TREND MICRO | research

Securing the Pandemic-Disrupted Workplace

Trend Micro 2020 Midyear Cybersecurity Report

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

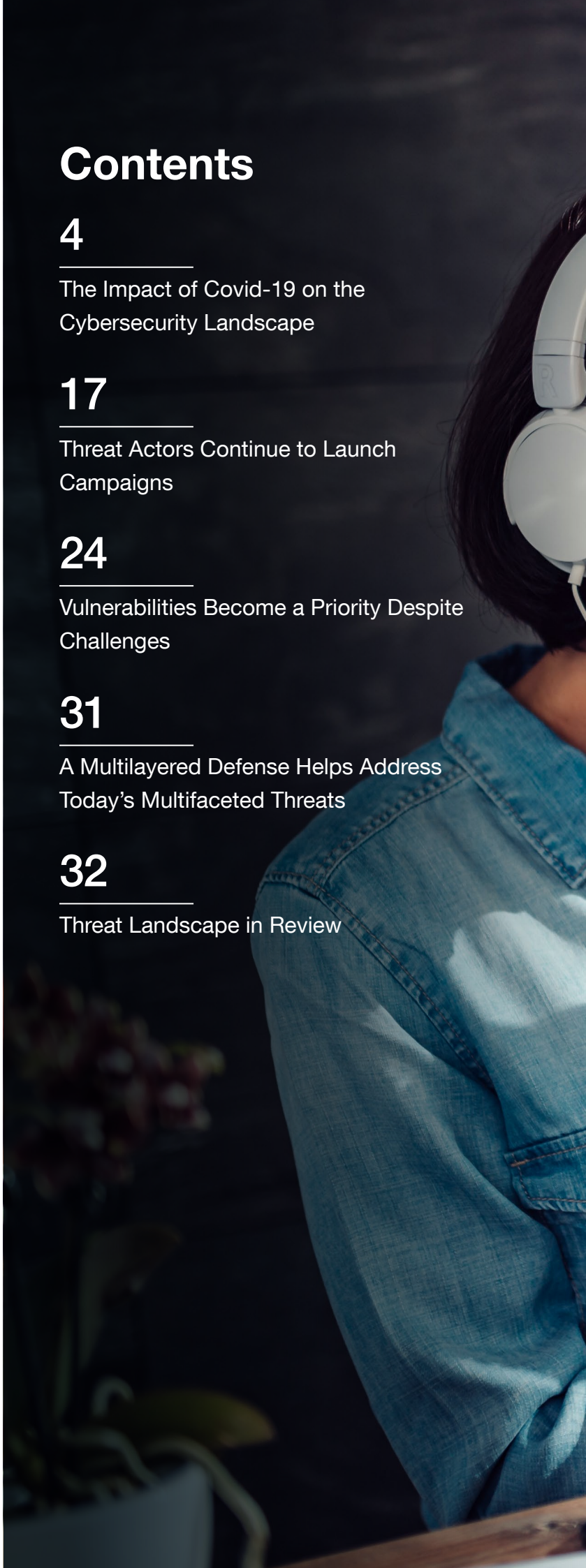
Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Published by
Trend Micro Research

Stock image used under license from
Shutterstock.com

For Raimund Genes (1963-2017)

Contents



In the Trend Micro Security Predictions report for 2020, we tried to predict the changes that would shape the cybersecurity industry as we entered a new decade. What we could not have anticipated was how the "new normal" — which would arise due to the Covid-19 pandemic — would affect the way we interact with the world.

For many people, working from home became not just an option, but a necessity as the pandemic forced organizations around the world to reconsider how and where they work. Unfortunately, the speed and urgency of the changes caught many businesses unprepared, leading to security gaps in both the home and the physical workplace.

Malicious actors took advantage of the situation by launching a slew of Covid-19-themed attacks using a diverse array of lures across a wide range of platforms, including emails, social media, malicious websites, and fake mobile apps. Video conferencing apps became a favorite target for cybercriminals as the need for effective communication led to increased usage. These attacks ranged from pranks such as Zoombombing to full-fledged campaigns involving malware bundled with app installers.

Threat actor groups relentlessly continued their campaigns. Some groups chose to expand their operations to new platforms and operating systems, while others built campaigns around seemingly outdated techniques or made use of malware types often thought to be harmless.

Ransomware continued to be highly targeted in nature, with one high-profile group deciding to drop its public operations to concentrate on private campaigns. Some ransomware operators have also threatened to expose the data they stole from their victims to the public.

Microsoft ended its support for Windows 7 early in the year, while at the same time devoted more resources to fixing vulnerabilities. The company patched a record number of bugs in the first half of 2020, which also included a number of significant vulnerabilities such as CurveBall.

Several industrial internet of things (IIoT) vulnerabilities that exist in decades-old third-party software components proved that there is a lack of standardization and safe coding guidelines when it comes to IIoT systems. Due to the large number and interconnectedness of the potentially impacted devices, it will be difficult to determine the impact of these bugs for the foreseeable future.

2020 has proven in many ways that the cybersecurity industry does not exist in a static bubble, but shifts and changes in accordance with and in response to the events of the world around it. In a year that has dramatically impacted most of our lives, we take a look at the most significant stories and trends to determine what has changed and what we can expect from the new normal.

The Impact of Covid-19 on the Cybersecurity Landscape

Covid-19-Themed Attacks Are on the Rise

From January to June 2020, the Trend Micro Smart Protection Network (SPN) detected nearly 9 million Covid-19-related threats. These threats consisted of emails, URLs, and malicious files that reference the pandemic either directly (for example, an app claiming to provide information on Covid-19) or indirectly (such as delays in providing services due to the virus). Thirty eight percent of such threats originated from the United States, followed by Germany (14.6%) and France (9.2%). The bulk of the detections occurred in April, aligning with the peak of Covid-19 infections in many countries — especially in Europe.

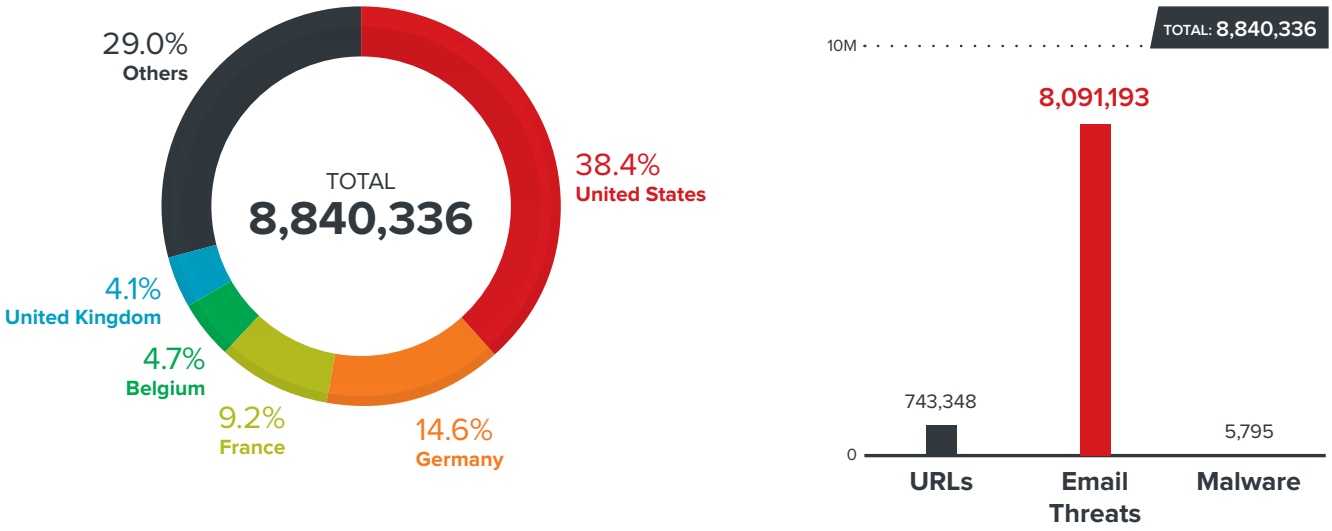


Figure 1. The number and distribution of Covid-19 threats in the first half of 2020

Source: Trend Micro Smart Protection Network infrastructure

The widespread impact of the pandemic led many people to try and find as much information as they could on Covid-19. Malicious actors capitalized on the situation, using schemes designed to take advantage of people's fears and anxieties.

Threat actors used a variety of lures. We compiled several Covid-19-related threats on a single page to provide the public with a summary of the tools and techniques used by cybercriminals.[1] Email threats, which made up 91.5% of all Covid-19 related threats, was the most commonly used entry point.

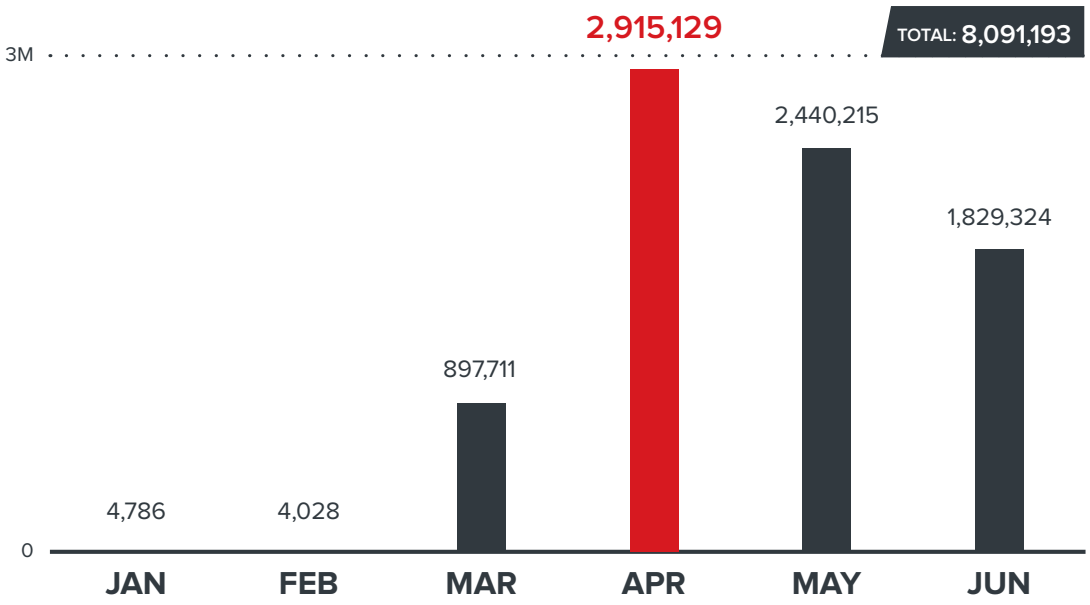


Figure 2. The monthly count for Covid-19-related email threats in the first half of 2020

Note: The data refers to Covid-19-related email threats detections

Source: Trend Micro Smart Protection Network infrastructure

We found email samples that claimed to provide the latest news and updates on the virus but instead delivered malware to its recipients. We also observed another scheme wherein malicious actors presented themselves as health organizations. A cryptocurrency wallet was then provided to the email recipients for donations.

Some spam messages did not directly reference Covid-19 but instead notified the recipient of shipping delays due to government restrictions resulting from the pandemic. While this is not a new gimmick for scammers, the use of Covid-19 to explain the said delays makes it both timely and believable. The message included attachments that showed a new shipping schedule but contained malware.

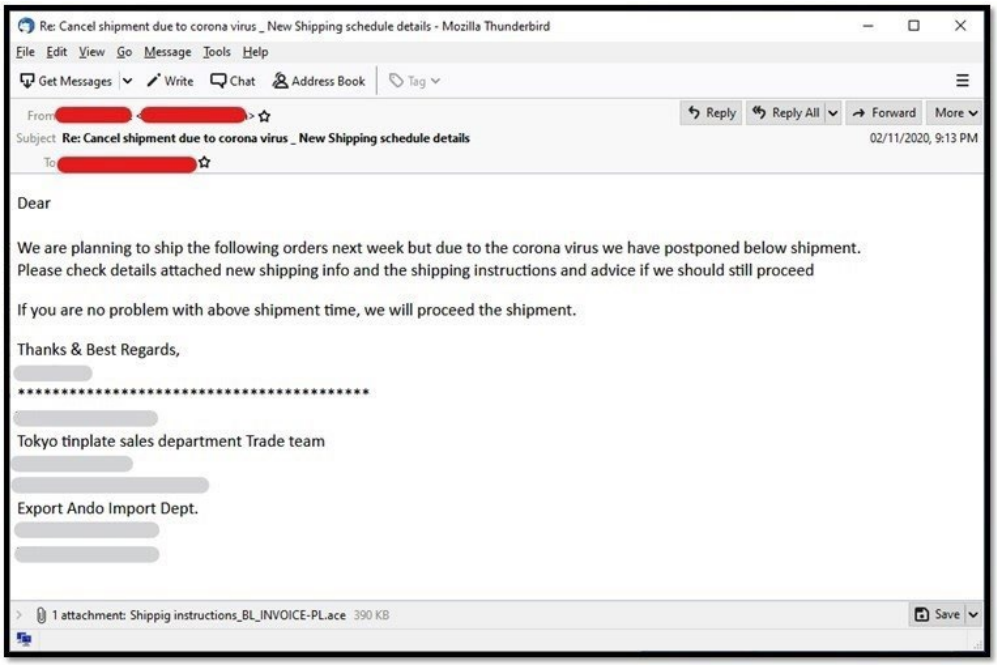


Figure 3. An email with a malicious attachment notifying the recipient of shipping delays

An overwhelming majority (93.5%) of the email threats we detected contained both a malicious file attachment and a malicious link. Surprisingly, detections for email threats with neither URLs nor attachments were higher than those that only had one or the other, indicating that malicious actors tended to use both links and attachments in their campaigns.

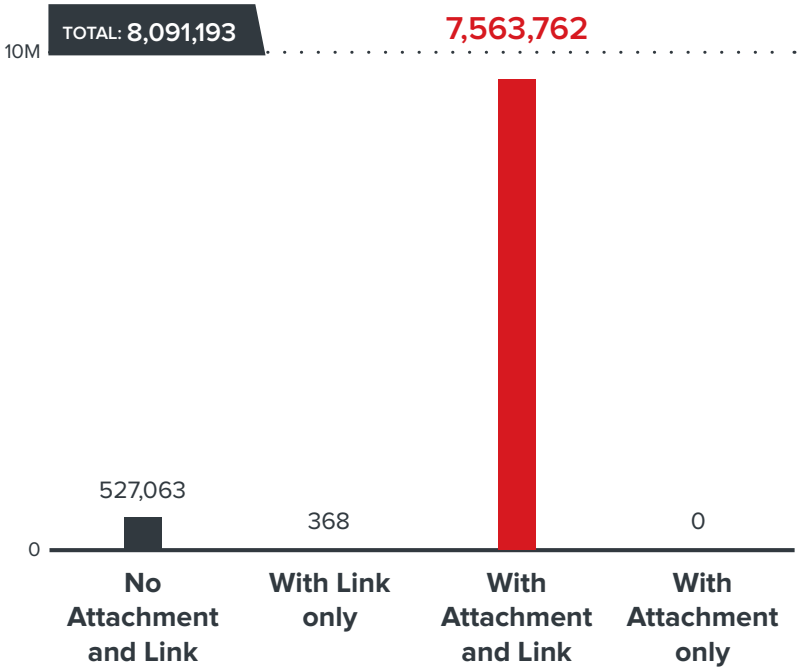


Figure 4. Distribution of Covid-19 related email threats detections based on whether they contained attachments and/or links.

Source: Trend Micro Smart Protection Network infrastructure

Scammers also used business email compromise (BEC) schemes using Covid-19-related topics as a hook. The effectiveness of these scams was likely bolstered by the fact that new remote work arrangements made it more difficult to keep track of communication between members of an organization.

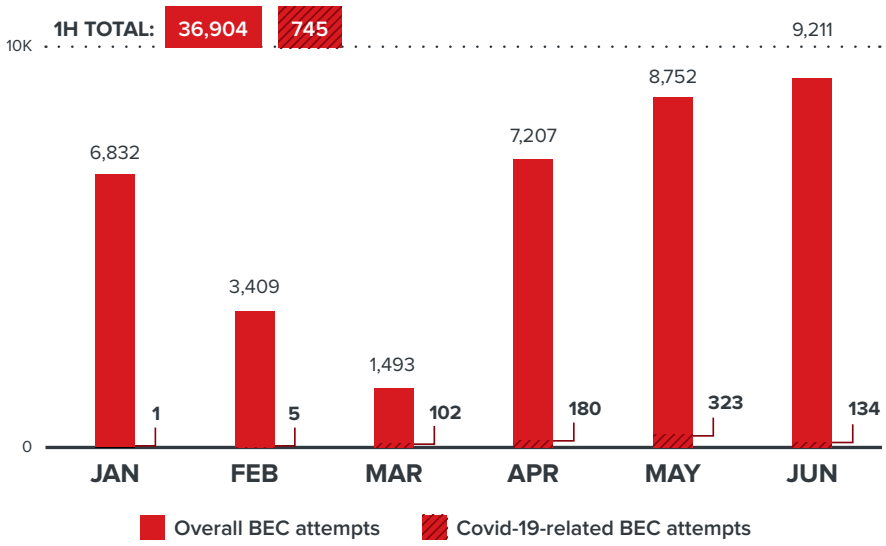


Figure 5. The number of Covid-19 BEC attempts compared with regular BEC attempts in the first half of 2020. Covid-19-related BEC attempts peaked in May.

Note: The data refers to the number of BEC attempts seen, which does not indicate whether the attacks were successful.

In one such case, researchers from Agari investigated a BEC campaign[2] that was being run by Ancient Tortoise, a threat actor group that uses aging (accounts receivable) report scams as part of its operation. In its newest scheme, the group sends emails to potential victims notifying them of a change in banks due to the pandemic — with the new "bank" being a mule account in Hong Kong.

The number of times users tried to access malicious Covid-19-related URLs grew as the year progressed, reaching its peak in April, while May and June saw sustained activity.

	Overall	Covid-19
January	94,488,577	3,916
February	100,468,874	9,497
March	111,026,602	34,197
April	224,187,318	348,767
May	252,588,246	168,576
June	146,542,789	178,395
Total	**929,302,406**	**743,348**

Table 1. The monthly count for Covid-19-related malicious URLs, compared with the overall count of malicious URLs in the first half of 2020

Note: The data refers to access of malicious Covid-19-related URLs that Web Reputation Services (WRS) detected.

Source: Trend Micro Smart Protection Network infrastructure

Many of these URLs were used for phishing scams. We detected the most attempts to visit Covid-19-themed phishing sites in April. Subsequently, a significant number of users who visited these websites were in some way affected by the scams.

	Overall	Covid-19
January	14,242,471	30
February	13,171,718	6,472
March	14,463,726	15,788
April	13,606,957	25,466
May	38,075,937	16,894
June	8,751,480	15,936

Table 2. The number of detected non-unique attempts to visit Covid-19 phishing websites, compared with the overall number of detected non-unique attempts to visit phishing websites in the first half of 2020

Note: Three instances of blocked access to the same URL is counted as three non-unique attempts

Source: Trend Micro Smart Protection Network infrastructure

	Overall	Covid-19
January	763,989	6
February	889,044	536
March	1,361,173	4,457
April	1,540,928	4,678
May	1,369,883	2,841
June	894,443	1,718

Table 3. The number of unique users affected by Covid-19 phishing websites, compared with the overall number of unique users affected by phishing websites in the first half of 2020

Note: One machine that attempted to access the same URL three times is counted as one unique user

Source: Trend Micro Smart Protection Network infrastructure

A couple of these sites promoted apps that allegedly protected its users from Covid-19. However, what these apps actually did was infect its users with a virtual malady: BlackNET RAT. This tool adds the machines it infects to a botnet that malicious actors can use to launch distributed denial-of-service (DDoS) attacks, upload files, execute scripts, and collect information, among others.[3]

Some malicious actors went for a more direct approach, skipping the use of malware and instead directly asking potential victims for their credit card information, as we saw in one website that was peddling non-existent World Health Organization (WHO)-approved vaccine kits for a "low price" of US$4.95.

Another website spoofed a UK government page to trick unsuspecting users into giving away their personal information and bank account credentials by promising some form of aid or relief. A closer look at the said website reveals a glaring error in the use of the word "relieve" — an instant giveaway that the page is not legitimate.

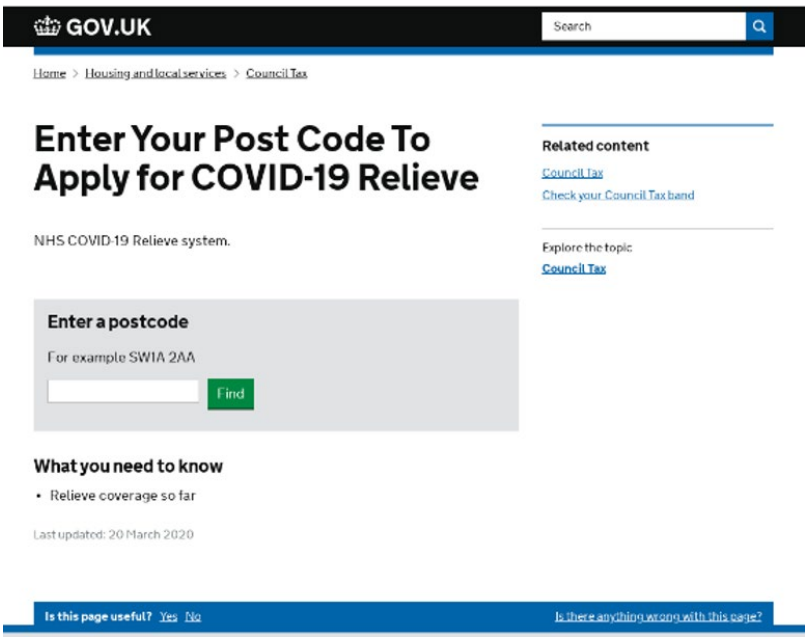


Figure 6. A fake government website designed to collect personal information and bank credentials. Note the wrong use of the word "relieve."

In other instances, attackers sent messages to potential victims through social media apps. One type of phishing scam we came across involved offers of free Netflix subscriptions to lure victims into clicking on a malicious link. Users would then either be redirected to a fake Netflix page designed to capture their login credentials or to a bogus survey that deceives respondents into sharing fraudulent links to their friends and social media groups.

We saw the introduction of several malicious Covid-19-related mobile apps during the first half of 2020. In April, we uncovered an app that, at first glance, seemed to provide updates on the virus.[4] However, the app's true purpose is to gather files and information from infected phones, such as messages from messaging apps, call logs, contact lists, photos, and device and system information.

Figure 7. A malicious mobile app that offers users "ways to get rid of coronavirus."

The use of Covid-19-themed traps to deliver malware was also common. May saw the appearance of a trojan called QNodeService that could download, upload, and execute files; steal credentials from Chrome and Firefox browsers; as well as perform file management.[5] The trojan was deployed by a downloader attached to a phishing email. The email was disguised as a tax relief notification that was being provided due to Covid-19. The use of "tax relief" was particularly devious: the US Internal Revenue Service had previously announced a Covid-19 tax relief program and the extension of the tax filing and payment deadline,[6] making the phishing email's subject matter very relevant to its recipients.

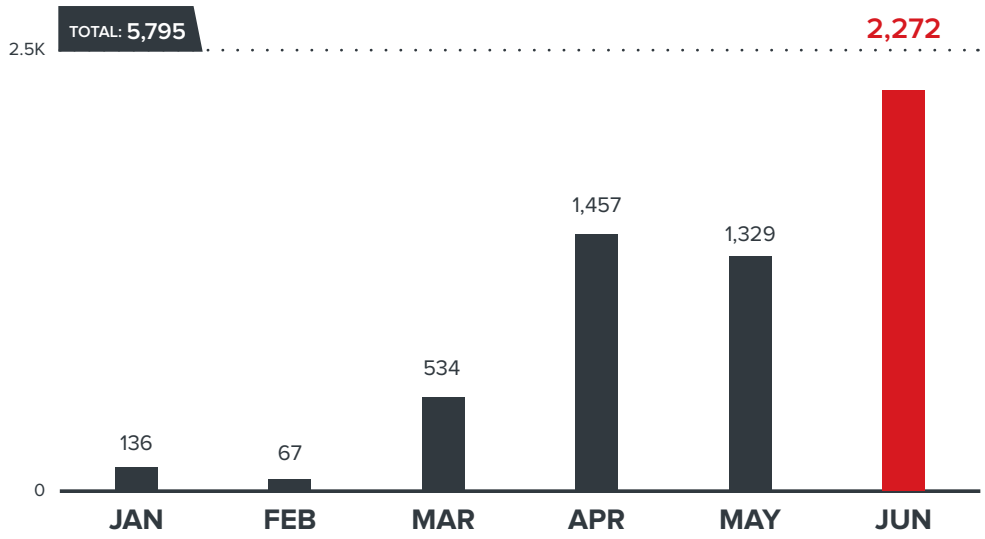


Figure 8. The monthly count for Covid-19-related malware detections in the first half of 2020

Source: Trend Micro Smart Protection Network infrastructure

Many themed tools and malware variants were being peddled in the underground by unscrupulous elements. By trawling forums catering to malicious online activities, we discovered multiple listings for Covid-19-related phishing exploits and malware.

Individual malicious actors were not the only ones interested in exploiting the pandemic: Advanced persistent threat (APT) groups also took advantage by launching their own Covid-19 campaigns. A notable example of this was a campaign that was seemingly enacted by Gamaredon, a threat actor group that has been active since 2013 and has been known for targeting the government of Ukraine.[7] Similar to other Covid-19 schemes, the threat actor behind the March 2020 campaign used emails containing a DOCX attachment that referenced the virus on the subject line. Clicking on the attachment would launch several malicious routines, eventually culminating in malicious macro codes executing a VBScript (VBS) and several additional payloads.

The activities of malicious actors during the first half of the year show that they are not above capitalizing on major events — especially something as impactful as a global pandemic. As the situation evolves during the second part of 2020, it will not come as a surprise to see attackers change their tactics to keep in step.

Businesses Start Adjusting to the New Normal

In the wake of Covid-19, organizations experienced major disruptions to the way they did business. Many companies were forced to shift to remote work setups to protect their employees from the fast-spreading pandemic.

Migrating the workforce from the physical workplace to the home can be a complicated task. Not only do organizations have to supply their workers with the proper tools to do their jobs properly, but they also have to guarantee that the flow of operations still happens as seamlessly — and as securely — as possible.

One aspect of remote work setups that organizations could potentially have to deal with is the issue of connectivity. In a chat with cybersecurity industry veteran and CEO of Liggett Consulting Mark Liggett,[8] he pointed out that businesses will have to provide their employees with a quick and efficient method to connect to their office systems. They will also have to deal with users moving from tightly controlled office networks to home networks, where the speed and quality of connections might not be up to par.

Unlike in an office setting, people working from home will often have their personal and private lives intermingling, therefore presenting a challenge for employers to try and strike a balance between security, productivity, and privacy. For example, some organizations have turned to using tracking tools to help them keep tabs on employee activities.[9] While these can help in the short term, they can also intrude too much into a person's private life, which could cause stress and discomfort. Businesses will have to discuss WFH arrangements with their employees, including setting boundaries between work and home, to minimize the need for these kinds of tools.[10]

Some companies already have systems in place that allow workers to transition to remote work arrangements with only minor issues. According to Ian Keller, chief security officer (CSO) of SBV Services, an end-to-end cash management services company based in South Africa, his company had already started enhancing their systems as part of its digitization strategy before the pandemic. This involved applying measures such as having an adequate number of VPNs and the implementation of proper security technology.[11]

Separating work from personal life can prove to be a challenge for remote workers. From a security standpoint, end users are the most important factor when it comes to a successful work-from-home setup. Security is easier to manage in the physical workplace since IT personnel have access to an office's physical endpoints. In a remote working environment, these same security teams will have to rely not only on their security tools and technologies but also on endpoint users operating their personal and work machines responsibly.

The need for effective cybersecurity became an especially important issue as more people work from home.[12] According to the Federal Bureau of Investigation (FBI), there has been a sharp increase in cybercrime reports since the start of the pandemic. FBI Deputy Assistant Director Tonya Ugoretz mentioned that the Internet Crime Complaint Center (IC3) had been receiving 3,000 to 4,000 cybersecurity-related complaints a day — a significant increase from the previous daily average of 1,000 reports.[13]

With the internet acting as the home-based employee's primary gateway to the workplace, inbound attacks on devices and routers saw an increase from the second half of 2019.

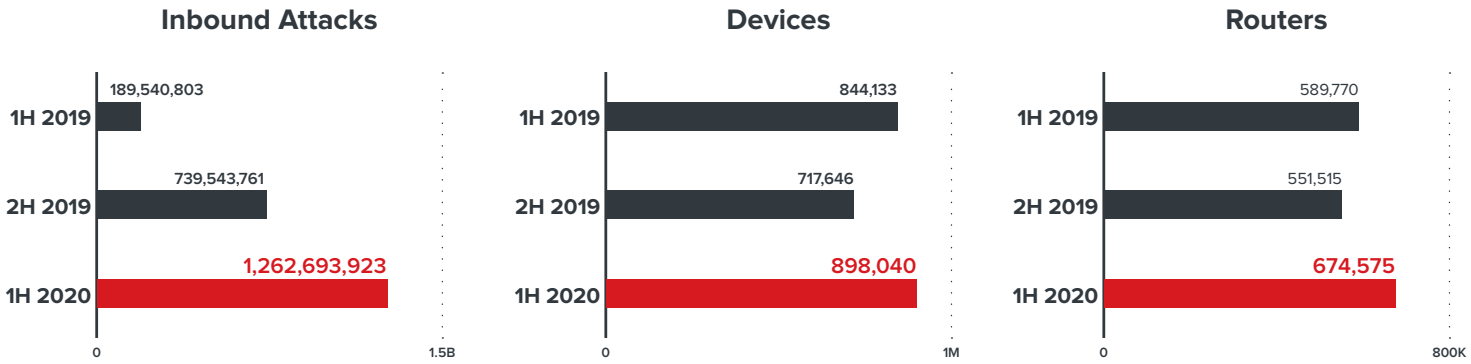


Figure 9. There was a significant increase in inbound attacks as well as attacks on devices and routers in the first half of 2020.

Note: Events were when rules were triggered for activities or behaviors from malicious, gray, and potentially unwanted applications, and were indicators that an attack might happen. Possible attacks were events closely related to threat activity.

Source: Trend Micro Smart Home Network solution

Malicious actors stepped up their attacks on user accounts that were used for remote access services: Brute force login attempts made up the overwhelming majority of all inbound attacks, at almost 89% of the total.

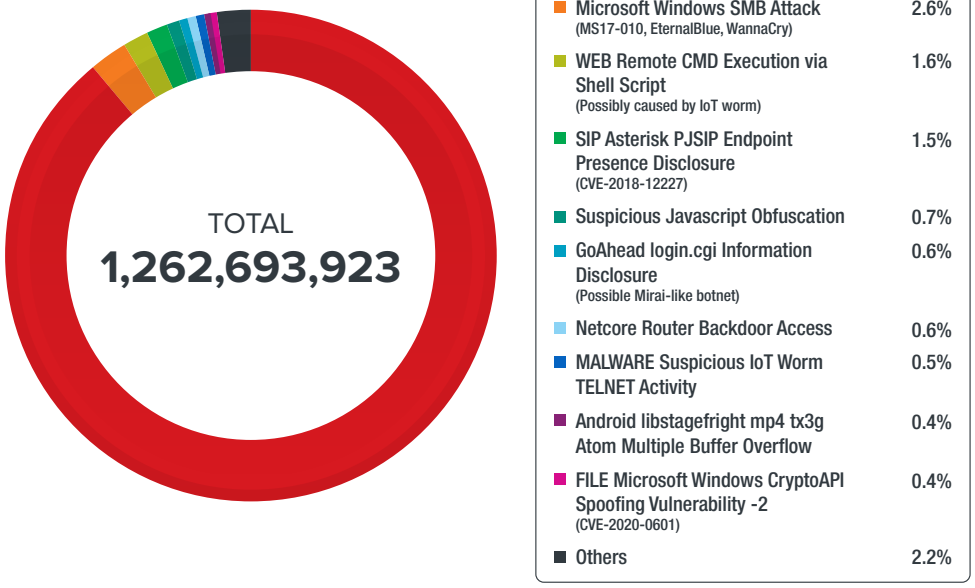


Figure 10. The distribution of top inbound attacks, based on Trend Micro Smart Home Network (SHN) data in the first half of 2020. Brute force logins were by far the most common type of inbound attack.

Note: Events were when rules were triggered for activities or behaviors from malicious, gray, and potentially unwanted applications, and were indicators that an attack might happen. Possible attacks were events closely related to threat activity.

Source: Trend Micro Smart Home Network solution

The exploitation of Microsoft Server Message Block (SMB) vulnerabilities accounted for approximately 40% of all outbound attacks, while brute force login attacks followed closely behind at 39%. In light of the current situation, malicious actors have been increasingly targeting home networks, using them as launch points for further attacks.

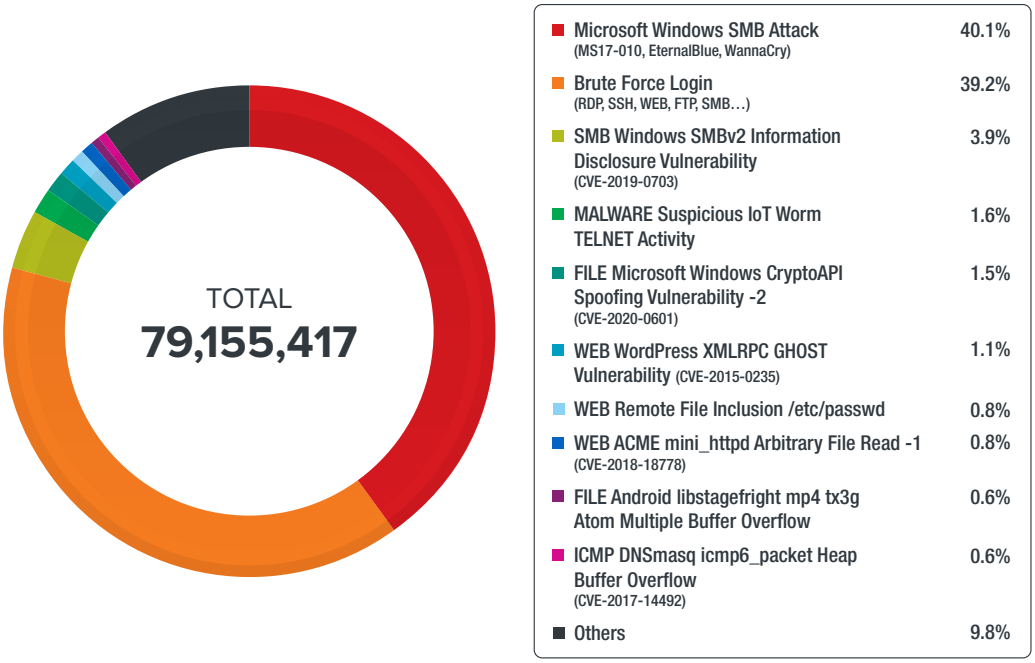


Figure 11. The distribution of top outbound attacks, based on Trend Micro Smart Home Network (SHN) data in the first half of 2020. Microsoft Windows SMB Attack accounted for approximately 40% of all outbound attacks.

Note: Events were when rules were triggered for activities or behaviors from malicious, gray, and potentially unwanted applications, and were indicators that an attack might happen. Possible attacks were events closely related to threat activity.

Source: Trend Micro Smart Home Network solution

The number of potential worm or IoT botnet attacks also increased. The quarterly trend for WEB Remote CMD Exec via Shell Script attacks, which signify the detection of malicious scripts that allow the downloading and execution of worms inside the system, revealed significantly increased activity in the second quarter of 2020. We also saw a similar trend for Suspicious IoT Worm Telnet Activity events, which is the detection of activities involving remote worm code execution.

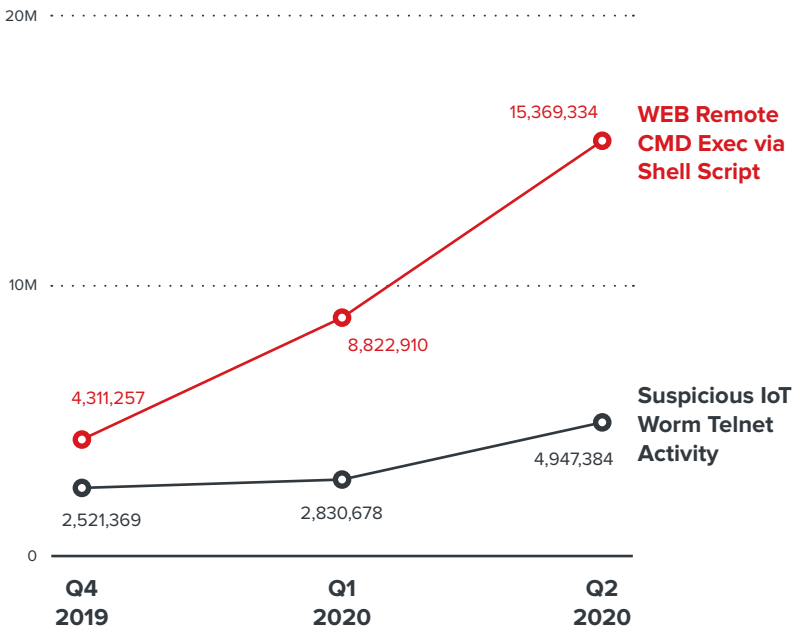


Figure 12. Event data from Trend Micro Smart Home Network (SHN) indicate an increase in potential IoT botnet and worm attacks

Note: Events were when rules were triggered for activities or behaviors from malicious, gray, and potentially unwanted applications, and were indicators that an attack might happen. Possible attacks were events closely related to threat activity.

Source: Trend Micro Smart Home Network solution

Zoombombing and Other Threats to Video Conferencing Apps Have Emerged

The need for constant communication has led to a dramatic increase in the use of video conferencing platforms such as Zoom, Cisco Webex, and Microsoft Skype.[14] Unfortunately, tricksters seem to have taken notice as they have been using a new form of disruptive intrusion for video chats and meetings. Colloquially known as Zoombombing due to the popularity of the Zoom app where it is often used, the prank involves outsiders entering private calls and meetings and performing disruptive acts such as sending obscene and offensive material, or even malware, to the meeting attendees.[15] Zoom has since implemented updates to their app that includes encryption and privacy control settings to minimize these kinds of antics.[16]

Beyond Zoombombing, malicious actors have also been busy registering domains related to video conferencing apps that are likely used for phishing activities, as discovered by Check Point Research.[17] The researchers also found malicious files referencing Zoom that led to the installation of InstallCore, which is a tool often used to install malware.

We found examples of malware families packaged together with Zoom installers. In April, we discovered the AutoIT compiled malware Trojan.Win32.MOOZ.THCCABO bundled with a legitimate Zoom installer, which we assumed came from fraudulent sites since it did not originate from Zoom's official download center.[18] Once downloaded into the system, the malware variant drops several files, including a cryptocurrency miner.

Later that month, we encountered a second example of a malicious app bundled with a legitimate installer. In this case, the sample included the monitoring tool known as RevCode WebMonitor RAT.[19] Similar to the previous malware, the files were obtained from a malicious source instead of the legitimate one.

Malicious actors did not limit themselves to bundling malware with legitimate Zoom installers. We also found malware files disguised as Zoom installers. One sample we analyzed drops a backdoor that allows users to execute remote commands. The malware variant runs a legitimate version of Zoom to avoid suspicion. We also found a fake installer that hid the Devil Shadow botnet. Once installed, it sends the information it gathers, including screenshots of the user's desktop and active windows, to its command and control (C&C) server. Like the first sample, it will install a legitimate Zoom executable.[20]

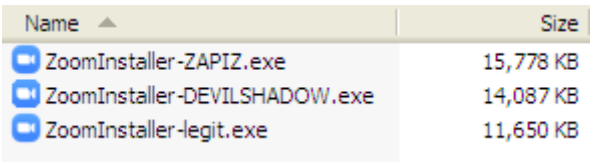


Figure 13. A comparison of file sizes between the legitimate Zoom installer and the fake ones carrying malware

Given that most of the Zoom-based malware — either bundled with legitimate installers or disguised as a fake app — come from malicious sources, it would behoove users to download their apps from the official Zoom download center to avoid potential complications.[21]

Threat Actors Continue to Launch Campaigns

Targeted Attacks Expand to New Platforms

While incidents and stories related to Covid-19 garnered the lion's share of attention so far in the year, threat actors have not let up on their attacks: Several noteworthy campaigns took place in the first half of 2020. We saw some threat actor groups using evolved techniques, while others expanded their presence to new platforms.

The Lazarus group, one of the most prominent threat actors, has been active since 2007 when they first launched a series of attacks against the South Korean government with the goal of disruption and sabotage.[22] The threat actor group has since been linked to several high-profile campaigns, including the infamous WannaCry ransomware attacks of 2017.[23]

We have observed Lazarus focusing on Apple-based platforms over the last few months. In November 2019, the group targeted Korean users via a MacOS backdoor hidden in a macro-embedded Microsoft Excel worksheet.[24] It then initiated a second campaign directed at Mac users in early 2020.[25]

This more recent campaign saw the attackers make use of what seemed to be a one-time password (OTP) tool called TinkaOTP that, on the surface, appears like a normal authentication tool. However, a closer look at the application sample revealed a remote access trojan (RAT) called DacIs, which Lazarus used in previous campaigns against Windows and Linux machines,[26] embedded in the tool. Moreover, the strings its C&C server uses to communicate with storage samples reveal further connections to Lazarus.

In addition to Lazarus, we also analyzed the operations of a couple of new groups. DRBControl,[27] one of the new groups we discovered with the help of Talent-Jump Technologies, Inc., was found targeting gambling and betting companies in South East Asia.

For its intrusion vector, DRBControl used three different versions of malicious DOCX files attached to spear-phishing emails that were sent to the target's support staff. It employed two previously unknown backdoors, both of which use a DDL sideloading technique via MSMpEng.exe, as well as several other malware families and post-exploitation tools as part of its routines. One notable aspect of the campaign is its use of the Dropbox API for both its C&C channel and as a delivery tool for various payloads. We also found similarities between DRBControl and other threat actors such as Winnti and Emissary Panda/LuckyMouse/APT 27 — particularly in the malware and other tools they used.

We also found a new group, which we dubbed Earth Empusa, that had set their sights on Uyghur-connected individuals in Tibet, Turkey, and Taiwan. The group was found compromising their targets' Android devices with a spyware called ActionSpy, which was delivered via phishing websites. The malware collects basic device information while also carrying out any commands sent by its C&C server. Earth Empusa also targeted iOS users by using watering hole attacks to inject malicious frameworks designed to steal information or exploit existing iOS vulnerabilities.

The strategies that these groups employed were not limited to the use of complex online infrastructure. Tropic Trooper, a threat actor group that has been active in Asia since 2011, uses a malware variant called USBferry that propagates via removable USB devices to gain a foothold into air-gapped systems, in particular, the physically isolated networks of the Taiwanese and Philippine militaries. Although the use of USBferry is not new — the first documented use of the malware variant occurred in 2014 — Tropic Trooper continues to use what is seemingly an old and outdated technique to infiltrate even the most protected systems.

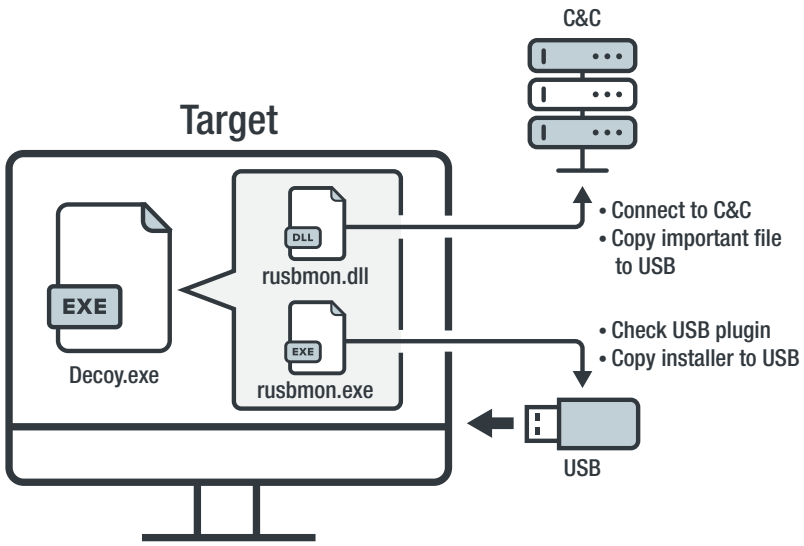


Figure 14. A sample attack scenario that involves the use of the USBFerry malware

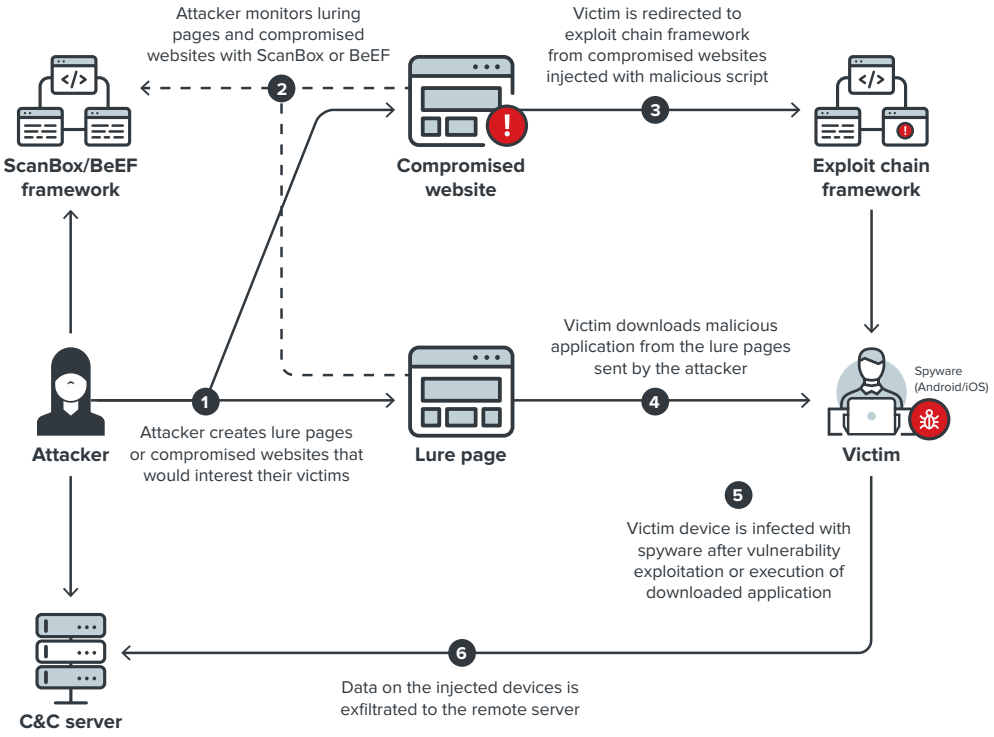


Figure 15. Infection chain used by Earth Empusa

Looking beyond the campaigns of named threat actor groups, we also saw the use of seemingly mundane malware types such as adware still being effective even in 2020. Earlier in the year, the Trend Micro Managed XDR team investigated an incident involving modular adware that was used to infect customer machines.[28] However, the surface simplicity of the adware — DealPly and ManageX — hid layers of complexity found in their installation and obfuscation techniques. Furthermore, the seemingly harmless nature of adware makes it difficult to correlate them to more dangerous threats.

Ransomware Operators Threatening to Expose Stolen User Data

The Trend Micro Security Predictions for 2020[29] forecasted that critical public infrastructure and government IT systems would be a primary focus for extortionists — with ransomware being their preferred weapon of choice. True enough, government-related organizations and businesses were the most highly targeted industry for ransomware operators, continuing the trend we observed in 2019.[30] Along with healthcare and manufacturing (the second and third most targeted industries, respectively), the top three logged a significantly larger number of attack attempts compared with the other industries. Other sectors that showed a relatively high number of attack attempts included finance, education, technology, oil & gas, insurance, and banking.

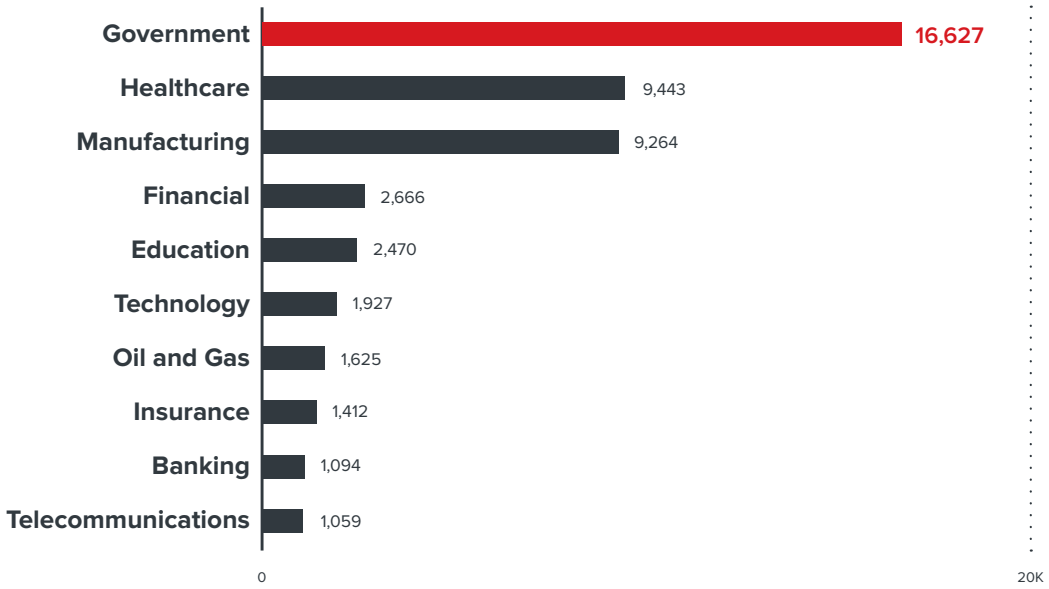


Figure 16. The top targeted identified industries based on ransomware file detections in the first half of 2020

Source: Trend Micro Smart Protection Network infrastructure

Comparing the first halves of 2019 and 2020, we observed a drop in ransomware-related components, which includes files, emails, and URLs. However, as we will note later, this tells only part of the story, as ransom demands have actually increased significantly.

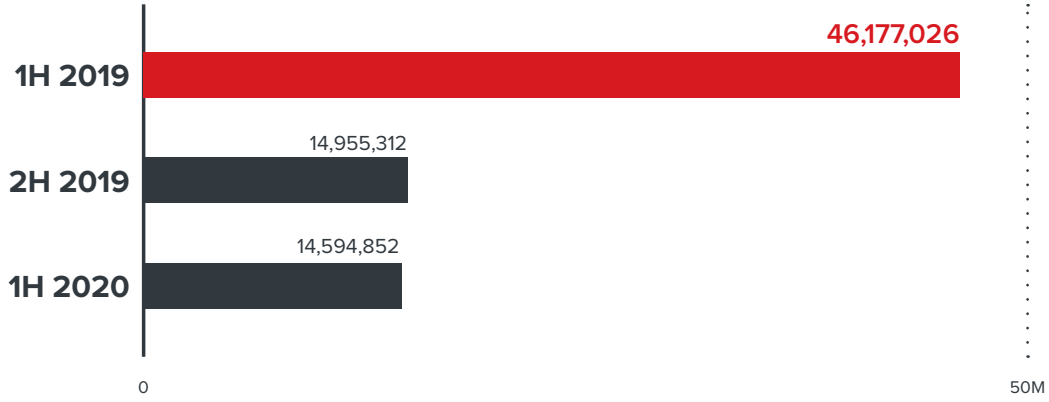


Figure 17. Half-year comparison of the number of detected ransomware-related components (files, emails, and URLs)

Source: Trend Micro Smart Protection Network infrastructure

Unlike in previous years in which ransomware operators went for small amounts spread over a large number of victims, current malicious actors have opted to demand heftier ransoms from targets that are more likely to pay, such as healthcare companies and local governments. Even past prominent ransomware families, such as WannaCry,[31] only took home a fraction[32] of what newer ransomware — such as Ryuk — could potentially earn in a single attack. Over the past few years, ransomware has evolved to become more personal and less opportunistic.The older modus of ransomware operators, which involved sending spam mail in the hopes of luring random individuals to click on links or download attachments, has given way to targeted campaigns that use vulnerabilities, weak applications, or stolen credentials to break into a company's system. The targeted nature of the attacks means that we often hear about ransomware attacks from the victim organizations themselves.

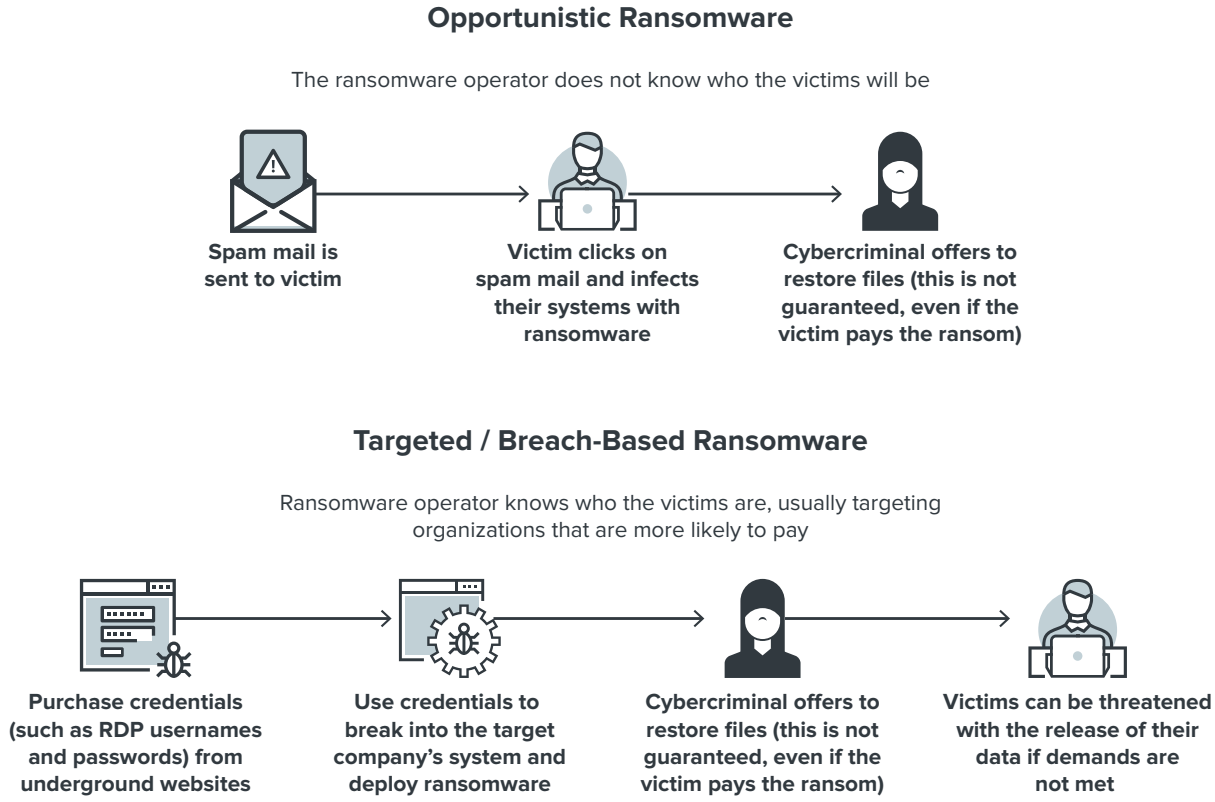
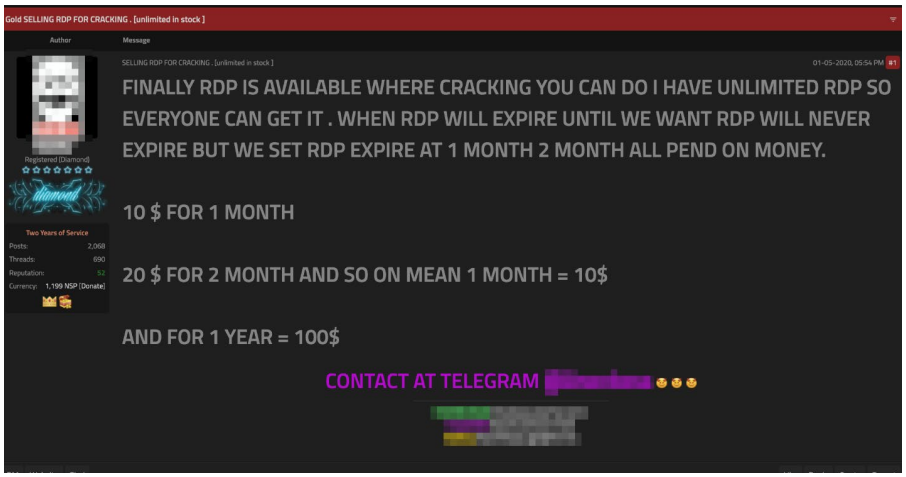


Figure 18. A comparison of common approaches used in opportunistic versus targeted ransomware attacks



IP	Country	State	City	ZIP	OS	RAM	Dwn.	Upl.	Direct IP	Admin Rights	Added	Price, $
103.*.*.*	IN	Gujarat	Ahmedabad		Windows Server 2012 Standard	–	6.29 Mbit/s	4.40 Mbit/s			add funds!	9.00
181.*.*.*	AR	Ciudad Autonoma de Buenos Aires	Buenos Aires		Windows Server 2016 Datacenter	–	10.65 Mbit/s	7.46 Mbit/s			add funds!	9.00
61.*.*.*	CN	Zhejiang	Ningbo		Windows Server 2016 Standard	–	9.84 Mbit/s	6.89 Mbit/s			add funds!	11.00
185.*.*.*	HK	Hong Kong	Hong Kong	-	Windows Server 2012 R2 Standard	–	7.42 Mbit/s	5.19 Mbit/s	✔		add funds!	11.00

Figure 19. Examples of vendors selling RDP credentials in the underground

In February, Electronic Warfare Associates (EWA),[33] a supplier of equipment and services to the Department of Defense (DOD), the Department of Homeland Security (DHS), and the Department of Justice (DOJ), was infected by the Ryuk ransomware. The ransomware encrypted the company's web servers and the websites of its subsidiaries. This was not the first time Ryuk has been deployed against specific organizations — in fact, much of its modus revolves around targeted attacks instead of the random distribution methods that ransomware operators used in the past.[34]

What makes this particular ransomware family so dangerous is that it goes after companies in critical industries such as logistics, technology, and government. The importance of the data stored and processed by these organizations provides the malicious actors behind Ryuk the impetus needed to insist on extremely hefty ransom amounts: According to a report from Coveware,[35] as of the first quarter of 2020, the average ransom demand for a Ryuk infection rose to US$1.3 million, from approximately US$800,000 in the fourth quarter of 2019.

But such attacks weren't just used to target government and public infrastructures — ransomware operators also fixed their sights on private companies. The malicious actors behind the Nemty ransomware even eschewed their public ransomware-as-a-service (RaaS) operation altogether to focus on private targeted campaigns.[36] One likely reason for the change is that private schemes are simply more lucrative than trying to wring small amounts from random victims. Another possible reason raised by

security researcher Vitali Kremez is that the switch provides the malicious actors an opportunity to recruit experienced malware distributors. Like Ryuk, Nemty gained notoriety in 2019 when they were reported to have publicly exposed the information stolen from their victims in addition to encrypting their data.[37]

The threat of information exposure seems to be a rising trend for newer ransomware: Maze, another fairly recent ransomware that was used in an attack against a major target, the IT services firm Cognizant,[38] is also noted for combining file encryption and data theft in its campaigns.[39]

We also discovered some notable new ransomware families in 2020. In May, several organizations in Taiwan were hit with a ransomware we named ColdLock.[40] Although ColdLock's routine or behavior doesn't differ much from that of other ransomware families, its effects could be devastating for its victims since it targets sections of the system that holds critical information, such as databases and email servers.

Perhaps the most prominent of the new ransomware families from the first half of the year is Nefilim. This ransomware shares similar code with Nemty — except for one rather important distinction: the lack of a RaaS component. Considering Nemty's change of focus from RaaS to private ploys, it's highly likely that Nefilim is Nemty ransomware's successor. Like Nemty and Maze, Nefilim also threatens its victims with the public exposure of stolen data.[41]

The Trend Micro Managed XDR team was able to analyze an actual Nefilim infection that occurred in mid-March. Using Trend Micro Deep Discovery Inspector™, we observed an attempt to download a malicious file that, in turn, attempted to download a RAR archive from a hosted virtual private server (VPS). The RAR archive contained several files, including the ransomware itself, Psexec.exe, and several batch files designed to be used together to run various commands.

In June, we unearthed additional Nefilim routines, showing that the ransomware is more complex than it seemed. The routines show the use of two possible entry points, either remote desktop protocol (RDP) or the exploit of a Citrix vulnerability, before using a local exploit for privilege escalation. The ransomware also made use of a handful of other tools and applications: Mimikatz to harvest credentials, AdFind to explore Active Directory, CobalStrike to control the environment, and MEGAsync to exfiltrate data. Based on our observations of Nefilim, the threat actors behind the ransomware appear to have crafted a sophisticated and well-planned campaign with an eye on specific targets.

Vulnerabilities Become a Priority Despite Challenges

End of the Line for Windows 7 While Microsoft Focuses on Updates

Although mainstream support for Windows 7 ended on January 13, 2015, Microsoft continued to offer extended support for the popular operating system until January 14, 2020, when Windows 7 finally reached its end-of-life (EOL)[42] — meaning it will no longer receive any further updates or security patches. While this should have served as an incentive for individuals and organizations to finally switch to a newer OS, there is still a relatively substantial number — approximately 20% — of Windows 7 users as of June 2020.[43]

Without the need to dedicate resources to Windows 7, it seems that Microsoft has been busy fixing vulnerabilities so far this year. After releasing a relatively low number of fixes in the monthly Patch Tuesday update for January, the number dramatically increased; the number of fixes went up to 99 in February, then exceeded 100 every month since March, with June having the highest count at 129.

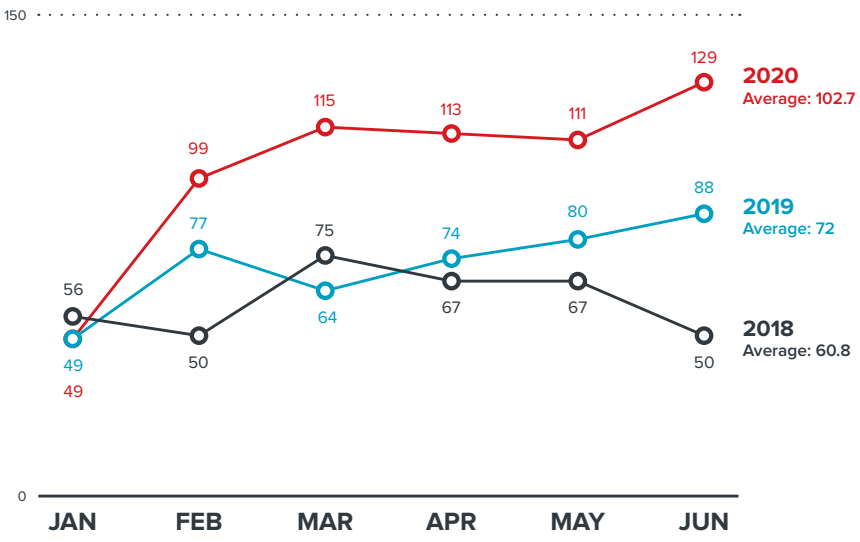


Figure 20. A comparison of the number of Patch Tuesday updates released for the first half-year periods of 2018, 2019, and 2020.

While the January Patch Tuesday update had the least amount of vulnerabilities patched, it addressed the most significant Microsoft vulnerability this year: CVE-2020-0601,[44] also known as CurveBall.

The bug concerns Microsoft CryptoAPI, a Windows component that handles cryptographic functions. In particular, it involves how CryptoAPI handles the validation of Elliptic Curve Cryptography (ECC) certificates and Public Key Infrastructure (PKI) trust. CurveBall is dangerous because a malicious actor exploiting this vulnerability can spoof ECC validity,[45] making a file or code appear to come from a trusted source. This exploit enables a number of attacks, such as man-in-the-middle (MITM) schemes, information decryption, and remote exploitation.[46] Various security researchers have released several proof-of-concept (POC) codes for the exploitation of CVE-2020-0601.[47, 48, 49]

Some of the other more notable vulnerabilities from Microsoft's cumulative round of updates include three actively-exploited bugs patched in April.[50] CVE-2020-1020[51] and CVE-2020-0938[52] are a pair of remote code execution flaws in the Adobe Type Manager (ATM) OpenType Library that could potentially allow an attacker to run code and perform actions on a user's machine. The third bug, CVE-2020-1027,[53] is an elevation of privilege vulnerability in the Windows kernel that could allow attackers to run code via elevated permissions.

The unusually large number of bug fixes places an additional burden on IT departments, not only due to the sheer volume but also because many IT staff have to maintain and update their systems remotely. However, especially given the current situation, applying these patches remains extremely important.

Two Vulnerabilities Join the List of Most Commonly Exploited Bugs

The US Cybersecurity and Infrastructure Security Agency (CISA) recently published a report detailing the 10 most-exploited vulnerabilities from 2016 to 2019.[54]

According to the analysis from the US government, flaws found in Microsoft's Object Linking and Embedding (OLE) technology and the open-source framework Apache Struts were the most commonly exploited by malicious actors. A US industry study that Recorded Future[55] released in early 2019 corroborated this data, revealing that four of the top 10 vulnerabilities mentioned in the CISA report appeared in their list.

In addition to the 10 original vulnerabilities, the US government added two other bugs to the list in 2020, both of which involve virtual private networks (VPNs). One is an arbitrary code execution vulnerability found in Citrix VPN appliances (CVE-2019-19781), while the other is an arbitrary file reading vulnerability found in Pulse Secure VPN servers (CVE-2019-11510). CVE-2019-19781 has already been found being actively exploited in the wild,[56] and is the Citrix vulnerability exploited by Nefilim that we mentioned earlier.[57] The most likely reason for the increased exploitation of these flaws is the surge in usage of VPN software due to the Covid-19 pandemic.

Vulnerability	Affected products	Associated Malware
CVE-2017-11882	Microsoft Office 2007 SP3/2010 SP2/2013 SP1/2016	Loki, FormBook, Pony/ FAREIT
CVE-2017-0199	Microsoft Office 2007 SP3/2010 SP2/2013 SP1/2016, Vista SP2, Server 2008 SP2, Windows 7 SP1, Windows 8.1	FINSPY, LATENTBOT, Dridex
CVE-2017-5638	Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1	JexBoss
CVE-2012-0158	Microsoft Office 2003 SP3, 2007 SP2 and SP3, and 2010 Gold and SP1; Office 2003 Web Components SP3; SQL Server 2000 SP4, 2005 SP4, and 2008 SP2, SP3, and R2; BizTalk Server 2002 SP1; Commerce Server 2002 SP4, 2007 SP2, and 2009 Gold and R2; Visual FoxPro 8.0 SP1 and 9.0 SP2; and Visual Basic 6.0	Dridex
CVE-2019-0604	Microsoft SharePoint	China Chopper
CVE-2017-0143	Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT	Several malware families including ones that exploit EternalSynergy and EternalBlue
CVE-2018-4878	Adobe Flash Player before 28.0.0.161	DOGCALL
CVE-2017-8759	Microsoft .NET Framework 2.0, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 and 4.7	FINSPY, FinFisher, WingBird
CVE-2015-1641	Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word for Mac 2011, Office Compatibility Pack SP3, Word Automation Services on SharePoint Server 2010 SP2 and 2013 SP1, and Office Web Apps Server 2010 SP2 and 2013 SP1	Toshliph, UWarrior
CVE-2018-7600	Drupal before 7.58, 8.x before 8.3.9, 8.4.x before 8.4.6, and 8.5.x before 8.5.1	Kitty
CVE-2019-11510	Pulse Connect Secure 9.0R1 - 9.0R3.3, 8.3R1 - 8.3R7, 8.2R1 - 8.2R12, 8.1R1 - 8.1R15 and Pulse Policy Secure 9.0R1 - 9.0R3.1, 5.4R1 - 5.4R7, 5.3R1 - 5.3R12, 5.2R1 - 5.2R12, 5.1R1 - 5.1R15	N/A
CVE-2019-19781	Citrix Application Delivery Controller, Citrix Gateway, and Citrix SDWAN WANOP	Nefilim

Table 4. The list of vulnerabilities, affected products, and associated malware, as mentioned in the CISA report.

Source: US Cybersecurity and Infrastructure Security Agency (CISA) and externally sourced data

The majority of the top 12 are older vulnerabilities that, theoretically, should be patched by organizations at the soonest possible time given how commonly they are exploited. However, many businesses still struggle when it comes to patching due to several challenges, including a lack of IT personnel to implement updates and testing inefficiencies.

Data gathered from Trend Micro Digital Vaccine ® (DV) filters showing the targeted vulnerabilities from 2017 to the beginning of 2020 affirm the CISA list, particularly when it comes to enterprise software like the Apache Struts and Drupal frameworks. Despite being a relatively new vulnerability, CVE-2019-11510 had the second-highest number of hits. The other new vulnerability from the top 12, CVE-2019-19781, also showed a significant amount of exploit attempts.

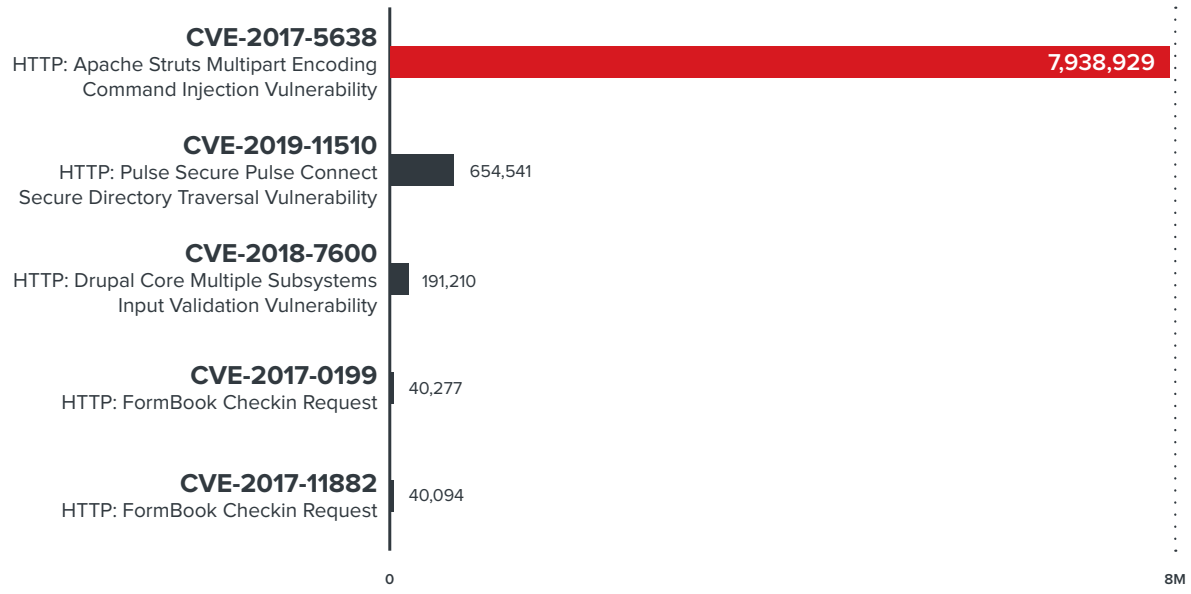


Figure 21. The five most-targeted vulnerabilities from January 2017 to June 2020.

Note: This table represents the combined vulnerability data from January 2017 to June 2020

Source: Trend Micro Digital Vaccine filters

IIoT Vulnerabilities Remain a Tangled Mess

The efficiency, safety, and flexibility of industrial internet of things (IIoT) devices have led to their widespread adoption as essential components of business operations. However, increased demand also means developers and manufacturers are releasing more devices and software to meet it, which also leads to the discovery of more vulnerabilities.

We observed a 16% increase in the number of industrial control system (ICS) vulnerabilities disclosed to the Trend Micro™ Zero Day Initiative™ (ZDI) program in the first half of 2020 compared to the same period last year. Of the disclosed bugs, 11 were considered zero-day vulnerabilities.

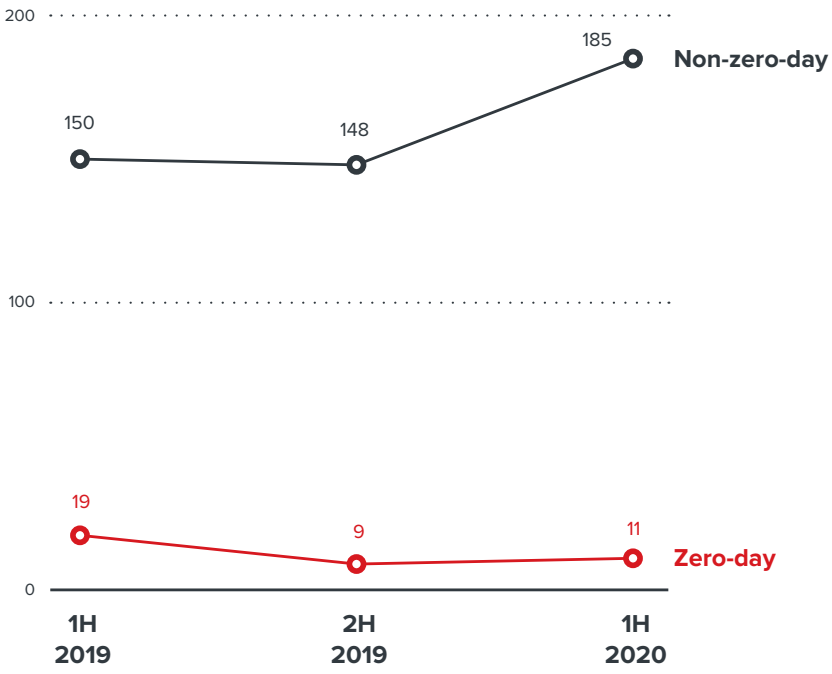


Figure 22. The number of ICS vulnerabilities disclosed to ZDI for the first and second halves of 2019 and the first half of 2020

Vulnerabilities in IIoT devices have the potential to cause significant damage, given that the exploitation of these bugs might disrupt business operations or, in the case of medical equipment, endanger lives. In 2019, security researchers at Armis discovered a set of eleven vulnerabilities — labeled "Urgent/11" — in medical devices that could put hospital networks at risk.[58] By exploiting these vulnerabilities, a malicious actor could take control of medical devices and use them to wreak havoc on the system — for example, by changing device functions or causing denial-of-service attacks. These bugs exist in a third-party software component called IPnet, which is responsible for supporting network communication between computers.

Normally, patching these bugs would be relatively straightforward. However, the original software vendor for IPNet no longer offers support for the software, with some manufacturers only being able to implement it on their machines via licensing agreements. In addition, these vulnerabilities affect a mishmash of different operating systems and devices,[59] making it difficult to determine who should be responsible for fixing the bugs.

Another batch consisting of 19 IIoT vulnerabilities was unearthed by the cybersecurity company JSOF in 2020.[60] Dubbed "Ripple20," these flaws encompass a wide range of industries — from healthcare and transportation to oil and gas, power, and manufacturing. It affects a third-party software that was developed by Treck Inc. in the 1990s that enables companies to connect their devices and software to the internet via TCP/IP.[61] Similar to Urgent/11, numerous manufacturers integrated this software component into their machines over the years, making it difficult to identify which devices and software are affected.

Based on what we've seen from these two sets of vulnerabilities, updating IIoT devices still has its fair share of issues — therefore, it won't be surprising to see regulations for standardized firmware update tools and cybersecurity APIs in IIoT devices in the future.

The Number of Published Vulnerabilities See a Sharp Increase

For the first half of 2020, ZDI published a total of 786 advisories that were sourced from both internal and independent researchers. This represents a substantial increase of 74% from the latter half of 2019.

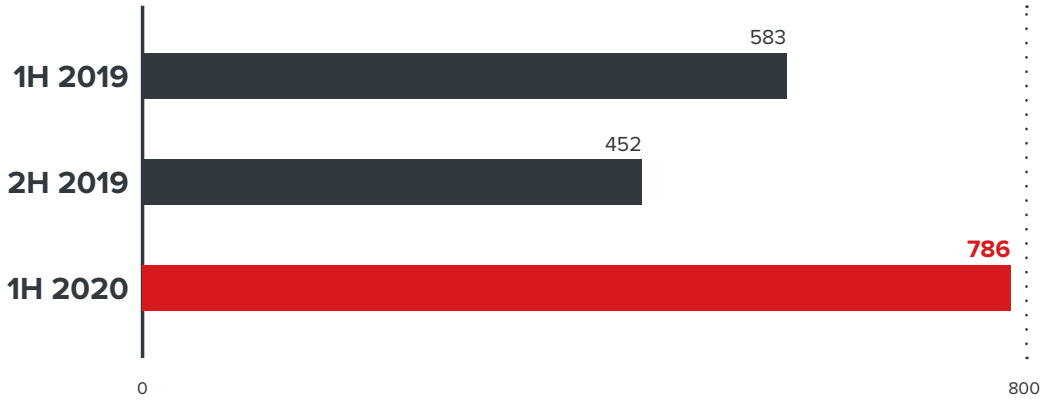


Figure 23. Half-year comparison of the number of vulnerabilities disclosed via the ZDI program

Source: Trend Micro™ Zero Day Initiative™ program

Among the disclosed flaws, Critical and High-severity vulnerabilities made up the bulk of the overall count. In terms of overall numbers, there was a significantly higher number of Critical and High-severity bugs as well; the count for the first half of 2020 nearly equaled (for High-severity) or even surpassing (for Critical) the 2019 total.

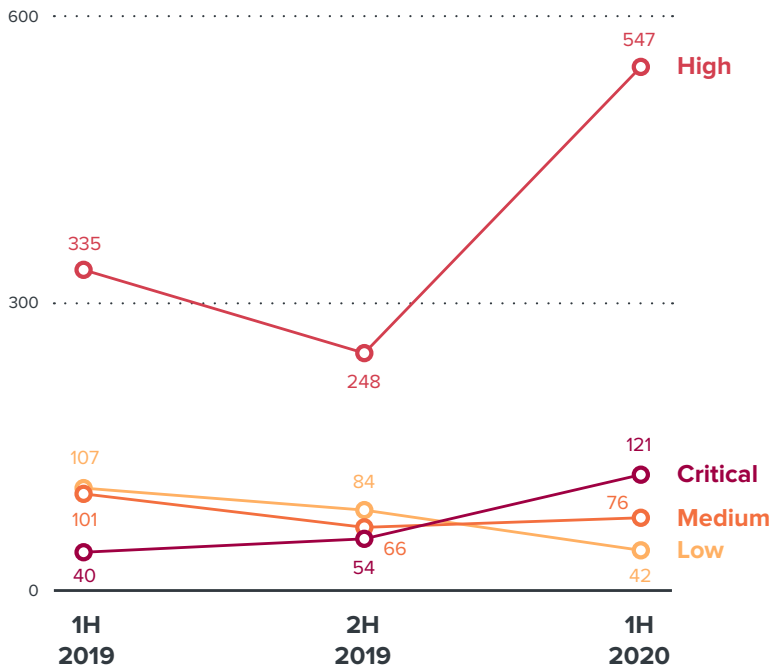


Figure 24. The half-year comparison of the severity breakdown, based on the CVSS, of vulnerabilities disclosed via our ZDI program. The first half of 2020 showed a significant increase in the number of Critical and High-severity vulnerabilities

Source: Trend Micro Zero Day Initiative program

Aside from the obvious issue of having more vulnerabilities that malicious actors can potentially exploit, the large number of critical and high-rated vulnerabilities also means that IT personnel who are already burdened with migrating their systems to a remote work setup will have to find a way to patch these bugs, either via remote patching or by having to rely on individual employees to update their personal machines

A Multilayered Defense Helps Address Today's Multifaceted Threats

The Covid-19 pandemic forced businesses to adapt to new working conditions. The health crisis also caught many by surprise. IT departments, in particular, bore the burden of their company's transition to a WFH setup, which often left them little time to devote to security tasks.

Unusual times call for robust security technology. Siloed tools and single layers of protection for the individual components of a company's system is proving to be insufficient. Instead, businesses should look for a multilayered solution that can provide a mix of threat-defense capabilities such as detection, investigation, and response across multiple platforms, including emails, endpoints, servers, networks, and cloud workloads. Ideally, these kinds of security solutions should be able to provide a wide range of indicators and analytics that would allow IT staff to see the bigger picture without having to dedicate a significant chunk of their time and resources to sift through a mountain of alerts and other data — time that could be better spent to ensure that their company's systems are running as smoothly as possible.

Although wrapped in a new veneer, the techniques that malicious actors use to capitalize on the pandemic have remained the same. Social engineering, in particular, has remained prevalent, and it has become even more effective due to the fear and uncertainty brought about by the virus. More than ever, organizations should take the time to educate home users on the best practices for cybersecurity via security awareness programs. For their part, individual users should always be vigilant and apply proper discretion and common sense when it comes to their online activities.

Patching remains as important as it has ever been, especially now that many workers are using their personal machines for work. Organizations should prioritize updating their systems at the soonest possible opportunity, and if possible, find a way to deliver these updates to users remotely. Businesses can consider virtual patching[62] to protect their systems and end-user machines, as well as minimize downtime while waiting for vendors to roll out official patches.

Threat Landscape in Review

In the first half of 2020, the Trend Micro™ Smart Protection Network™ infrastructure was able to protect users from over 27 billion threats — a number that encompasses email threats, malicious files, and malicious URLs.

27,823,212,959

The number of threats blocked in the first half of 2020

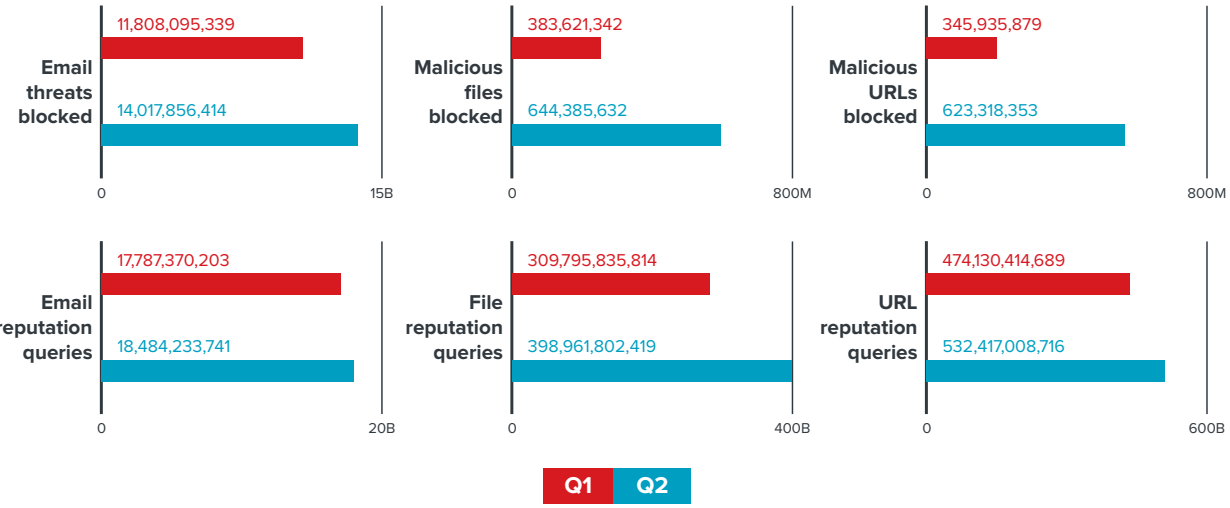
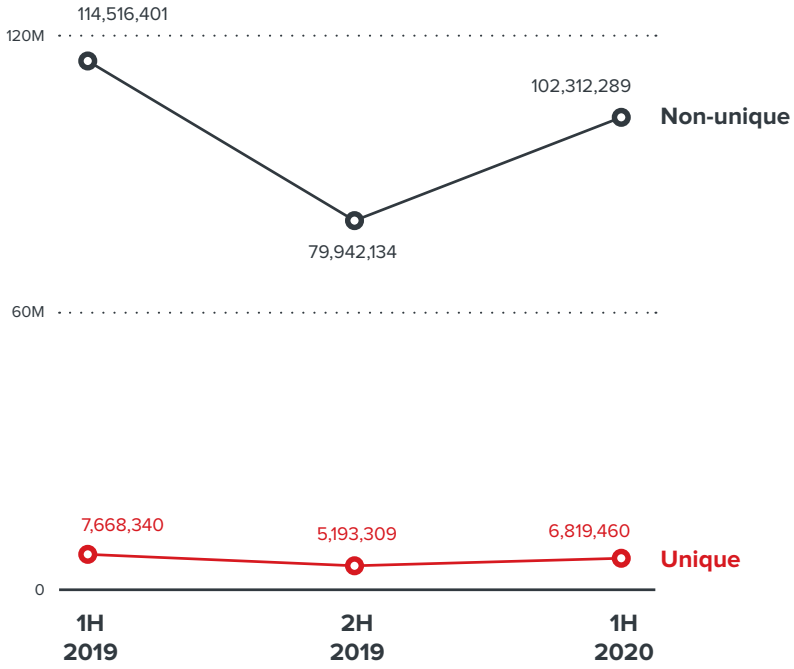


Figure 25. The number of blocked email threats, malicious files, and malicious URLs increased from the first to the second quarter of the year. Email, file, and URL reputation queries also saw similar spikes.

Source: Trend Micro Smart Protection Network infrastructure

Attempts to access phishing sites, both unique and non-unique, increased in the first half of 2020 from the second half of 2019.



Unique phishing URL example: One machine that attempted to access the same URL three times is counted as one affected user

Non-unique phishing URL example: Three instances of blocked access to the same URL is counted as three attempts

Figure 26. The number of unique and non-unique phishing URLs from 2019 to the first half of 2020

Source: Trend Micro Smart Protection Network infrastructure

PDF files were by far the most commonly used file type in spam attachments in the first half of 2020, accounting for over 50% of the total. Aside from HTML files, which were also common, the other file types did not see much usage.

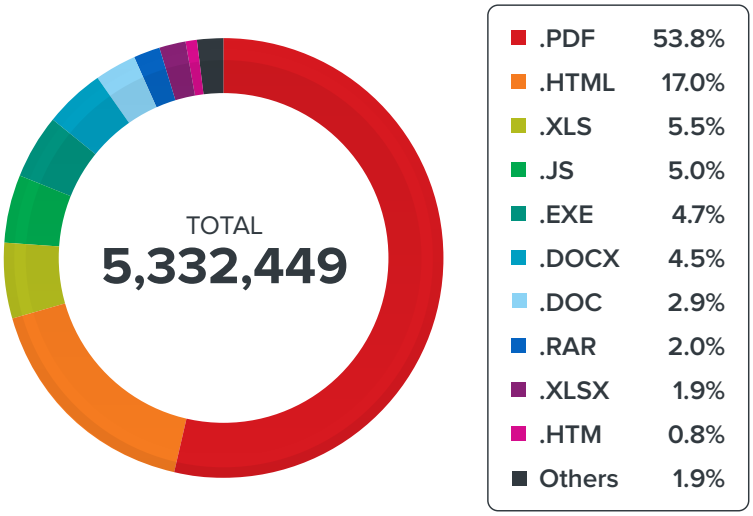


Figure 27. The distribution of file types used as attachments in spam emails in the first half of 2020; PDF was overwhelmingly the most-used file type

Source: Trend Micro Email Reputation Services

The first half of 2020 saw the appearance of 68 new ransomware families, a 45% increase from the 47 discovered in the first half of 2019.

January	February	March	April	May	June
AKOLOCKER	ANTEFRIGUS	BB	BALLISTIC	BLUECHEESER	AVADDON
AVEST	BALACLAVA	CORVINA	BEARCRYPT	COLDLOCK	BLACKCLAW
BITPYLOCKER	CAI	MADO	CORONAWINLOCKER	CORONALOCK	BLACKKINGDOM
KESLAN	CRYPENCODE	NEFILIM	CREEPY	GONNACRY	BLACKMOON
ZEOTICUS	CRYPTOPXJ	PYSA	CRYLOCK	PONYFINAL	CHIMERA
	CRYTOX	TRIPLEM	GEMINICE		CYBERTHANOS
	DEMONCRYPT	WANNAREN	JEST		ESCAL
	FTCODE		LBKUT		FUNICORN
	LEDIF		ONALOCKER		KRYGO
	MAKOP		OOGLEGO		LICKYAGENT
	MORRISBATCHCRYPT		SADOGO		LOCMENT
	ONYXLOCKER		SFILE2		POWLOCK
	RAGNAROK		UPPER		QRNALOCK
	RANSCRAPE		VOID		RFREEFIL
	TRSOMWARE		WREATH		SAPPHIRE
	WANNACASH				SUCHCRYPT
	WANNASCREAM				WORLDCRY
	WILBOY				ZORAB

Table 5. More ransomware: 68 new ransomware families appeared in the first half of 2020

Sources: Trend Micro Smart Protection Network infrastructure and analysis of externally sourced data

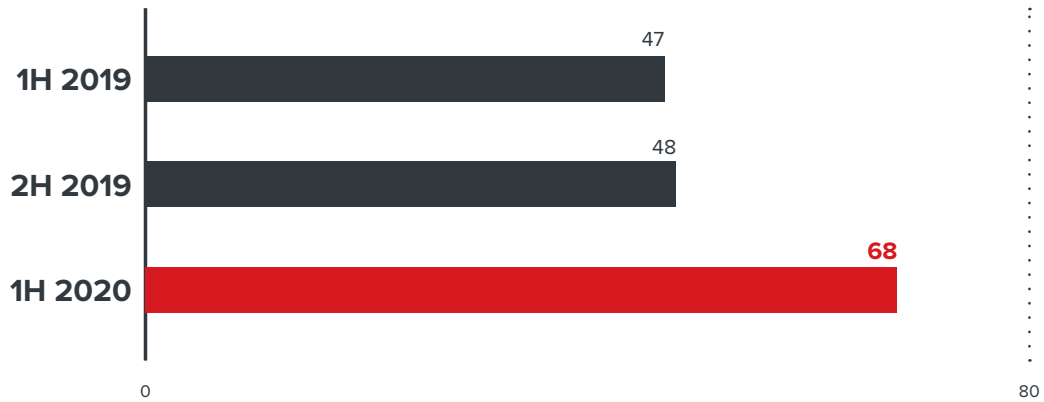


Figure 28. Comparison of new ransomware family detections for half-year periods from the first half of 2019 to the first half of 2020.[63, 64]

The number of threats to mobile devices remained sizeable in 1H 2020. While the number of mobile apps that were blocked by the Trend Micro Mobile App Reputation Service (MARS) decreased from the second half of 2019, we observed a 22% increase in mobile device-related malicious samples.

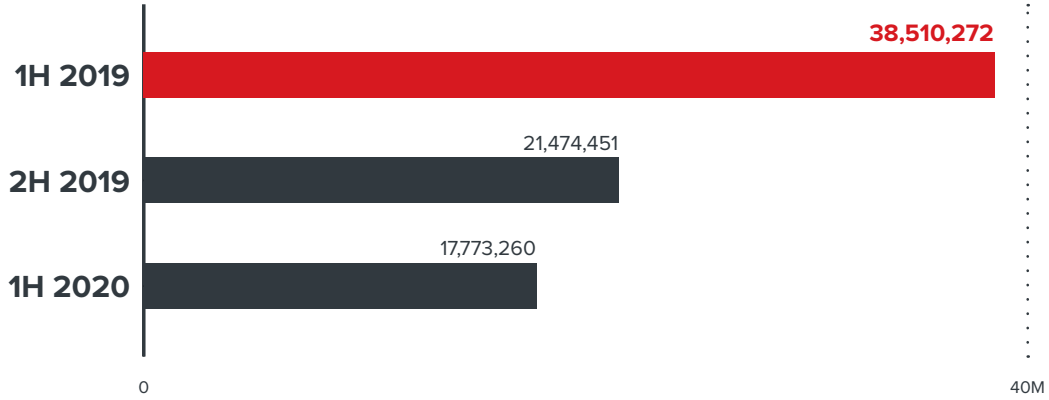


Figure 29. A half-year comparison of the number of blocked malicious Android app shows a downward trend since the first half of 2019

Source: Trend Micro Mobile App Reputation Service

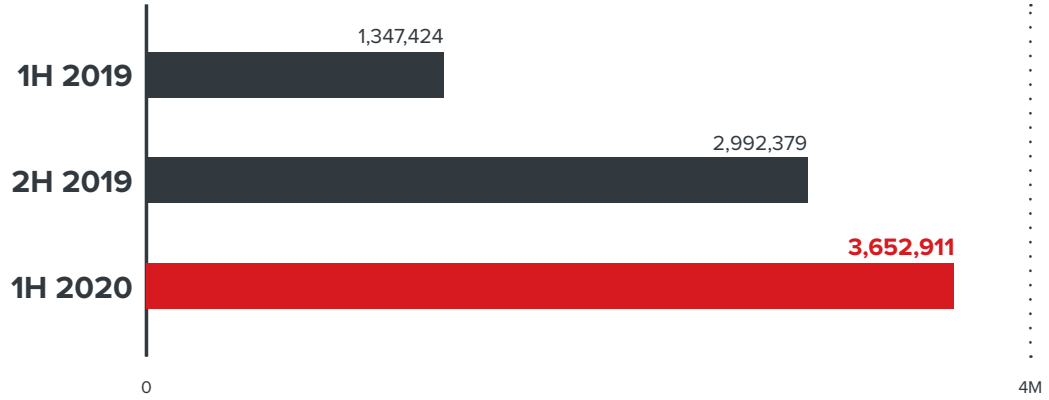


Figure 30. A half-year comparison of the number of detections for mobile device-related malicious samples shows an upward trend

Sources: Trend Micro Mobile App Reputation Service and analysis of externally sourced data

We also covered several notable mobile threat incidents in the first six months of the year. In January, we discovered a trio of information-stealing mobile apps that had links to the SideWinder APT group.[65] One of the three apps, Camero, was found to be the first instance of exploitation of the use-after-free vulnerability CVE-2019-2215.[66]

In late March, we found evidence of a campaign named Operation Poisoned News that targeted iOS users in Hong Kong. The campaign used watering hole attacks with links leading to news stories that were posted on various forums. While these links did lead to actual news sites, they contained hidden iframes that executed malicious code designed to exploit vulnerabilities in iOS 12.1 and 12.2. Clicking on the links infected devices with a mobile malware called LightSpy that allows an attacker to execute shell commands and manipulate files on affected devices.[67]

Ad fraud remained a popular technique for cybercriminals and fraudsters targeting mobile devices. We analyzed several apps on Google Play and found that, while they presented themselves as utility apps, they actually performed ad fraud and other malicious routines.

In one example, we investigated a number of optimization apps that had the supposed ability to clean up unwanted files and improve the performance of mobile devices.[68] However, we discovered that the apps performed mobile ad fraud and downloaded malware to infected devices. We also found other examples where fraudulent advertisements were presented to unwary users using barcode readers[69] and other types of apps.

In terms of overall numbers, BEC scams increased by 19% from the second half of 2019, perhaps due to the number of malicious actors trying to capitalize on the Covid-19 pandemic.

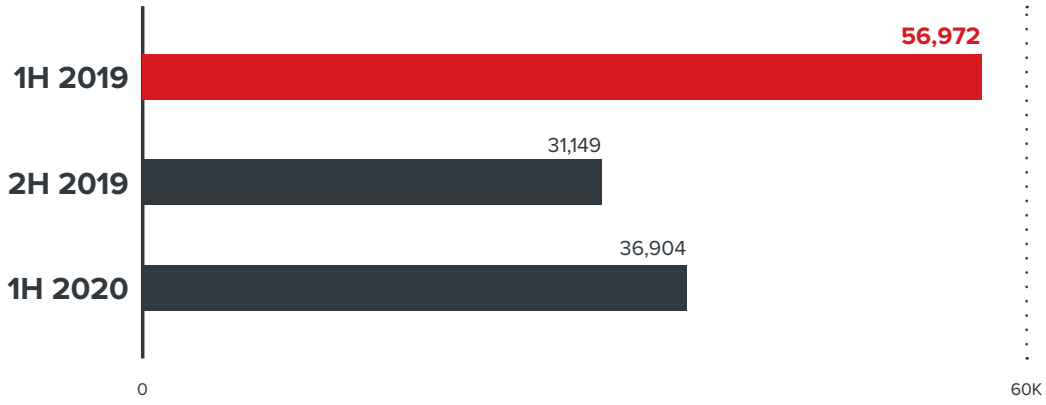


Figure 31. A half-year comparison of BEC attempts show a slight increase in the first half of 2020

Note: Data refers to the number of BEC attempts seen, which does not indicate whether the attacks were successful.

The CEO was the most spoofed organizational position in the first half of 2020, representing roughly 30% of all spoofed positions. While this was still a fairly sizeable percentage, it shows a significant decrease from 2019, when the CEO position represented approximately 41% of all spoofed positions.[70] BEC scammers may be experimenting by spoofing other positions to gauge their effectiveness.

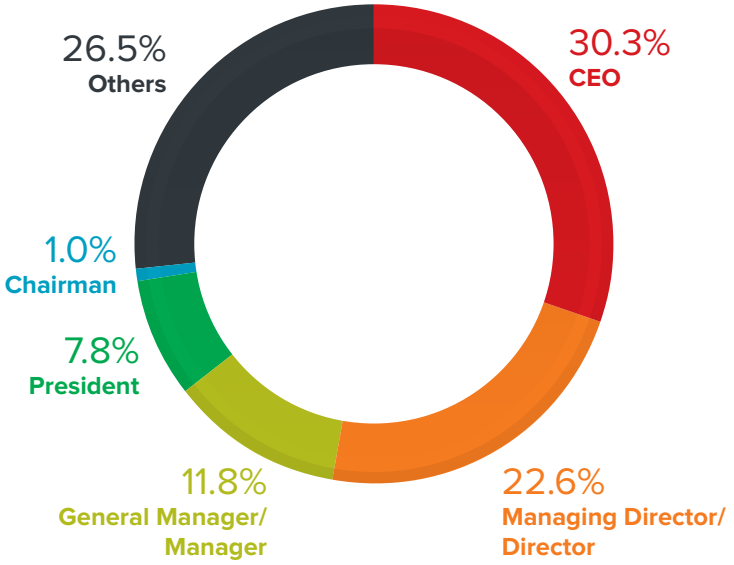


Figure 32. The distribution of spoofed organizational positions in BEC attempts detected in 2020; CEO was the most spoofed position for BEC attempts, followed by Managing Director/Director

Note: Data refers to a sample set of BEC attempts seen, which does not indicate if the attacks were successful. BEC attempts consist of CEO fraud

Scammers continued to target executives and employees that were connected to a company's finances, such as Finance Managers and Directors of Finance.

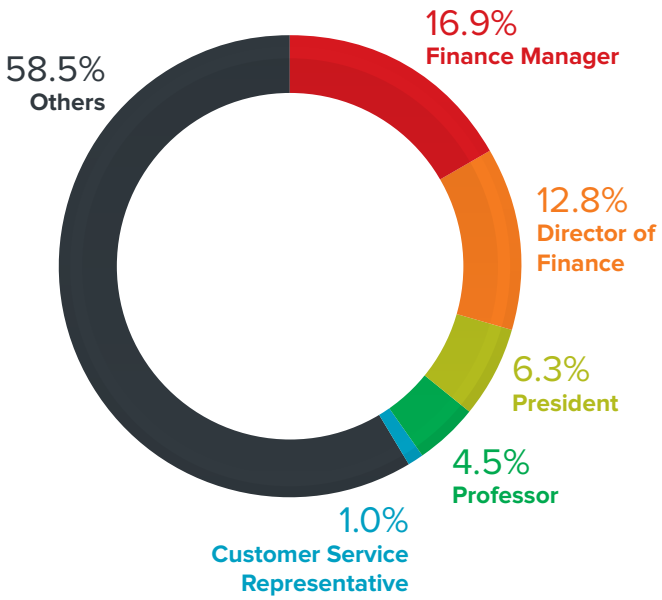


Figure 33. The distribution of targeted positions in BEC attempts in the first half of 2020; organization leaders in financial departments were the most targeted positions for BEC attempts

Note: Data refers to a sample set of BEC attempts seen, which does not indicate if the attacks were successful. BEC attempts consist of CEO fraud

In our security roundup for 2019,[71] we noted that fileless threats have become much more common, and this was proven by the higher number of detections for the year. In contrast, the first half of 2020 showed a significant decrease (approximately 71%) in the number of blocked fileless threats.

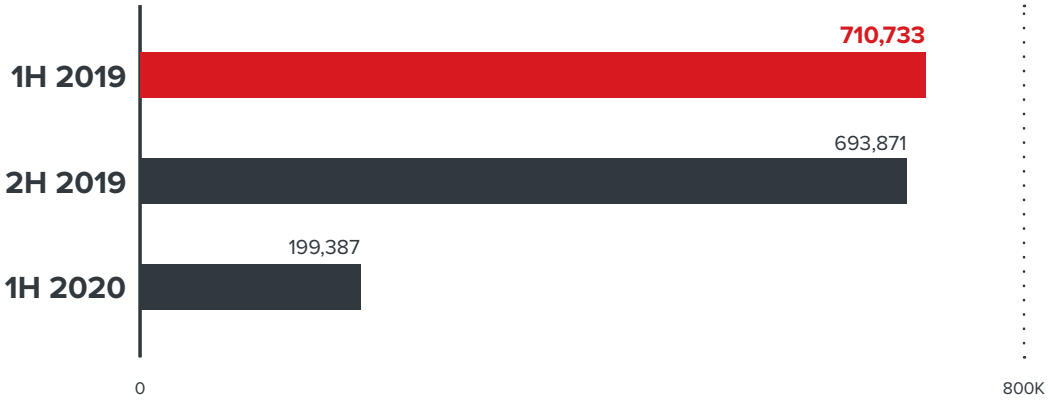


Figure 34. A half-year comparison of the number of blocked fileless events indicate a significant decrease in the first half of 2020

Source: Trend Micro Smart Protection Network infrastructure

References

1 Trend Micro. (April 24, 2020). *Trend Micro Security News*. "Developing Story: COVID-19 Used in Malicious Campaigns." Accessed on July 20, 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains.

2 Patrick Peterson. (March 19, 2020). *Agari Email Security Blog*. "Business Email Compromise (BEC): Coronavirus a Costly New Strain of Email Attack." Accessed on July 20, 2020 at https://www.agari.com/email-security-blog/business-email-compromise-bec-coronavirus-covid-19/.

3 Malwarebytes Labs. (March 24, 2020). *Malwarebytes Labs*. "Fake "Corona Antivirus" distributes BlackNET remote administration tool." Accessed on July 20, 2020 at https://blog.malwarebytes.com/threat-analysis/2020/03/fake-corona-antivirus-distributes-blacknet-remote-administration-tool/.

4 Tony Bao and Junzhi Lu. (April 14, 2020). *Trend Micro Security Intelligence Blog*. "Coronavirus Update App Leads to Project Spy Android and iOS Spyware." Accessed on July 20, 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/coronavirus-update-app-leads-to-project-spy-android-and-ios-spyware/.

5 Matthew Stewart. (May 14, 2020). *Trend Micro Security Intelligence Blog*. "QNodeService: Node.js Trojan Spread via Covid-19 Lure." Accessed on July 20, 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/qnodeservice-node-js-trojan-spread-via-covid-19-lure/.

6 Internal Revenue Service. (May 27, 2020). *Internal Revenue Service*. "Coronavirus Tax Relief and Economic Impact Payments for Individuals and Families." Accessed on July 20, 2020 at https://www.irs.gov/coronavirus/coronavirus-tax-relief-and-economic-impact-payments-for-individuals-and-families.

7 Hiroyuki Kakara and Erina Maruyama. (April 17, 2020). *Trend Micro Security Intelligence Blog*. "Gamaredon APT Group Use Covid-19 Lure in Campaigns." Accessed on July 20, 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/gamaredon-apt-group-use-covid-19-lure-in-campaigns/.

8 Trend Micro. (June 30, 2020). *Trend Micro Security News*. "CSO Insights: Liggett Consulting's Mark Liggett on Connectivity and Visibility in Securing Remote Work." Accessed on July 20, 2020 at https://www.trendmicro.com/vinfo/us/security/news/security-technology/cso-insights-liggett-consulting-s-mark-liggett-on-connectivity-and-visibility-in-securing-remote-work.

9 Bobby Allyn. (May 13, 2020). *National Public Radio*. "Your Boss Is Watching You: Work-From-Home Boom Leads To More Surveillance." Accessed on July 21, 2020 at https://www.npr.org/2020/05/13/854014403/your-boss-is-watching-you-work-from-home-boom-leads-to-more-surveillance.

10 Trend Micro. (March 26, 2020). *Trend Micro Security News*. "Working From Home? Here's What You Need for a Secure Setup." A2ccessed on July 21, 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/working-from-home-here-s-what-you-need-for-a-secure-setup.

11 Trend Micro. (May 22, 2020). *Trend Micro Security News*. "CSO Insights: SBV's Ian Keller on the Challenges and Opportunities of Working Remotely." Accessed on July 20, 2020 at https://www.trendmicro.com/vinfo/us/security/news/security-technology/cso-insights-sbv-s-ian-keller-on-the-challenges-and-opportunities-of-working-remotely.

12 Trend Micro. (April 22, 2020). *Trend Micro Security News*. "Know the Symptoms: Protect Your Devices While Working From Home." Accessed on July 20, 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/know-the-symptoms-protect-your-devices-while-working-from-home.

13 Catalin Cimpanu. (April 18, 2020). *ZDNet*. "FBI says cybercrime reports quadrupled during COVID-19 pandemic." Accessed on July 20, 2020 at https://www.zdnet.com/article/fbi-says-cybercrime-reports-quadrupled-during-covid-19-pandemic/.

14 Emily Bary. (April 1, 2020). *MarketWatch*. "Zoom, Microsoft Teams usage are rocketing during coronavirus pandemic, new data show." Accessed on July 20, 2020 at https://www.marketwatch.com/story/zoom-microsoft-cloud-usage-are-rocketing-during-coronavirus-pandemic-new-data-show-2020-03-30.

15 Trend Micro. (March 31, 2020). *Trend Micro Security News*. "Malicious Domains and Files Related to Zoom Increase, 'Zoom Bombing' on the Rise." Accessed on July 20, 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/malicious-domains-and-files-related-to-zoom-increase-zoom-bombing-on-the-rise.

16 Kari Paul. (April 23, 2020). *The Guardian*. "Zoom releases security updates in response to 'Zoom-bombings'." Accessed on July 20, 2020 at https://www.theguardian.com/technology/2020/apr/23/zoom-update-security-encryption-bombing.

17 Check Point. (2020) *Check Point Blog*. "COVID-19 Impact: Cyber Criminals Target Zoom Domains." Last accessed on July 20, 2020 at https://blog.checkpoint.com/2020/03/30/covid-19-impact-cyber-criminals-target-zoom-domains/.

18 Raphael Centeno and Llallum Victoria. (April 3, 2020). *Trend Micro Security Intelligence Blog*. "Zoomed In: A Look into a Coinminer Bundled with Zoom Installer." Accessed on July 20, 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/zoomed-in-a-look-into-a-coinminer-bundled-with-zoom-installer/.

19 Raphael Centeno, Mc Justine De Guzman, and Augusto Remillano II. (April 29, 2020). *Trend Micro Security Intelligence Blog*. "WebMonitor RAT Bundled with Zoom Installer." Accessed on July 20, 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/webmonitor-rat-bundled-with-zoom-installer/.

20 Raphael Centeno and Llallum Victoria. (May 21, 2020). *Trend Micro Security Intelligence Blog*. "Backdoor, Devil Shadow Botnet Hidden in Fake Zoom Installers." Accessed on July 20, 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/backdoor-devil-shadow-botnet-hidden-in-fake-zoom-installers/.

21 Zoom. (n.d.). *Zoom*. "Download Center." Accessed on July 20, 2020 at https://zoom.us/download.

22 Trend Micro. (January 24, 2018). *Trend Micro Security News*. "A Look into the Lazarus Group's Operations." Accessed on July 20, 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-look-into-the-lazarus-groups-operations.

23 Olivia Solon. (May 15, 2017). *The Guardian*. "WannaCry ransomware has links to North Korea, cybersecurity experts say." Accessed on July 20, 2020 at https://www.theguardian.com/technology/2017/may/15/wannacry-ransomware-north-korea-lazarus-group.

24 Gabrielle Joyce Mabutas. (November 20, 2019). *Trend Micro Security Intelligence Blog*. "Mac Backdoor Linked to Lazarus Targets Korean Users." Accessed on July 20, 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/mac-backdoor-linked-to-lazarus-targets-korean-users/.

25 Gabrielle Joyce Mabutas. (May 11, 2020). *Trend Micro Security Intelligence Blog*. "New MacOS Dacls RAT Backdoor Shows Lazarus' Multi-Platform Attack Capability." Accessed on July 20, 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/new-macos-dacls-rat-backdoor-show-lazarus-multi-platform-attack-capability/.

26 Jinye and Genshen Ye. (December 17, 2019). *Network Security Research Lab at 360*. "Dacls, the Dual platform RAT." Accessed on July 20, 2020 at https://blog.netlab.360.com/dacls-the-dual-platform-rat-en/.

27 Daniel Lunghi et al. (February 18, 2020). *Trend Micro*. "Download Uncovering DRBControl: Inside the Cyberespionage Campaign Targeting Gambling Operations." Accessed on July 21, 2020 at https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-drbcontrol-uncovering-a-cyberespionage-campaign-targeting-gambling-companies-in-southeast-asia.

28 RonJay Caragay et al. (April 16, 2020). *Trend Micro Security Intelligence Blog*. "Exposing Modular Adware: How DealPly, IsErIk, and ManageX Persist in Systems." Accessed on July 20, 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/exposing-modular-adware-how-dealply-iserik-and-managex-persist-in-systems/.

29 Trend Micro. (November 19, 2019). *Trend Micro*. "The New Norm: Trend Micro Security Predictions for 2020." Accessed on July 20, 2020 at https://documents.trendmicro.com/assets/rpt/rpt-the-new-norm-trend-micro-security-predictions-for-2020.pdf.

30 Trend Micro. (February 25, 2020). *Trend Micro*. "The Sprawling Reach of Complex Threats." Accessed on July 20, 2020 at https://documents.trendmicro.com/assets/rpt/rpt-the-sprawling-reach-of-complex-threats.pdf.

31 Trend Micro. (May 12, 2017). *Trend Micro Security Intelligence Blog*. "Massive WannaCry/Wcry Ransomware Attack Hits Various Countries." Accessed on August 3, 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/massive-wannacrywcry-ransomware-attack-hits-various-countries/.

32 Andy Greenberg. (May 15, 2017). *Wired*. The WannaCry Ransomware Hackers Made Some Real Amateur Mistakes. Accessed on August 3, 2020 at https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes/.

33 Trend Micro. (February 04, 2020). *Trend Micro Security News*. "Ryuk Ransomware Infects US Government Contractor." Accessed on July 20, 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ryuk-ransomware-infects-us-government-contractor.

34 Trend Micro. (May 21, 2019). *Trend Micro Security News*. "Ryuk Ransomware Shows Diversity in Targets, Consistency in Higher Payouts." Accessed on July 20, 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ryuk-ransomware-shows-diversity-in-targets-consistency-in-higher-payouts.

35 Coveware. (2020). *Coveware*. “Ransomware Payments Up 33% As Maze and Sodinokibi Proliferate in Q1 2020.” Accessed on July 20, 2020 at https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report.

36 Trend Micro. (April 17, 2020). *Trend Micro Security News*. “Nemty Ransomware Ceases Public Operations, Focuses on Private Schemes.” Accessed on July 20, 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/nemty-ransomware-ceases-public-operations-focuses-on-private-schemes.

37 Lawrence Abrams. (March 2, 2020). *Bleeping Computer*. “Nemty Ransomware Punishes Victims by Posting Their Stolen Data.” Accessed on July 20, 2020 at https://www.bleepingcomputer.com/news/security/nemty-ransomware-punishes-victims-by-posting-their-stolen-data/.

38 Trend Micro. (April 20, 2020). *Trend Micro Security News*. “Maze Ransomware Attacks US IT Firm.” Accessed on July 20, 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/maze-ransomware-attacks-us-it-firm.

39 Trend Micro. (January 6, 2020). *Trend Micro Security News*. “Ransomware Recap: Clop, DeathRansom, and Maze Ransomware.” Accessed on July 20, 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-clop-deathransom-and-maze-ransomware.

40 Trend Micro. (May 6, 2020). *Trend Micro Security Intelligence Blog*. “Targeted Ransomware Attack Hits Taiwanese Organizations.” Accessed on July 20, 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/targeted-ransomware-attack-hits-taiwanese-organizations/.

41 Trend Micro. (March 23, 2020). *Trend Micro Security News*. “Nefilim Ransomware Threatens to Expose Stolen Data.” Accessed on July 20, 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/nefilim-ransomware-threatens-to-expose-stolen-data.

42 Microsoft. (n.d.). *Microsoft*. “Support for Windows 7 has ended.” Accessed on July 20, 2020 at https://www.microsoft.com/en-ww/microsoft-365/windows/end-of-windows-7-support.

43 StatCounter. (n.d.). *StatCounter*. “Desktop Windows Version Market Share Worldwide.” Accessed on July 20, 2020 at https://gs.statcounter.com/os-version-market-share/windows/desktop/worldwide.

44 Microsoft. (January 16, 2020). *Security Update Guide*. “CVE-2020-0601 | Windows CryptoAPI Spoofing Vulnerability.” Accessed on July 20, 2020 at https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601.

45 John Simpson. (February 13, 2020). *Trend Micro Security Intelligence Blog*. “An In-Depth Technical Analysis of CurveBall (CVE-2020-0601).” Accessed on July 20, 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/an-in-depth-technical-analysis-of-curveball-cve-2020-0601/.

46 Trend Micro. (January 17, 2020). *Trend Micro Security News*. “Blocking A CurveBall: PoCs Out for Critical Microsoft-NSA Bug CVE-2020-0601.” Accessed on July 20, 2020 at https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/blocking-a-curveball-pocs-out-for-critical-microsoft-nsa-bug-cve-2020-0601.

47 Ollypwn. (January 17, 2020). *GitHub*. “CurveBall.” Accessed on July 20, 2020 at https://github.com/ollypwn/CurveBall.

48 Saleem Rashid. (February 25, 2020). *GitHub*. “Badecparams.” Accessed on July 20, 2020 at https://github.com/saleemrashid/badecparams.

49 Kudelski Security. (March 22, 2020). *GitHub*. “Chainoffools.” Accessed on July 20, 2020 at https://github.com/kudelskisecurity/chainoffools.

50 Dustin Childs. (April 14, 2020). *Zero Day Initiative*. “The April 2020 Security Update Review.” Accessed on July 20, 2020 at https://www.thezdi.com/blog/2020/4/14/the-april-2020-security-update-review.

51 Microsoft. (April 14, 2020). *Security Update Guide*. “CVE-2020-1020 | Adobe Font Manager Library Remote Code Execution Vulnerability.” Accessed on July 20, 2020 at https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1020.

52 Microsoft. (April 14, 2020). *Security Update Guide*. “CVE-2020-0938 | Adobe Font Manager Library Remote Code Execution Vulnerability.” Accessed on July 20, 2020 at https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0938.

53 Microsoft. (April 14, 2020). *Security Update Guide*. “CVE-2020-1027 | Windows Kernel Elevation of Privilege Vulnerability.” Accessed on July 20, 2020 at https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1027.

54 Cybersecurity & Infrastructure Security Agency. (May 12, 2020). *Cybersecurity & Infrastructure Security Agency*. "Alert (AA20-133A) Top 10 Routinely Exploited Vulnerabilities." Accessed on July 20, 2020 at https://us-cert.cisa.gov/ncas/alerts/aa20-133a.

55 Recorded Future. (February 4, 2020). *Recorded Future*. "2019 Vulnerability Report: Cybercriminals Continue to Target Microsoft Products." Accessed on July 20, 2020 at https://www.recordedfuture.com/top-vulnerabilities-2019/.

56 Derek Abdine. (January 17, 2020). *Rapid 7 Blog*. "Active Exploitation of Citrix NetScaler (CVE-2019-19781): What You Need to Know." Accessed on July 20, 2020 at https://blog.rapid7.com/2020/01/17/active-exploitation-of-citrix-netscaler-cve-2019-19781-what-you-need-to-know/.

57 Mathew J. Schwartz. (June 22, 2020). *Bank Info Security*. "Nefilim Ransomware Gang Tied to Citrix Gateway Hacks." Accessed on July 20, 2020 at https://www.bankinfosecurity.com/nephilim-ransomware-gang-tied-to-citrix-gateway-hacks-a-14480.

58 Armis. (2019). *Armis*. "Urgent/11 11 Zero Day Vulnerabilities Impacting VXWorks, The Most Widely Used Real-Time Operating System (RTOS)." Accessed on July 20, 2020 at https://www.armis.com/urgent11/.

59 Trend Micro. (October 2, 2019). *Trend Micro Security News*. "FDA Warns Against URGENT/11 Vulnerabilities Affecting Medical Devices and Hospital Networks." Accessed on July 20, 2020 at https://www.trendmicro.com/vinfo/ph/security/news/internet-of-things/fda-warns-against-urgent-11-vulnerabilities-affecting-medical-devices-and-hospital-networks.

60 JSOF. (2020). *JSOF*. "Ripple20 19 Zero-Day Vulnerabilities Amplified by the Supply Chain." Accessed on July 20, 2020 at https://www.jsof-tech.com/ripple20/.

61 Trend Micro. (June 22, 2020). *Trend Micro Security News*. "Millions of IoT Devices Affected by Ripple20 Vulnerabilities." Accessed on July 20, 2020 at https://www.trendmicro.com/vinfo/ph/security/news/internet-of-things/millions-of-iot-devices-affected-by-ripple20-vulnerabilities.

62 Trend Micro. (June 25, 2019). *Trend Micro Security News*. "Security 101: Virtual Patching". Accessed on July 27, 2020 at https://www.trendmicro.com/vinfo/ph/security/news/vulnerabilities-and-exploits/security-101-virtual-patching.

63 Trend Micro. (August 27, 2019). *Trend Micro*. "2019 Midyear Security Roundup: Evasive Threats, Pervasive Effects." Accessed on July 20, 2020 at https://documents.trendmicro.com/assets/rpt/rpt-evasive-threats-pervasive-effects.pdf.

64 Trend Micro. (February 25, 2020). *Trend Micro*. "The Sprawling Reach of Complex Threats." Accessed on July 20, 2020 at https://documents.trendmicro.com/assets/rpt/rpt-the-sprawling-reach-of-complex-threats.pdf.

65 Ecular Xu and Joseph C Chen. (January 6, 2020). *Trend Micro Security Intelligence Blog*. "First Active Attack Exploiting CVE-2019-2215 Found on Google Play, Linked to SideWinder APT Group." Accessed on July 20, 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/first-active-attack-exploiting-cve-2019-2215-found-on-google-play-linked-to-sidewinder-apt-group/.

66 CVE - Common Vulnerabilities and Exposures (CVE). (n.d.). *CVE - Common Vulnerabilities and Exposures (CVE)*. "CVE-2019-2215." Accessed on July 20, 2020 at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2215.

67 Elliot Cao et al. (March 24, 2020). *Trend Micro Security Intelligence Blog*. "Operation Poisoned News: Hong Kong Users Targeted With Mobile Malware via Local News Links." Accessed on July 20, 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/operation-poisoned-news-hong-kong-users-targeted-with-mobile-malware-via-local-news-links/.

68 Lorin Wu. (February 6, 2020). *Trend Micro Security Intelligence Blog*. "Malicious Optimizer and Utility Android Apps on Google Play Communicate with Trojans that Install Malware, Perform Mobile Ad Fraud." Accessed on July 20, 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/malicious-apps-on-google-play-communicate-with-trojans-install-malware-perform-mobile-ad-fraud/.

69 Jessie Huang. (June 4, 2020). *Trend Micro Security Intelligence Blog*. "Barcode Reader Apps on Google Play Found Using New Ad Fraud Technique." Accessed on July 20, 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/barcode-reader-apps-on-google-play-found-using-new-ad-fraud-technique/.

70 Trend Micro. (February 25, 2020). *Trend Micro*. "The Sprawling Reach of Complex Threats." Accessed on July 20, 2020 at https://documents.trendmicro.com/assets/rpt/rpt-the-sprawling-reach-of-complex-threats.pdf.

71 Trend Micro. (February 25, 2020). *Trend Micro*. "The Sprawling Reach of Complex Threats." Accessed on July 20, 2020 at https://documents.trendmicro.com/assets/rpt/rpt-the-sprawling-reach-of-complex-threats.pdf.

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

TREND MICRO™ | research

©2020 by Trend Micro, Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, Trend Micro Smart Protection Network, Trend Micro Zero Day Initiative, Trend Micro Smart Home Network, Trend Micro Deep Security, and Trend Micro TippingPoint Threat Protection System are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.