Sofacy Group, (a.k.a. APT28, Sandworm, X Agent, Pawn Storm, Fancy Bear, Sednit) which has been linked to the Russian military intelligence agency, the GRU. They have also seized a key domain that was used to infect home routers.

It was also noted by Cisco researchers that the "pattern of the attack indicates that the malware is part of a state-backed effort to create a versatile and effective botnet or data harvesting campaign, and shows the hallmarks of previous Eastern European malware efforts." Additionally, parts of this malware overlap code from the BlackEnergy malware which was responsible for multiple large-scale attacks that targeted devices in Ukraine, which was also attributed to a Russian government-backed threat actor.

Adobe Flash

On January 31, an Adobe Flash zero-day vulnerability was identified by the South Korea's KISA (KrCERT/CC). North Korean threat actors were targeting South Korean entities. It was exploited in the wild since as early as November 14, 2017. FireEye iSIGHT Intelligence and Cisco assess that a North Korean hacker group tracked by them — dubbed TEMP.Reaper and Group 123 — is behind the exploitation of this vulnerability. The group appears to be using TTPs that were previously used by the North Korean threat actor at the nation-state level.

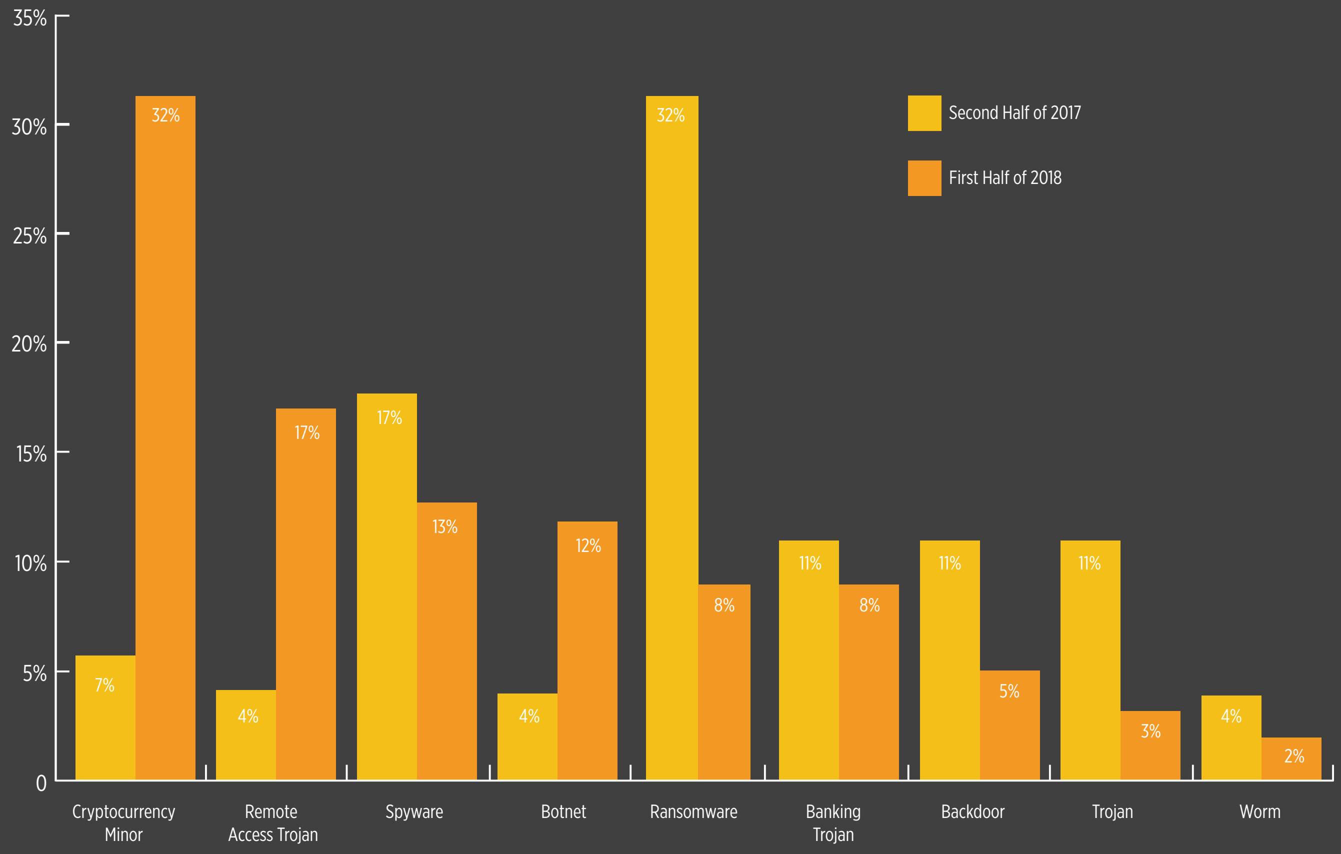
The main victims have been South Korean targets who have been affected by malware hosted on third-party South Korean sites, most likely a malware named DOGCALL (aka ROKRAT), a remote access Trojan that opens a back door on the compromised computer. It may also download potentially malicious files and steal information, meaning the threat actor can do pretty much everything on the compromised computer.

MALWARE AND ATTACKS

Top Malware Families

The chart below depicts the types of malware with the highest number of attacks. Notably, cryptominers had the highest increase in the number of new malware attacks, from seven percent of reported attacks in the second half of 2017 to 32 percent in the first half of 2018. At the same time, ransomware — the darling of cybercriminals in years past — saw a decline in attacks, essentially swapping market share with cryptominers. While ransomware and the other malware families are still a concern, malicious cryptomining has simply proved too attractive in terms of return on investment.

Malware Families by Type



Top Malware Attacks

IN THE FIRST HALF OF 2018

Cisco Smart Install Flaw

The attack took place on March 2018 when a group of hackers by the name of JHT utilized a vulnerability in Cisco Smart Install allowing the attackers to execute a remote code on Cisco routers. This attack affected approximately 200,000 routers across the world.

Drupalgeddon2

As the name implies the attack's targets were Drupal servers. This attack took place on March 28 as several groups of malware campaigns exploited Drupal's content management system. All Drupal versions from version 6 to version 8 were at risk due to this attack.

VPNFilter

Various types of routers have been infected by this malware attack. The VPNFilter is a modular, multi–stage malware that works mainly on home or small office routers. The malware had compromised more than 500,000 routers. Infection of such a large scale allow the malware's creators to utilize the affected nodes as a private VPN, making the trace back to the origin of a targeted attack very difficult.

Ransomware on the Decline

In 2017 ransomware was the undisputed payload of choice for attackers. In June 2017, at its peak, researchers at Malwarebytes reported 7 out of every 10 malware payloads were ransomware. But it was downhill from there — by July of that year, the ratio of ransomware dropped to less than 30 percent of all malware payloads. By December, the ratio had fallen below five percent.[3]

Why the decrease?

- In order to pull off a successful ransomware heist, the victim needs to lack reliable backups (or the time/resources required to use them). The victim also must have quick, easy access to cryptocurrency and trust the attacker to uphold their end on the bargain after he receives payment.
- To uphold that bargain, the attacker needs to be able to decrypt and release the files back to the victim. Failing to do so will initiate the law of diminishing returns — if the attacker can't be trusted, victims will see no point in paying a ransom to receive nothing in return. This was the case of NotPetya, which appeared to be ransomware at first, but, as victims reportedly weren't getting data back after ransoms were paid, fewer decided to pay up for what was ultimately a destroyer.
- Independent researchers have produced many standalone programs to decrypt files. These "vaccine" applications can somewhat minimize the impact of a ransomware attack.
- Growing awareness of ransomware threats along with the declining rate of file storage have ensured organizations put backups in place and utilize better protection tools.

As a cumulative result of these factors, for many threat actors, ransomware has ultimately become more trouble than it's worth. Especially with the rise of cryptocurrency miners which eliminate the issue of uncooperative victims

All that being said, ransomware may be on the decline, but it's definitely not dead and buried.

Cryptominers Reign Supreme

Cryptocurrency miners may be the new kid on the block, but they're taking over. With high–profit opportunity and a low chance of being discovered or stopped, this malware tool provides a money–making safe haven for cybercriminals.

Check Point noted that, "Every 10 minutes, Bitcoin commits a new block of transactions to its ledger and awards 12.5 BTC to its miner. At Bitcoin's current exchange rate ($10,515 as of 7 Mar 2018), that's around $130,000 paid to miners every 10 minutes, or $6.8bn per year." With such potential for profitability, it's no wonder that cryptominers have usurped the malware throne from ransomware. Ransom payments were almost entirely completed via untraceable cryptocurrency. Cryptominers cut out the middle man, going straight to the source.

[3] Crowe, Jonathan. 10 Must-Know Cybersecurity Statistics for 2018. Barkly. July 9, 2018. https://blog.barkly.com/2018-cybersecurity-statistics

Cryptominer Primer

Essentially, cryptomining uses computational power to create new blocks in the blockchain of cryptocurrencies like Bitcoin. As more blocks are added to the chain, more power is needed. Cryptomining starts entering malicious territory when it uses other's computational power without their explicit permission.

During 2017, the cryptocurrency market grew nearly 20-fold. As of today, there are more than 1,500 different types of cryptocurrencies. And this continued rise has caught the eye of financially motivated threat actors.

Malicious Cryptomining Purely for Financial Gain

Cybercriminals have taken an interest in utilizing the computing resources of compromised systems to mine cryptocurrency. They've targeted Windows servers, laptops, Android devices and even IoT endpoints. And cryptominers have become their own class of malware, including cryptominer–dedicated applications, browser–based applications and cryptocurrency wallet stealers.

Compared to other types of malware, unauthorized cryptomining on a host is often undetected or shrugged off as a nuisance. Being able to fly under the radar means less risk for cybercriminals, and the longer they go undetected, the more cryptocurrency they can mine. It's this longevity of profit that's making cryptominers rival one-time ransomware payments.

Why is Unauthorized Cryptomining a Problem for Enterprise?

In an enterprise environment, unauthorized or malicious cryptomining can have a major impact. Its consumption of computational resources can cause business-critical assets to slow down or stop functioning effectively. It also leaves an open door to let in other, more destructive or disruptive malware that can spread throughout an organization.

Also, a large organization is a large computational opportunity for the hacker, with a lot of potential computational power to be used when no one notices.

How You Can Stay Safe

Cryptomining malware often relies on vulnerability exploits. Patching those vulnerabilities — especially on high-value servers — is the best first step. Also, ensure proper security controls are in place around servers to limit their exposure.

Organizations and individuals can also block browser–based cryptomining software by installing a plugin to warn you when a site is trying to use your machine to mine or that blocks the mining domains.

Lastly, individuals should be vigilant (as always) to avoid phishing emails with suspicious links and attachments; double check the wallet address you're sending cryptocurrency to; and don't download mobile applications from any source other than the official application store.

CONCLUSION

In order to accurately prioritize remediation, organizations have to keep up with the threat landscape as it evolves. As trends in vulnerabilities, exploits and threat shift, so too must defense strategies. Keeping up with the latest threat intelligence — and taking proactive measures based on that intelligence — can make the difference between an intrusion and a damaging cyberattack or data breach.

Systematically incorporating threat intelligence in your vulnerability management and overall security management program is key to directing efforts in the right place. By combining information of your vulnerabilities, assets, network topology and security controls with intelligence of the current threat landscape, organizations will ensure resources are focused on risks most likely to be exploited by an attacker.

About This Report

All information and data in this report without explicit reference is provided by the Skybox™ Research Lab, a team of security analysts who daily scour data from dozens of security feeds and sources as well as investigate sites in the dark web. The Research Lab validates and enhances data through automated as well as manual analysis, with analysts adding their knowledge of attack trends, cyber events and TTPs of today's attackers. Their ongoing investigations determine which vulnerabilities are being exploited in the wild and used in distributed crimeware such as ransomware, malware, exploit kits and other attacks exploiting client– and server–side vulnerabilities. This information is incorporated in the threat–centric vulnerability management (TCVM) approach of Skybox's vulnerability management solutions, which prioritize the remediation of exposed and actively exploited vulnerabilities over that of other known vulnerabilities.

For more information on the methodology behind the Skybox Research Lab and to keep up with the latest vulnerability and threat intelligence, visit www.vulnerabilitycenter.com.

About Skybox Security

Skybox provides the industry's broadest cybersecurity management platform to address security challenges within large, complex networks. By integrating with 120 networking and security technologies, the Skybox™ Security Suite gives comprehensive attack surface visibility and the context needed for informed action. Our analytics, automation and intelligence improve the efficiency and performance of security operations in vulnerability and threat management and firewall and security policy management for the world's largest organizations.

www.skyboxsecurity.com | info@skyboxsecurity.com | +1 408 441 8060

SKYBOX® SECURITY