SKYBOX SECURITY

2020 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 analysis 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, 2020.

CONTENTS

EXECUTIVE SUMMARY

The COVID–19 crisis has made a significant impact on the cybersecurity landscape. The sector's existing challenges — including the cybersecurity skills shortage, under–resourced security programs and increasingly fragmented estates — have been exacerbated as organizations scramble to enable their remote workforce and secure expanded network perimeters. While this critical work has been taking place, cybercriminals and nation–state threat actors have been working hard to capitalize on the chaos.

The *2020 Vulnerability and Threat Trends Report Mid-Year Update* shows how criminals have taken advantage of the disruption caused by the pandemic. While organizations were vulnerable and distracted, hackers developed new ransomware samples and advanced existing tools to attack critical infrastructure — including vital research labs and health care organizations.

The sophistication of the malware and methods used by attackers over the first half of 2020 highlight just how complex cybersecurity management has become. Add to this the 20,000 new vulnerabilities likely to be reported in 2020, and it's clear that the burden placed on security teams is only going to increase — even if we manage to enter a post–COVID reality later this year. If organizations do not have full visibility over their entire security environment, and if they are unable to focus remediation on their most exposed vulnerabilities, then they could fall victim to attack at a time when business continuity, brand trust and fiscal stability are paramount.

The report emphasizes the need for organizations to adopt risk–based strategies so that they can manage the mass of new vulnerability reports and deal with heightened threat levels. It is only through gaining full and unerring network visibility, modeling the environment and analyzing exposure that organizations will be able to gain the insight and focus that they need to emerge from the pandemic unscathed.

KEY FINDINGS

20,000+ New Vulnerability Reports Likely in 2020

Over 9,000 new vulnerabilities have been reported in the first six months of 2020 (a 22–percent increase on reports published over the same period in 2019), and we are on track to see more than 20,000 new vulnerabilities this year — a new record. This will be a figure that defines the complex landscape within which security professionals operate.

50% Increase in Mobile Vulnerabilities Highlights Dangers of Blurring Line Between Corporate and Personal Networks

Vulnerabilities on mobile OSs increased by 50 percent, driven solely by Android flaws. This rise has come at the same time as home networks and personal devices increasingly intersect with corporate networks as a result of the move towards a mass, remote workforce. These trends should focus the need for organizations to improve access controls and gain visibility of all ingress and egress points to their network infrastructure.

Ransomware and Trojans Thrive During COVID–19 Crisis

The creation of new ransomware and malware samples has soared during the COVID–19 crisis, a time that has also seen a significant increase in exploits taking advantage of Remote Desktop Protocol (RDP). These tools are enabling cyberattackers to capitalize on individual concerns and take advantage of overwhelmed security teams.

Attacks on Critical Infrastructure Adding to the Chaos

Attacks on national infrastructures, pharmaceutical firms and health care companies have increased as criminals become emboldened by chaos spurred by the pandemic. These attacks have added to the turbulence and could hamper countries' abilities to respond to the health crisis.

RESULTS

VULNERABILITIES & EXPLOITS

20,000+ New Vulnerability Reports Likely in 2020

The first half of 2020 saw a major increase in new vulnerability reports (9,799 in 2020 compared to 7,318 in 2019, representing a 34-percent increase). This figure also exceeds the previous high reported in the first six months of 2018 (8,485) and indicates a record-smashing tally for 2020.

Extrapolating forward from previous years' trends, it is likely that more than 20,000 vulnerabilities will be assigned in 2020. While possible that all new vulnerabilities may not be published, annotated and analyzed by the National Vulnerability Database (NVD) until years later, the likelihood of hitting the watershed 20,000 figure reaffirms the uphill battle that security teams across the world are having to fight: making sense of which vulnerabilities pose the greatest risk to their organization.

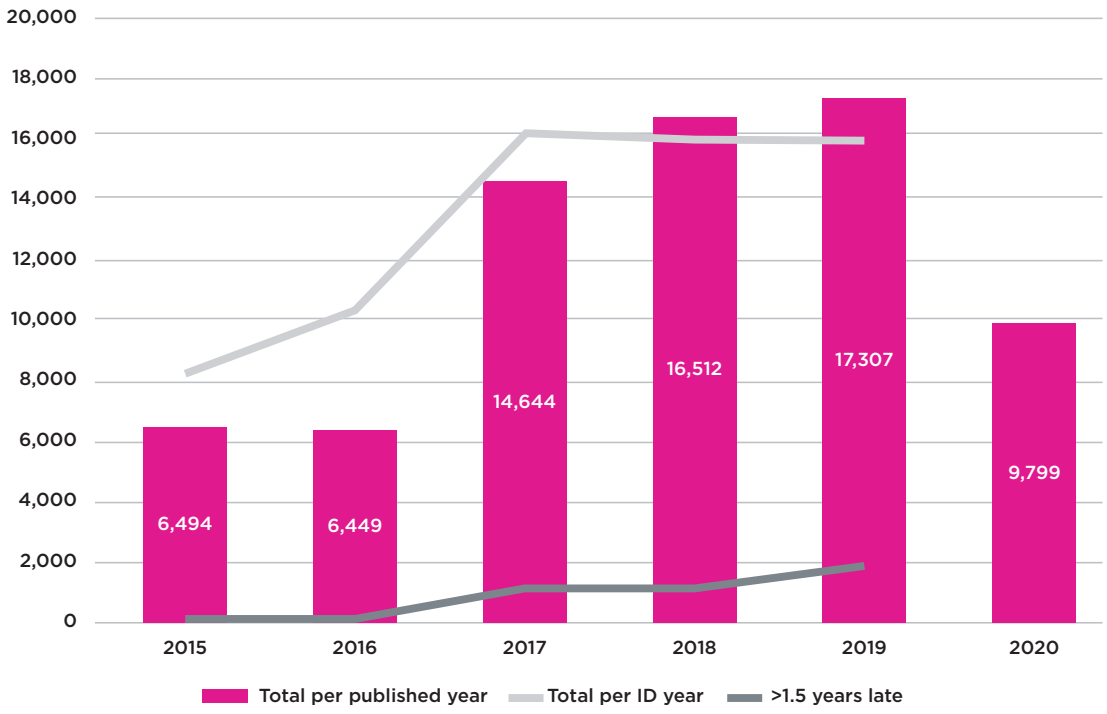

FIG 1 | New CVEs by year and the year those vulnerabilities were identified.

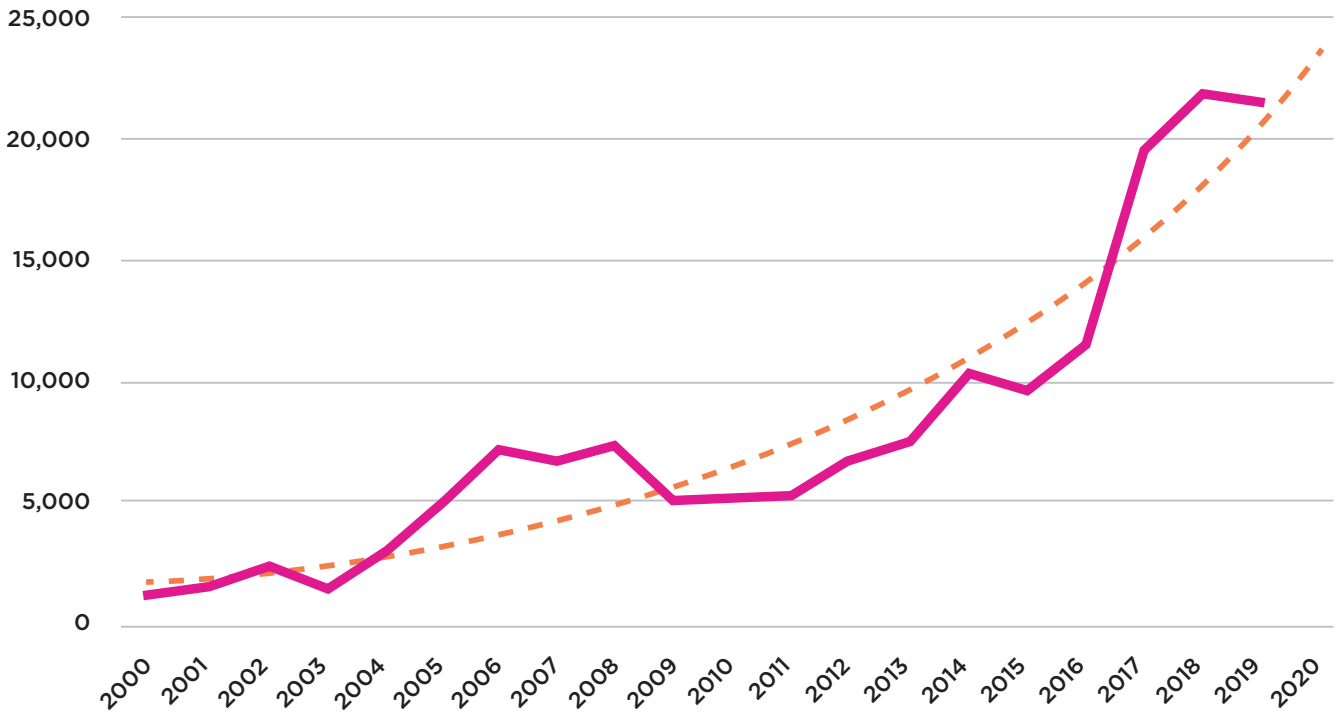

FIG 2 | CVEs allocated by the MITRE Corporation per year from 2000 through 2019. Dotted line is assuming exponential growth in 2020.

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.

It's important to remember that higher vulnerability counts don't necessarily mean that technology is becoming less secure; rather, the more likely scenario is that more efforts are being put into vulnerability research by vendors and third parties. However, higher vulnerability counts can further complicate an organization's prioritization and remediation processes. To deal with the inevitable increase of vulnerability occurrences within an organization, security programs need to have established processes to contextualize vulnerabilities based on exposure, exploitability and other factors to keep remediation focused on critical risks.

Middle-of-the-Pack Severity Could Create Major Risks

The need for an intelligent and more automated approach to remediation is evident when looking at the spread of CVSS scores by category. The severity spread for new vulnerabilities reported in the first six months of 2020 looks very similar to 2019's figures. Vulnerabilities with a high severity score compose 42 percent of the total vulnerability count, with medium-severity vulnerabilities following behind with 40 percent of the total. Critical-severity vulnerabilities make up 15 percent of all new reports.

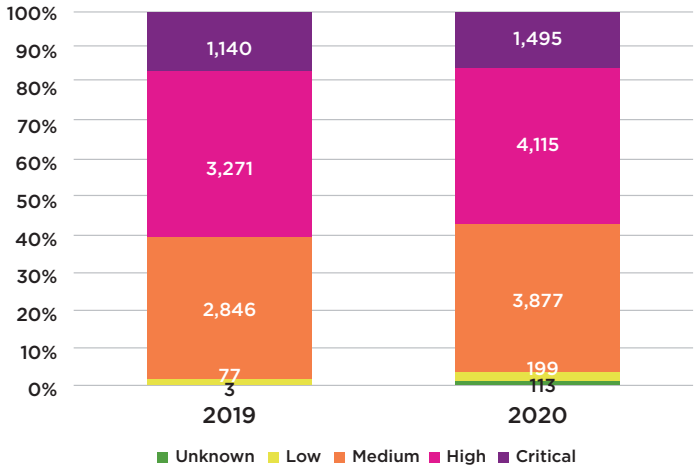

FIG 3 | New vulnerabilities' CVSS scores split by severity level

Although organizations are naturally inclined to prioritize the remediation of critical- and high-severity vulnerabilities before medium-severity instances, this generic approach to prioritization could allow attackers to take advantage of any exposed medium vulnerabilities. Criminals know that medium-severity flaws can sit unpatched within an organization's systems for a long period; depending on where these flaws exist, they could give an attacker access to a critical asset or enable lateral movement.

While CVSS scores are useful for understanding the properties of a vulnerability in isolation, they are created without contextual understanding of an individual organization's security environment. This is context that needs to be ingrained in the way that security programs are run; security teams need to understand which of their vulnerabilities are unprotected by security controls and exposed to threat origins — regardless of CVSS score — to lower their overall risk profile.

50% Increase in Mobile OS Vulnerabilities

Mobile OS vulnerabilities have risen by 50 percent compared to the first six months of 2019. This surge can wholly be attributed to an increase in new Google Android vulnerabilities, which more than doubled in count to 492, compared to the 230 reported in the same period last year. That mobile OS vulnerabilities have not followed suit by increasing by over 100 percent is down to a decrease in new vulnerabilities reported by Android's main market competitor, Apple, whose iOS saw new vulnerability reports decrease by 20 percent to 121, from 152 last year.

The sudden rise in Android vulnerabilities should, however, be understood with the caveat that they are unpredictable in terms of content and distribution. While more than 150 appeared in June 2020, there were only 20 published in June 2019. It is possible that the current trend for mass Android vulnerability reports could dissipate throughout the year.

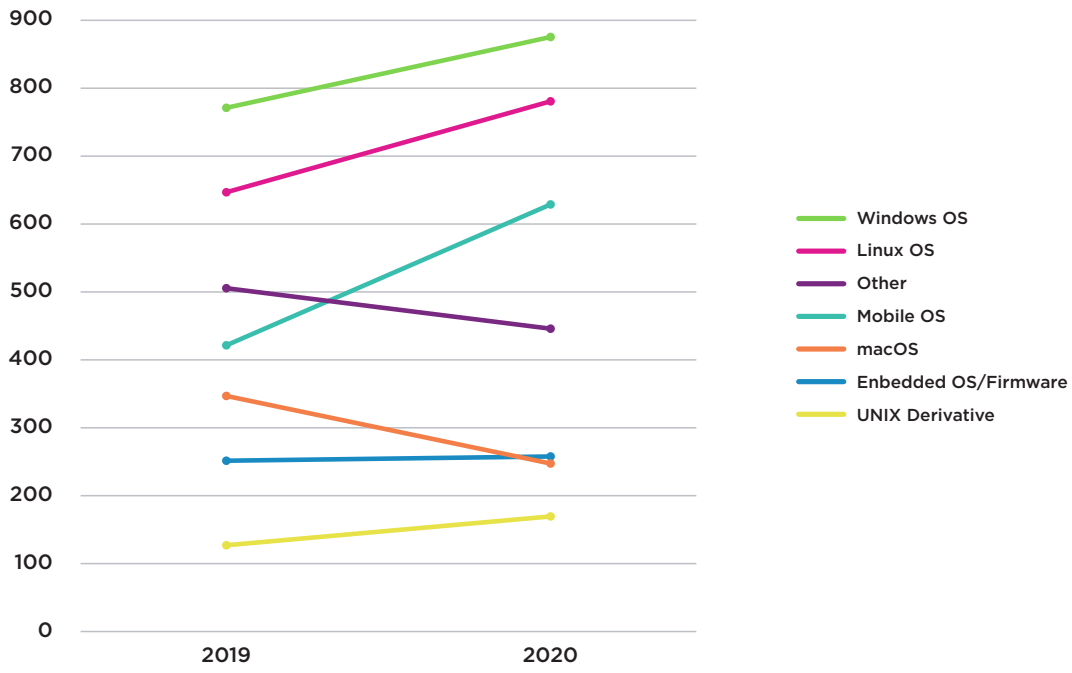

FIG 4 | Vulnerabilities by operating system January – June

Business Apps Join Ranks of Most Vulnerable Products

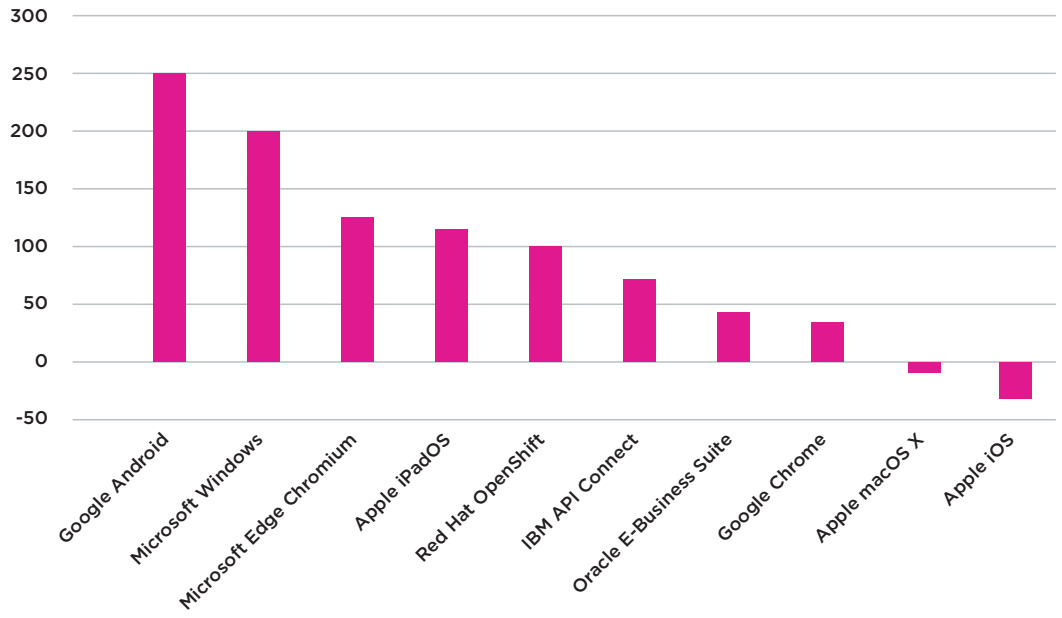

FIG 5 | Change in vulnerability counts of most vulnerable products January – June 2019 vs 2020 figures

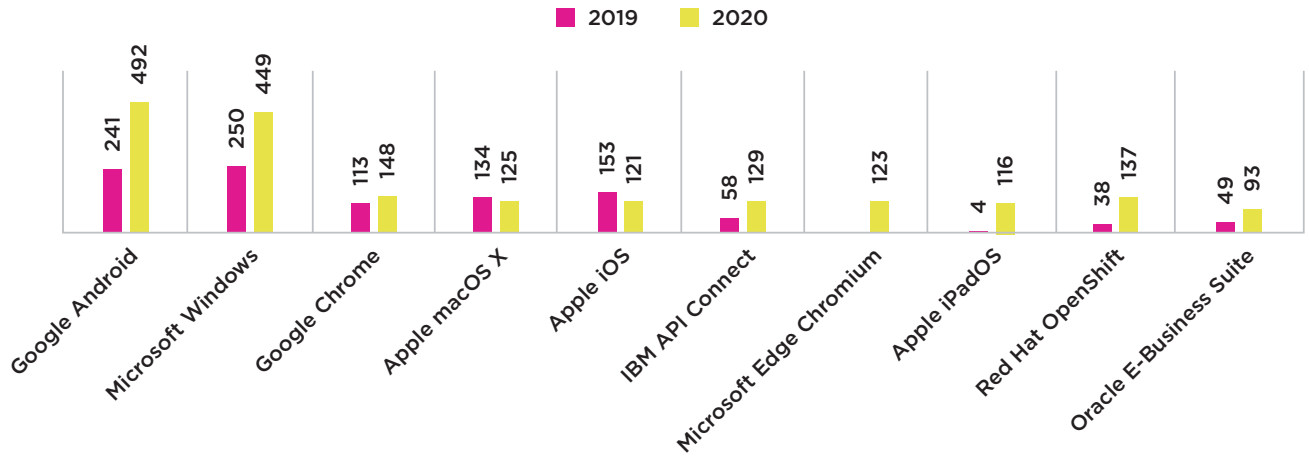

FIG 6 | New vulnerabilities for 2020's most vulnerable products

This list of most vulnerable products should not be misunderstood to be a list of products that are poorly designed and lack adequate security. The volume of vulnerabilities within each of these products is both a result of their ubiquity — the more well-known and widely used the product, the more third-party research into its flaws — and their transparency. Large vendors invest heavily in discovering their vulnerabilities to improve the security of their products. Many go a step further by offering bug bounties. That Android and Windows sit so far ahead of all other products should not be considered to be inherently negative.

Android's 104 percent increase in new vulnerability reports cements the position of most vulnerable product that it gained at the end of 2019. Its outpacing of previous category leader Microsoft can be seen as Android went from tailing Microsoft by 3.5 percent in the first six months of 2019 to outgrowing them by over 10 percent in 2020.

Microsoft has reported the second-largest growth so far this year, reporting a 80 percent increase in new vulnerabilities. The only products in the list that have reported fewer new vulnerabilities than they did over the same period last year are Apple iOS and macOS.

Of the five new products on the list, three are business apps (IBM API Connect, Red Hat OpenShift, Oracle E-Business Suite). The other two — Edge Chromium and iPadOS — are commonly deployed in workstation, domestic and commercial environments, emerging from nonexistence to become patch-hungry weak points that demand admin attention.

The rise of these products, and the increase of the vulnerabilities that exist within them, has come at a time when organizations have switched to working remotely en masse. The line separating personal and corporate environments has been blurred, with attackers now better able to take advantage of flaws within home networks to gain access to an organization's critical assets. Securing a widened network perimeter has become a strategic priority for most businesses; managing the crossover between personal and professional devices and ensuring that the vulnerabilities that sit within both cannot be exploited is now a prime concern.

Read more > How to Enforce Security in a Post-Pandemic World

Microsoft Inherits Vulnerabilities as it Moves to Edge Chromium

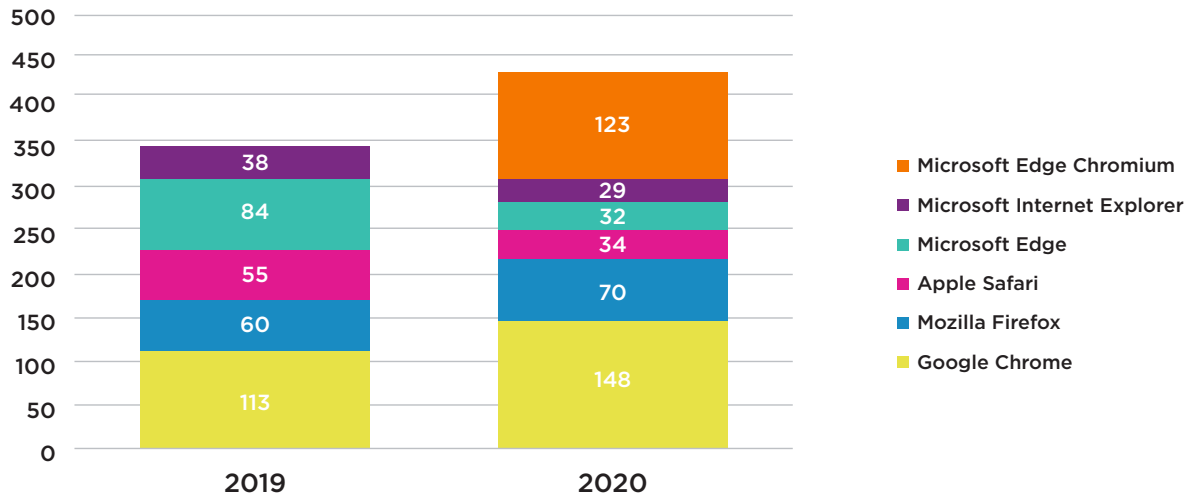

FIG 7 | Most vulnerable browsers

In January 2020, Microsoft infused the body of its Edge browser with Chrome's soul. This led to its new Edge Chromium browser inheriting some Chrome vulnerabilities; of its 123 flaws, the only one not inherited from Chrome is an Internet Explorer flaw (SBV-118612). This archaic vulnerability can still be exploited in Microsoft's new, improved, gutted and overhauled browser because it still retains an IE engine that can be invoked, if desired, within an optional emulation mode.

Excluding Microsoft Edge Chromium, Google Chrome was the only browser that saw its share of new vulnerabilities increase. With the exception of Mozilla Firefox, which saw a tiny rise in its vulnerability count, all other browsers saw a decrease in the number of new vulnerability reports.

Overall, Microsoft Edge Chromium's entry into the market has seen the total number of browser vulnerabilities jump to 436, compared to the 350 that were reported over the first six months of 2019.

THREATS AND MALWARE

New OT Advisories Increase

The total number of new advisories published by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has increased by 16 percent over the first six months of 2020 when compared to the same period in 2019. Siemens holds the greatest share of flaws, with many vulnerabilities still found in the Unix and Linux operating systems that underlie Siemens devices' firmware. The increase in new advisories should be welcomed as a sign that both ICS-CERT and Siemens are improving their reporting capabilities and are operating with greater transparency than previously possible: it was only in 2019 that ICS-CERT started publishing advisories for vulnerabilities that exist within subcomponents of third-party products.

The increase in new ICS-CERT advisories comes at a time when OT networks are ever-more exposed to IT infrastructures as well as being more directly connected with third-party vendor environments. On top of this, the nation-state threat to OT infrastructure is growing, with a handful of notable exploits already enacted so far this year.

Read more > Attackers Target Critical Infrastructure

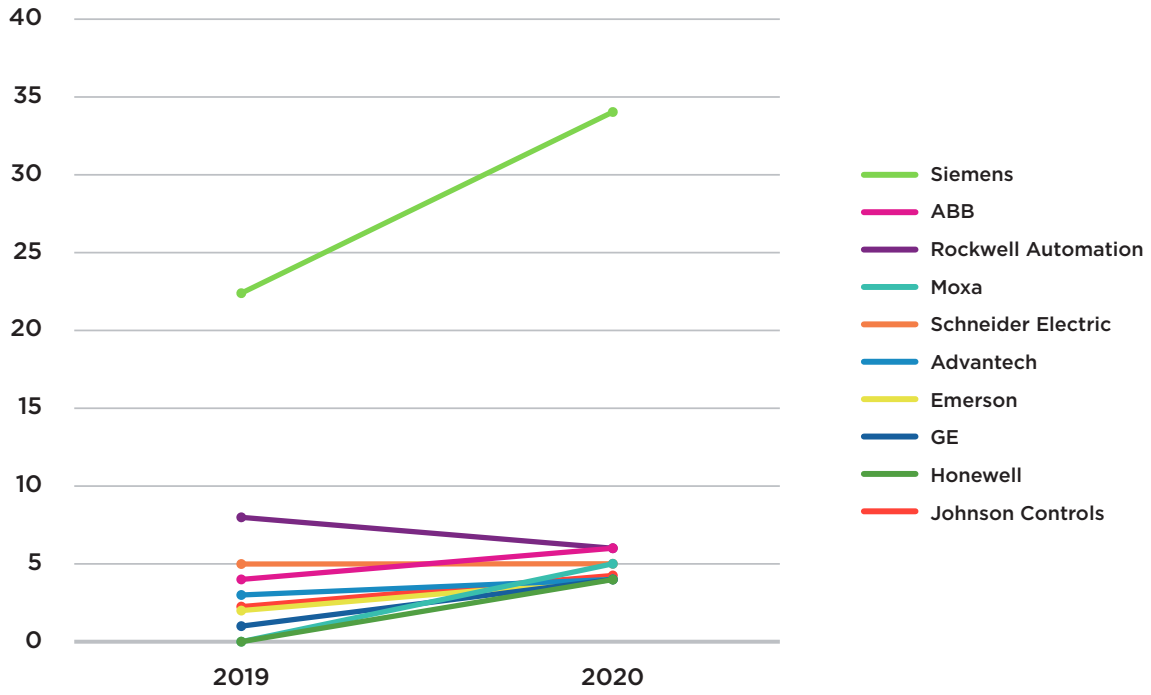

FIG 8 | ICS-CERT new advisories January – June

Creation of New Ransomware and Trojan Samples Soar During COVID-19 Crisis

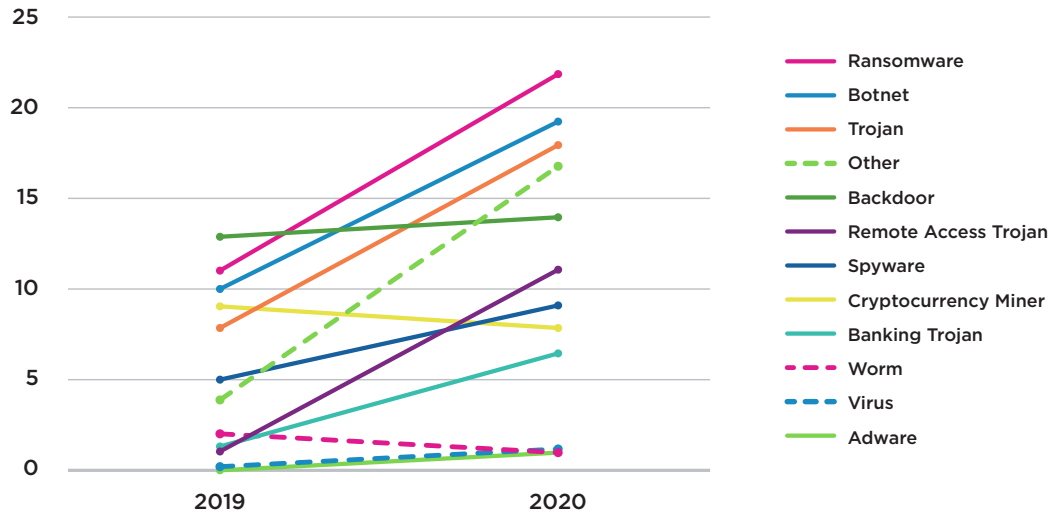

FIG 9 | New post-exploitation malware January – June

This chart tracks malware that has been delivered during or after the exploit of a vulnerability and has a few exclusions, which include malware delivered by phishing. Almost all malware types have seen an increase in new samples over the first six months of 2020, with cryptocurrency miners and worms being the only malware that have had fewer new samples created when compared to 2019.

Notable is the increase of new ransomware and trojans, with eleven more ransomware samples created than over the same period in 2019, and 27 more trojans (across banking trojans, trojans and remote access trojans).

Of all malware types, the one with the most transparent motivation is ransomware. Its effects tend to be immediate, as attackers place deadlines on their ransoms. But a ransomware module per se is usually the last piece to be delivered in a malware chain, with criminals outsourcing infiltration to other programs.

One example of this outsourcing activity is the well-known cooperation between Emotet and Ryuk, in which the former grants access to servers and data and the latter harvests the ransom. This could explain the parallel climbs of new malware modules in the trojan and botnet categories, both of which can serve as vehicles for the popular ransomware category.

Ransomware is increasing in usage because it is also increasing in sophistication. Sodinokibi, otherwise known as REvil, is one such example of well-engineered ransomware, having expanded along several vectors over 2020. Originally used as a standard phish-and-destroy tool, it has been actively used in ransomware attacks and campaigns since 2019, picking up Oracle (SBV-100938, et al.), VPN client (SBV-101038) and native Windows (SBV-91728) infection vectors along the way.

The particular growth path taken by Sodinokibi's developers should be seen as an example of the organizational prowess that attackers now possess. They have created ransomware that is profitable, adaptable, proven and scalable. They have the strategic nous of large enterprises paired with strong technical capabilities that enable them to achieve their goals. It is clear that organizations are not facing up to lone wolves anymore — they are having to stave off threats from well-coordinated criminals.

HOW COVID-19 HAS EMBOLDENED CRIMINAL USE OF RANSOMWARE

Threat actors trying to leverage chaos for their benefit is nothing new, and the COVID-19 pandemic is no different. As the pandemic was spreading across the globe, people everywhere were seeking information that would ease their sense of uncertainty, or even give them some hope of returning to normal life. Google searches related to the coronavirus peaked in the U.S. on March 15, according to Google Trends public data. Attempts for malicious attacks surged accordingly, although not in parallel, with 78 reported campaigns related to the pandemic observed between March 1 and June 30, 2020.

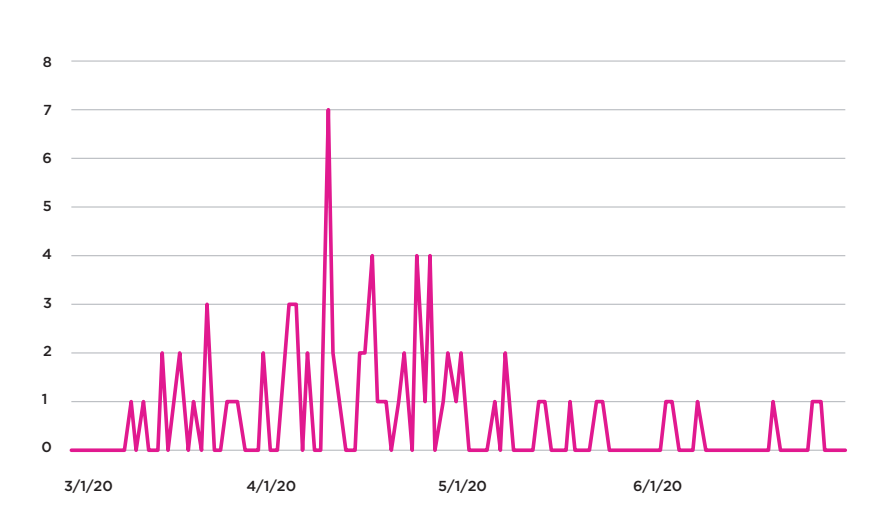

FIG 10 | Daily reports of COVID-19 malware campaigns

More than 60 percent of these reports were in April when governments ordered lockdowns in dozens of countries. This situation created fertile ground for ransomware attacks. Often camouflaging the ransomware as a courier of new information about the coronavirus, attackers tried to lure their victims into clicking a malicious link. In Italy, one of the most badly hit countries from COVID-19, attackers created a web page mimicking the Italian Federation of Pharmacists website to lure users into downloading ransomware disguised as a COVID-19 dashboard. Other ransomware targeted users of different popular applications such as Android OS and Microsoft Office.

Read more > Mitigating Risk of Ransomware

INSIGHTS

ATTACKERS TARGET CRITICAL INFRASTRUCTURE

While the world was busy fighting the COVID–19 pandemic, attackers have been thriving on the chaos of the crisis and have made their presence known with attacks on national infrastructure, pharmaceutical firms and health care entities.

Notable among the nation–state attacks on critical infrastructure was a cyberwar fought between Israel and Iran. After Iran attacked Israeli water facilities on the last weekend of April 2020, Israel fought back by bringing one of Iran's busiest seaports to an abrupt halt a week later. Normally, nation–state actors are not as open as Israeli and Iranian officials have been about these attacks — if this openness is replicated in future acts of cyber warfare, then we could see a reduction in traditionally subversive and secretive tactics and an increase in overt and well–publicized attacks.

While those attack motives likely precede the COVID–19 crisis, the pandemic has also emboldened criminals to disrupt pharmaceutical firms and health care companies. The need for these organizations to maintain operations has increased their threat profile: criminals have already successfully extorted $1.14m from the University of California San Francisco's medical research institution, forced the Brno University Hospital to shut down its entire IT network and hit ExecuPharm with a ransomware attack in March. While ExecuPharm is not playing a central role in the development of COVID–19 vaccines or treatment, the other two are, and targeting any part of the medical infrastructure at this time threatens the health and well–being of the entire general public.

One feature common in critical infrastructure — as diverse as water treatment, transport and pharmaceuticals — is their hybrid infrastructure that contains difficult–to–protect OT devices. To stave off increased threats, critical infrastructure entities need to develop holistic cybersecurity management strategies that cover the entirety of their estate. The reality, currently, is that most organizations are still a long way from being able to achieve this. IT and OT professionals have very different skillsets, work in different environments and are known to operate within rigid silos, making a hybrid security program a major challenge.

Dismantling these silos needs to happen through iterative change. The teams charged with operating and developing OT devices need to develop foundational knowledge that can be used to protect these notoriously difficult–to–patch network areas. Considering their training in electrical engineering, it is only natural that they may have an aversion to implementing IT–derived cybersecurity measures. Further, they may lack full awareness of the risks that exist within the internet–connected devices and third–party networks that are becoming increasingly interlinked with their OT devices.

Read more > How to Improve OT Security

MULTI-VENDOR VULNERABILITIES MAINTAIN A STRONG PRESENCE

The trend for vulnerabilities to have an extended reach and be able to impact a greater number of vendors is continuing throughout 2020. Considering how COVID–19 has disrupted security teams' day–to–day activities, gaining an understanding of these influential multi–vendor vulnerabilities needs to become a critical concern.

One such new vulnerability is a classic buffer overflow in peer-to-peer communication protocol implementation pppd. Responsibly disclosed in March, along with proof–of–concept exploit code (cf. SBV-113673), the flaw increases the likelihood that hackers will be able to slip in root code execution during an attack. This is because the function that they are taking advantage of is the kind of low–level process that tends to be run with very high privileges on a system, interacting with the kernel and its drivers. Check Point (SBV-118985), Cisco (SBV-114052) and Google (SBV-118073) were among the dozens of popular vendors issuing fixes for this issue.

Further, there have been several new influential vulnerabilities disclosed that sit within the Spectre family — these flaws are both new variations on the paradigm and resurrections of the exact problems brought back by code regressions in various software. Each new flaw reported garners less attention than the last (e.g., SBV-118886). This is because admins are learning to classify them as high–cost, low–payout and difficult–to–exploit bugs and because vendors have been effectively rolling out patches (e.g., SBV-118881). Despite this, it is still important to remain vigilant for further instances of influential Spectre vulnerabilities.

The existence of these vulnerabilities underscores the importance for organizations to gain full visibility of all vulnerabilities and assets within their environment. If they cannot track any of their vulnerabilities, they will not know which may need additional patching.

PUBLIC SECTOR FEARS INCREASE OVER LEGACY WINDOWS VULNERABILITIES

Microsoft terminated support for Windows 7 in January, now only offering organizations the option to pay for security updates for $50 per PC. It is estimated that around 200 million PCs still run older Windows versions, with Windows 7 making up the majority of this figure. Not all of these machines will be connected to corporate networks, but as the COVID–19 crisis has blurred the lines between personal and corporate environments, the threat that attackers could gain leverage through systems that either cannot be patched or are expensive to patch has increased.

At particular risk of criminals exploiting exposed vulnerabilities on old OSs are public sector organizations. In the U.K. alone, the National Cyber Security Centre (NCSC) found that at least 318 public sector networks still routinely use Windows XP despite Microsoft having pulled nearly all support for the operating system in 2014.

The reality is that upgrading systems to a new OS is rarely straightforward. In some industries, upgrading simply isn't viable. These are operating systems that are often used within critical OT devices (primarily in human–machine interface apps, in addition to other software which controls OT) and other relatively isolated workstations. Businesses cannot easily take these systems offline and, even when they can, they are notoriously difficult to upgrade. Within the public sector, budgetary limitations are also preventing organizations from implementing upgrades.

Despite these limitations, it is still critical for businesses to work out a way to protect their networks. By failing to address the security issues related to the termination of Microsoft's support, they are being left wide open to attack. There are many companies, for example, who have still to apply RDP patches — something that should be seen as critical following the significant number of RDP exploits that have taken place over the first half of the year.

The options that organizations have to mitigate risk on legacy OSs are limited. While some vulnerabilities have network–based mitigation alternatives to patching, like applying an IPS–based signature, this will not always be possible. Where upgrading is not an option for whatever reason, the need for vigilance and visibility is paramount. Organizations that are knowingly exposing themselves to threats need to reduce their risk profile by first identifying all ingress and egress points, modeling their network to determine all attack vectors, employing network segmentation and creating strict access controls.

Read More > Cybersecurity in Government, Osterman Research Paper

RECOMMENDATIONS

REMEDIATE THE RIGHT VULNERABILITIES

Strong remediation practices are going to be crucial if you are going to weather the current storm. You need to gain a full, unerring understanding of how exposed each of your vulnerabilities are to attack. To do this, you first need visibility — of vulnerabilities themselves, the assets they exist on and the surrounding network topology and security controls. All of these elements from within the organization as well as intelligence of the external threat landscape give context to a vulnerability and will inform remediation priorities.

By modeling the organizational environment in which a vulnerability occurrence exists, security teams can effectively understand the exposure of vulnerabilities to threat origins — a critical component of risk-based vulnerability prioritization. Analyzing exposure takes vulnerability prioritization out of the theoretical realm occupied by generic scoring systems like CVSS and places it in the real world, revealing which vulnerabilities are most likely to be used in an attack on your organization.

For example, if a security program bases vulnerability prioritization solely on CVSS scores, it could waste resources patching a vulnerable asset protected by layers upon layers of defense-in-depth security controls. At the same time, a medium-severity vulnerability may never be prioritized for patching, despite it being left exposed to a known threat origin. Considering the volume of vulnerabilities accumulating every year, risk-based strategies are going to be key to focusing action where it has the biggest impact on reducing the risk of attack.

To focus remediation efforts on this small subset of vulnerabilities, organizations need to better understand the context of their vulnerabilities within their infrastructure and the threat landscape. This includes having a firm grasp on several details regarding the vulnerability itself, as well as:

- Asset exposure to threat origins considering surrounding network topology and security controls
- Asset value and potential impact to the organization if compromised
- Exploit activity in the wild
- Exploit use in packaged crimeware (e.g., ransomware, exploit kits)
- Exploit availability and potential impact of the exploit

By analyzing the interconnections of the vulnerability and these elements, organizations can firmly tether remediation to risk reduction. It's a "quality over quantity" approach that may see vulnerability totals within an organization remain high but the likelihood of attack dramatically decrease.

Read More > Risk-Based Vulnerability Management

HOW TO ENFORCE SECURITY IN A POST-PANDEMIC WORLD

The chaos surrounding COVID-19 has forced seismic and unprecedented change upon businesses around the world, many of which now have to be concerned with securing a large, remote workforce. This has placed a great deal of pressure on security teams as they strive to manage new risks that have emerged from their expanded network perimeter.

This shift can have a large, short–term impact on over–stretched IT and security teams. One of the biggest risks that they have to manage concerns employees who generally do not work remotely and who need to access corporate resources remotely. If this risk is not properly mitigated, it could open the door to new viruses, malware or other digital interlopers due to their lack of secure home networks and other personal devices.

As the dust settles and we cautiously start to think about a post–pandemic age, organizations need to reassess their security strategies and posture. This report has highlighted the landscape that lies ahead for security teams — they will potentially have over 20,000 new vulnerabilities to sort through and will be contending with heightened threat levels — as they battle to avoid non-compliance and avoid attack during an era of great economic uncertainty.

To address these new vulnerabilities, you need to develop a clear roadmap. You need to access and analyze data to learn about how prepared they are to contend with increasingly sophisticated threat agents. .This roadmap needs to incorporate several critical capabilities:

- Having an infrastructure–wide view of all corporate assets wherever they reside
- Analyzing access and network paths to critical systems and between network segments
- Addressing critical–risk vulnerabilities on vital business assets, especially those that have exposures from external attack or less secure internal network segments
- Ensuring proper secure configuration of VPN, firewalls, security and networking device and all other ingress and egress points to critical assets

Gaining these capabilities will allow you to better support the necessary digital transformation initiatives that will have to be introduced to support your remote workforce.

MITIGATING RISK OF RANSOMWARE

The strategy behind detecting and mitigating a ransomware attack should be grounded in a holistic approach. You first need to investigate and identify all affected endpoints. When you suffer a ransomware attack, you need to assume that all credentials present on these endpoints are now available to attackers, whether the accounts associated with them were active during the attack or not. Using indicators of compromise (IOCs) alone to determine the impact of a ransomware attack will not be enough because threat actors are known to change their tools and systems once they can determine their victims' detection capabilities.

After initial identification has been conducted the following steps are necessary:

- Isolate affected devices as soon as possible by either removing the systems from the network or shutting them down to prevent further ransomware attacks throughout the network
- Isolate or power off affected devices that have yet to be fully corrupted to gain more time to clean and recover data
- Take backup data and devices offline immediately
- Secure any hijacked data that can be secured
- Change all account and network passwords — once the ransomware is removed from the system, you also need to change all system passwords

The best form of defense against ransomware attacks is to ensure that they never happen in the first place. This can be achieved by modeling your entire attack surface — including infrastructure, assets and vulnerabilities — to gain full and unerring visibility over your entire security environment, understanding the context that surrounds your critical assets and vulnerabilities, and establishing remediation strategies that empower you to target your most exposed flaws before criminals can exploit them.

HOW TO IMPROVE OT SECURITY

Operations teams should first look to introduce rule flows, take advantage of dynamic firewalls, improve control access and establish ways to mitigate risk that originates from connected third–party environments. Being in command of each of these areas will give them the confidence to embrace solutions that allow them to identify and mitigate all vulnerabilities within their environment without disrupting uptime.

Further, they need to increase the pace of their scans — many only perform one or two scans a year and then only on the devices that they can take offline. The ability to discover the vulnerabilities that exist within critical OT devices and technology needs to be a prime concern for operations teams.

Only when these core capabilities are achieved will organizations with hybrid IT–OT networks be able to holistically manage risk. At that stage, they 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

Read more > Hybrid IT-OT, A Unified Approach

CONCLUSION

With 20,000 new vulnerabilities likely to be reported in 2020, the pressure for security teams to understand, normalize and act on the data within their environment is increasing. The report has highlighted how attackers are honing their focus on organizations with large, hybrid environments. The opportunity presented to them by the emergence of a mass, remote workforce has proven irresistible; the ransomware that they are developing profitable; and exposed critical infrastructure too alluring for them to pass up. The time for organizations to improve security and stop emboldened attackers in their tracks is now.

To navigate the significant challenges thrown up by the pandemic, the CISO needs to cut through the complexity inherent to their job. The first step to creating simpler and more efficient security programs is having a firm grasp of both internal and external threat context. This report has laid out the current state of play for external threats. To understand internal threat context, you need to correlate vast and varied intelligence sources from within your infrastructure. It is only then that you will have a security program robust enough to carry you through into a post-COVID world.

ABOUT SKYBOX SECURITY

At Skybox Security, we provide you with cybersecurity management solutions to help your business innovate rapidly and with confidence. 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