SKYBOX® SECURITY

2019 VULNERABILITY AND THREAT TRENDS

RESEARCH REPORT

CONTENTS

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 solution, 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.

EXECUTIVE SUMMARY

Vulnerabilities don't exist in a vacuum. The risk they pose to your organization depends on a variety of factors both internal and external that are in a near-constant state of change. Keeping up with that change is vital to limiting your organization's risk of attack. That's why we publish this report — to give CISOs and security leaders the perspective they need to see the trends shaping the threat landscape and, in turn, their defense strategy.

The *2019 Vulnerability and Threat Trends Report* examines new vulnerabilities published in 2018, newly developed exploits, new exploit-based malware and attacks, current threat tactics and more. Such analysis helps to provide much needed context to the more than 16,000 vulnerabilities published in the previous year. The insights and recommendations provided are there to help align security strategies to effectively counter the current threat landscape. Incorporating such intelligence in vulnerability management programs will help put vulnerabilities in a risk-based context and focus remediation on the small subset of vulnerabilities most likely to be used in an attack.

KEY FINDINGS

2018 will be remembered as the year when cryptomining rose in prominence, overtaking ransomware as the cybercriminal tool of choice.

Cryptomining attacks represented 27 percent of all incidents last year, rising from 9 percent in 2017 and far surpassing ransomware's 13-percent share in 2018. Its rise in popularity could be owed to the fact that cryptomining attacks are faster to execute, generate profit for the attacker over a longer period of time and often can occur without the victim's knowledge.

2018 brought more examples of exploits derived from patches.

This phenomena makes it ever more important for security teams to track exploitability and be able to quickly understand where and how to deploy temporary mitigations when immediate network-wide patching proves impossible.

Cloud security is strong but not bulletproof.

While cloud networks are relatively secure, attacks continue to occur like that against Tesla's AWS network in February 2018. The attack exploited an insecure Kubernetes console to launch a malicious cryptominer. Applications used to manage cloud deployments and misconfigurations also can pose a significant risk in cloud security, especially in increasingly complex, hybrid and fragmented networks.

Internal exposures pose a significant risk in vulnerable operational technology networks.

OT networks are still worryingly vulnerable, with attacks increasing by 10 percent in 2018 over the previous year. OT attacks can range in motive and impact, but the WannaCry outbreak in Taiwan Semiconductor Manufacturing Company is a prime example of how the combination of ransomware, worms and internal exposure can wreak havoc on a network — and a company's bottom line.

RESULTS

VULNERABILITIES & EXPLOITS

2018 has exceeded the previous year's vulnerability influx, tacking on a 12-percent rise over 2017's total of number of vulnerabilities published. As seen in the chart below, 2018 saw 16,412 new CVEs published vs. 14,595 in 2017. It seems 2017's initial raising of the bar is here to stay, and we expect 2019 to boast a similar tally.

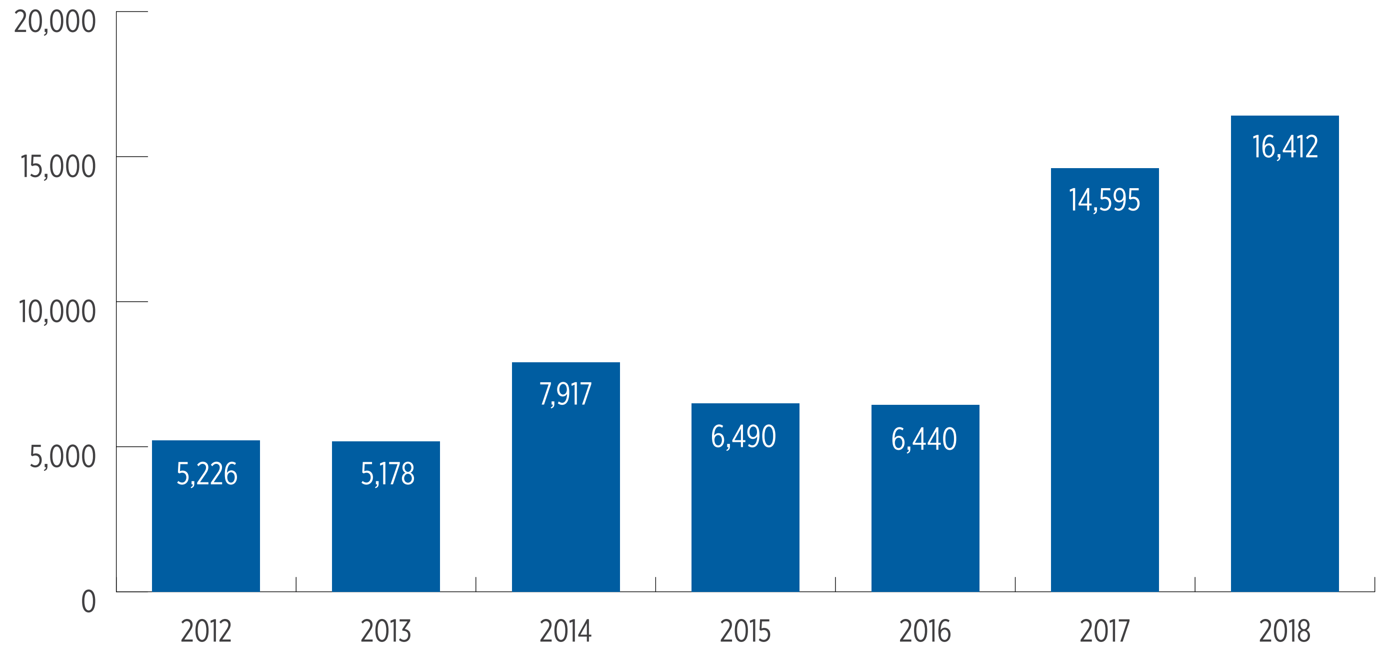


FIG 1 | New CVEs by year

In terms of Common Vulnerability Scoring System (CVSS) scores, 2018 kept pace with the previous year, with vulnerabilities scoring low, medium, high and critical at similar rates. High-severity vulnerabilities accounted for the majority, but medium-severity vulnerabilities also held a sizable portion: 34 percent. As we've seen many times in the past, medium severity doesn't necessarily equal medium risk, and this large portion of vulnerabilities can't be ignored.

Remediate the right vulnerabilities >

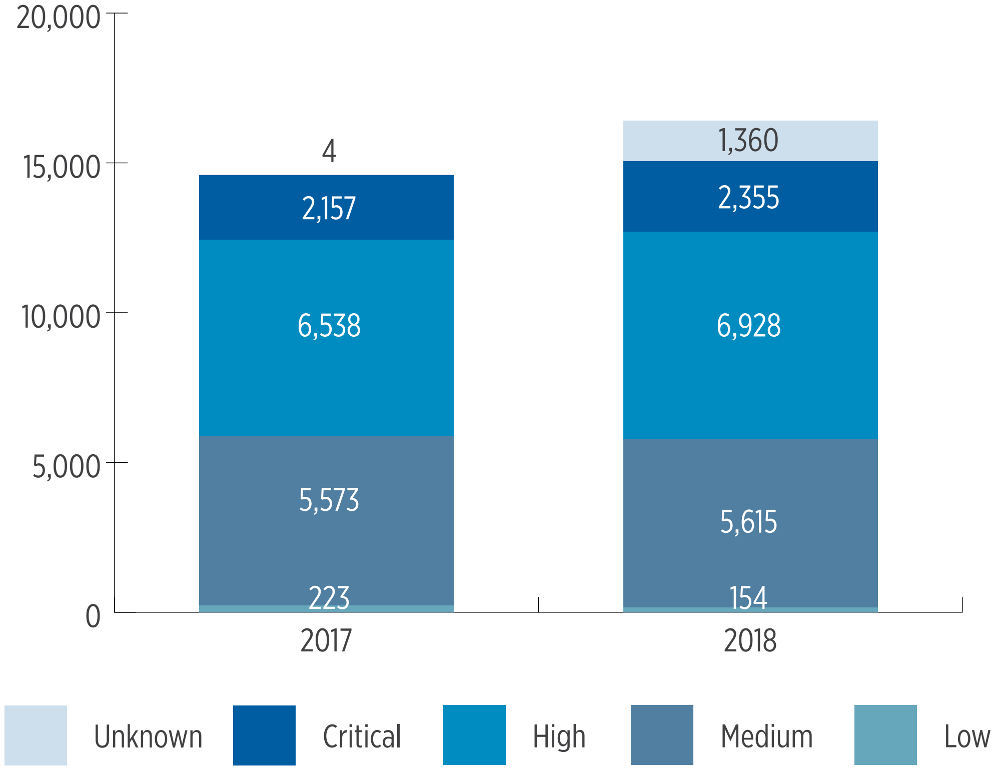


FIG 2 | New vulnerabilities by CVSS score

Vulnerabilities by Category

When analyzing the distribution of vulnerabilities by the type of systems on which they exist, a similar trend can be seen in 2018 when compared with 2017: business applications and internet and mobile vulnerabilities account for the majority.

As presented in the charts below, these categories each account for more than 20 percent of vulnerabilities published in 2017 and in 2018. The most vulnerable product in 2018 was Google Android, and the business application with the highest number of vulnerabilities was Oracle MySQL.

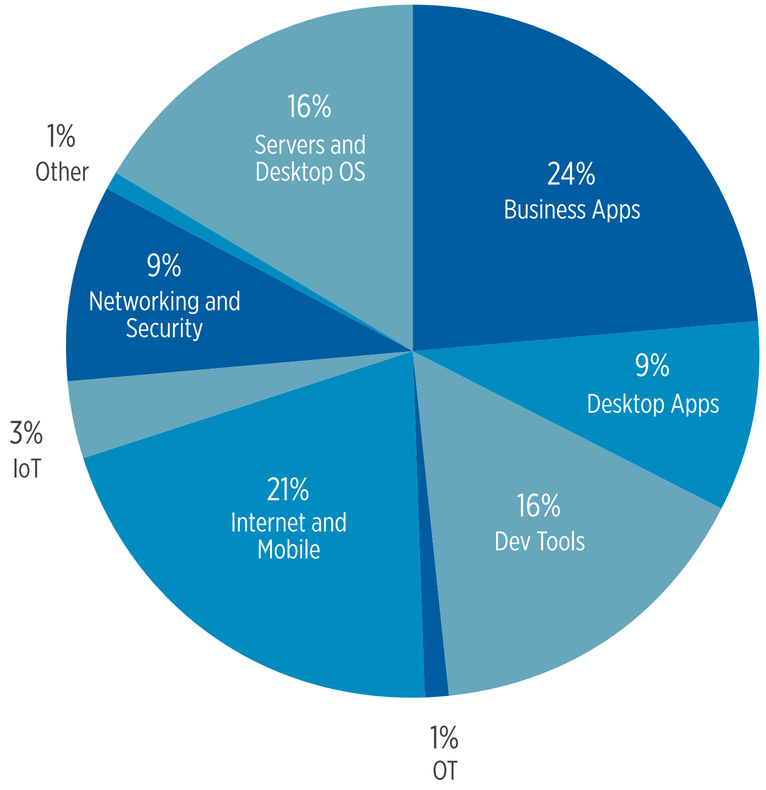


FIG 3 | 2017 Vulnerabilities by category

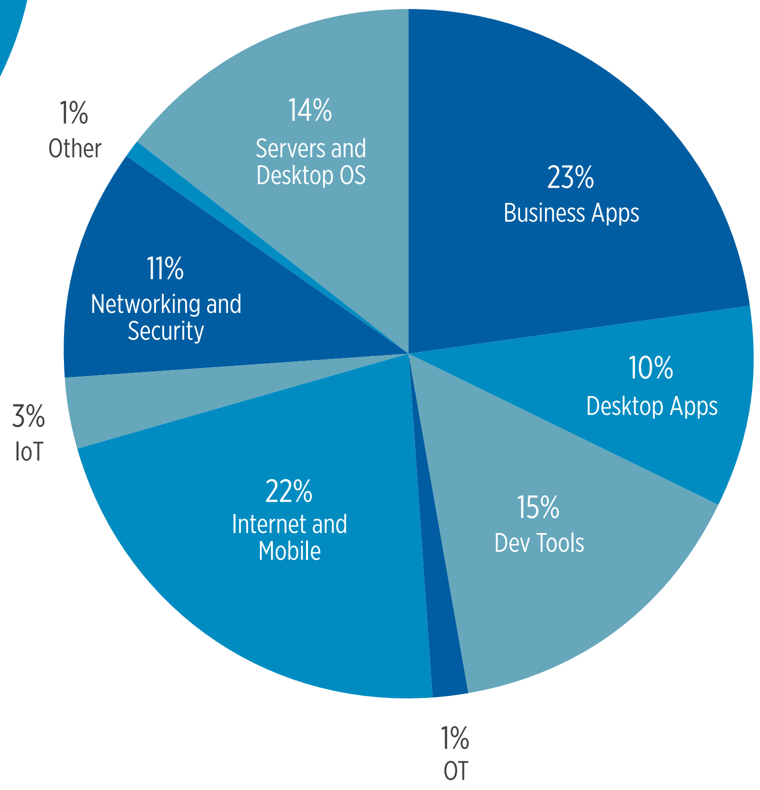


FIG 4 | 2018 Vulnerabilities by category

Top 10 Most Vulnerable Products

20 percent of all newly published vulnerabilities in 2018 are found in the 10 products detailed in the chart below. The top 10 carry a combined total of 3,167 vulnerabilities, with the remaining products tracked by the Skybox Research Lab being responsible for 13,245 vulnerabilities combined. As in 2017, tech titans Google, Microsoft and Apple are still at the top of the list.

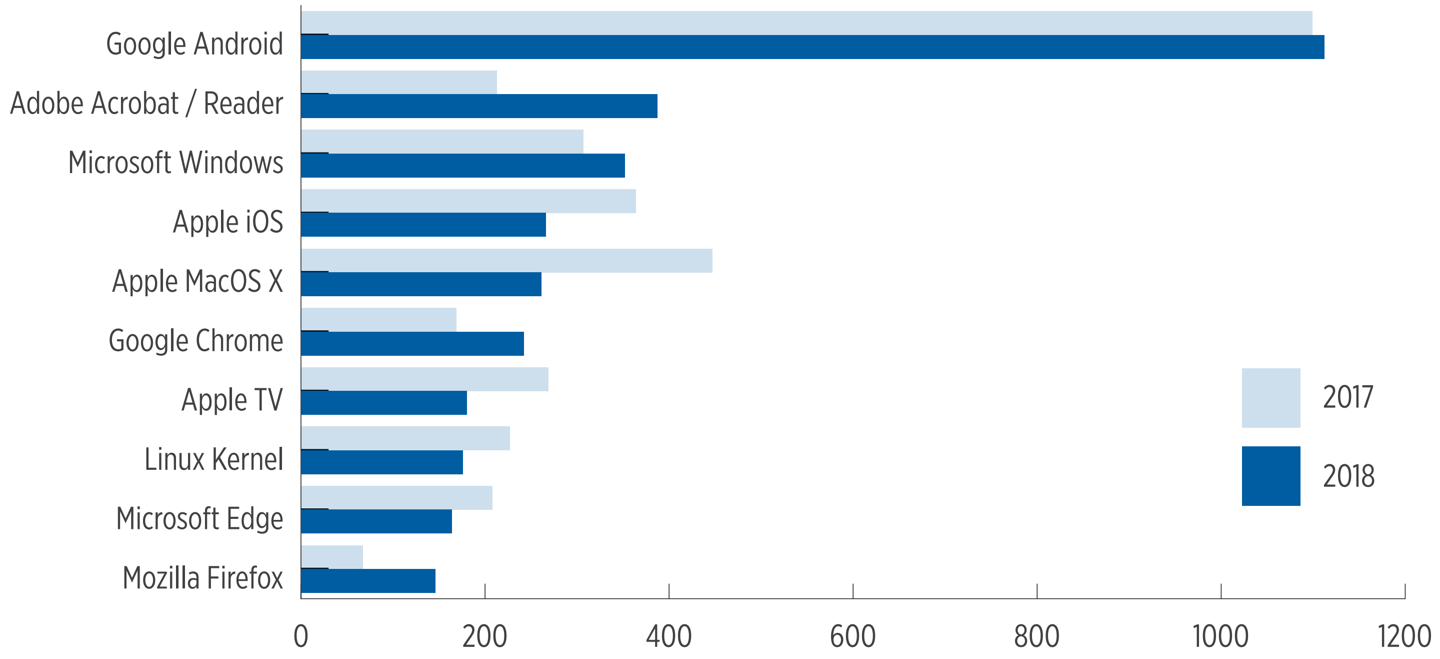


FIG 5 | Vendors with the most newly published vulnerabilities

Google Android's inauspicious lead shows that it now accounts for 35 percent of all vulnerabilities in the top 10 list, and 7 percent of the total vulnerabilities published in 2018. On the other hand, fewer vulnerabilities were published for Apple products in 2018 than they were the previous year. This decrease shouldn't necessarily be seen as a trend, however. The number of vulnerabilities published by Apple is almost on par with its 2016 figures (1,233 in 2018 vs 1,264 in 2016); it seems more likely that 2017 was an outlier year for the company.

It's important not to read too deeply into these raw figures: just because a product is listed in the top 10, it doesn't mean that it is innately more vulnerable than a product that didn't make the list. It's more likely that these products' tallies are so high because they are so ubiquitous, and because they apply more research and resources, as well as attract more attention.

Most Exploited Vendors

Microsoft is the vendor with the highest percentage of vulnerabilities exploited in the wild. The tech giant sits at the top of the list with 19 percent, followed by Oracle with 17 percent, and with Cisco and Adobe tied for third place at 11 percent.

However, Microsoft's share of exploits has decreased significantly from a high of 36 percent in 2017, while Oracle, Cisco and Adobe's percentage share increased. Microsoft's decrease can be attributed to two factors. The first is that 2017 was the year when The Shadow Brokers hacker group rose to prominence, disclosing a number of NSA exploits for multiple vulnerabilities in Microsoft's products. The second is the rise of cryptomining: Microsoft's products aren't as attractive to cryptominers as other systems.

It's also worth noting when looking at the chart that the number of Oracle exploits was actually lower in 2018 than 2017, but because Microsoft experienced such a dramatic drop in exploits, Oracle now has a larger overall percentage share.

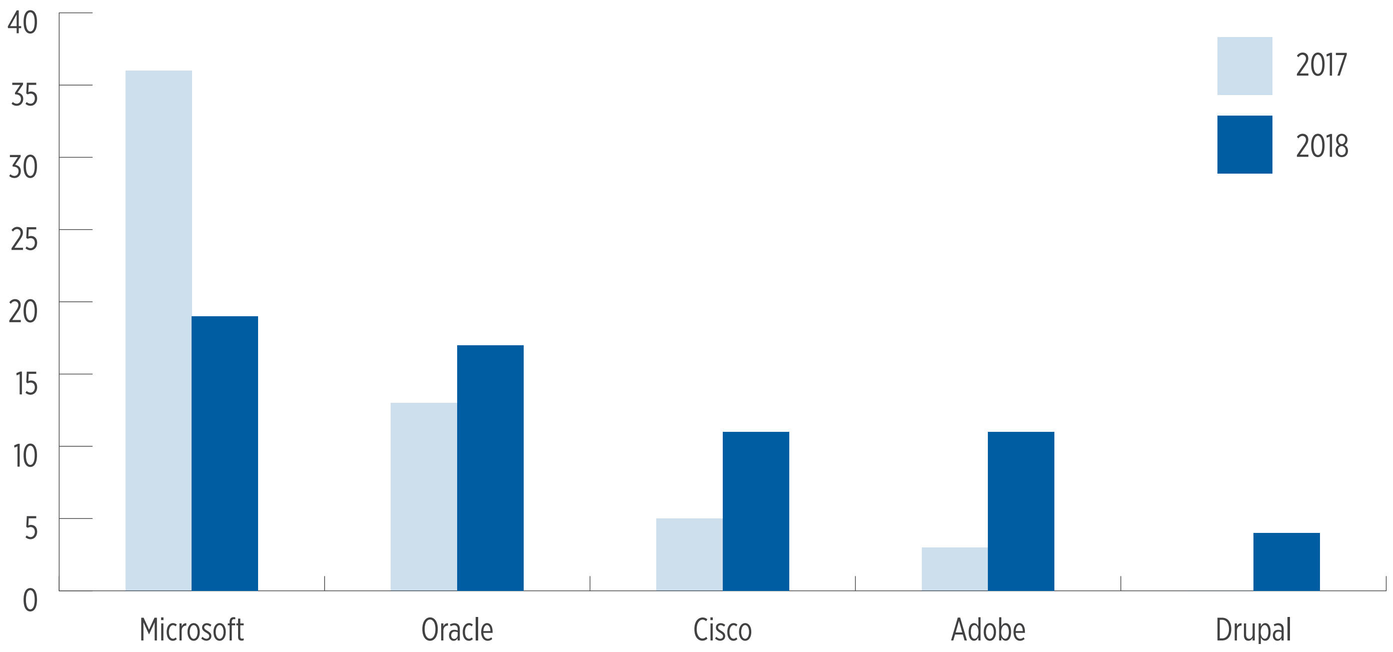
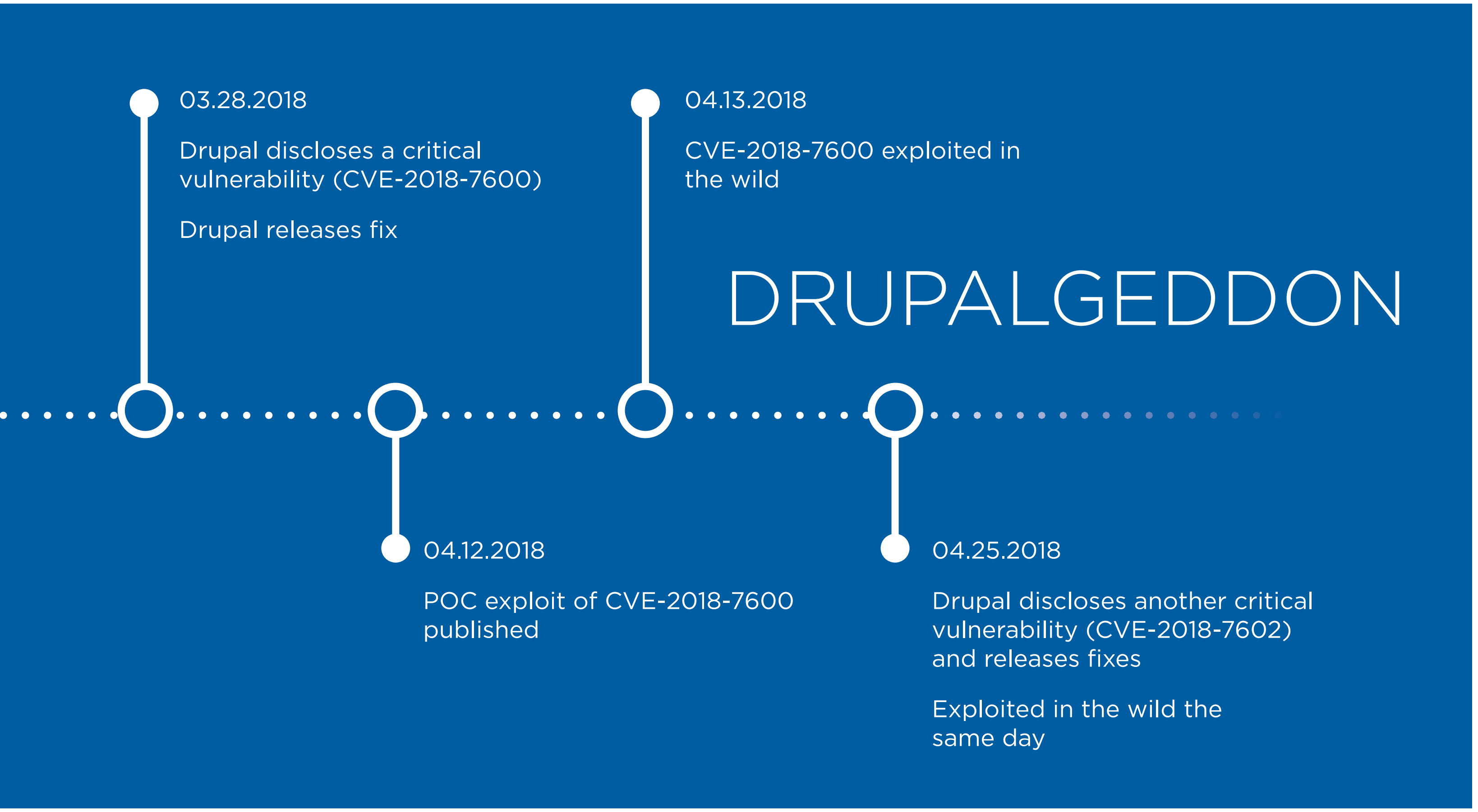


FIG 6 | Vendors with the highest percentage newly exploited vulnerabilities

Drupal, a tool used by more than one million organizations to manage web content, images, text and video, is a new addition to the most exploited vendors list. Its growing popularity may well be the reason why the open source content-management framework saw a vulnerability exploited two times in a single month. On March 28, 2018, the Drupal team discovered a critical vulnerability (CVE-2018-7600) which allowed potential attackers to take control of vulnerable websites. They immediately released updated versions, allowing websites to patch the issue as quickly as possible. Two weeks later, on April 12, a proof-of-concept was published and, shortly after, fully fledged exploits were used in the wild. Dubbed "Drupalgeddon2," websites worldwide were put at risk when the Monero cryptominer and Muhstik botnet made attempts to exploit it.

Later that month on April 25, another Drupal vulnerability (CVE-2018-7602) was discovered, with updates released shortly after. On this occasion, the attack ("Drupalgeddon3") attempted to turn affected systems into Monero cryptominer bots and began only a couple of hours after the updates were published. This is clear sign that attackers are waiting to pounce when Drupal acts, as they are with other high-profile vendors. But with open-source systems like Drupal, it's much easier for attackers to gain access. Security-conscious users beware.



DRUPALGEDDON

03.28.2018

Drupal discloses a critical vulnerability (CVE-2018-7600)

Drupal releases fix

04.12.2018

POC exploit of CVE-2018-7600 published

04.13.2018

CVE-2018-7600 exploited in the wild

04.25.2018

Drupal discloses another critical vulnerability (CVE-2018-7602) and releases fixes

Exploited in the wild the same day

THREATS

An Online World Sees Web Browser Vulnerabilities Continue to Rise

On the whole, vulnerabilities that exist in browsers are still on the rise. There were 20 percent more vulnerabilities published on browser-based products in 2018 than there were in 2017. There are a couple of exceptions; Microsoft Edge and Apple Safari's vulnerabilities decreased in 2018. This decrease may be because they're less popular with attackers, because there has been a shift in attack tactics or because of a change in their bug bounty mechanisms.

Web browsers still favored by attackers >

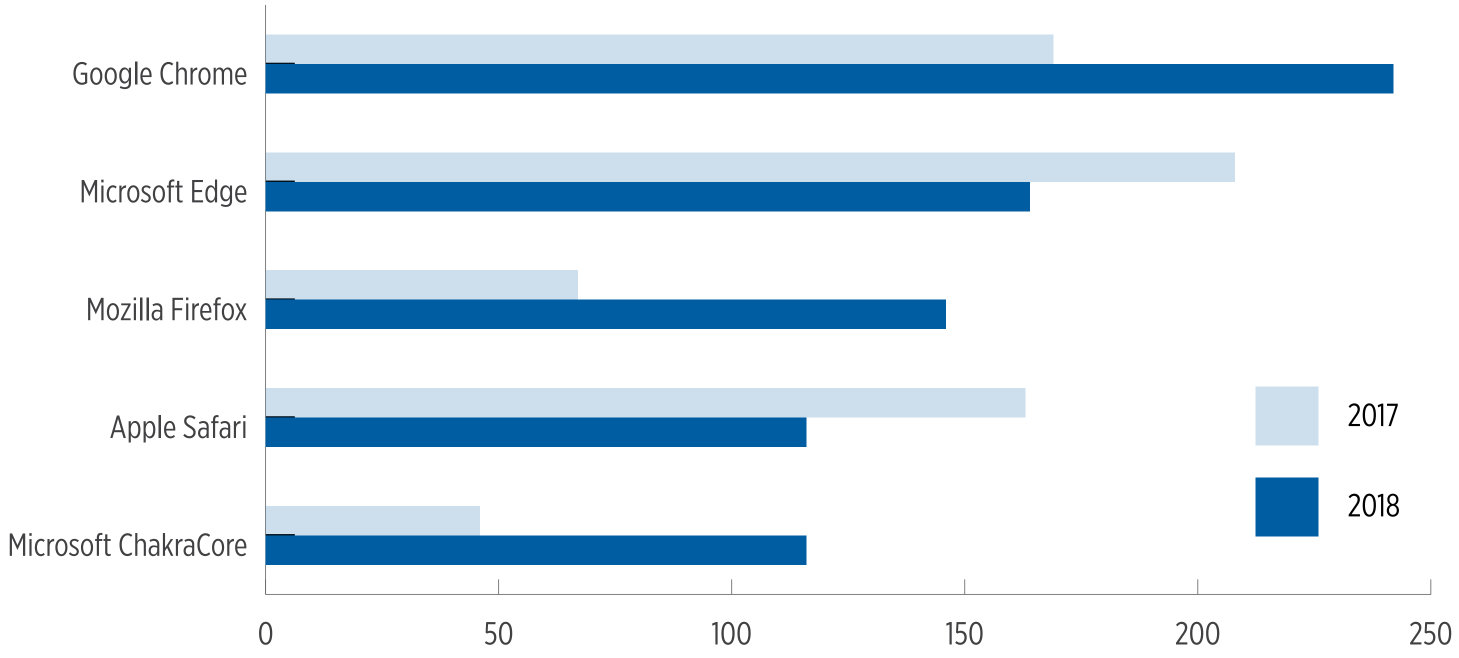


FIG 7 | Browsers with the most newly published vulnerabilities

MALWARE & ATTACKS

Top Malware Families

The popularity of different malware methods changed in 2018, as can be seen in the chart below. The number of ransomware attacks decreased from 28 percent of malware attacks in 2017 to 13 percent in 2018. This is significant: ransomware dominated the threat landscape in 2017. This dissipation doesn't mean that ransomware presents any less of a threat, but it does indicate a change in the way that attackers are working. Their attentions are now shifting towards cryptomining. In 2017, cryptocurrency miners accounted for only 9 percent of attacks. In 2018, that number jumped to 27 percent.

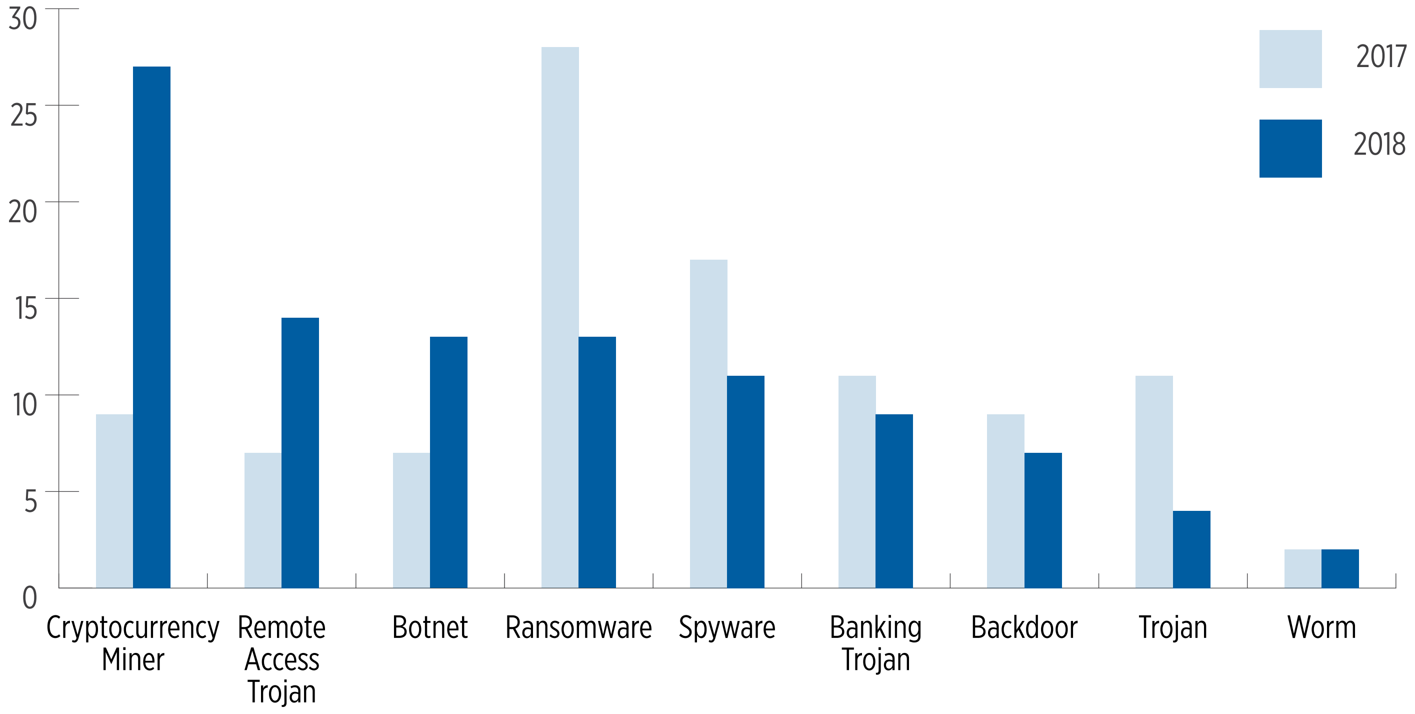


FIG 8 | Percentage of attacks attributed to malware families

OT Attacks on the Rise

Operational technology (OT) is a part of the hardware and software that monitors and controls how physical devices perform. OT is common in critical infrastructure organizations such as manufacturers and utilities.

In the past, OT was used to control systems that were not connected to the internet. But as digital transformation efforts spread within the industrial environment, many of today's OT systems are linked to corporate IT networks, leverage common internet protocols and are increasingly connected via wireless technologies — all making them accessible targets for cybercriminals. These systems play a fundamental role in ensuring that many elements of a modern society are able to function. That's why they are a prize target for attackers, particularly those with nation-state aims and backing.

The number of advisories published by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), an authority for OT security professionals, increased slightly from 174 in 2017 to 192 in 2018. It's possible that this moderate 10-percent increase will get worse in 2019; the potential is significantly higher, particularly when you consider how slowly OT security is improving in comparison to IT security.

Attacks on ICS computers are also steadily increasing. In the first half of 2018, 41 percent of ICS computers were attacked at least once, a five-point rise over statistics for the same period in 2017.[1] We anticipate this figure will continue to rise in 2019.

These attacks aim to take control of systems and machines and to disrupt their normal activities, to steal data or simply cause damage. Naturally, this is a domain of particular interest to nation-state threat actors who place campaigns in the digital space alongside diplomatic attacks and conventional warfare as a way of gaining advantage against their adversaries. For obvious reasons, many of these attacks have not been, and will not be, published for public consumption.

Source: Kaspersky Labs https://www.kaspersky.com/about/press-releases/2018_ics-computers-attacked-in-h1

INSIGHTS

Another Record-Breaking Year: What Does it Mean?

Looking at the raw figures alone in terms of number of new vulnerabilities published, it's easy to jump to the conclusion that we're living in a more vulnerable cyber world. But that's not necessarily the case: there are other factors at play that affect the tally and its impact. The primary factor is an increase in reporting abilities. The MITRE organization and the National Vulnerability Database (NVD) both increased their resources, meaning that they were able to give out more CVEs. This invariably boosted the numbers.

Another major factor is more research. The intensity of vendor and third–party vulnerability research has grown in recent years, resulting in more requests for CVE identification; though this may be cold comfort for security professionals in charge of vulnerability and patch management.

There are also a number of other factors, all tied up with the increasing complexities of operating within a digital world, that are increasing opportunities for attackers and making life more difficult for enterprises. In this section of the report, we'll dive into the details about some of these complexities, bringing in real–world case studies to illustrate the most pressing risks that organizations faced in 2018 — and will continue to be forced to confront in 2019.

Fragmented Supply Chain Is Increasing Risk Exposure

Enterprises invest a great deal of effort in creating strong cybersecurity protocols to protect their work environments. But this effort can be negated by weak links in the supply chain. It's increasingly common today for enterprises to outsource many of their processes and to purchase fully formed products — from office supplies to cloud storage — from different vendors. The cyber connections of each of these vendor relationships could present attackers with a foothold into a corporate network.

When you consider the increasingly large quantity of vendors and suppliers involved in corporate supply chains, it's inevitable that organizations are going to be more exposed to risks as they delegate elements of their network infrastructure to third parties.

Attackers love to target weak spots, and supply chains offer many, such as:

- **Inherited risk:** A third–party supplier might have a lower standard of cybersecurity and level of protection than their client. And, as third–party connections can often develop blind spots in the attack surface, enterprises may not understand where they're introducing risk to their network.

- **Compromised software:** When software is installed and connected to the network, improper security protocol might result in a cyberattack. Big organizations invest time and money in having extended security protocols to protect their data and networks. One issue is that they assume that the small suppliers that they purchase software from are following the exact same standards and protocols as they do. In reality, this is almost never the case.

  Additionally, the growing use of open–source applications has created new attack opportunities for cybercriminals. Organizations may think that they have limited the risks present in these applications by introducing protocols that identify and ban unwanted pieces of software, but potential attackers can still inject malicious code into legitimate applications which can very easily spread when distributed to a large pool of trusting customers.

- **IoT devices:** As the use of internet–connected devices continues to soar, it makes sense that cyberattacks on internet of things (IoT) devices are on the rise. The breadth and scale of the potential attacks that we will see in 2019 is huge — they could hit anything from smart cameras to smart buildings, coffee machines to dishwashers. Owing in part to the fact that the technology is so new, there are multiple ingress points that attackers can take advantage of that organizations may not have even considered as being part of their security infrastructure.

  These devices have their own supply chains which are not under the direct supervision of the organization which they are being used in and, accordingly, are likely to have less stringent security defenses. The red flags around IoT technology couldn't be clearer. But despite the fact that many of the devices are insecure, and despite being known for using default — and sometimes even hard-coded, passwords — it's unavoidable that this technology will continue to rise in prominence in the workplace. It may be expensive and time–consuming to create the cybersecurity protections needed for these devices, but it should be considered to be a fundamental priority for any enterprise in 2019.

Reduce third–party risk >

Cloud's Potential Impact on the Attack Surface

Enterprises understand what they need to do to secure traditional IT infrastructure. But when it comes to using a public cloud, there is a mist of confusion around how to maintain the same stringent security standards. While the cloud is relatively secure, if attacks on cloud service providers (CSP) are successful, it's possible for hackers to rapidly impact a wide network of companies across the globe. This issue is of great concern to the cybersecurity community and, because there are currently no cloud–focused international protocols, it's unlikely that this sense of unease is going to dissipate anytime soon. As such, it's even more important for enterprises to stay alert, to thoroughly examine the security protocols of their CSP, to gain visibility of their entire environment and to ensure that both parties uphold their end of the bargain in the shared responsibility model.

Strengthen cloud network security >

TESLA CLOUD ATTACK AND THE COMPUTATIONAL THREAT

In February 2018, hackers exploited an insecure Kubernetes console to siphon processing power from Tesla's cloud environment in order to mine cryptocurrencies. Tesla worked with Amazon Web Services (AWS) which also included Amazon S3 (Simple Storage Service). Access to this data allowed the hackers to gain information about the telemetry and other vehicle data metrics from Tesla's testing fleet; but harvesting the data wasn't the attack's main purpose. Instead, this should be seen an example of how the security landscape is expanding beyond data theft to computational power theft. The evasive measures undertaken by the hackers in this instance highlight just how sophisticated the computational threat of cryptojacking has become: it can slow users' computers while simultaneously costing the organization a fortune in power bills.

Misconfigurations Introduce Risk

Humans continue to be a massive weak link when it comes to cybersecurity. This is particularly evident when looking at the rise in misconfigurations of access points and key management, whereby cloud servers are vulnerable to breaches due to incorrect configuration. Because cloud server configuration often requires complex, specialized knowledge and training, it's likely that an individual lacking the requisite skills or knowledge will make a mistake during configuration.

In addition, the incorporation of third-party software in the cloud introduces more fragmentation to enterprise environments. This makes network visualization more of a challenge, leaving many organizations in a position where they cannot say that they have full control over their attack surface — you can't protect what you can't see.

This is not to say that these misconfigurations are only found in the cloud. They are also still present in on-premises networks. If a network device uses a default username and password, if a third-party app uses weak encryption protocols or if no proper logging is enabled, organizations are putting themselves at risk of attack. All of these weaknesses can, and will, be used either in an easy way to stage an attack or for hackers to gain lateral movement within the organizational network.

OT Attacks Are of an Increasing Concern

The WannaCry attack on Taiwan Semiconductor Manufacturing Company (TSMC) in August 2018 is indicative of the disruption that is caused by attacks on OT networks. After first being addressed in Microsoft's MS17-010 bulletin on March 4, 2017, the malware made an unwelcome return on August 3, 2018, when an employee installed some infected software without running a virus scan. When it connected to the network, WannaCrypt, a variant of the ransomware WannaCry, infected more than 10,000 unpatched computers and "fab tools" at multiple TSMC foundry sites in Taiwan.

The attack forced a day-long production halt and incurred a couple days' recovery time, a disruption that appears to have had a dramatic effect on the company's financial performance. Ironically, in this incident, the isolation of the affected network from the internet — generally a crucial safeguard for sensitive OT systems — contributed to the ransomware's ability to traverse it.

Because OT systems are so crucial to everyday life, and because they are being made more accessible, it makes perfect sense for attackers to continue with their assaults. It's almost certain that there will be an increasing number of these attacks in 2019 and beyond.

Protect your OT network >

SHAMOON

Shamoon (also known as Disttrack) is a disk-wiping malware whose notoriety has grown over the last seven years. It has been implicated in three waves of attacks against the enterprise systems of OT companies, increasing its scope and geographical reach with each iteration. Its most recent attack was also its most destructive.

Following incidents in 2012 and 2016/7, Shamoon returned again on December 10, 2018. The attack's first reported victim was oil giant Saipem, and its impact was felt around the world. It removed all data from several hundred Saipem computers across Saudi Arabia, the UAE, Kuwait, India and Scotland, replacing the data with garbage and rendered the systems useless when they rebooted in an unrecoverable state. All variants of Shamoon to date rely on a hard-coded list of machine names to spread.

What this means is that the data threat is tailored to its victim using information obtained beforehand. A blog on the firm's website announced that no data was stolen or lost (all wiped data could be retrieved thanks to backups) and that Saipem did not expect to lose any revenue. It is still likely that the oil giant was functionally disrupted: its business interface with the outside world was effectively crippled for the duration of the attack and its aftermath.

Web Browsers Are Still Favored by Attackers

It's normal for websites to use elements from multiple sources, many of which are not controlled by the site owners. The risks of exposure to dangerous scripts and plugins that live on websites are well documented. Visit an affected website and you could get stung. Distributing malware through websites still has great appeal for attackers: they hit a lot of people and can do so without risking detection. From the perspective of a cybercriminal, what's not to love?

The increases in vulnerabilities detected in Google Chrome, Microsoft ChackraCore and Mozilla Firefox (as detailed in the section *An Online World Sees Web Browser Vulnerabilities Continue to Rise*) are indicative of the general trend towards a higher number of vulnerabilities in browsers, and continue to raise concern in the cybersecurity industry. 2018's results aren't a one-off. Based on previous years' trends, they're a sign that things are only getting worse. As the world marches steadily into the digital arena, it's inevitable that browser-based vulnerabilities and exploits will only continue to undergo significant increases.

FLASH ISN'T DEAD YET

Adobe Flash has been known to be a top target for attackers for a long time. Installed on countless devices, both for personal and enterprise use, and present in millions of web browsers across the globe, its bugs have been leveraged for a large number of attacks.

Flash is an easy target for two main reasons. First, it has a very poor update mechanism that places the onus of vigilance on its users, most of who will only agree to update if they run into problems. Second, Flash is included in many standard and widely available, ready-to-use exploit kits. These kits don't need advanced skills for deployment, which lowers the bar of entry for would-be cybercriminals to ply their trade.

During 2018, eight vulnerabilities were published on Flash. Of these, three were actively exploited in the wild:

CVE-2018-4878

- Use-after-free vulnerability
- A remote attacker could exploit the flaw by enticing users to open documents, web pages or emails that contain Flash files, which could lead to arbitrary code execution.

CVE-2018-15982

- Use-after-free vulnerability
- A remote attacker could exploit the flaw to execute arbitrary code on the affected system

CVE-2018-5002

- Stack-based buffer overflow vulnerability
- A remote attacker could exploit the flaw to execute arbitrary code

Abode has released security updates for all vulnerabilities.

As Adobe Flash has become notorious for exposing its users to threats, there has been a decrease in the number of users. Adobe itself has encouraged users to move to alternative technologies and has announced the product's end of life in 2019. With a shrinking user base, Flash has garnered less attention. In 2018, there was a 60-percent decrease in the number of new vulnerabilities detected.

Despite all this, several websites continue to use and depend upon Flash for their immediate future — as will attackers looking for a tried-and-true exploitable collection of flaws.

Cryptocurrency Malware Offers Profitable Opportunities for Criminals

It's clear that 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. Cryptominers have created their own class of malware, including cryptominer-dedicated applications, browser-based apps and cryptocurrency wallet stealers.

Malicious cryptominers took a step up in 2018, replacing ransomware almost completely as the cybercriminal's tool of choice. One of the main reasons behind this trend is because cryptomining attacks are faster to execute and will generate more profit for the attacker over a longer period of time. From the criminal's point of view, it's a win-win.

Additionally, while ransomware requires an engagement with users, cryptomining runs in the background; users are often unaware that an attack is being conducted. It's far more likely that users will notice a giant ransom message that takes over their screen and turns all their files into nonsense than it is they'll notice 70-80 percent of their CPU or graphics card is being used to generate virtual coins.

It's this last point that should be of concern for enterprises. While cryptomining may seem like a relatively innocuous threat, it's important to remember these attacks may overwhelm system capacity. They slow down processes which could even lead to machines being damaged. More than that, the cryptominer's end goal may extend beyond gathering currency. They may be more interested in gaining a foothold in your network which could be used to access other parts of your environment. It's the sleeping dog that you shouldn't let lie: it may well wake up and bite you.

RISE IN CRYPTOMINING HAS LITTLE TO DO WITH BITCOIN

Cryptocurrency attacks gained popularity in 2018. But it's not because of BitCoin. Yes, BitCoin is the most common type of cryptocurrency and is still popular for use in underground activities, but it's not being widely mined in malware attacks.

The currency of choice for cryptominers is Monero. It's an open-source cryptocurrency that provides an alternate monetization platform with better anonymity preferences. This means that potential attackers can use it to mine easily on any machine while leaving no trace of the money that was transferred through it. As such, Monero mining is preferable over Bitcoin mining, despite its lower value.

RECOMMENDATIONS

Remediate the Right Vulnerabilities

While CVSS scores are an important aspect of understanding the risk a vulnerability poses to your organization, understanding the likelihood of its exploitability should also be given due consideration. Some of the vulnerabilities which have the most pressing need for remediation could be hiding in plain sight: for example, a CVSS medium-severity vulnerability may be under active exploit in the wild while a critical-severity vulnerability has no exploit developed. In this case, the medium-severity vulnerability would pose a greater risk and is a higher remediation priority — even moreso if it's exposed in your network.

In order to focus remediation efforts on the small subset of vulnerabilities most likely to be used in an attack, organizations need to use a threat-centric vulnerability management (TCVM) approach, which calculates vulnerability risk based on:

- Exploit activity in the wild
- Exploit use in packaged crimeware (e.g., ransomware, exploit kits)
- Exploitation availability and potential impact
- CVSS score
- Asset value
- Asset exposure

These last two factors — asset value and exposure — are of course specific to each unique organization. That's why it's so important to stay abreast of changes both in the threat landscape and within your infrastructure, and to correlate this information to accurately prioritize remediation. Such insight will also help organizations extract more value from existing security controls such as firewalls and intrusion prevention systems.

To learn more about the TCVM approach, click here.

Reduce Third-Party Risks

As referenced in the section *Fragmented Supply Chain Is Increasing Risk Exposure*, there is an inherent risk to working with third-party vendors. As a result, enterprises need to create tight security protocols in order to reduce risk from supply-chain attacks. To improve security in your supply chain:

- Know who your vendors are and what security protocols they have in place
- Require certain levels of security compliance and protection from all third-party vendors, with a no-tolerance policy towards vendors that fail to meet strong security standards
- Implement multi-factor authentication to reduce access to your environment via third-party connections
- Control the access to your hardware and software to reduce the risk of potential tampering

Strengthen Cloud Network Security

Each type of cloud needs to be evaluated based on the access and control you have to implement security measures: for example, in software as as serivice (SaaS) environments you may not have any access to implement security, whereas in infrastructure as a service (IaaS), you have a great deal of control. Cloud environments should also be evaluated for detection capabilities; in the case of a breach, it's important to know who's responsible for discovery and notification.

For standrad IaaS, improper configurations of access controls and key management are common drivers behind cloud attacks. To avoid these risky misconfigurations:

- Don't assume that the cloud incarnation of a program will behave in the same way as the local version — follow the provider's guidance for development and deployment to avoid preventable pitfalls
- Enforce strict multi-factor authentication and be stringent with the authorization of managed policies
- Make sure to have backup policies in place and manage them properly — if you have too many, you're exposed to leakage; too few, and you're exposed to loss
- Continuously and thoroughly test your cloud infrastructure; model the network infrastructure and incorporate vulnerabilities and threat intelligence to gain an accurate view of how susceptible you are to attacks

Protect Your OT Network

The sheer lack of visibility to OT networks and their risks makes them a prime target for attacks. Such networks are often controlled by different teams than IT networks, prohibit active scanning and are notoriously difficult to patch.

Nonetheless, responsibility for cyber risk even within the OT space often still lies with the CISO. To holistically manage risk, organizations with OT networks must:

- Passively collect data from the networking and security technology within the OT environment
- Build an offline model encompassing IT and OT to understand connectivity and how risks could impact either environment
- Use purpose-built sensors to passively discover vulnerabilities in the OT network
- Incorporate threat intelligence and asset exposure to prioritize OT patches
- Leverage the model to identify patch alternatives to mitigate risk when patching isn't an option

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 threats shift, so too must defense strategies. Whether you're protecting against the rise of cryptominers, safeguarding OT in critical infrastructure or simply trying to keep up with what patch to deploy next, incorporating accurate and up-to-date intelligence will give you the edge you need to be proactive against a dynamic threat landscape.

The beginning of this report stated that vulnerabilities don't exist in a vacuum and that their risk is shaped by the context around them. The same can be said of security measures. Having the ability to correlate vast and varied intelligence sources from within your infrastructure as well as the vulnerabilities and threats in play will create a security program greater than the sum of its parts.

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