SKYBOX SECURITY

2020 VULNERABILITY AND THREAT TRENDS

RESEARCH REPORT

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 Skybox® Security's vulnerability management solution, which prioritizes 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.

CONTENTS

EXECUTIVE SUMMARY

The number of new vulnerabilities reported every year can be overwhelming. This mass of flaws introduces new complexity to enterprise security environments and places additional stress on stretched resources to remediate the right vulnerabilities first. Vulnerabilities cannot be managed in isolation. They need to be understood with knowledge of continuously changing internal and external factors — it is only with this context that organizations can enact intelligent remediation strategies. We publish this report to give CISOs and security leaders the perspective they need to see the trends shaping the vulnerability and threat landscape and, in turn, their defense strategy.

The *2020 Vulnerability and Threat Trends Report* (now in its third annual edition) examines new vulnerabilities published in 2019, 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 17,000 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

New CVE reports stabilized, with the volume of medium–severity vulnerabilities increasing

The number of new vulnerabilities reported over 2019 increased by a modest 3.8 percent, indicating that we could be seeing more stability after a couple of years of rapid growth. Of the new reports, 40 percent are medium-severity vulnerabilities, up from 34 percent last year. Hackers know that medium-severity doesn't equate to medium risk: they see these vulnerabilities as an opportunity. They know that security teams are distracted by remediating masses of critical- and high-severity vulnerabilities and, therefore, know that they are ripe for attack. Security teams need to pay attention to this expanding segment and understand that an exposed medium-severity vulnerability can be far more dangerous than an isolated higher-severity vulnerability.

Microsoft vulnerabilities increased dramatically over 2019

The number of new vulnerabilities within Windows OS's increased by 66 percent between 2018 and 2019, making Microsoft the owner of the industry's most vulnerable operating systems. The number of vulnerabilities within Windows products, as opposed to OSs also increased by 75 percent, presenting a stark contrast to Android's 73 percent drop.

Multi-vendor vulnerabilities are becoming an increasing concern

Influential vulnerabilities, or those with a broad reach across multiple vendors, are becoming more common. These include flaws found in Intel processors, PDFs, network stack IPnet and Netflix which affect tens of vendors, When a new vulnerability is identified, it is important for security teams to assess how many products within their ecosystem are affected.

OT advisories increased by 53 percent

2019 saw a record number of new OT advisories shared by the Industrial Control Systems Cyber Emergency Response Team (ICS–CERT). Most of these are attributed to Siemens and a sign that both ICS-CERT and Siemens' reporting capabilities are improving. The need to find ways to protect critical OT networks is becoming more acute than ever — particularly as they continue to become connected to internet–connected IT systems.

RESULTS

VULNERABILITIES & EXPLOITS

New Vulnerability Reports Start to Stabilize

There were 17,220 new vulnerabilities reported over 2019, representing a modest 3.8 percent increase over last year's figures. For the moment, it appears that last year's trends are keeping up and that counts are remaining stable. This lack of major movement should not distract from the burden being placed on security teams by this increasing mountain of vulnerabilities. Over 2019, we have also seen the National Vulnerability Database (NVD) continue to catch up on backdated vulnerabilities. The net effect of the NVD's backfill efforts is represented by the dark gray line in FIG 1 below.

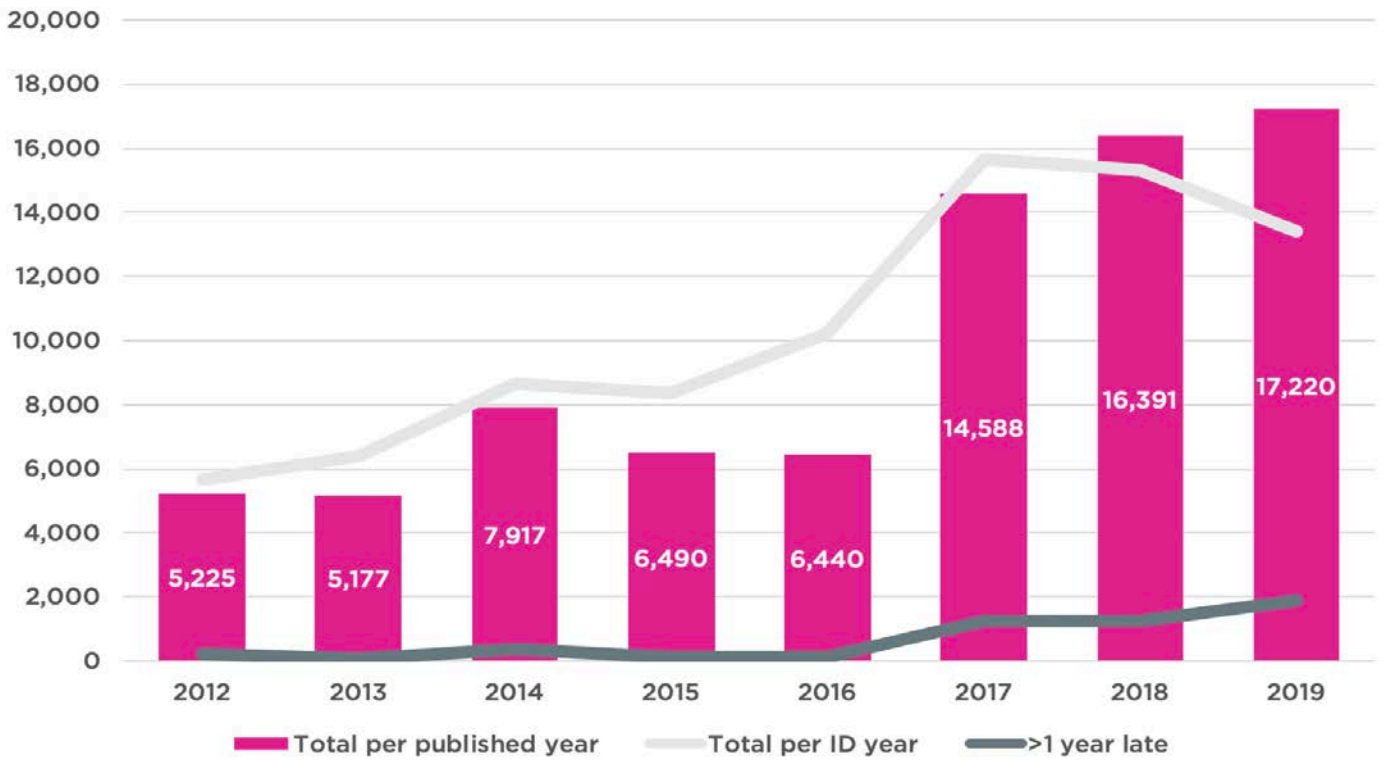

FIG 1 | New CVEs by year and the year those vulnerabilities were identified.

Medium-Severity Vulnerabilities Increase Share

In terms of Common Vulnerability Scoring System (CVSS) scores, the spread of vulnerabilities scoring low, medium, high and critical is occurring at similar rates to those seen in 2018. Although high-severity vulnerabilities still account for the majority, they are starting to lose ground to medium-severity vulnerabilities. Last year, medium-severity vulnerabilities accounted for 34 percent of all instances. This year, they hold a larger portion: 40 percent.

Medium-severity does not equate to medium risk. Organizations depend on CVSS scores to determine their remediation strategies; if they see that they have critical- or high-severity vulnerabilities within their infrastructure, they will instinctively choose to remediate these before any medium-severity flaws. This means that a mass of medium-severity flaws can sit unpatched within an organization's networks for a long period of time. Attackers know this, which is why medium-severity vulnerabilities are so attractive to them. If a highly exposed medium-severity vulnerability is left unpatched, its exploit can cause a great amount of damage.

This increasing share should, therefore, spark some concern. Security teams need to think about prioritizing remediation based on how exposed their vulnerabilities are and should stop relying on CVSS scores. These scores are useful for understanding the properties of a vulnerability in isolation, but do not and cannot reflect its exposure level within each unique security environment.

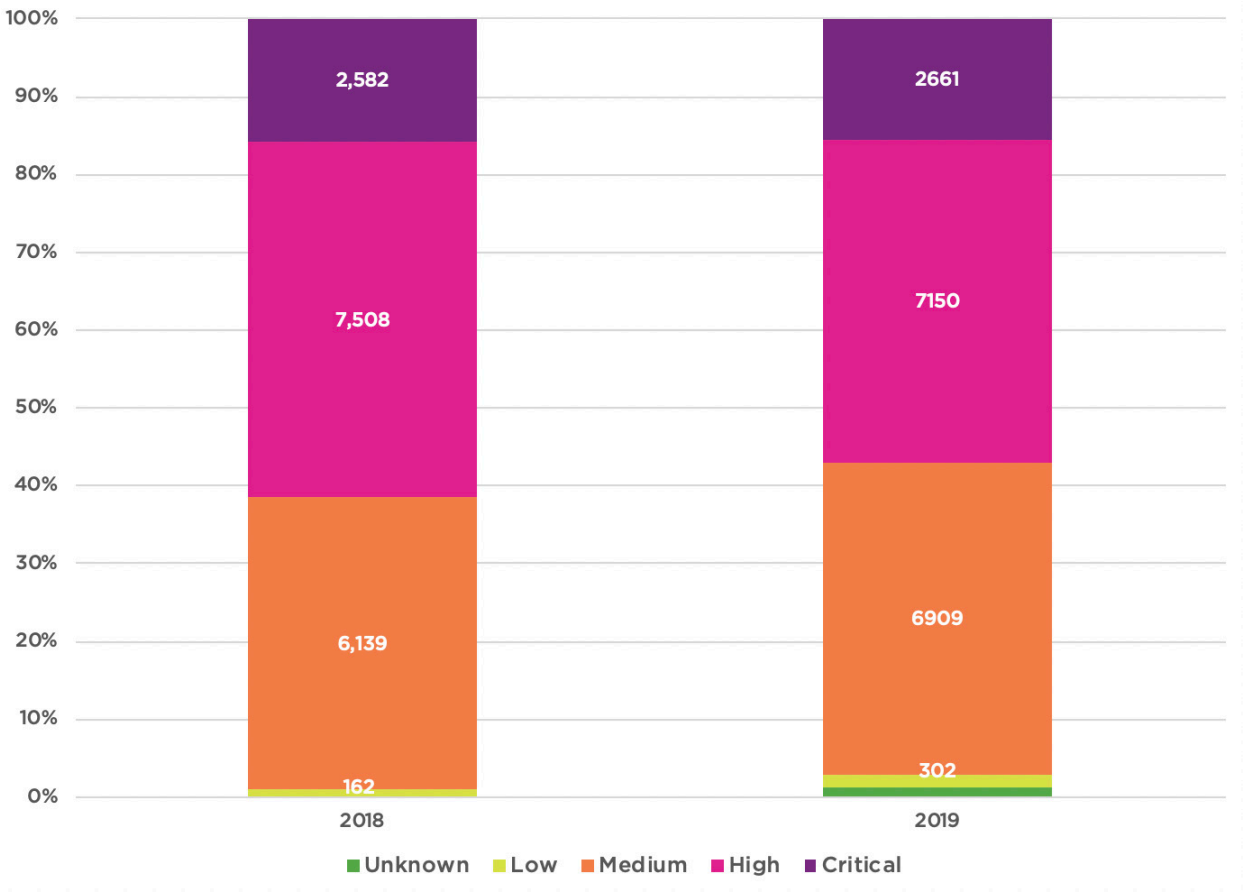

FIG 2 | New vulnerabilities' CVSS scores split by severity level

Windows Tops Most Vulnerable Operating Systems List

Here, we are establishing which operating system (OS) has contributed the highest number of vulnerabilities to the NVD. Also included here are vulnerabilities which require, but do not implicate, the OS. This means that if the OS is involved in a vulnerability but does not necessarily cause it, that vulnerability is still counted. Further, if three different editions of a particular piece of software running on Windows are all vulnerable, but only one edition running on Linux is vulnerable, then we are counting that as three vulnerabilities for Windows and one for Linux. Additionally, if both Internet Explorer and Edge share the same vulnerability when running on Windows 2008, 2012 or 2019, we count that as six vulnerable configurations for Windows.

Having an awareness of the methodology used here is important when analyzing these results and understanding why Windows became the most vulnerable OS in 2019, its total number of vulnerabilities jumping by over 66 percent to 1,497. The only other OS to experience a similar jump is macOS, with a vulnerability count that increased by 74 percent to 771.

In both cases, these marked rises can be attributed to Adobe products. Adobe's reporting practices have led to this inflation: they report vulnerabilities in bulks of dozens at a time, with some of the biggest products (namely Reader and Acrobat) sharing CVEs and possibly even a codebase. Adobe also maintains many product editions in parallel and still report on all – as an example, there are currently five supported editions of Acrobat.

The other notable story here is the 23 percent decrease in mobile OS vulnerabilities. Because the number of new IoS vulnerabilities barely changed this year (there was a moderate increase from 281 vulnerabilities reported in 2018 to 296 in 2019), this drop can be attributed to a considerable reduction in published Android CVEs.

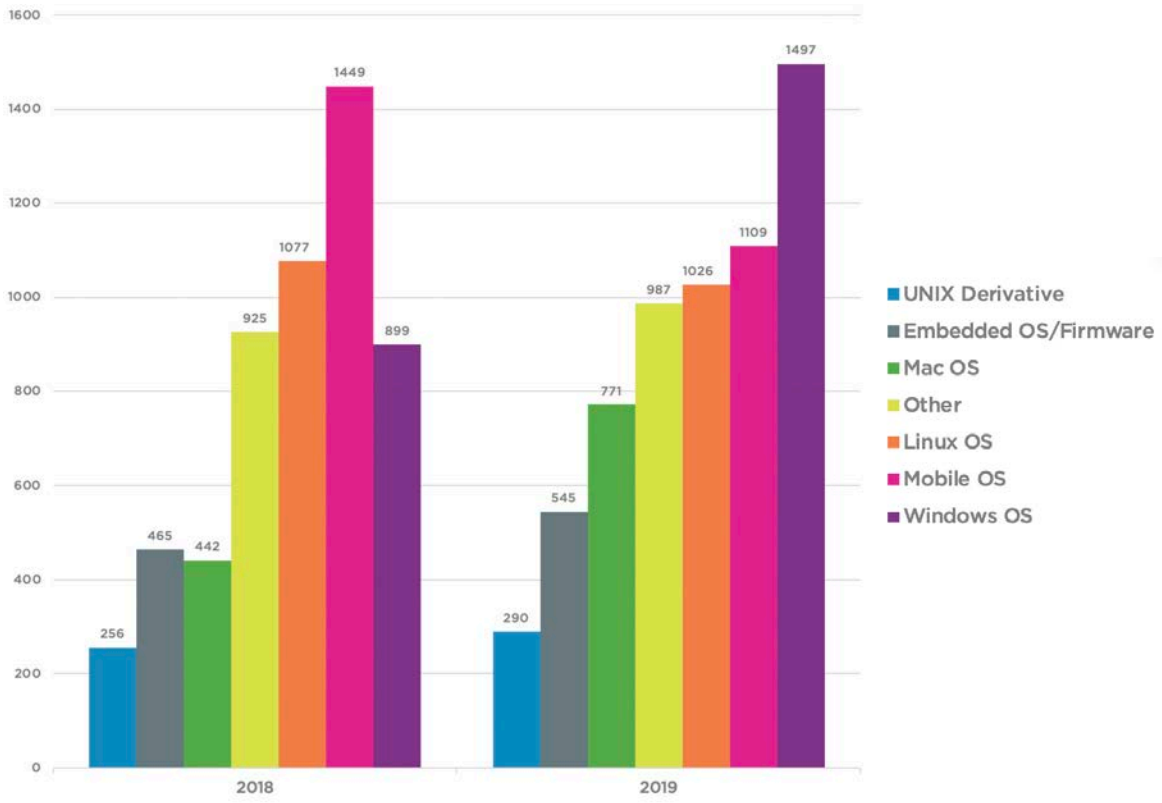

FIG 3 | Most vulnerable operating systems

Diving deeper into the data, we can see the spread of new vulnerabilities published on each Windows OS. While it should be no surprise that the tech giant's newer OSs are attracting the highest number of new vulnerabilities, its older systems are still not being ignored.

There were even three new vulnerabilities reported in 2019 which affect the obsolete Windows XP, namely 101835 (more commonly known as Bluekeep), 105545 (an inter-program capture-the-flag bug) and 110711 (which, if exploited, would allow for information to be leaked via remote desktop protocol).

Chrome Maintains Lead as Most Vulnerable Browser

Almost all browsers experienced a decrease in total vulnerability counts over 2019, with the exception of Apple Safari (which experienced a minor increase of three percent) and Google Chrome (with 11 percent more vulnerability reports.) This means that vulnerabilities on Chrome now account for 38 percent of all browser vulnerabilities, up from 32 percent in 2018.

This increase could be explained by Chrome taking some of Microsoft Edge's share as Microsoft moved towards use of open-source Chromium throughout the latter half of the year.

FIG 4 | Most vulnerable browsers

Android Still Most Vulnerable Product

Android maintains its lead as the most vulnerable product, with Windows starting to narrow the gap. Android reported 73 percent fewer vulnerabilities in 2019 than in 2018, with Windows increasing its total vulnerability count by 75 percent. If both products continue on the same trajectory throughout 2020, Windows will take pole position.

Elsewhere, application services company F5 has seen a 42 percent increase in vulnerability counts, with an average of one new or updated vulnerability being published on a daily basis. This pattern can largely be attributed to inherited vulnerabilities in third-party components.

Global hosting cPanel is new to the chart this year, with its total number of new vulnerability reports increasing from two in 2018 to 215 in 2019. This rise should, however, be seen as anomalous. These vulnerabilities are not all new, with most dating back to 2016. The large majority had been public knowledge on cPanel's security site for years before being incorporated into the NVD over the last year.

It is possible that cPanel will maintain its position as one of the most vulnerable products throughout 2020: there are still a number of cPanel vulnerabilities waiting in the wings that are public knowledge but have not yet been assigned CVEs. Any questions about why the NVD is suddenly taking a keen interest in cPanel can be explained by its proximity to Exim, which was hit with a potentially severe exploit in June 2019[1], and is frequently bundled with cPanel.

Increasing from two in 2018 to 215 in 2019. This rise should, however, be seen as anomalous. These vulnerabilities are not all new, with most dating back to 2016. The large majority had been public knowledge on cPanel's security site for years before being incorporated into the NVD over the last year.

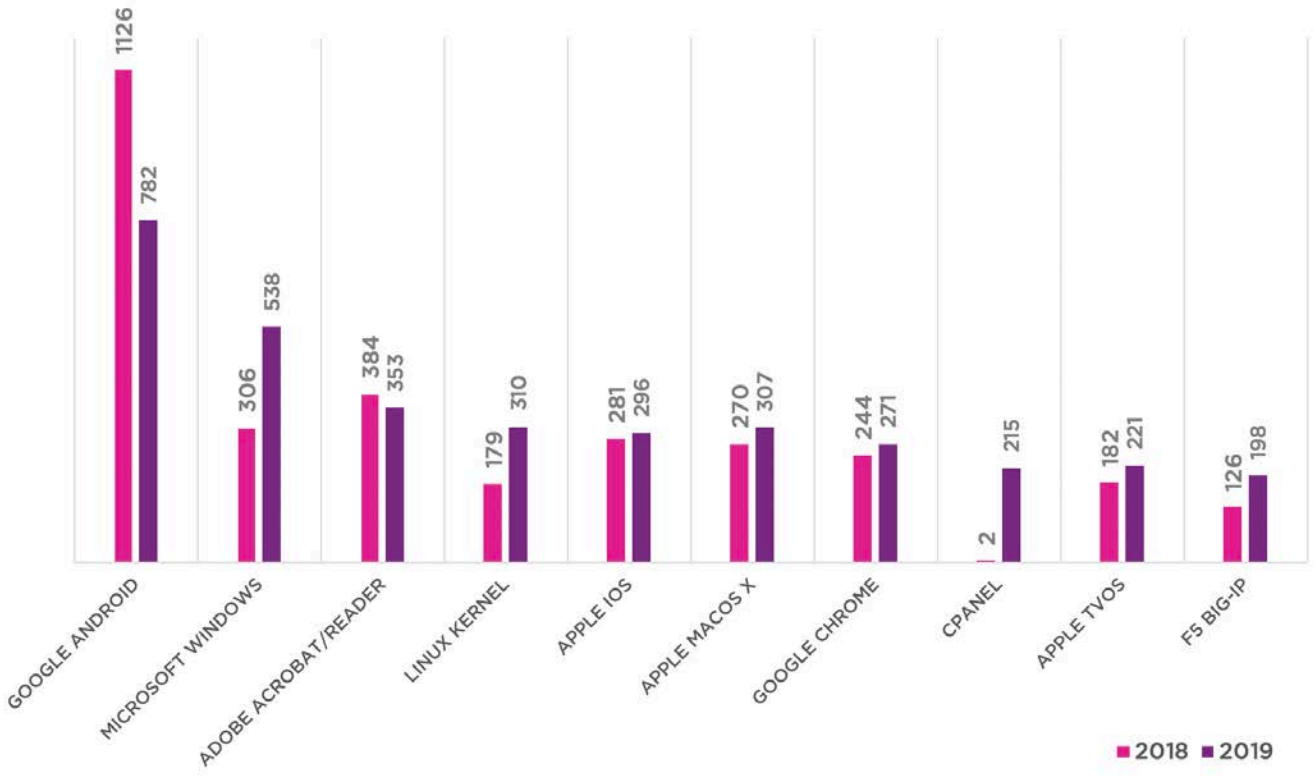

FIG 5 | Most vulnerable products

1 Source: Skybox Security https://blog.skyboxsecurity.com/exim-vulnerability/

Top Malware Families

FIG 6 illustrates a shift from the surge in usage of cryptocurrency mining software experienced in 2018 dissipated over 2019, with a 48 percent reduction in new samples. This decline can be primarily attributed to declining profit margins. Cryptominers may offer attackers a low profile but they also provide limited yields, something that has been exacerbated by the decreasing value of cryptocurrency. As these slow–trickle revenue generators became less interesting, more traditional malware (like backdoors and ransomware — both categories which saw significant increases in new samples being created in 2019) which offers big gains and is delivered with high impact have become more attractive.

It is also worth emphasizing that we are just looking at new malware samples which were created in 2019. It is highly likely that preexisting cryptominers which have already been developed and installed are already doing just as much damage as they have been in previous years. The threat posed by cryptominers should not be overlooked just because there were fewer new samples created in 2019.

Of note is the fact that many botnets and backdoor malware samples overlap or even, at times, work together. This is because achieving code execution and/or persistence via backdoors can go hand in hand with establishing and maintaining a botnet.

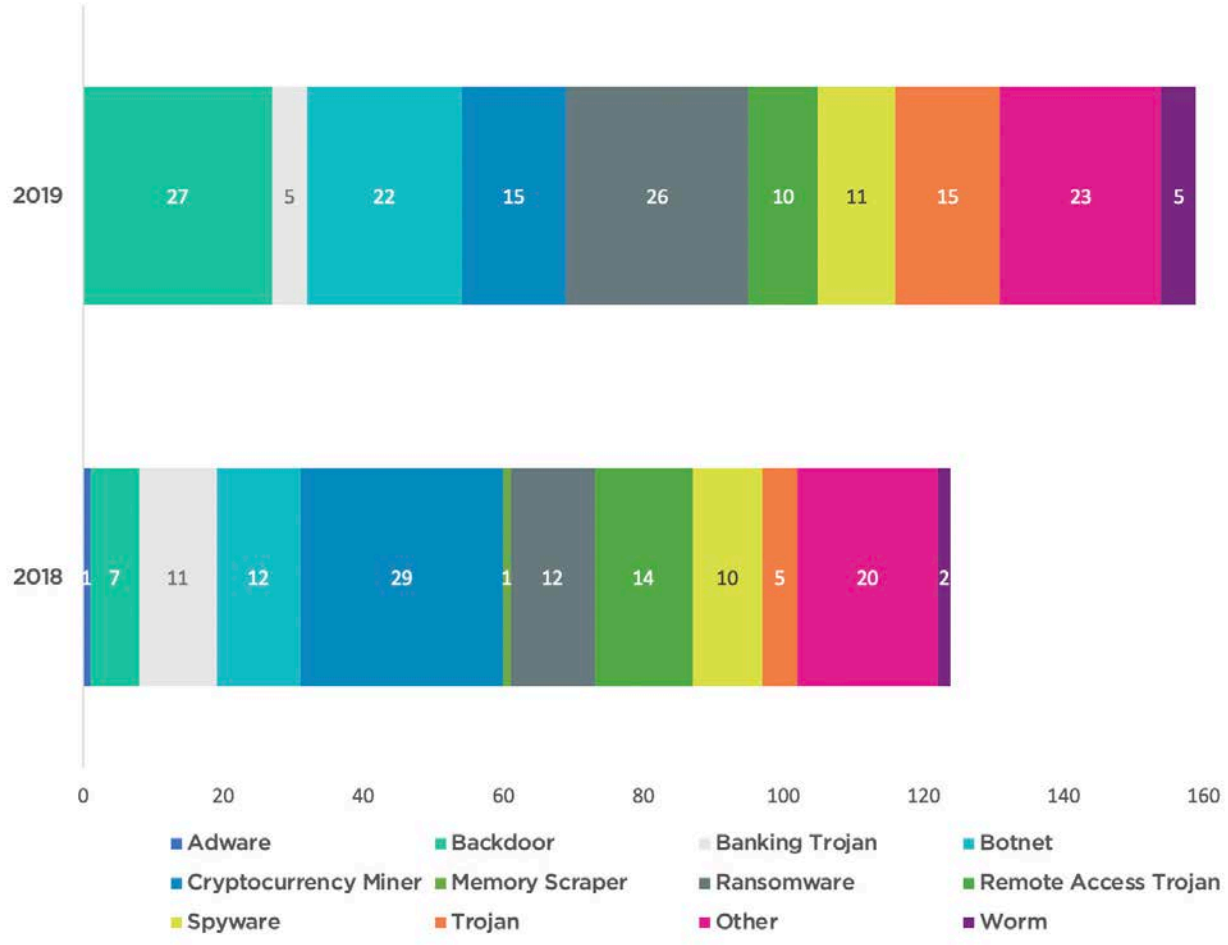

FIG 6 | New malware samples in 2019, split by family

Most Exploited Vendors

Here, in FIG 7, we are only counting distinct new samples that take advantage of new exploits. It's quite possible, therefore, that the instances of overall attacks over the course of 2019 are not proportional to the new exploits charted in this paper. Our methodology here differs from the way that we measure vulnerabilities associated with OSs and products (explained the opening paragraph of the 'Most Vulnerable Operating Systems' section on page nine). So, although it is true that Adobe published a large number of vulnerabilities last year, it is also true that they have suffered fewer new exploits this year and have, therefore, dropped off the list of most exploited vendors.

Microsoft has become the most exploited vendor, with a 120 percent increase in exploits over 2019. Conversely, Oracle experienced 45 percent fewer exploits over the same period. Microsoft's new lead includes the much–anticipated Bluekeep exploit which came and went with less spectacle than anticipated in late 2019.

Adobe has dropped off the list of most exploited vendors this year. Apple takes its place after experiencing several high-profile exploits, including an iOS device takeover which was reported by a Google employee and patched by Apple, but with very little detail divulged on the actual event.[2]

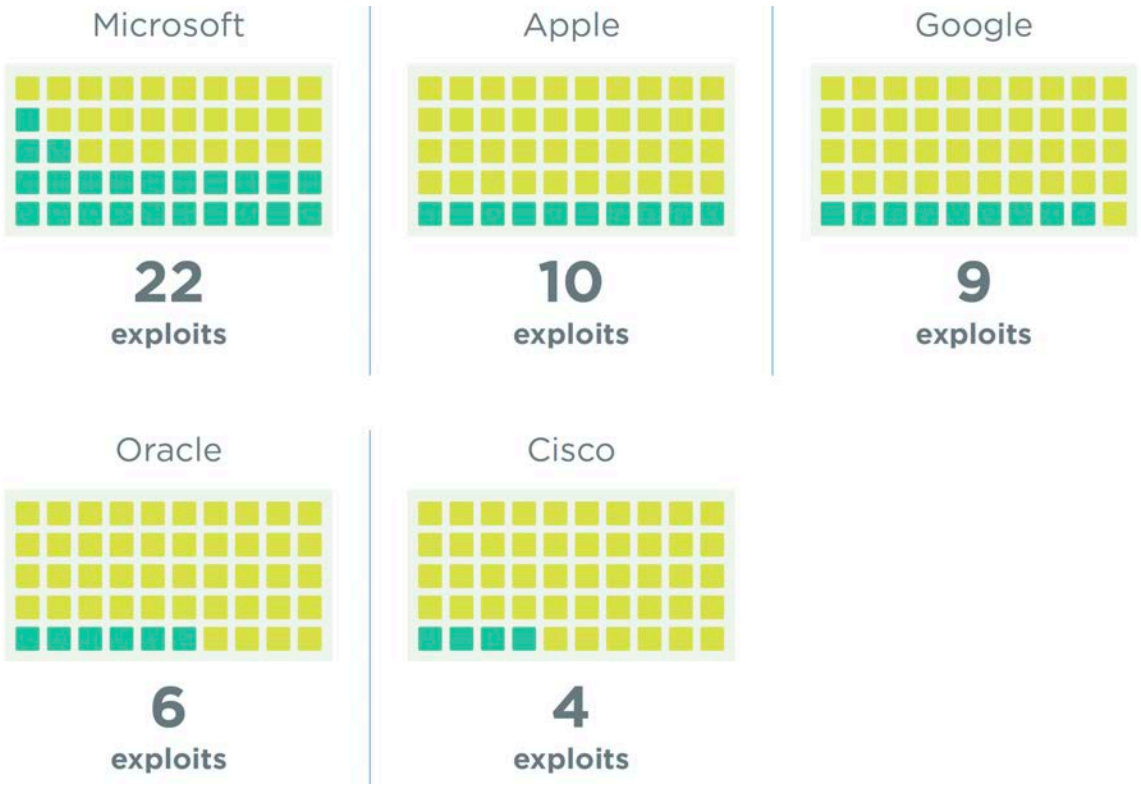

FIG 7 | 2019's most exploited vendors

2 Source: ZDNet https://www.zdnet.com/article/google-warns-about-two-ios-zero-days-exploited-in-the-wild/exim-vulnerability/

Zero-Days in 2019

The graph below shows how long it took for proof of concept (PoC) exploits, and exploits in the wild, to be created after the affected vendor released a patch. There are a couple of lessons that can be learned from these wild exploitation patterns. It is notable that it only takes a matter of weeks for exploit code to be created — in the vast majority of cases, the exploit code can be prevented by applying a patch. If security teams take steps to see which vulnerabilities have public PoCs before they are exploited in the wild, they may be better able to understand which vulnerabilities within their environments need to be remediated first.

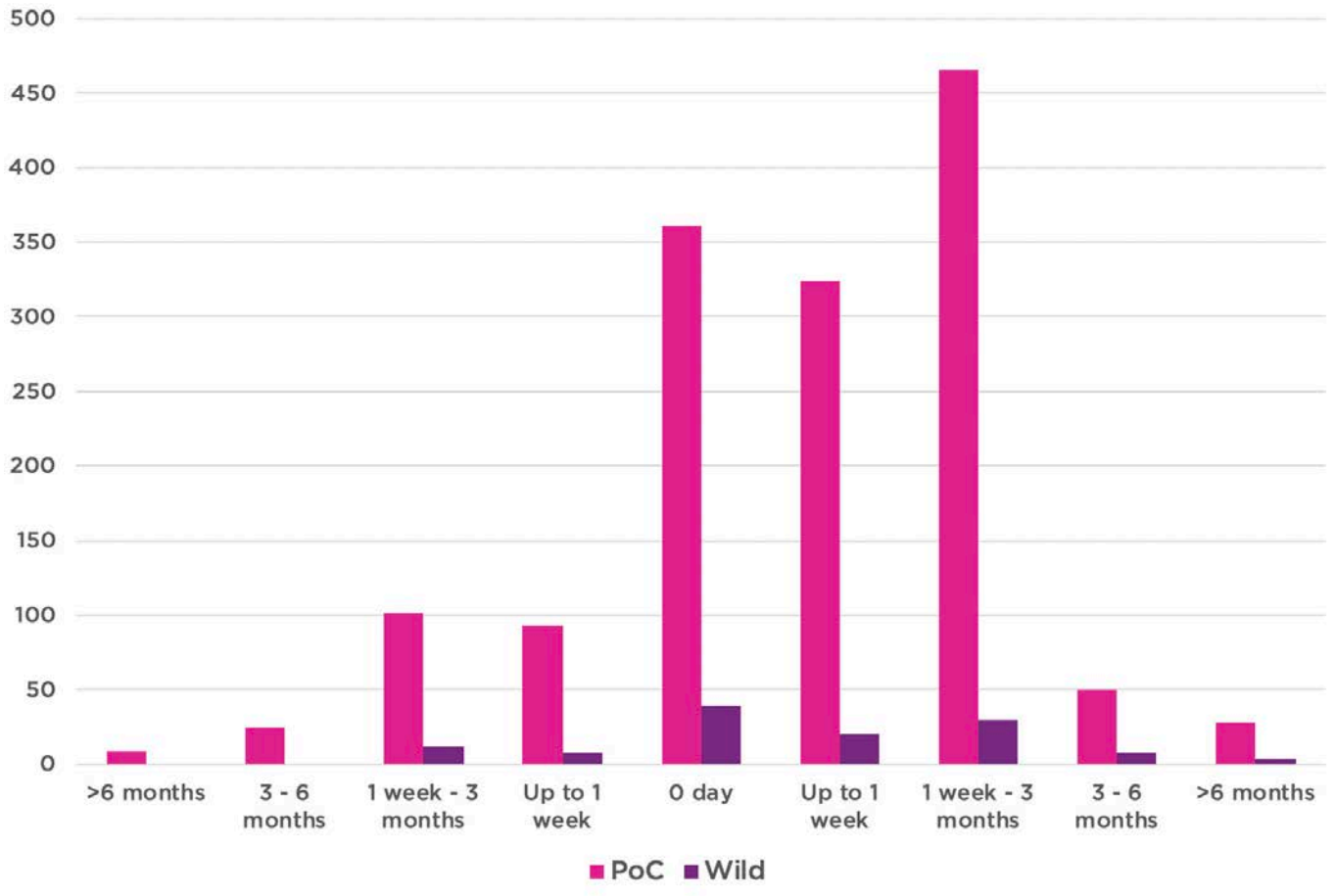

FIG 8 | Exploitation of zero-day vulnerabilities in 2019, split between proof of concept (PoC) exploits and those exploited in the wild

Siemens Leads New OT Vulnerabilities

Over 2019, the Industrial Control Systems Cyber Emergency Response Team (ICS–CERT), a U.S. government authority for operational technology (OT) professionals, has turned its attention towards vulnerabilities that exist within subcomponents of third–party products. These are flaws that can manifest across vendors, something that ICS–CERT has acknowledged by publishing joint advisories that address multiple vulnerable vendors in the same document.

One of the most significant OT vulnerabilities published in 2019, with a 10/10 severity level, was ICSA-19-043-033, which warned about several vulnerabilities within WibuKey's digital rights management product. This vulnerability allows privilege escalation and has remote code execution (RCE) attributes: if exploited, the attacker could take control of the affected control and monitoring system. Considering how OT devices are increasingly connected to the wider business' IT environment, this vulnerability highlights the pressing need for organizations with OT networks to improve the security which surrounds their critical infrastructure.

The number of new ICS–CERT advisories published by vendors has remained relatively stable, with one notable exception: the team published 53 percent more Siemens advisories in 2019 than it did in 2018. The reason behind this rise could be attributed to both ICS–CERT and Siemens' improved reporting capabilities. It is possible that Siemens' IT team now has greater consciousness of the organization's OT environment. If true, this should be welcomed as a sign that its IT and OT teams are working in a less siloed way.

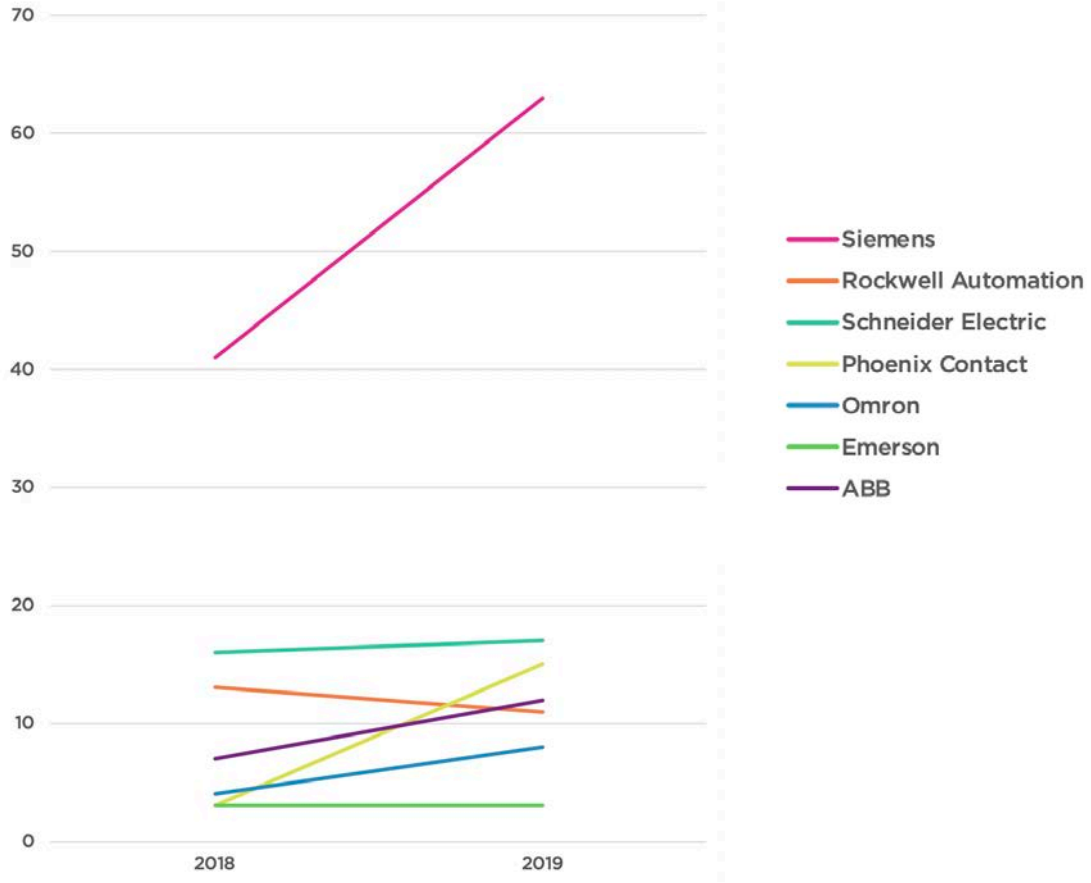

FIG 9 | New ICS-CERT advisories shared in 2018 and 2019, split by vendor

10 VULNERABILITIES WITH HIGHEST ASSOCIATED MALWARE PROGRAMS

As seen in FIG 8, very few vulnerabilities are actually exploited in the wild. In fact, less than one percent will ever be actively exploited. Knowing which vulnerabilities have been exploited, however, and which are most attractive to malicious actors holds great importance to the CISO and their security teams.

The top ten vulnerabilities by number of associated malware programs are each used by around 50 types of malware. The most prolifically used, CVE-2018-8174, otherwise known as DoubleKill, is currently being used by 62 such programs and, as such, leads the list.

1. CVE-2018-8174

When DoubleKill1 came out, it was considered to be a methodological breakthrough because of its ability to hop from Microsoft Office into the Internet Explorer kernel — something that had not been seen in exploit code before[3].and fears of its potency have proven to be well-founded. A real zero-day in April 2018, it is the youngest vulnerability in the top ten and its inclusion in big-name exploit kits like Rig and Fallout has made it popular with criminals. Considering how dangerous this vulnerability is, it should not be a surprise that criminals have latched onto it: proof of how astute and flexible attackers can be when attaching their malware to powerful flaws.

2. CVE-2016-4117

First reported in 2016, this Adobe Flash vulnerability has become a magnet for malware owing to its RCE attributes. Adobe Flash has long been a favorite for criminals because it's a popular product with a very poor update mechanism and is included in many standard and widely available, ready-to-use exploit kits.

3. CVE-2016-0189

This scripting engine memory corruption vulnerability, which allows remote attackers to execute arbitrary code via a crafted website, impacts Microsoft VBScript 5.7 and Jscript 5.7 engines, as used in Internet Explorer 9 through 11.

3 Source: Skybox Security https://blog.skyboxsecurity.com/double-kill-exploit/

4. CVE-2018-4878

Another Adobe Flash vulnerability, this time a use-after-free flaw which, if exploited, could be used by attackers after having enticed users to open documents, web pages, or emails that contain corrupted Flash files.

5. CVE-2014-6332

This RCE vulnerability, first discovered in 2014, has gained traction because, if exploited, it allows attackers to execute remote code on a number of popular Windows servers.

6. CVE-2015-8651

A flaw that allows hackers to execute arbitrary code through unknown vectors, this 2015 vulnerability once again proves the popularity of Adobe Flash among cybercriminals.

7. CVE-2015-5119

A use-after-free vulnerability that affects Adobe Flash and that can be exploited with the use of specially-crafted Flash content or Microsoft Office documents.

8. CVE-2013-2551

More evidence that use-after-free vulnerabilities are magnets to malware. This flaw, which exists in Microsoft IE, could allow attackers to execute arbitrary code through a site that then triggers access to deleted objects.

9. CVE-2016-1019

The final Adobe Flash vulnerability in the list, attackers are attracted to attributes that allow them to either execute arbitrary code on affected machines or enact a denial-of-service (DoS) attack.

10. CVE-2016-7200 and CVE-2016-7201

These vulnerabilities are bundled together here because they are, to all intents and purposes, almost indistinguishable from each other. They both impact MS Edge and, if exploited, could allow for the remote execution of code.

INSIGHT

Multi-Vendor Vulnerabilities are on the Rise

While the overall increase in vulnerability reports over 2019 may not be too remarkable, a number of vulnerabilities within the mix have a greater reach and impact a greater number of vendors than those seen in previous years. For that reason, they can be considered to be influential — an influence that security professionals need to be aware of in order to best protect their organizations. Below, we chart some of the most influential vulnerabilities and explain why they have such wide reach.

- **Netflix HTTP/2 DoS vulnerabilities**

In August 2019, Netflix discovered eight resource exhaustion vectors[4] which affect a variety of third-party HTTP/2 implementations and that can be used to launch DoS attacks against affected servers. Of the eight vulnerabilities disclosed in the advisory, three are amongst the most influential within the NVD. These are CVE-2019-9517, which impacts 17 different vendors, CVE-2019-9512, which reaches 16 vendors, and CVE-2019-9515, which affects 14.

Although none of these vulnerabilities work on HTTP/1.1, and data are not at risk, the ubiquity of HTTP/2 has led to the vulnerabilities becoming so widespread.

- **PDFex vulnerabilities**

PDFex is a portmanteau of PDF exfiltration. These vulnerabilities, which include SBVs 107862, 107863, 107864 and 107865, enable attackers to exfiltrate and manipulate encrypted PDF data[5]. They work because PDF encryption uses Cipher Block Chaining (CBC) which doesn't have any innate integrity checks.

Because PDFs are so widely used, it should perhaps be unsurprising that these vulnerabilities impact a large number of vendors. Those impacted include Adobe, Apple and Foxit among a handful of others. Many of these vulnerabilities have published PoCs, so it is important for organizations to apply patches across all affected products.

- **URGENT/11 vulnerabilities**

A group of 11 zero-day vulnerabilities were found in IPnet, a stack used in real-time operating systems (RTOS) which include Integrity by Green Hills, ThreadX by Microsoft, Nucleus RTOS by Mentor, ITRON by TRON Forum and ZebOS by IP Infusion[6]. These vulnerabilities, if exploited, could have serious repercussions: videos have been shared of attackers taking over a wide range of RTOS devices, from the innocuous — Xerox machines — to the critical — hospital bedside monitors[7]. Because of this, both DHS and the FDA released advisories.

These vulnerabilities are so widespread because nobody wants to write their own device firmware. More than that, the 'big names' have yet to stake their claim in the industry, meaning that all affected

4 Source: GitHub https://github.com/Netflix/security-bulletins/blob/master/advisories/third-party/2019-002.md
5 Source: PDF Insecurity https://pdf-insecurity.org/index.html
6 Source: Armis https://www.armis.com/urgent11/
7 Source: Wired https://www.wired.com/story/urgent-11-ipnet-vulnerable-devices/

devices have been bought from Interpeak, IPnet's owner until 2006. The protocols that these devices use are old, the software implementing them is old, the systems are very hard to upgrade and the devices running the RTOS may have long half-lives. It's clear that these bugs have been around for many years and will be around for many more.

Important to note here is that these vulnerabilities only have a CVSS score of three, which means that they have a "low" rating. This is an instance where having contextual understanding of the environment matters. Systems that run RTOS are, almost by definition, more sensitive to disruption. Any organization with critical infrastructure which could be impacted by these vulnerabilities needs to look beyond simple CVSS scoring and assess the high risk that they actually pose to their sensitive networks.

- **Long-tail vulnerabilities**

A long-tail vulnerability is one that affects between three to nine vendors. This year, there were 118 such vulnerabilities reported in the NVD. Vulnerabilities that exist within Java are the most common here, with 25 vulnerabilities affecting either three or four different vendors. Second to Java is tcpdump, a data-network packet analyzer program, with 15 long-tail vulnerabilities, with various Apache applications holding the third highest tally at 12.

Criminals Getting More Creative With Exploit Kits

A handful of new exploit kits were developed over the course of 2019[8]. While none of them were innovative in terms of the weak points which they choose to attack, several were notable for their creative means of execution — a sign, if one were needed, that criminals are working hard to outsmart end-users and security professionals alike.

Take Capesand, a member of the new cohort, as an example. The way that it works is the mark of a new trend within the development of exploit kits: instead of just relying on vulnerabilities, as is traditional, it also uses social engineering to help enable successful exploits. It uses convincing malicious advertising, or "malvertising," about popular current trends to drive users to live mirrors of popular sites[9]. The mirrored site contains a hidden frame which is then used to load the exploit kit. It provides attackers with a more elegant way to get their foot in the door.

There is also a new trend towards the development of fileless, pseudo-exploit kits[10]. These are drive-by downloads that lack proper infrastructure. They are typically used by smaller, more unsophisticated attackers who are looking to take advantage of vulnerabilities with proven exploits that and have been left unpatched by any given individual or organization.

These pseudo-exploit kits focus on a small, fixed number of vulnerabilities and, owing to the fact that they are not distributed for reuse, have an even smaller number of users.

8 Source: MalwareBytes https://blog.malwarebytes.com/threat-analysis/2019/07/exploit-kits-summer-2019-review/
9 Source: Trend Micro https://blog.trendmicro.com/trendlabs-security-intelligence/new-exploit-kit-capesand-reuses-old-and-new-public-exploits-and-tools-blockchain-ruse/

10 Source: Malware Bytes https://blog.malwarebytes.com/threat-analysis/2019/08/say-hello-to-lord-exploit-kit/

In isolation, these kits may seem insignificant to most mature security teams. But as corporate security environments continue to fragment with the introduction of more IoT devices and IaaS cloud microservices, the opportunity for one of these kits to exact a payload will increase — particularly if more are produced and used throughout 2020.

New Intel Baseboard Management Controller (BMC) Vulnerabilities Emerge

After a decade of relative inactivity — Intel only published two vulnerabilities on BMCs over the last decade, SBV-111435 in 2010 and SBV-28084 in 2018 — the tech firm revealed 13 new flaws in 2019. This increase in reports coincides with Intel's scheduling alignment with Microsoft for advisory publication and could mean that we will see even more flaws disclosed over 2020.

The vulnerabilities relate to Intel's Baseboard Management Controllers (BMCs), which are specialized service processors used to monitor the physical state of a computer, network server or other sensor–enabled network devices.

Several of the new vulnerabilities are rated as high severity (namely SBVs 110120, 110117, 110123, 110124, 110170 and 110171). This is partly because BMCs are seen as being high–value targets — there is no protection standing between them and the hardware that they serve because they provide direct access. If exploited, these vulnerabilities could enable attackers to gain low–level server access.

Intel's historic lack of reporting activity has led to the company gaining a reputation for producing secure, difficult–to–hack products. But this recent increase shows that even the most secure companies need to be monitored with vigilance.

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 more so 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 better understand the context of their vulnerabilities and assets. This includes having a firm grasp 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 criticality 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 the 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.

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 throughout the organization, 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

Security teams are forced to operate within an environment of great turbulence. Whether protecting against emerging malware, threats to the OT network or simply trying to keep up with what vulnerability to fix next, incorporating accurate, up-to-date threat intelligence in vulnerability management programs will give organizations they edge they need to counter a dynamic threat landscape.

In order to succeed, the CISO needs to find ways to cut through the complexity which weighs down on them and their team. The first step to creating simpler, more efficient security programs is having an understanding of both internal and external threat context. This report has laid out the current state of play for external threats. It is up to you to harness the visibility and context of you internal environment and to correlate vast and varied intelligence sources from within your infrastructure to create a robust and enduring security program.

ABOUT SKYBOX SECURITY

At Skybox Security, we provide you with cybersecurity management solutions to help your business innovate securely. We get to the root of cybersecurity issues, giving you better visibility, context and automation across a variety of use cases. By integrating data, delivering new insights and unifying processes, you're able to control security without restricting business agility. Skybox's comprehensive solution unites different security perspectives into the big picture, minimizes risk and empowers security programs to move to the next level. With obstacles and complexities removed, you can stay informed, work smarter and drive your business forward, faster.

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