SKYBOX® SECURITY

2019 VULNERABILITY AND THREAT TRENDS

Mid-Year Update

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.

References to figures from this year refer to data sets from January 1 through June 30, 2019.

CONTENTS

EXECUTIVE SUMMARY

Vulnerabilities don't exist in a vacuum. The risk they pose to your organization depends on a variety of internal and external factors 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: Mid–Year Update* examines new vulnerabilities published in the first half of 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 thousands of vulnerabilities published every year. The insights and recommendations provided are here to help align security strategies which can effectively manage the complex challenges of 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

Only a tenth of vulnerabilities have a developed exploit.

The good news is that of the more than 7000 vulnerabilities published in the first half of 2019, a small fraction will ever have an exploit, with less than one percent exploited in the wild. The bad news: increasing network complexity makes it difficult to understand which of those vulnerabilities are exposed to potential attacks or exist on important assets, representing a critical risk.

Cloud container vulnerabilities in steady climb.

As use of various cloud services has grown, so too have their vulnerabilities. Vulnerabilities in container software have increased by 46 percent in the first half of 2019 compared to the same period in 2018. Looking at the two year trend of container vulnerabilities published in first halves, container vulnerabilities have increased by 240 percent.

Trend of broad–reaching vulnerabilities continues, with heavy concentration in CPU side-channel info leaks.

Vulnerabilities often exist across programs or software modules which share code. In the first half of 2019, chip-level vulnerabilities like Spectre/Meltdown were particularly numerous, making collateral damage of "downstream technology" such as operating systems or browsers running on affected architecture. In the first half of 2019, 40 vulnerabilities had the capability to impact three or more vendors.

Tide turns away from cryptomining — ransomware, botnets and backdoors fill the vacuum.

In 2018, malicious cryptomining reigned supreme as the cybercriminal tool of choice. But with the decline in cryptocurrency value, and with Coinhive shutting down, attackers have turned back to their old reliables. Usage of ransomware, botnets and backdoors jumped 10, eight and 18 percentage points, respectively, between the first half of 2018 and the same period this year.

RESULTS

VULNERABILITIES & EXPLOITS

New Vulnerabilities' Record-Breaking Trend Pauses

The first half of 2019 has seen a decrease in reported vulnerabilities compared to the same period in the previous two years, suggesting that 2018 may have been an anomaly. This is not to say that there has been a marked decline, nor that this is the start of a sea change. The numbers still more than double those of earlier years. This is due, in part, to internal changes at the MITRE Corporation and NIST's National Vulnerabilities Database between 2016 and 2017 which allowed them to process a greater volume of vulnerability data.

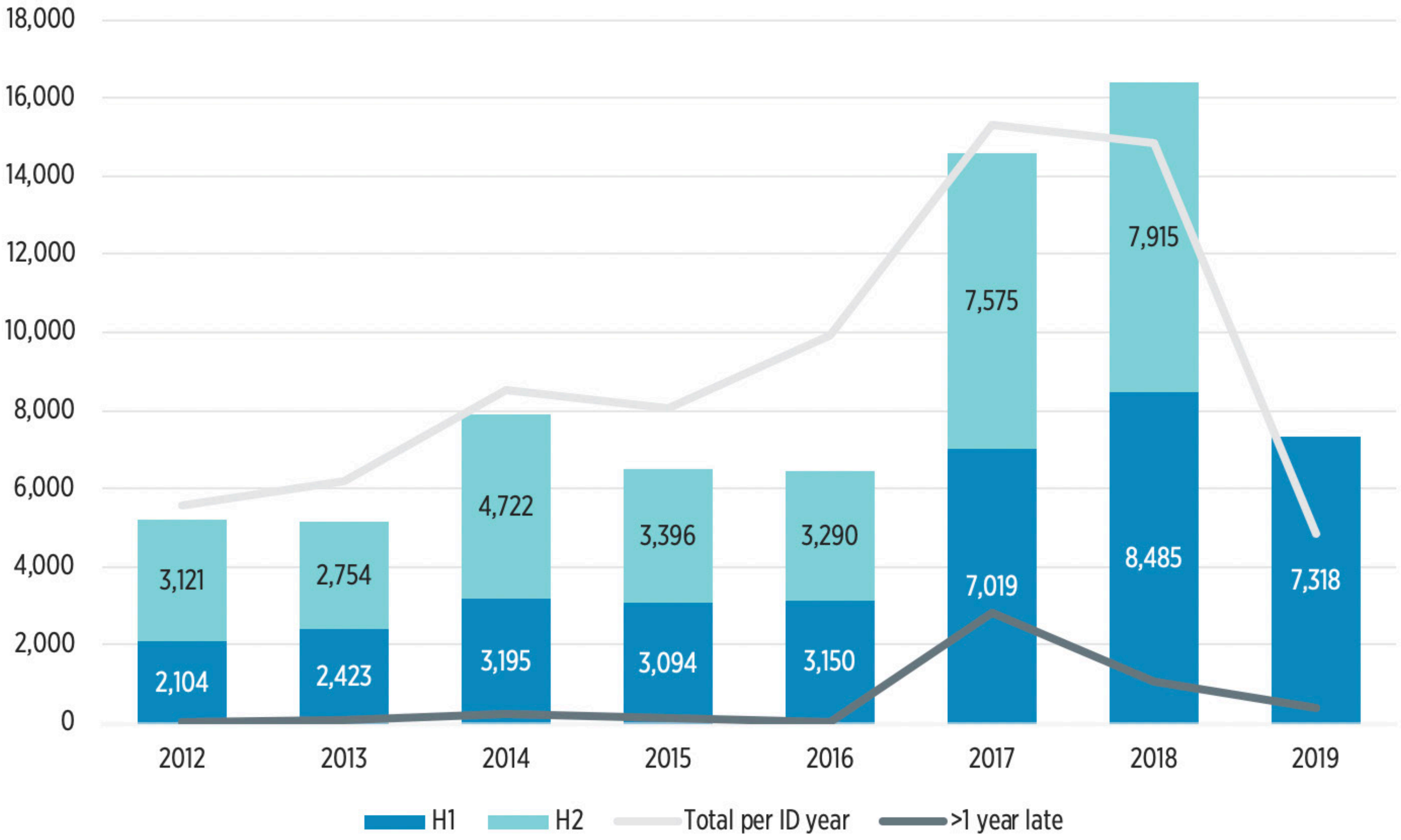

FIG 1 | New CVEs by half year and the year those vulnerabilities were identified.

As an estimate of the latency between a CVE's assignment and initial publication of its details by NVD, we can track the "ID year" (the year portion of the CVE ID number) of each CVE, under the assumption that CVE Numbering Authorities (CNAs) normally will not assign old IDs to new issues.[1] Many CVEs with years predating 2019 in their IDs may be analyzed and processed months or years after their assignment by their vendors or other CNAs. ID years show a slightly more subtle trend than counting vulnerabilities by NVD publish date, which may help explain the apparent jump in vulnerabilities which have been reported in recent years and also set expectations for the rest of 2019 and the future.

The ramp-up in vulnerabilities between 2016 and 2017 can be seen in this context as a continuation of an upward trend that began years earlier. At the same time, the number of vulnerabilities whose publish date was more than a full year after its ID year increased by two orders of magnitude – from 54 to 2825 – between the first halves of 2016 and 2017, then settled down to just over 1000 in 2018 H1, and continued along that trajectory with 377 in 2019 H1. These facts taken together suggest that there was substantial catching-up in processing older vulnerabilities beginning in 2017, which has since leveled out.

We might project that overall numbers will continue to trend upward slowly, as they have since the inception of the CVE in 1999, as the apparent backlog is alleviated and assignment and publication keep better pace with vulnerability reporting.

[1] Source: Mitre https://cve.mitre.org/cve/cna/rules.html

The distribution of CVSS scores has slid back slightly from the critical severity end of the scale. 15 percent of 2019's reported vulnerabilities have been of critical severity, compared to last year's 17 percent at this time, and the previous year's 13 percent. Among the other severity levels, only medium had a noticeable change with an increase of just over one percent.

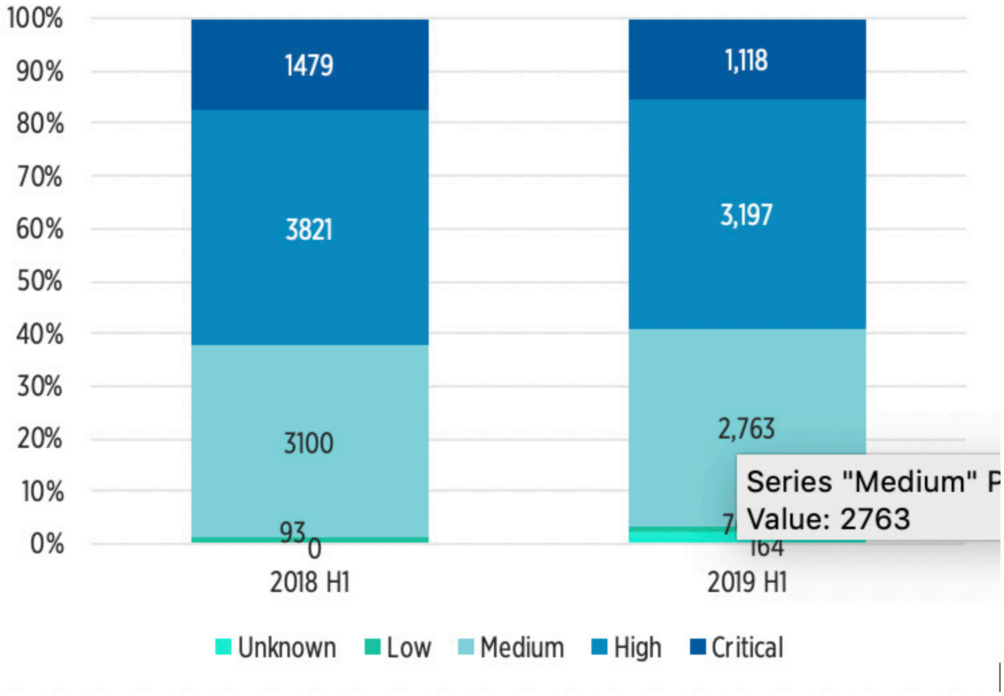

FIG 2 | New vulnerabilities by CVSS score

Vulnerabilities by Category

Business and desktop apps have accumulated more vulnerabilities this year than they did during the same period last year, but those vulnerabilities are now concentrated in a considerably smaller number of programs. Desktop app vulnerabilities were dominated by those in the Adobe Acrobat and Reader family of products, which have nearly doubled from 96 to 181. In business apps, the top five products (Foxit PhantomPDF, IBM API Connect, MySQL, Oracle E-Business Suite, and Oracle VM VirtualBox) now account for over 17 percent of vulnerabilities in the category. The IoT category saw the biggest gains proportionally in terms of vulnerability count and product count, with its long tail occupied mostly by medical devices, including Medtronic implantable cardiac devices which were called out in a high profile FDA Safety Communication due to their encryption weaknesses.[2]

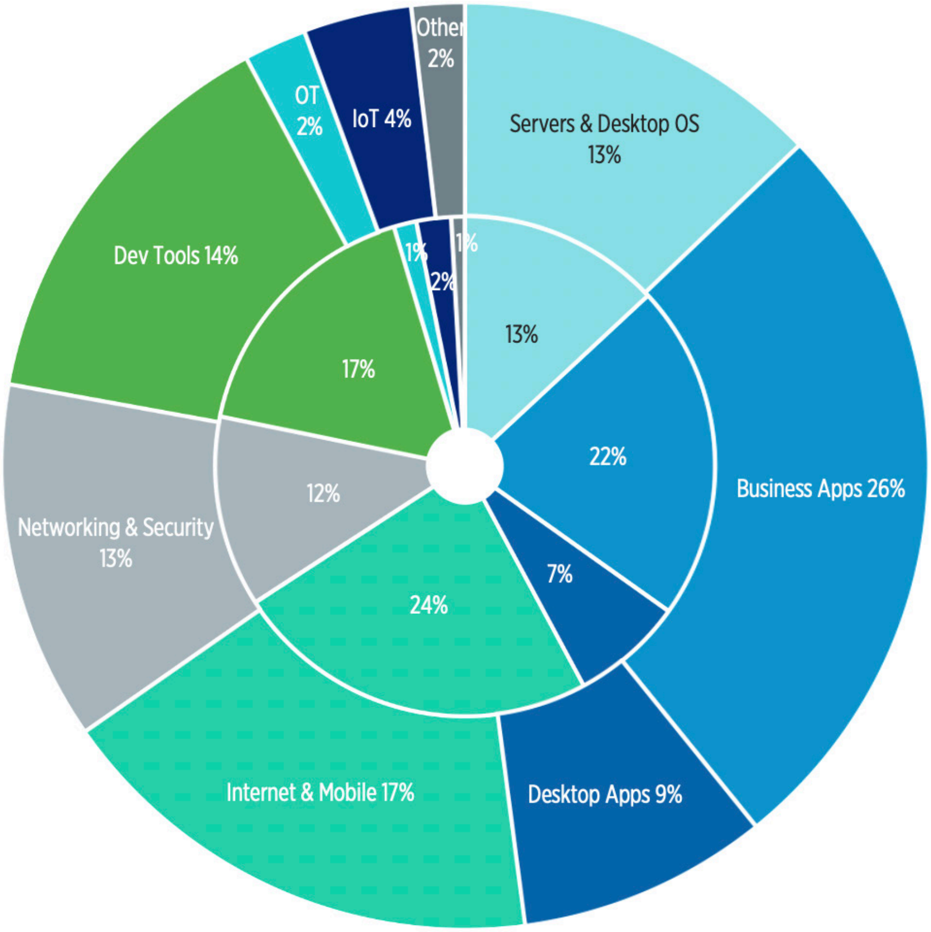

FIG 3 | Breakdown of newly published vulnerabilities by category. Inner circle represents vulnerabilities from 2018 H1; outer circle represents vulnerabilities from 2019 H1.

[2] Source: U.S. Food and Drug Administration https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-affecting-medtronic-implantable-cardiac-devices-programmers-and-home

Top 10 Most Vulnerable Products

The 10 most vulnerable products comprise less than one percent of the products covered by Skybox and yet hold 19 percent of total vulnerabilities. These are products which demand a lot of an organization’s attention and, unsurprisingly, belong in large part to some of the world’s most recognized companies. While not a household name, corporate application management company f5’s flagship BIG–IP system has broken into the top 10 list for the first time after hovering on the outskirts for several years. It displaces the Linux Kernel to become the ninth most vulnerable product in 2019 H1.

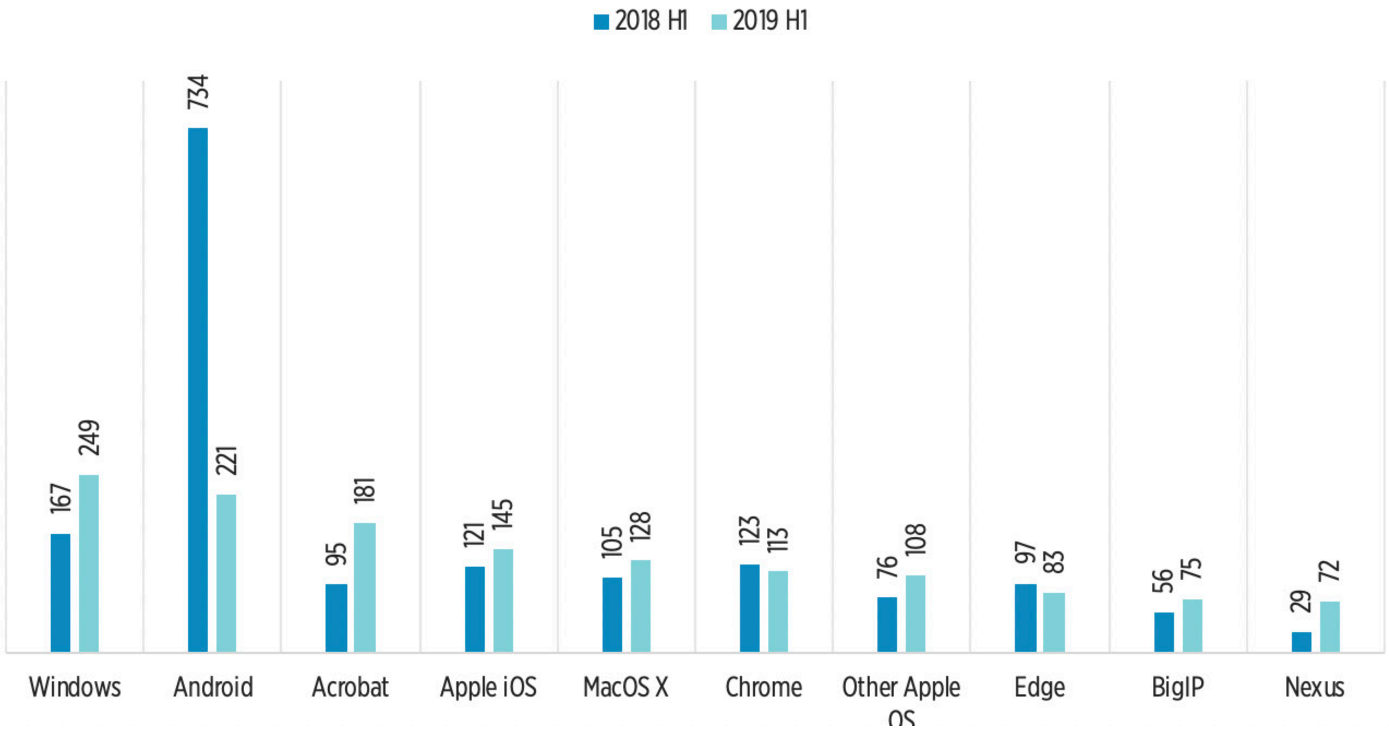

FIG 4 | Vendors with the most newly published vulnerabilities

The biggest change in the list can be seen at the top, where Windows surpassed Android OS by 30 vulnerabilities. While the number of Android vulnerabilities has dramatically decreased, Windows vulnerabilities have seen a not-insignificant increase over recent months. There is no clear cause for the vast disparity in Android vulnerabilities between 2018 H1 and 2019 H1, but it is noteworthy that support for the last of the Nexus devices (5X and 6P) ceased in December 2018. Following that move, Google has all but stopped reporting vulnerabilities unique to its current flagship Pixel devices, publishing a mere two this year, as opposed to dozens per month in the same period last year.[3] Apparently the result of a deliberate change, it has also optimistically renamed its device–specific “Security Bulletins” as “Update Bulletins,” focusing on improvements deemed non-threatening but important enough to be patched quickly.

[3] Source: Android Police https://www.androidpolice.com/2018/11/06/end-era-final-nexus-phones-may-just-gotten-last-update/

In another notable change, Nexus — Cisco's line of Nexus data center switches — burst into the top 10, displacing Firefox. The raft of serious reported vulnerabilities in the Cisco devices' operating system could be a consequence of a change within the company's PSIRT, considering that the majority were discovered in-house and only a small handful came from third-party researchers.

OS Vulnerabilities

Many applications are environment-sensitive and, as a result, vulnerabilities only crop up under certain conditions. The main determining environmental factor is the operating system. Cross-platform software may only be vulnerable to a given issue on some of its platforms. The operating systems considered here are those which have themselves been deemed vulnerable, or those whose presence is a necessary precondition to vulnerability in some other program.

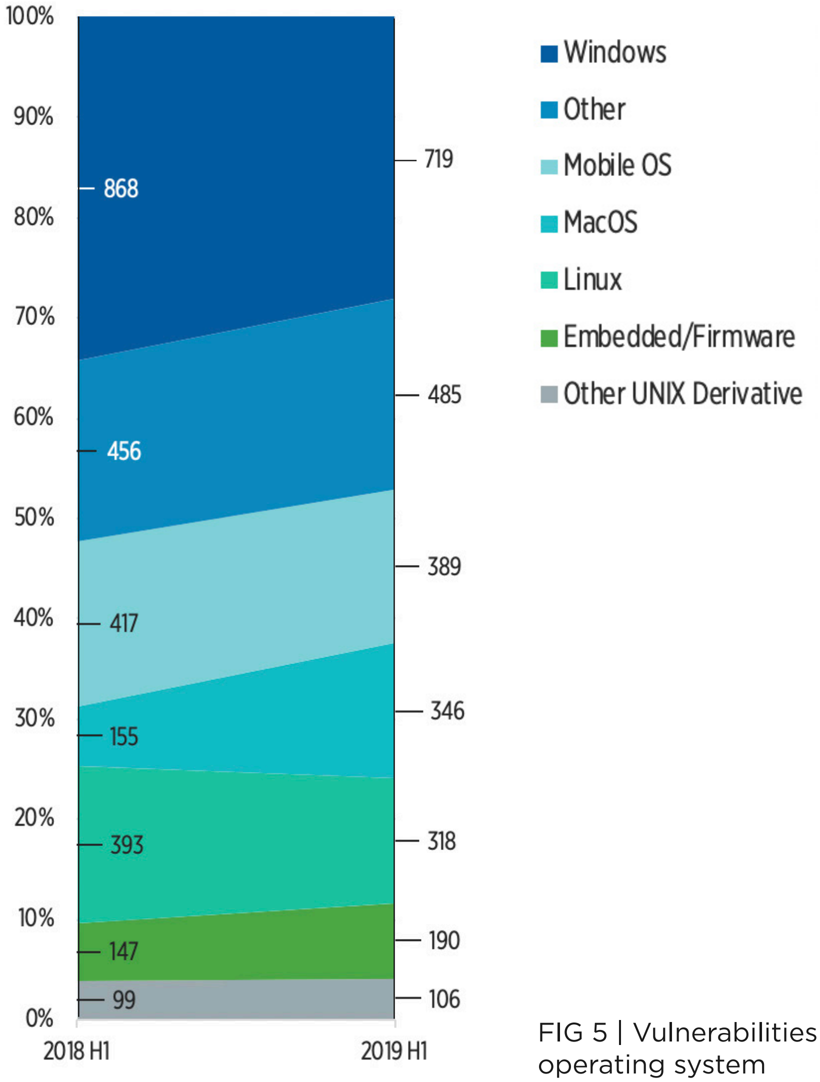

FIG 5 | Vulnerabilities by operating system

4 Source: Windows Latest https://www.windowslatest.com/2019/06/12/windows-10-june-2019-updates-and-bluetooth-problem/

Windows, in all its incarnations, and Linux lost quite a bit of its share. This is perhaps due to an increased focus on code security at the expense of functionality, as observed in a June security update that deliberately removed Bluetooth from some devices.[4] Linux OSs saw a similar proportional decline in new vulnerabilities as well. At the same time, vulnerabilities involving MacOS have more than doubled to claim that territory - MacOS added 191 vulnerabilities versus the 149 subtracted from Windows and the 75 from Linux.

Other operating systems have stayed relatively stable in their counts between halves, with seven more vulnerabilities in UNIX systems not included in other categories, 43 more for all manner of embedded device firmware, and an aggregate decline of 28 vulnerabilities observed in mobile operating systems.

Broad-Reaching Vulnerabilities

Code reuse often leads to “vulnerability reuse” across programs or across modules within the same software. When the vulnerable code is in a shared, low–level library; a popularly bundled tool; or even a protocol, it has the potential to have horizontal impact on either a:

- **Larger scale:** affecting at least 10 different vendors
- **Smaller scale:** affecting between three and nine vendors

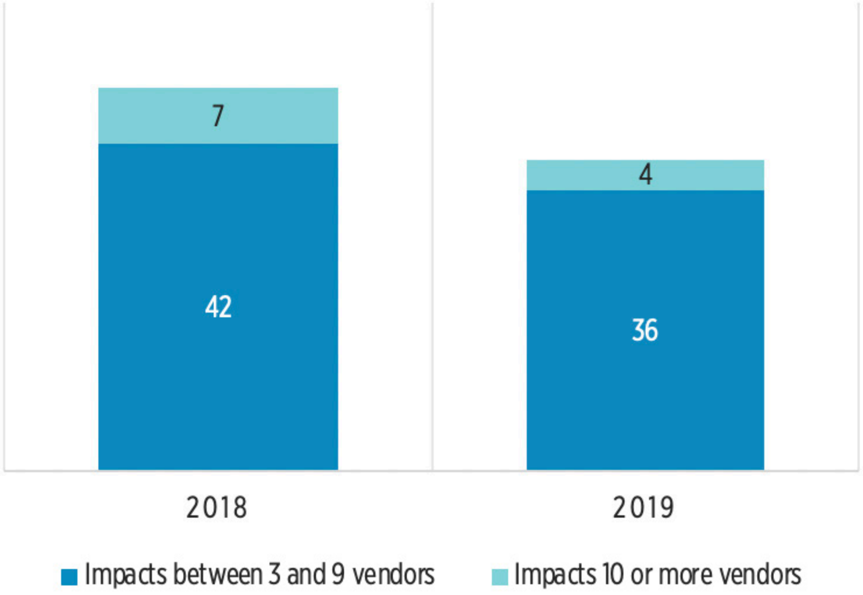

FIG 6 | Vulnerabilities affecting multiple vendors

In 2019, such vulnerabilities were heavily concentrated around CPU side-channel information leaks like Spectre/Meltdown and their derivatives, as well as flaws in Java and its derivatives.

Across 2018 and 2019 to-date, the more influential flaws have concerned information leaks at the processor level (there was one significant exception to this in 2018: the large scale and extensively exploited remote router compromise "ETERNALSILENCE") and, as such, have fallen into the larger scale category. Anything running on the affected architecture — like Windows or a browser — is collateral damage. Their data flow through the OS, so they are subject to the leak. One significant example of this is the original set of Spectre/Meltdown, vulnerabilities which existed on Intel, AMD and ARM processors and which became a hot topic in early 2018. Considering how prolific these three vendors are, and how they have produced almost all chips created over the last 20 years, it meant that the majority of chip-based devices contained the flaw.

The issues this year — known collectively by the less catchy phrase "microarchitectural data sampling vulnerabilities" (MDS vulnerabilities) are in Intel processors alone, and may still be accumulating vendor fixes and admissions of vulnerability.[5]

There has been a change in the distribution of influential flaws in the smaller scale category. In 2018 H1, more than 65 percent were Java-related; this year they have been spread more liberally, with only 25 percent Java-related and the remainder made up of OpenSSH, cURL and even the WiFi standard WPA. The decline in Java vulnerabilities could well be tied to an overall decline in Java usage and a turn to alternatives.

The small scale category this year holds true to the pattern of "low level = broad reach." The command-line tool cURL is ubiquitous in homebrew code and commercial software. A vulnerability like CVE-2018-16890 in the underlying library — libcurl — renders applications ranging from Oracle's Secure Global Desktop to Siemens industrial communications control SINEMA software to the spectrum of UNIX-like OS flavors remotely disruptable by a maliciously crafted signal. Likewise, OpenSSL is a tool commonly invoked by network software and the firmware running on routers and switches. A vulnerability like CVE-2019-1559 in OpenSSL potentially weakens the encryption of home, commercial and even security devices that rely on it for encrypted communication across the internet.

[5] Source: Wired https://www.wired.com/story/meltdown-spectre-bug-collision-intel-chip-flaw-discovery/

NOTABLE VULNERABILITIES

FEB 2019

FaceTime Eavesdropping for Beginners

A bug in Group FaceTime allowed a caller to listen through an Apple device's microphone without the victim even accepting a call. In the unfolding of the story, Apple's tortuous vulnerability reporting apparatus was laid bare to the nontechnical world.

MAR 2019

MacOS Zero–Day Dirty Cow Flashback

Apple piled up a number of zero–day vulnerabilities including one which allows processes to invade each other's memory space and corrupt the contents. Google's vulnerability research team, Project Zero, revealed this in March and a patch has not yet appeared.

Vulnerabilities in Unscannable Cisco Devices

Cisco's networking operating systems NX-OS and FXOS got a security overhaul, releasing a number of new versions for the Nexus and Firepower lines to address vulnerabilities, some of which have publicly known exploits (e.g. SBV-98762 and SBV-98763). Problem is, these vulnerabilities wouldn't appear in active vulnerability scans.

APR 2019

Failure to Launch French Chat App

Within the first day after France released its new secure chat application for government users a bug was found, escalated to the developers of the underlying technology, attributed to a standard Python parsing function, and fixed. Voilà.

MAY 2019

BlueKeep's WannaCry Déjà Vu

Just as WannaCry remained dangerous long after its public disclosure due to its potency on unpatched Windows systems, the imminent threat of BlueKeep hangs in the air. Any computer with Remote Desktop before Windows 8 is vulnerable to an attack with similar wormable capabilities to the ransomware which spread around the world.

More CPU Data Leakers

Every few months since January 2018, batches of bugs have been discovered that take advantage of sophisticated ways data flow into and out of modern CPUs. The four that came out in May only affect Intel chips and patches have been released to OEMs.

JUN 2019

Zero–Day to Take Down a Windows Fleet

The dust kicked up around SymCrypt was less about the sample exploit dropped into the public by Project Zero and more about the manner in which they did it. The sample exploit code can trigger an infinite loop in X.509 certificate processing on millions of Windows servers.

Exploits

The number of exploits deployed in the wild for known vulnerabilities is always a fraction of those for which proofs of concept are developed. Both this year and last year, about one tenth were exploited in the wild. The greatest number of both types is against internet and mobile applications. This segment has a notoriously low bar for entry in terms of developer qualifications due to the global and open nature of the internet. A working sample of a cross-site scripting exploit for a poorly engineered WordPress plugin can be a single line of URL parameters to pass to the site through standard means (i.e., a browser address bar). Additionally, browsers are the point of contact between end users and the world in millions of instances, so they are also the point of ingress for bad actors. The popular browsers, especially Google Chrome, could therefore give black-hat hackers the most bang for their buck.

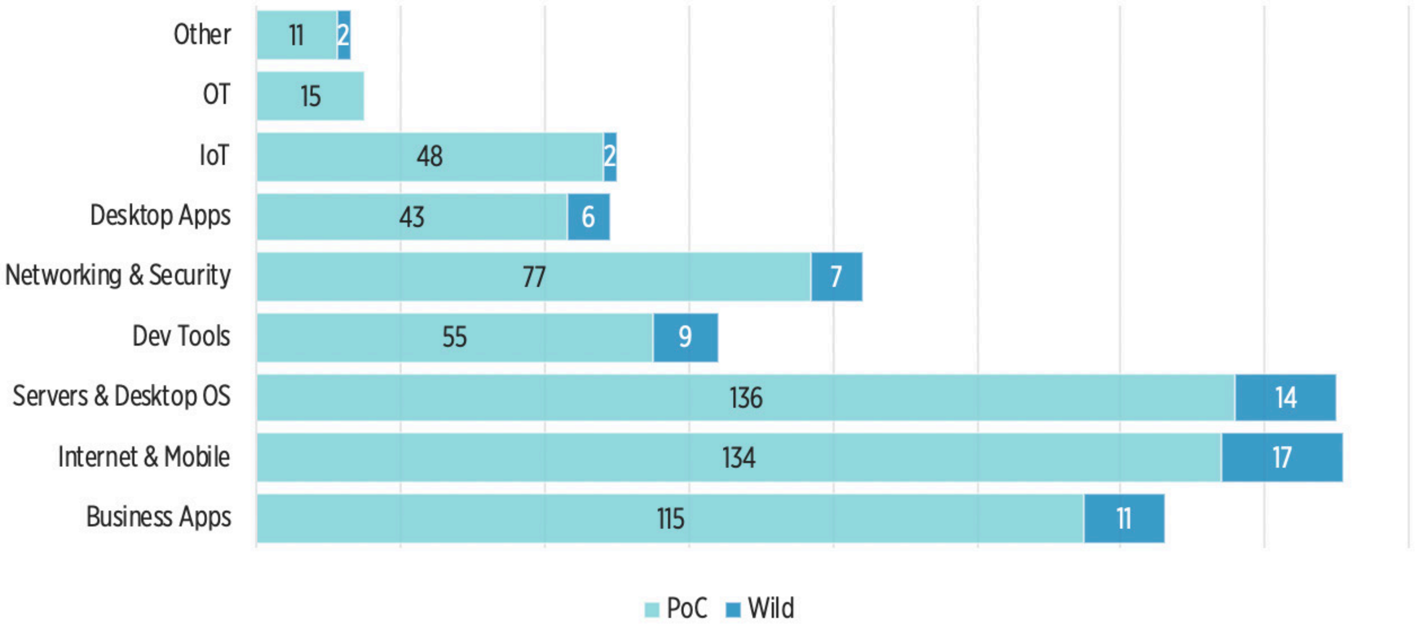

FIG 7 | Exploits by software category in 2019 H1

Of the new vulnerabilities exploited in the wild, the relative majority exploited internet and mobile apps, 50 percent of which were WordPress plugins.

[6] Source: ZDNet https://www.zdnet.com/article/hacker-group-has-been-hijacking-dns-traffic-on-d-link-routers-for-three-months/

The exploited vulnerabilities in networking and security products in 2018 were spread around among firmware of home/commercial/industrial equipment. The field was narrowed in 2019 to almost entirely consist of Cisco products which are usually deployed in large-scale business or public infrastructure. The exception was a DNS hijacking exploit that was used in a rash of attacks on consumer D-Link routers earlier this year.

New vulnerabilities remotely exploited in the wild with no user interaction have slipped slightly between 2018 H1 and 2019 H1 from 46 to 43.[6]

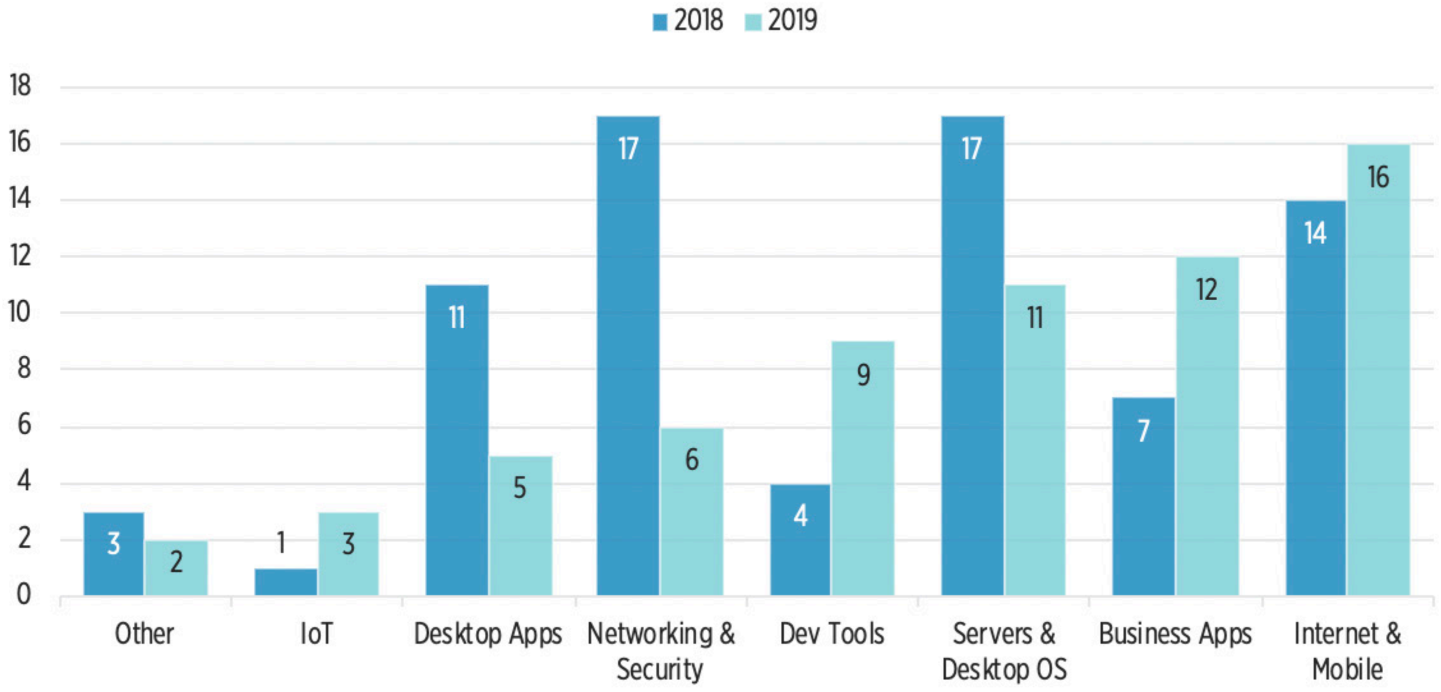

FIG 8 | Newly published vulnerabilities exploited in the wild in 2018 and 2019 H1

Apple's advisories on a privilege elevation/jailbreaking vulnerability (CVE-2019-7286) became the latest vendor-reported vulnerability with a preexisting exploit in the wild in 2019 H1. While first believed to only affect iOS, information and fixes for tvOS and Watch OS trailed two months after Apple's rapid application of the initial patch.

There have also been notable advisories on exploits with a sample exploit but currently no known malicious exploitation. Two relate to Oracle Communications applications on notorious system vulnerabilities — the root issue was publicly disclosed in January with Oracle patches appearing in mid–April as part of the company's quarterly bulk advisory.

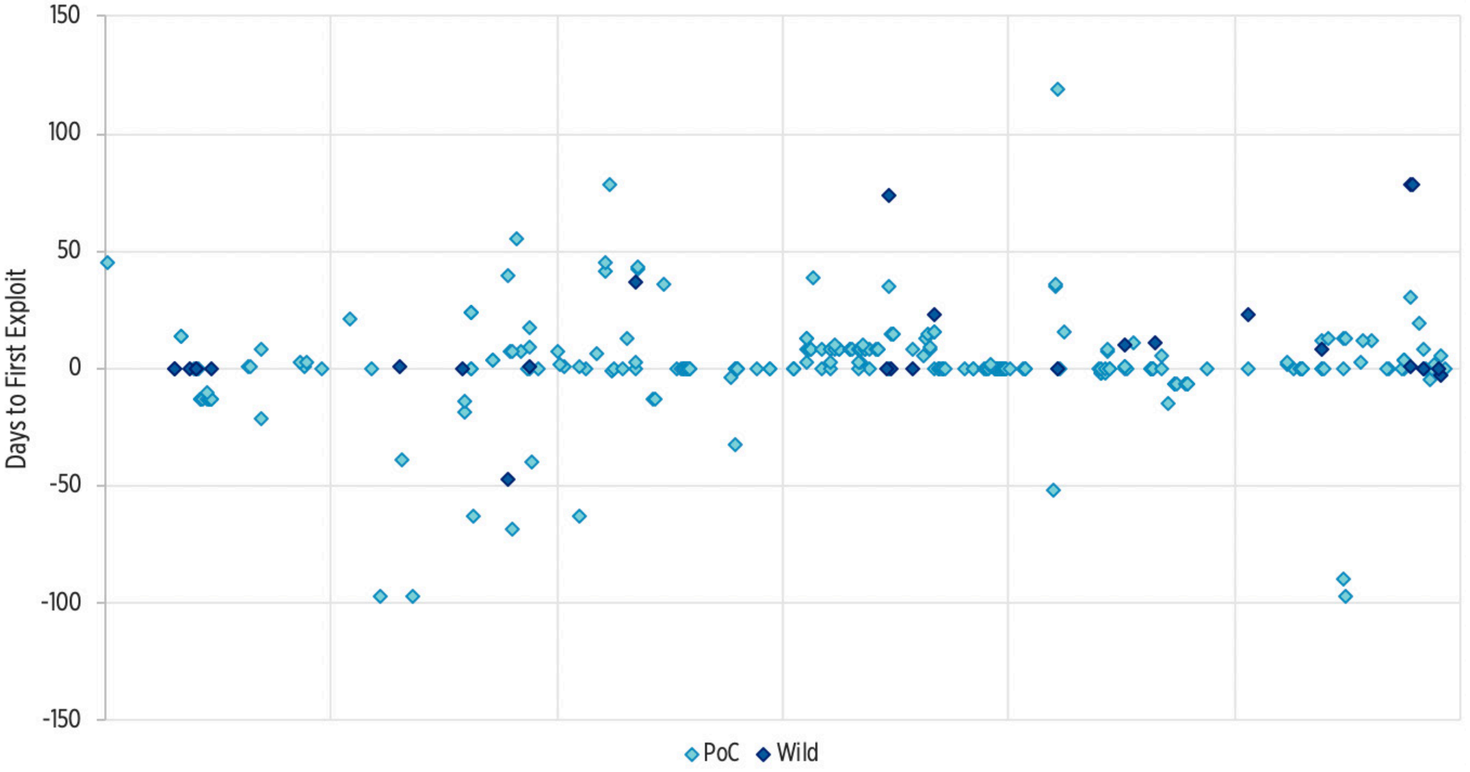

FIG 9 | Number of days between when vulnerabilities were reported and exploited in 2019 H1

Cloud Container Vulnerabilities

Vulnerabilities in containers, which create a distinction between virtual servers hosted on a shared machine, have increased by 46 percent in the first half of 2019 compared to the same period in 2018, and 240 percent compared to 2017 H1 figures.

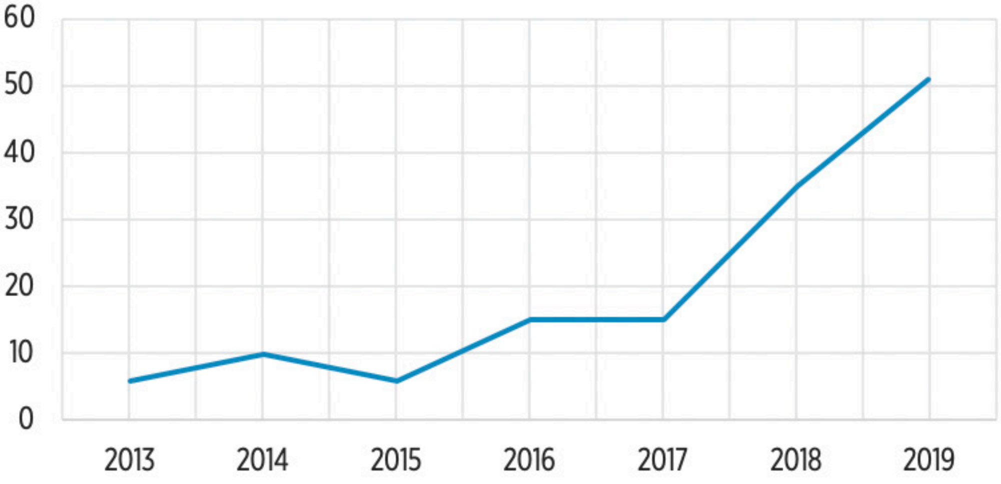

FIG 10 | Container product vulnerabilities in first half of the given year

Containers have also produced a number of interesting vulnerabilities so far this year.

CVE-2019-5736 allows root code execution on a host from a guest OS in a container. It was discovered, exploited and patched in-house but affected many container runtime systems. Owners and operators of private or hybrid cloud environments with Docker, Kubernetes, containerd and others had to patch. While the same was also true for all Linux distributions using runC, customers AWS and Google Cloud were given instructions so that they could patch their own instances.

In May, this vulnerability, alongside three others, was revealed to exist within Docker. As the adoption of cloud infrastructure for regular workflows[7] grows, so does Docker's profile. Docker is a popular set of SaaS and PaaS products which use virtualization to allow for the creation of independent containers; container vulnerabilities present an administrator with a set of challenges similar to those presented by virtualization in general. A system running in a container is internally vulnerable to the guest application with the weakest security, and externally vulnerable to management and other software designed to interface with it.

There are concerns about the maturity of cloud service vendors' cybersecurity, and the risk that may be introduced if they have a lack of robust security processes in place. One example of how cloud companies can introduce risk came at the start of the year when more than 24 million financial documents stored on an incorrectly deployed ElasticSearch server were leaked. The leak was traced back to data and analytics company Ascension with the fault being attributed to the now-defunct firm OpticsML.[8] The leak happened because of a lack of basic cyber hygiene: they failed to use a password. As a result of this mistake, files from major corporate enterprises and some U.S. federal departments were left out in the open. A warning tale about how much trust should be placed in the hands of third parties.

[7] Source: Tripwire https://www.tripwire.com/solutions/devops/tripwire-dimensional-research-state-of-container-security-report-register

[8] Source: Tech Crunch https://techcrunch.com/2019/01/23/financial-files

Operational Technology Vulnerabilities

The first half of 2019 saw nearly 50 new advisories from ICS-CERT and a spate of new attacks, with LockerGoga stealing the headlines.

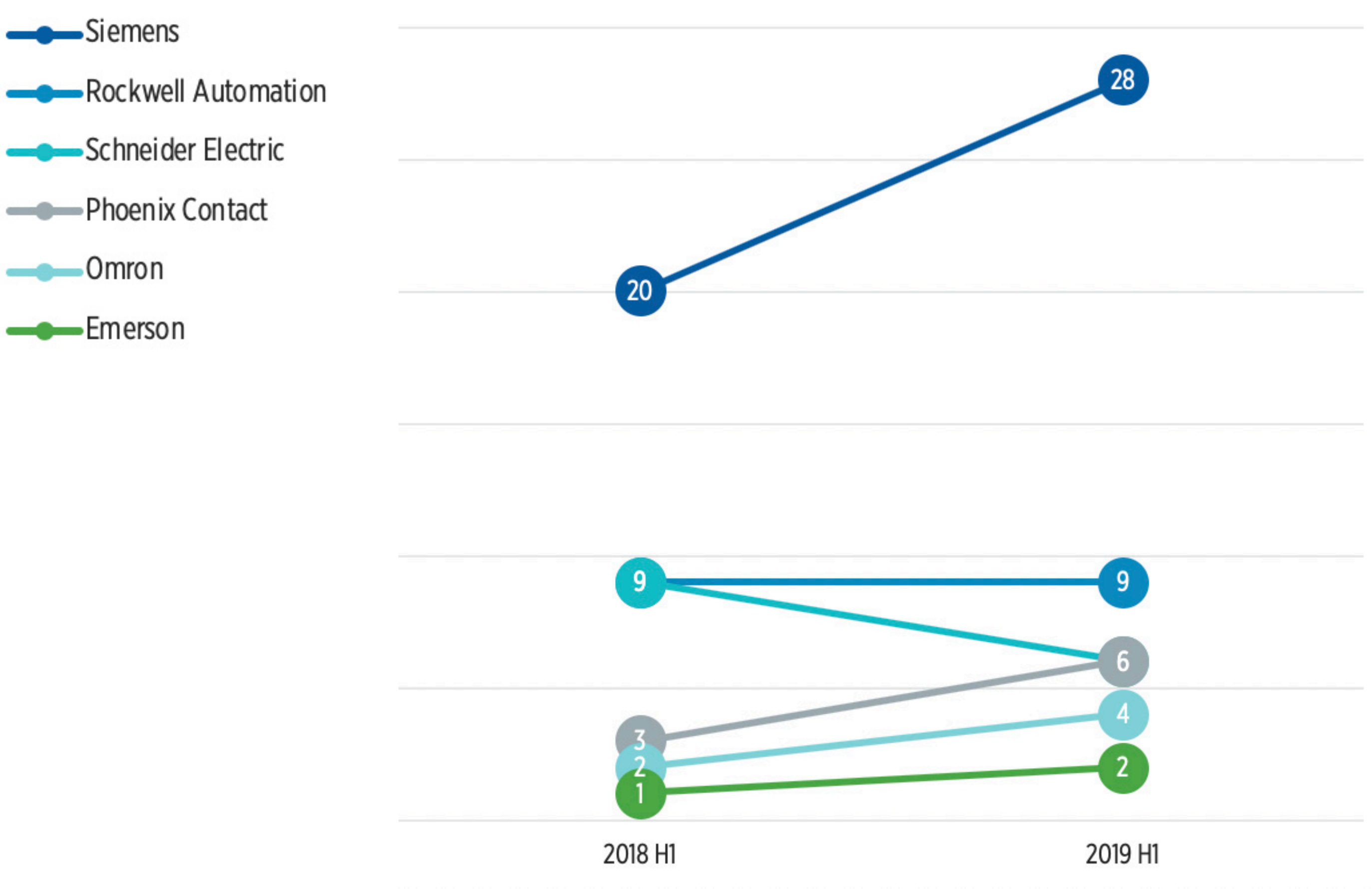

FIG 11 | ICS-CERT new advisories

Siemens consistently leads the pack in advisories compiled by ICS-CERT. This holds true in 2019 H1. The advisories usually contain multiple related vulnerabilities published together in response to a security-related discovery in their products, or occasionally in response to an incident.[9] Lately, Siemens has increased its publication of vulnerabilities in third-party products which are implemented or incorporated in their systems, including a recent bulletin containing 42 CVEs in a single device — the programmable logic controller SIMATIC S7 S7-1500 CPU 1518(F)-4 PN/DP MFP. All of the vulnerabilities exist in the GNU subsystem on which the controller's firmware is based; Siemens provides its own firmware upgrades for some of the flaws.

[9] Source: US CERT https://www.us-cert.gov/ics/advisories

LOCKERGOGA: AN OVERVIEW

LockerGoga ransomware is particularly severe in the degree with which it cripples an affected system, disallowing access to all accounts and shutting it down. This has the effect of obscuring the ransom demand, making fulfilling its demands or otherwise taking steps to remove it extremely difficult. Infection vectors for all LockerGoga attacks, if known, have not been made public – such details are often kept secret.

- LockerGoga appeared in January and wreaked havoc on a series of industrial companies across the northern hemisphere
- Altran, a global engineering consulting firm based in France, was also attacked in January, forcing it to temporarily shut down its IT network and applications[10]
- It reared its head again in March in an attack on Norwegian metal manufacturer Norsk Hydro, as well as two US-based firms: adhesives manufacturer Hexion and silicone manufacturer Momentive[11]

Operational technology (OT) is a part of the hardware and software that monitors and controls how physical devices perform. In the past, OT was used to control systems that were not networked, such as manufacturing and utilities.

As digital transformation spreads within the industrial environment, many of today's OT systems are being transited or tunneled over corporate networks. Common internet protocols are leveraged to enable this move, meaning that once-isolated OT systems and devices are becoming increasingly connected via wireless technologies. This, in turn, makes them targets for cybercriminals. These are systems that are vital to the functioning of modern societies and are therefore very attractive targets for cybercriminals, particularly nation-state threat actors.

In recent years, the volume of attacks against OT networks has increased. These are attacks which aim to take control of systems or machines, disrupt normal activities, steal data, or to cause significant damage.

[10] Source: Reuters https://www.reuters.com/article/us-altran-tech-cyber/frances-altran-tech-says-it-was-hit-by-cyber-attack-idUSKCN1PM0IJ

[11] Source: Vice https://www.vice.com/en_us/article/8xyj7g/ransomware-forces-two-chemical-companies-to-order-hundreds-of-new-computers

Most Exploited Vendors

Microsoft, Oracle, and Cisco maintained the distinction of most exploited vendors in 2019 H1, with Microsoft displacing Oracle as the most exploited vendor so far this year. Apple, whose actively exploited vulnerabilities accounted for eight percent of the total, released a fix for its Apple TV Software (the precursor to tvOS) in May to address the Broadpwn vulnerability. Broadpwn was the nickname given to an arbitrary code execution flaw found almost two years prior to this fix, and its late reporting by Apple could indicate that its applicability to Apple TV Software was known to the company well in advance but suppressed until the fix was ready.

MOST EXPLOITED VENDORS			
2018 H1		2019 H1	
MICROSOFT	11%	MICROSOFT	28%
ORACLE	14%	ORACLE	15%
CISCO	11%	CISCO	10%
ADOBE	14%	APPLE	8%

Edge Edging Out IE?

The total number of vulnerabilities for this set of browsers in Figure 12 remains practically unchanged.

While the percentage of vulnerabilities in IE is proportionally the same, Edge has gained a number of new vulnerabilities – almost the same number as those "relinquished" by Firefox. This shift is probably just a sign of the Microsoft browsers' relative ages.

It is interesting to note that Mozilla's security department publicly changed its policy on responding to bug reports in the second half of 2018. Now, it preemptively immunizes reporters vying for bug bounties from threats or legal action. This was a policy decision in keeping with the firm's vocal ethos to build a foundation based on principles of openness. From the outset it looked like this move could have opened the door to greater numbers of vulnerabilities being reported, but instead we have seen a 44 percent reduction in the number of published reports. This could well be due to the security attitude reflected in Firefox's new approach.

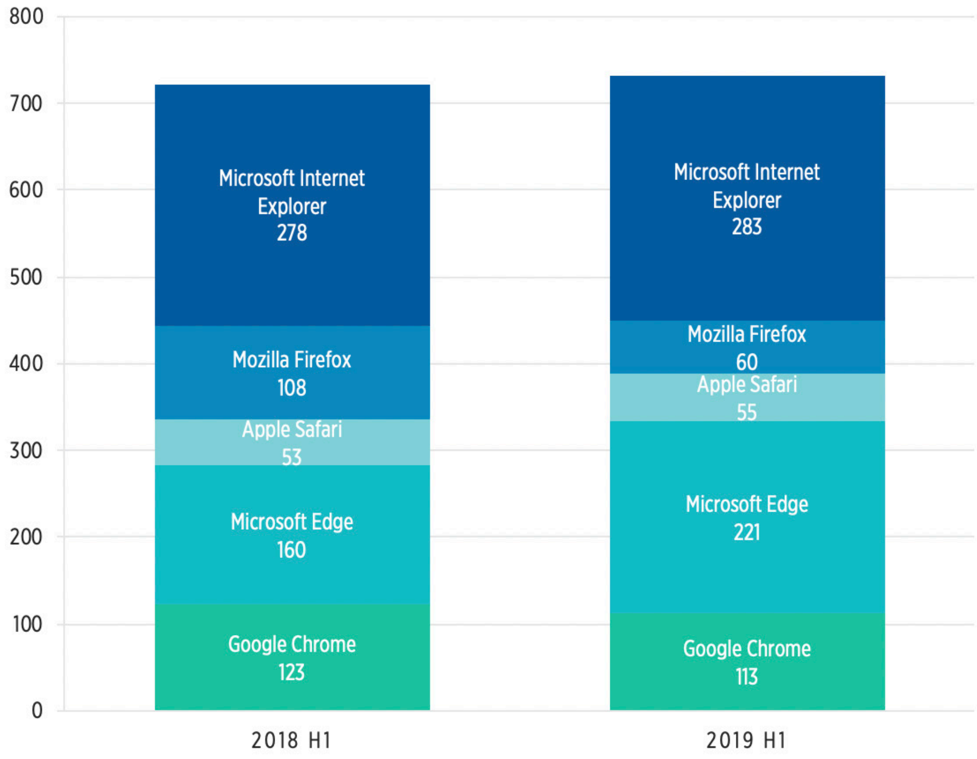

FIG 12 | Most vulnerable browsers

MALWARE & ATTACKS

Top Malware Families

Ransomware, backdoors and botnet malware have filled in the vacuum left by the retreat of last year's cryptocurrency mining malware surge.

The complexity of the malware ecosystem is due in part to its utter lack of checks on the malleability of the products. As a result, it is very common for malicious programs to comprise a patchwork of elements from other programs and to behave differently depending on the adversarial context. Many of the botnet 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, many of which are variations or derivatives of Mirai, a malware first discovered in August 2016.

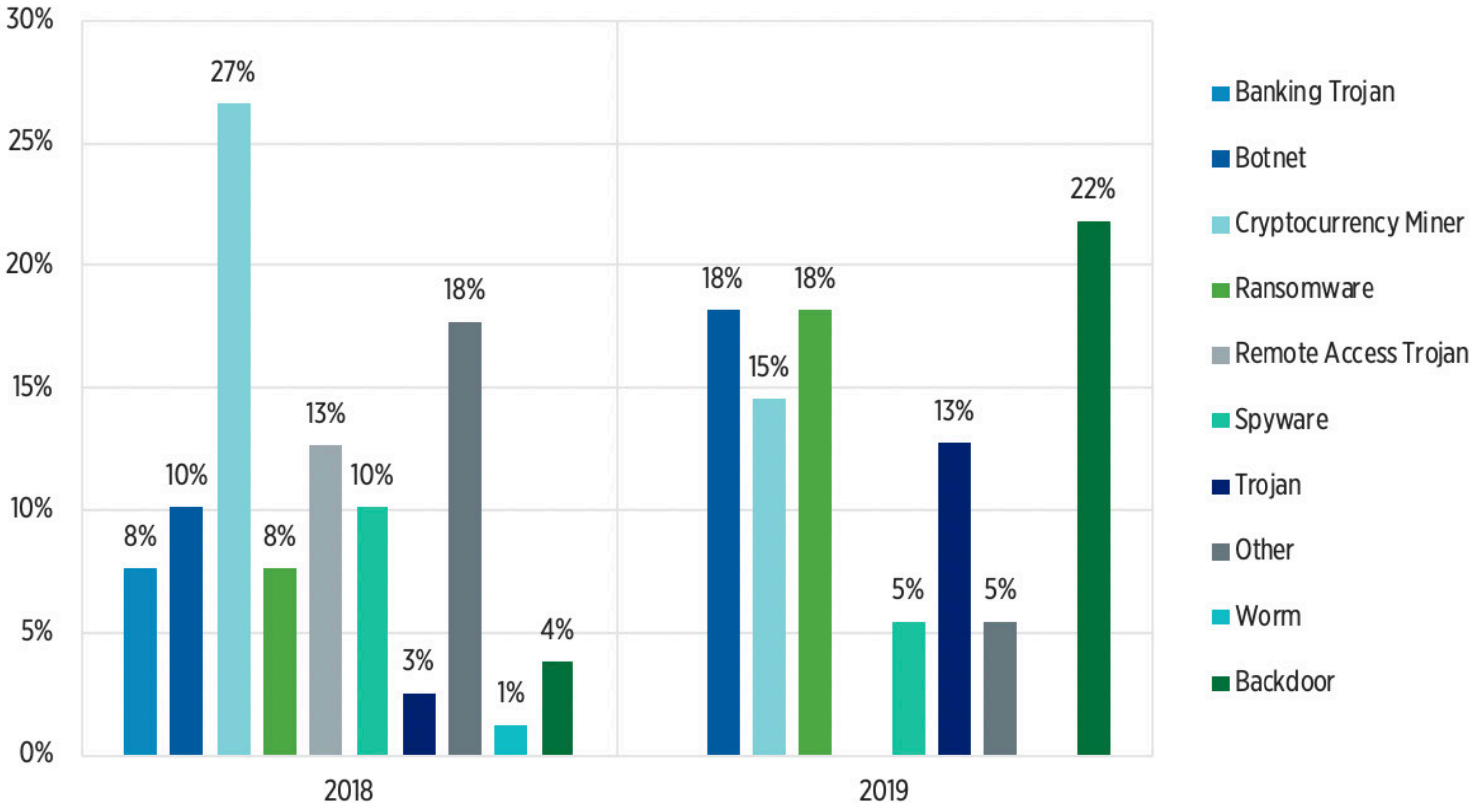

FIG 13 | Percentage of attacks attributed to malware families

Old malware techniques, even if public and with available fixes, are still a threat. The finger of blame for this is usually pointed towards poor IT maintenance and a lack of proper cyber hygiene but evidence of this is hard to come by. Phishing, which requires both technical and human contributions to be successful, remains an industry-wide problem that few understand how to resolve.

This report looks exclusively at newly introduced malware that takes advantage of, or is delivered with the help of, technical vulnerabilities. It does not include those attributable to human error. This is because all experts agree technical vulnerabilities need to be addressed by clearly defining and limiting the size of the attack surface. On the other hand, finding a solution to vulnerabilities which arise as the result of human error has caused the development of two divergent schools of thought in the industry: while some argue that change can be made through habits of heightened vigilance, others believe that the (as yet largely aspirational) realm of machine learning should soon be able to insulate users from phishing lures without their knowledge. This report is focused on identifying addressable, technical malware types which organizations can protect against in practice, instead of in theory.

INSIGHTS

Cryptocurrency Miners Decline Sharply

The worth of the largest cryptocurrencies has dropped dramatically in 2019 H1 when compared to early 2018. This price drop means that there is less incentive for criminals to invest resources in mining cryptocurrency even by legitimate means. Mining requires a lot of physical machinery, physical maintenance and power: for a lot of attackers, it is simply not worth their effort.

This has had a knock-on effect on the wider cybercrime world, where fewer mining programs are being developed.

This decline is compounded by the closure of Coinhive, a big cryptojacking provider, in February after it reported a reduction in profitability and wanted to distance itself from its technology’s facilitation of illegal practices.

Cloud Risks

Recently, we have seen a big increase in container adoption and usage, thus more focus has been placed on the security of cloud containers. Containers provide operating system virtualization without operating system images. With containers in place, virtual servers can be treated as a true replacement for physical servers. There are clear benefits the servers, namely the speed of deployment and dissolution, access to fine-tuned controls and the ability to easily monitor server status through one central interface. Containers simplify cloud development — it is easy to escape a container via the runtime layer — which makes it attractive to a lot of organizations. Still, businesses need to approach containers with caution.

Ease of deployment may lend to lapses in patch management: old images can be pulled off the shelf, replicated and deployed more readily than an old physical server can. And while agility in development is positive from a business standpoint, any project that depends on quickly bringing up and tearing down servers could suffer from greater exposure to vulnerabilities in those old images. The practical benefits of containers may be enticing but that does not mean that their vulnerabilities can be overlooked. Robust processes need to be developed to assess container vulnerabilities, determine their exposure in light of surrounding security measures and contextualize with exploit activity.

IoT Potential Cyber Risks

Internet of Things (IoT) technology has opened the door to new and better ways to manage data, improve communication and increase profits. Overall, it has enhanced productivity in businesses and in our personal lives.

This ability to connect devices to the network has created new potential opportunities for cyberattacks.

Besides the usual headline-making risks, one of the main risks inherent to IoT devices lies in manufacturing plants. Vulnerable IoT devices could be used to hijack a machine's critical functionality. For example, ladder logic (a graphical programming language) could be injected into a control device or programmable logic controller. If this low-level code, which is never refreshed, is inserted into a high-priority machine which is rarely, if ever, rebooted, it has a better chance of persisting over time. The machines in question are usually air-gapped and communicate on proprietary, system-specific protocols, which makes finding a solution to the problem of new threats being introduced by IoT devices to old devices incredibly difficult.

There are some specific attacks which could greatly impact OT systems and devices:

- Exclusion attacks (e.g., running the motor while the oil pump is turned off)
- Wear attacks (e.g., keeping the clutch at 90 percent will reduce the lifespan of the equipment)
- Inertial attacks (e.g., large machinery is not designed for rapid acceleration or deceleration, and doing so will reduce lifespan)
- Surge attacks (e.g., systems are designed to handle a certain amount of product, and exceeding this limit may cause equipment damage)

Aside from concerns around the impact that IoT products will have on OT, they are also still struggling with password-related security issues which stem from both the product manufacturer and its customers.

As IoT product creators race to release new products ahead of their competitors, product cycles are being shortened. This has led to security issues being given lower priority. The default passwords on the devices are often weak and are even frequently posted online for faster device setup. If a customer fails to rapidly change to more secure passwords, potential attackers will be easily able to remotely hack the IoT products.

Adding to this problem is the fact that many IoT manufacturers do not encourage customers to change default passwords. In some cases, they cannot even be changed. Even when they can, customers are known to use weak passwords and permissive network communications which allow the device to communicate with anyone.

RECOMMENDATIONS

Establish Risk–Based Vulnerability Management

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 and unprotected by security controls.

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 risk–based vulnerability management 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 importance
- Asset exposure

These last two factors — asset importance 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 own 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 risk–based vulnerability management, click here.

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 a service (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 standard 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 more than 130 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