



 TREND
MICRO™

| research 

A Constant State of Flux

Trend Micro 2020 Annual 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

Contents

4

Targeted Attacks Focus on Critical Industries and Lucrative Victims

15

Covid-19 and Remote Work Cause Major Shifts in Cybersecurity

23

Organizations Face Threats in Cloud, IoT, and Mobile Environments

32

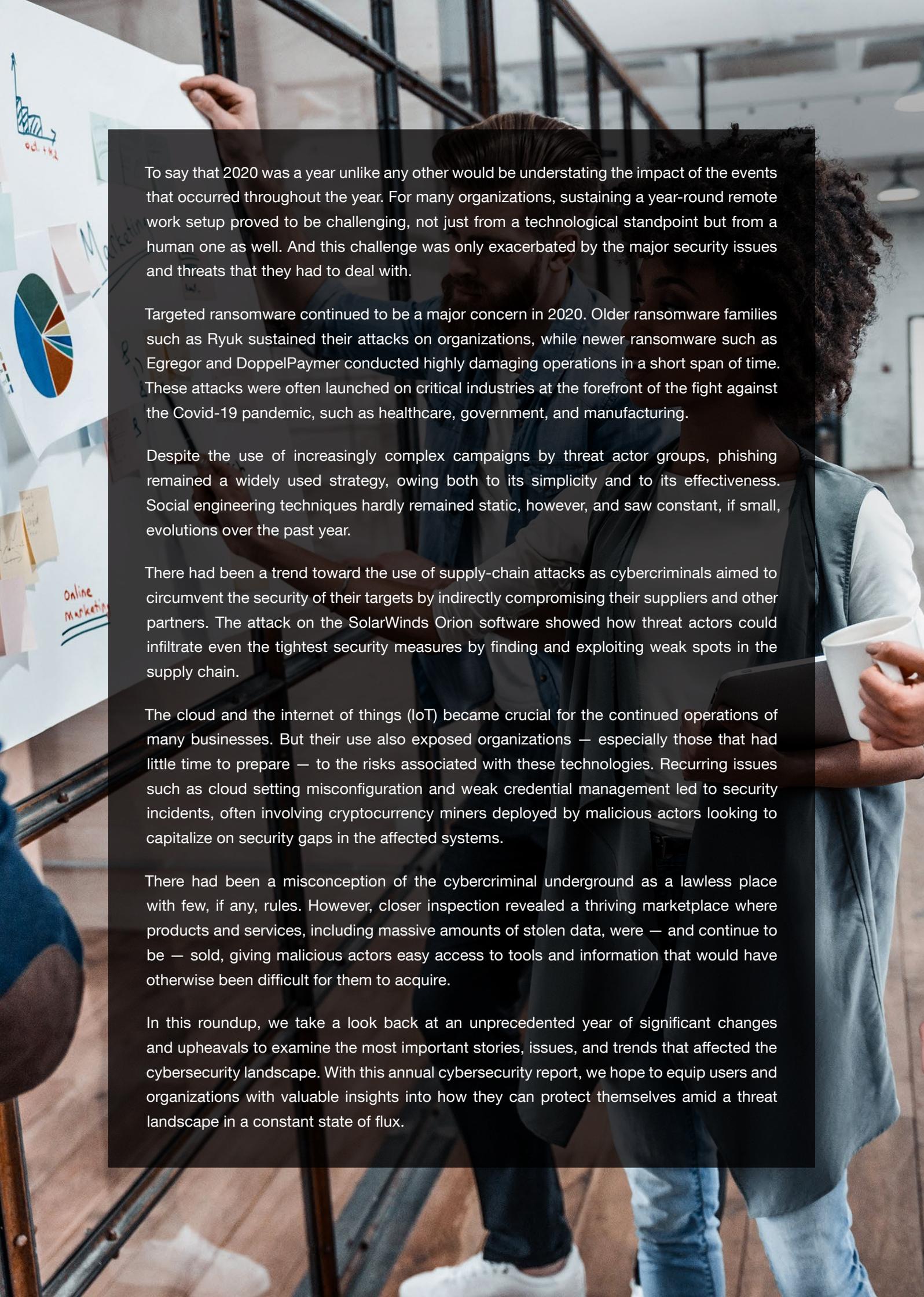
A Greater Number of Dangerous Vulnerabilities Threaten Organizations

35

Modern Threats Require Comprehensive Defense Strategies and Multilayered Security Technologies

37

Threat Landscape in Review

A group of people in a meeting room looking at a whiteboard with charts and graphs. The whiteboard has a line graph, a pie chart, and some text. The text on the whiteboard includes "od. i. k2", "Marketing", and "Online Marketing".

To say that 2020 was a year unlike any other would be understating the impact of the events that occurred throughout the year. For many organizations, sustaining a year-round remote work setup proved to be challenging, not just from a technological standpoint but from a human one as well. And this challenge was only exacerbated by the major security issues and threats that they had to deal with.

Targeted ransomware continued to be a major concern in 2020. Older ransomware families such as Ryuk sustained their attacks on organizations, while newer ransomware such as Egregor and DoppelPaymer conducted highly damaging operations in a short span of time. These attacks were often launched on critical industries at the forefront of the fight against the Covid-19 pandemic, such as healthcare, government, and manufacturing.

Despite the use of increasingly complex campaigns by threat actor groups, phishing remained a widely used strategy, owing both to its simplicity and to its effectiveness. Social engineering techniques hardly remained static, however, and saw constant, if small, evolutions over the past year.

There had been a trend toward the use of supply-chain attacks as cybercriminals aimed to circumvent the security of their targets by indirectly compromising their suppliers and other partners. The attack on the SolarWinds Orion software showed how threat actors could infiltrate even the tightest security measures by finding and exploiting weak spots in the supply chain.

The cloud and the internet of things (IoT) became crucial for the continued operations of many businesses. But their use also exposed organizations — especially those that had little time to prepare — to the risks associated with these technologies. Recurring issues such as cloud setting misconfiguration and weak credential management led to security incidents, often involving cryptocurrency miners deployed by malicious actors looking to capitalize on security gaps in the affected systems.

There had been a misconception of the cybercriminal underground as a lawless place with few, if any, rules. However, closer inspection revealed a thriving marketplace where products and services, including massive amounts of stolen data, were — and continue to be — sold, giving malicious actors easy access to tools and information that would have otherwise been difficult for them to acquire.

In this roundup, we take a look back at an unprecedented year of significant changes and upheavals to examine the most important stories, issues, and trends that affected the cybersecurity landscape. With this annual cybersecurity report, we hope to equip users and organizations with valuable insights into how they can protect themselves amid a threat landscape in a constant state of flux.

Targeted Attacks Focus on Critical Industries and Lucrative Victims

Ransomware Operators Maintain Their Sights on Prominent Targets

Modern ransomware attacks often display characteristics¹ that differentiate them from the more opportunistic ransomware attacks of the past. Instead of using a “shotgun” method, recent ransomware operators are more methodical, typically going after the high-value assets of organizations in critical industries. Their attacks also display an array of techniques such as exploiting unpatched vulnerabilities, abusing weak remote desktop protocol (RDP) security, and using other malware families as part of the routines.

Furthermore, whereas organizations in the past only had to worry about their data being encrypted, ransomware operators have taken things a step further, threatening to prevent organizations from accessing their data while also adding the possibility of leaking stolen data — typically via leak sites — if the victims fail to meet their demands.²

Because of the importance of the targets, ransom demands have increased exponentially over the past few years. According to the insurance company Coalition, the amount being extorted from its policyholders doubled from 2019 to the first quarter of 2020 alone.³

At the forefront of this ransomware evolution were familiar names such as Ryuk and Sodinokibi, prominent among the ransomware families that had largely defined the modern ransomware landscape. 2020 also saw the rise of relatively new ransomware such as Egregor and DoppelPaymer, both of which already made their mark, especially during the second half of the year.

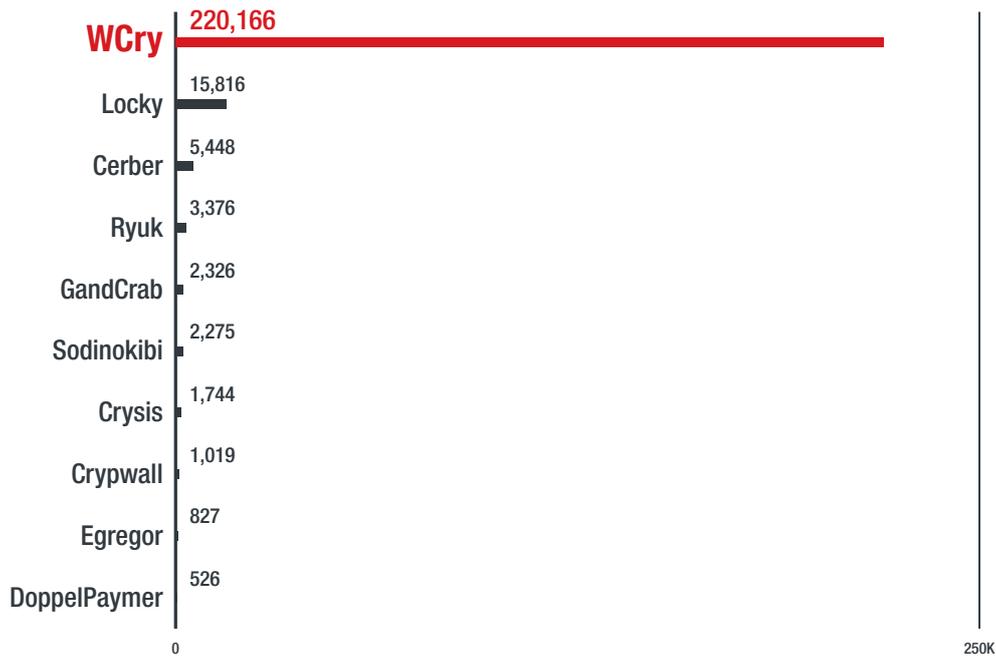


Figure 1. Egregor and DoppelPaymer both ranked in the top 10 despite being relatively new ransomware families:
The 10 most detected ransomware families in 2020

Source: Trend Micro™ Smart Protection Network™ infrastructure

Despite a few quiet months in 2020, Ryuk continued to plague organizations in essential industries. After starting the year with an attack on the US government contractor Electronic Warfare Associates (EWA) in February,⁴ Ryuk kept a relatively low profile from May to September before ending the year with a series of high-profile campaigns against organizations in the healthcare sector — even prompting an advisory from the US Cybersecurity and Infrastructure Agency (CISA) regarding its activities.⁵

Ryuk has traditionally been known to employ a sizeable range of delivery methods, perhaps the most common being the use of other malware such as Emotet and Trickbot. It has also been observed employing certain tools that are not necessarily malicious per se but have been known to be exploited for malicious purposes. These include the penetration software Cobalt Strike⁶ and Metasploit,⁷ and the post-exploitation framework PowerShell Empire.⁸ Many of these can actually serve as early warning signs of an impending ransomware attack, if detected in the initial stages.

In late 2020, Ryuk added yet another weapon to its arsenal: a new dropper known as BazarLoader (or BazarBackdoor), a loader trojan distributed through phishing emails containing attachments or links to malicious websites.⁹ While BazarLoader is not particularly noteworthy in and of itself, that operators are continuously adding capabilities to Ryuk means that vulnerable industries should be particularly wary of the ransomware in the months or even years to come.

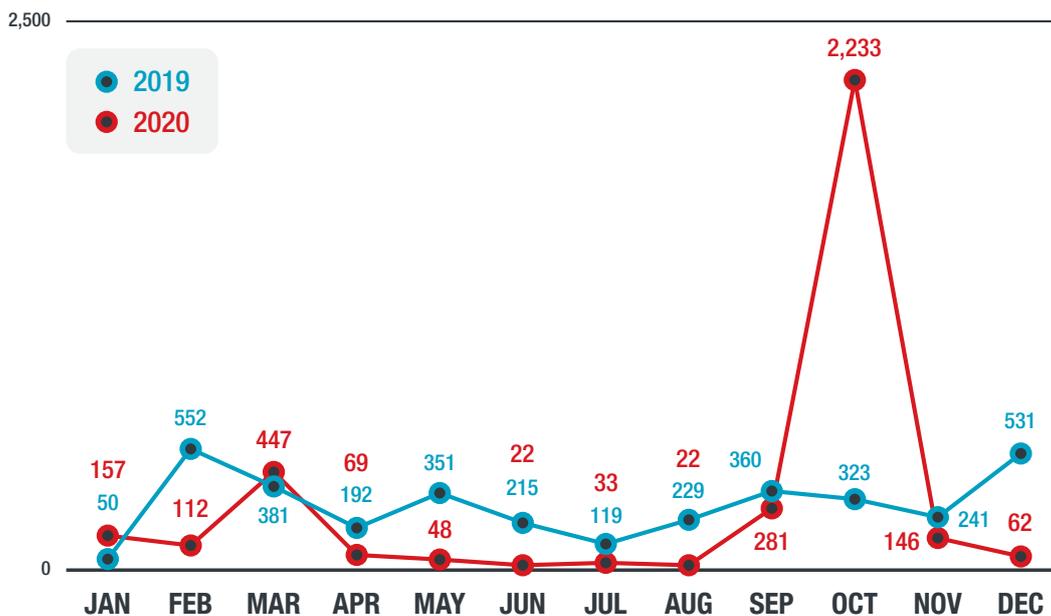


Figure 2. A spike in detections of Ryuk occurred in October 2020:
A comparison of the numbers of detections of Ryuk in 2019 and 2020

Source: Trend Micro Smart Protection Network infrastructure

Aside from Ryuk, a number of new families made their presence felt in 2020. Among the more notable ransomware families from the year’s batch were Nefilim and ColdLock, which were both discussed in our 2020 midyear cybersecurity report.¹⁰

In September, Egregor first made an appearance, eventually leading to a string of high-profile attacks on major retailers in December.¹¹ Considered a possible spinoff of the Sekhmet ransomware because of certain shared characteristics,¹² Egregor has been mentioned as the replacement of choice for the previous affiliates of the now-retired Maze ransomware.¹³ One interesting characteristic of Egregor is that it is typically distributed as a payload alongside the remote access trojan (RAT) Qakbot, which suggests either that there is a partnership between the malicious actors behind Egregor and Qakbot or that Egregor is a new payload from the actors behind Qakbot.¹⁴

The operators of Egregor implement the same double extortion technique used by operators of other modern ransomware families, whereby an attacker pressures the victim into paying the ransom by threatening the release of stolen information through a leak site. Facing a two-pronged predicament — public exposure as well as loss of data — the victim would be compelled to yield to the attacker’s demand.

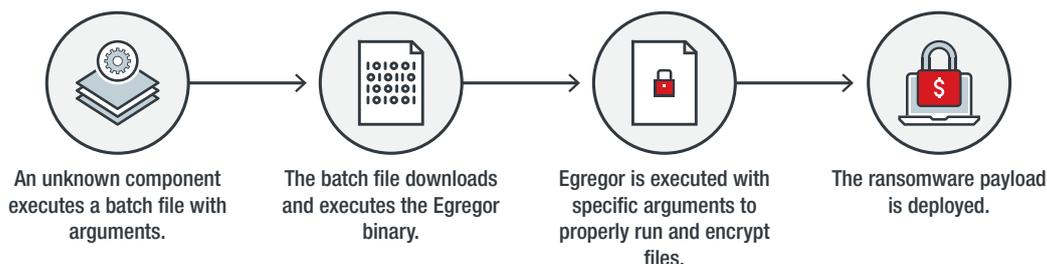


Figure 3. The attack chain of the Egregor ransomware

Another prominent ransomware that made waves in 2020 was DoppelPaymer.¹⁵ Although not a new ransomware family — it had been active since 2019 — DoppelPaymer surged in activity in late 2020 to the extent that the US Federal Bureau of Investigation (FBI) was forced to release an advisory warning organizations about its attacks.¹⁶

DoppelPaymer is believed to be based on BitPaymer, an older ransomware family that targets medical organizations,¹⁷ as they share similarities in code, ransom notes, and payment portals. DoppelPaymer employs advanced techniques such as requiring the correct command-line parameter in order to run (possibly implemented to avoid detection and analysis). It also uses various tools such as Process Hacker, which terminates services and processes to prevent access violation during the encryption routine.¹⁸

As with other cases of targeted ransomware, DoppelPaymer’s primary targets are organizations in critical industries such as healthcare, emergency services, and education.

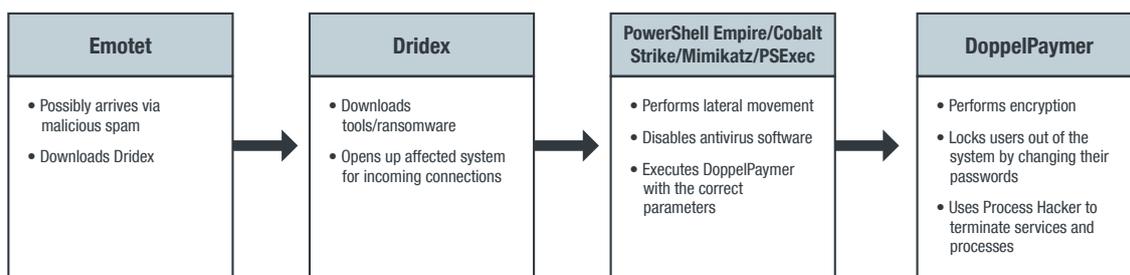


Figure 4. The infection routine of the DoppelPaymer ransomware

As we can observe from these and other campaigns, ransomware operators ramped up attacks on critical industries such as government and healthcare, perhaps because of how important they were in dealing with the Covid-19 pandemic. The manufacturing industry also became a prime target for ransomware operators.¹⁹ A ransomware attack on a manufacturing facility could have grave consequences for the victim organization, such as disruptions in business and supply chain operations, delays in product engineering and design, and even data theft. Banking was another frequently targeted industry, presumably because of the size and wealth of the companies involved in the field.

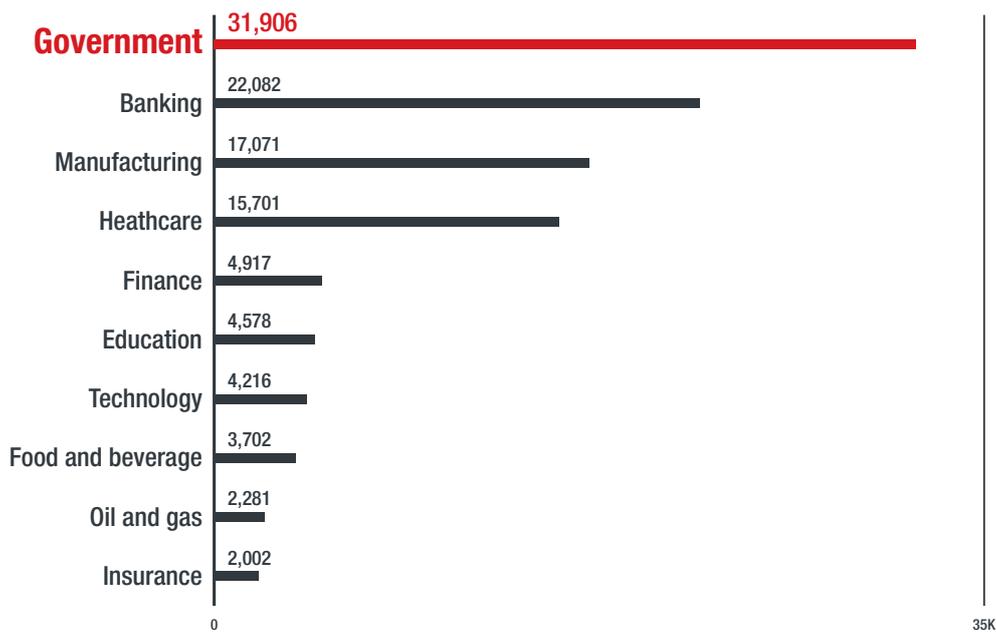


Figure 5. Government, banking, manufacturing, and healthcare were the industries hit hardest by ransomware attacks: The 10 industries most targeted by ransomware attacks in 2020

Source: Trend Micro Smart Protection Network infrastructure

Ransomware operators have also been expanding their target range to other operating systems. For instance, although RansomExx does not appear in the list of the 10 most detected ransomware families in 2020, it was still notable for having a variant that was used to attack Linux servers. Based on our analysis, RansomExx’s main target is the general VMware environment, that is, machines that are used for storing VMware files.²⁰

Campaigns Take Aim at Specific Demographics Using Sophisticated Tools and Techniques

In addition to targeted ransomware attacks, we observed a number of campaigns from both veteran threat actors and newer groups.

Many of these campaigns exhibited complicated structures and processes, indicating that although the campaigns seemed to be fairly new, the people behind it were not. In October, we published a research paper on a campaign we called Earth Kitsune, which involved threat actors compromising North Korea-related websites and using them to host malware.²¹

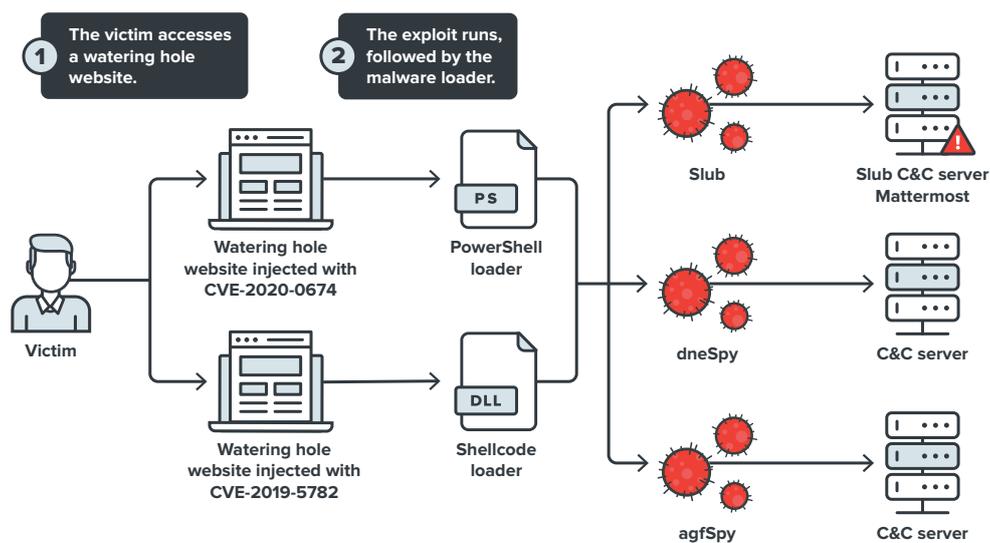


Figure 6. The infection chain used by the Earth Kitsune campaign

Earth Kitsune employed two vulnerabilities, the Google Chrome vulnerability CVE-2019-5782 and the Internet Explorer vulnerability CVE-2020-0674, to compromise the target websites. It also used a trio of backdoors: Slub for exfiltrating information, and agfSpy and dneSpy for gaining additional control over an affected user's machine.

Our follow-up research on Earth Kitsune²² painted a picture of a complex and expansive campaign that combined a large infrastructure with a wide array of tools and exploits. In other words, the campaign was carried out not by mere amateurs but by a group of experienced and skilled actors who had their eyes set on a very specific demographic.

We also tracked a campaign called Earth Wendigo,²³ which had very similar themes and motives. Like Earth Kitsune, this campaign targeted a particular group of people: in its case, individuals with an interest in issues concerning Tibet, the Uighur region, and Hong Kong. The goal of the threat actor behind this campaign was to obtain information via exfiltrated mailboxes.

Earth Wendigo gains initial access to a system via spear-phishing emails that contain obfuscated JavaScript code, which then loads malicious scripts from a remote server. The scripts are designed for a variety of functions, including infection of the target via two methods. The first method involves the exploitation of a cross-site scripting (XSS) vulnerability on the webmail system, while the second involves the registration of malicious JavaScript code to a web browser feature known as Service Worker. For lateral movement, the campaign uses malicious code injection to modify the victim's email signature.

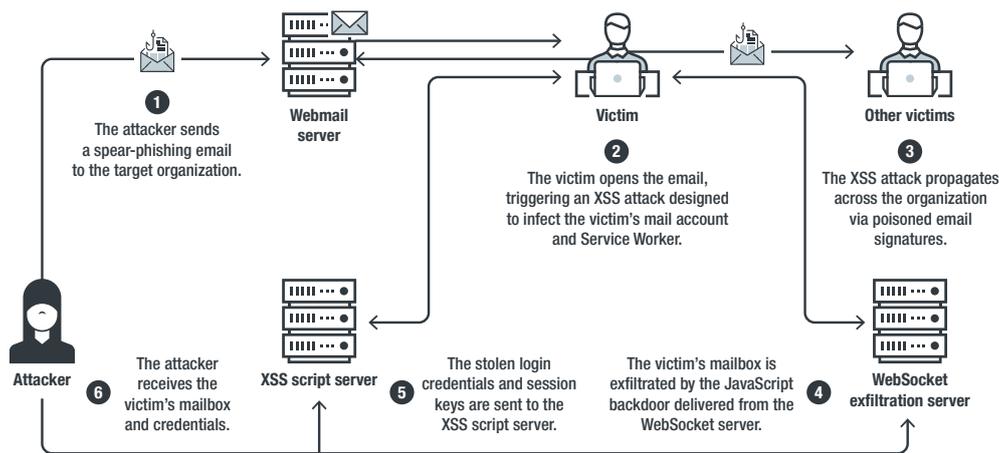


Figure 7. The attack flow used in the Earth Wendigo campaign

Aside from these campaigns from newer groups, we also tracked the activities of SideWinder, a group that primarily operates in the South Asian region. The group was particularly active in 2020, launching spear-phishing attacks that had Covid-19-related themes or discussed territorial disputes and other diplomatic issues between South Asian countries and China.²⁴ Apparently, SideWinder's primary social engineering technique was the use of current events in luring its victims into visiting its phishing pages.

To accommodate the increasing complexity of their campaigns, malicious actors have had to look beyond their repertoire and employ external tools and services for their activities. As discussed in a research paper we published last year, the access-as-a-service model, which involves underground sellers providing access to hacked devices and enterprise networks, has become popular with cybercriminals looking to gain a foothold into their targets' systems. The levels of access being sold vary, from simple account credentials and RDP access to full network access in some cases.²⁵ Notable users of this model include the operators of Ryuk, who have been observed using third-party malware such as Trickbot to gain access to infected networks.²⁶

Threat Actors Employ Basic but Effective Techniques

While we saw campaigns from highly skilled groups such as the ones that created Earth Kitsune and Earth Wendigo, we also found other threat actors relying on less complex methods in their operations.

The Pawn Storm group had been active since it first emerged in 2004, when it launched a number of attacks on groups and individuals involved in high-profile industries.²⁷ But in 2020, instead of going for the more complex strategies employed by other threat groups, Pawn Storm seemingly opted for more mundane fare in some of its campaigns. It used fairly basic techniques such as brute-force attacks on

internet-facing services and common tools such as RATs.²⁸ In fact, had it not been for our experience and knowledge with the tools and techniques used by Pawn Storm, it would have been difficult to attribute these campaigns to the group based purely on analyzed samples.

Indeed, just because a technique is simple does not mean that it is inherently less successful than a sophisticated one. A strong testament to this is phishing, which remains highly effective despite being one of the oldest tricks in the book. At its core, phishing is a very simple technique. An attacker does not need to have technical skills or knowledge to perform phishing; all that is needed is an innate understanding of human psychology and some form of social engineering designed to exploit it.

However, phishing techniques do not remain static. In fact, they are also constantly evolving. An example of this evolution is a trend we observed in 2020: the use of form builder services, such as those used to create surveys, to host phishing sites.²⁹

One of the primary appeals of form builders is that, unlike fake domains and website builders, they require only basic knowledge on how forms are made and little time to set up. While this means that pages made with form builders typically look amateurish in comparison with fake domains that are painstakingly built from scratch, it also means that even inexperienced would-be cybercriminals can effortlessly create and use them for phishing schemes. Fortunately, most organizations do not use forms for important processes such as password updates or email verification, so it should be relatively easy for potential victims to spot form-based phishing scams.

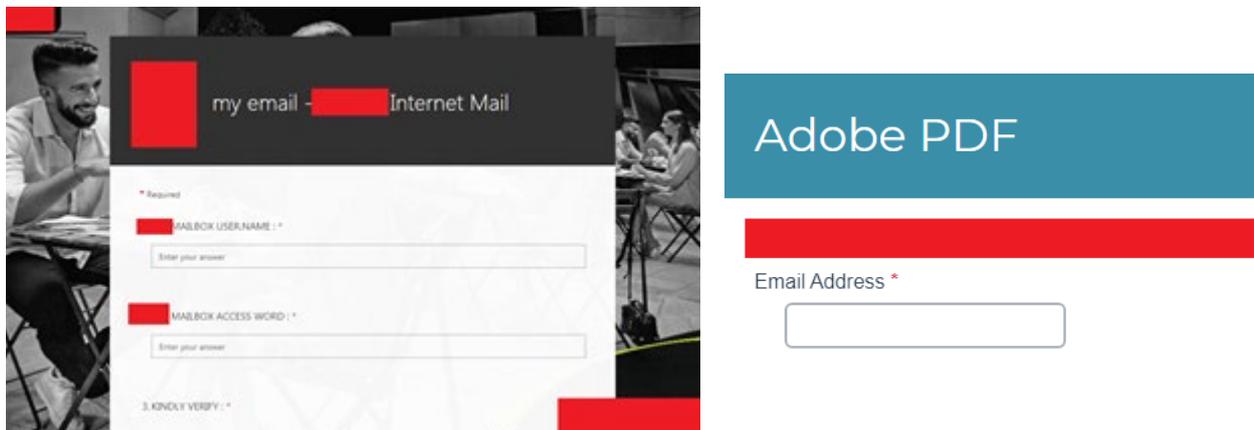


Figure 8. Examples of an email credential phishing form (left) and a fake Adobe login page made from a form (right)

Comparing the year-on-year numbers in our phishing data, we observed an interesting change. While the number of blocked non-unique phishing URLs decreased, the number of blocked unique phishing URLs increased. One possible reason for this is that malicious actors had become less reliant on recycling phishing URLs for their campaigns and more intent on tailoring URLs based on their targets.

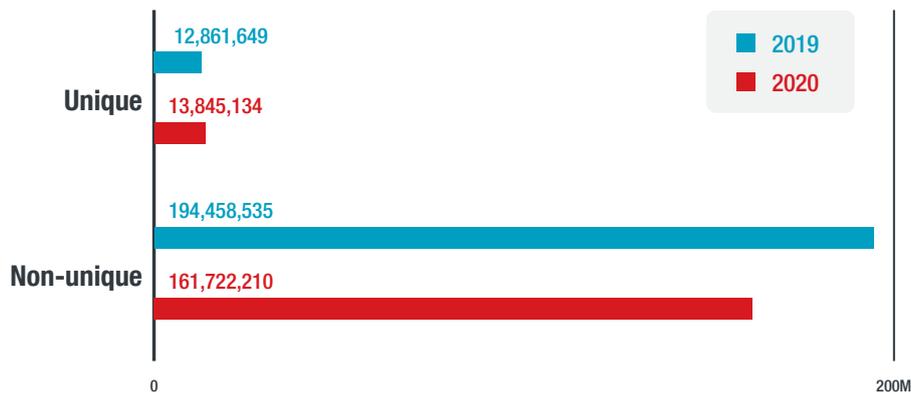


Figure 9. Blocked unique phishing URLs increased while blocked non-unique ones decreased: A comparison of the numbers of blocked unique phishing URLs (e.g., three instances of blocked access to the same URL on the same machine counted as one attempt) and the numbers of blocked non-unique phishing URLs (e.g., three instances of blocked access to the same URL on the same machine counted as three attempts) in 2019 and 2020

Source: Trend Micro Smart Protection Network infrastructure

We also observed a 38% decrease from 2019 to 2020 in blocked phishing URLs that spoofed Microsoft 365 (formerly Office 365), one of the most widely used productivity software suites in the world, which includes the popular email application Outlook. However, this should not be taken as a sign that malicious actors had dialed down their attacks; it is possible that they had expanded their repertoire with the rise in usage of other essential work tools such as communication apps.

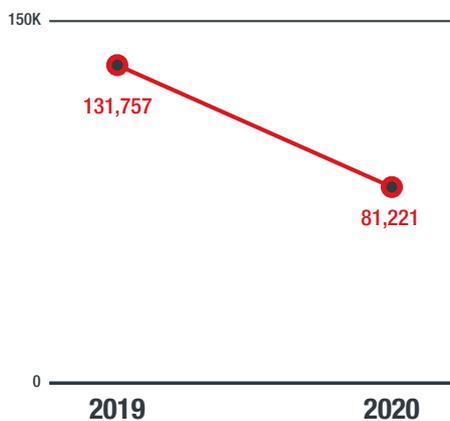


Figure 10. The number of blocked unique phishing URLs that spoofed Microsoft 365 (including Outlook) decreased by 38%: A comparison of the numbers of blocked unique Microsoft 365-related phishing URLs in 2019 and 2020

Note: Data included queries for Office 365.

Source: Trend Micro Web Reputation Service

Our data shows that there were millions of attempts to access the top phishing domains, proving how effective they were in luring victims. In addition, the top domains in terms of access attempts per unique visitor had counts in the hundreds of thousands.

URL	Count
clk.apxadtracking.net	27,722,234
apc994.com	5,558,410
157.240.2.20	4,667,619
p01.notifa.info	3,185,011
api.bdisl.com	2,441,834
newgirlseveryday.info	1,831,524
lopw.page.link	1,778,225
kolw.page.link	1,751,821
johr.page.link	1,737,865
firebasestorage.googleapis.com	1,710,295

Table 1. There were millions of attempts to access the top 10 phishing domains, with the topmost URL alone accounting for more than 27 million non-unique access attempts: The 10 phishing URLs with the most blocked non-unique access attempts (e.g., three instances of blocked access to the same URL on the same machine counted as three attempts) in 2020

Source: Trend Micro Smart Protection Network infrastructure

URL	Count
www.vrspacely.com	241,022
apc994.com	217,267
peachtrackercn.com	214,550
clk.apxadtracking.net	167,951
p01.notifa.info	119,762
api.dot-metrix.com	119,148
qwertyamerica.com	116,230
api.bdisl.com	116,201
sw.wpu.sh	101,121
d11yldzmag5yn.cloudfront.net	97,498

Table 2. On a per-unique-machine basis, there were hundreds of thousands of attempts to access the top phishing domains: The 10 phishing URLs with the most blocked unique access attempts (e.g., three instances of blocked access to the same URL on the same machine counted as one attempt) in 2020

Source: Trend Micro Smart Protection Network infrastructure

Threat Actors Continue to Compromise Organizations via Supply Chains

While it is difficult for threat actors to directly attack organizations with strong security systems in place — for example, government entities that house extremely sensitive data — they could circumvent these defenses by indirectly compromising the less secure portions of the organizations' supply chains.

In essence, a supply-chain attack takes advantage of the trust model between an organization and its suppliers to allow an attacker to gain a foothold into the target's system. This makes it difficult to counter or even detect. Not only do organizations implicitly assume that the products and services offered by their partners are safe to interact and conduct business with, but they also often have no way to actively check for threats lurking in their supply chains beyond what they can see in their own systems.

Supply-chain attacks had become so notorious that in February 2020, the FBI issued a security alert concerning them. In particular, the alert warned of supply-chain attacks being launched by threat actors on software companies in order to obtain access to their strategic partners, including organizations supporting industrial control systems in the energy industry.³⁰ These were done via Kwampirs, a RAT that was used to gain entry to the victims' machines and networks, after which follow-up activities could be performed, such as delivering additional components or payloads.³¹

One of the most highly publicized supply-chain attacks in recent years was the attack involving SolarWinds. In December, reports began circulating about a sophisticated attack targeting several organizations, including US government agencies, via a compromised update of Orion, SolarWinds' widely used network management system software.³² Given the nature of some of the targets, the attack could have far-reaching consequences.

According to the information provided by the company, the malicious actors behind the attack inserted a vulnerability into certain Orion software builds that could allow attackers to compromise servers running Orion.³³ This meant that once the relevant update was pushed to customers, the attackers were able to deploy a powerful backdoor, known as Sunburst, on the affected machines. Once implanted into the systems, Sunburst gave the attackers complete access to the affected networks. The attackers could then issue commands to gather system information, write and delete files, create and delete registry keys, and disable analysis tools, among other malicious activities. A second-stage payload, a backdoor known as Supernova, was also part of the attack. The attackers used Supernova to inspect and respond to HTTP requests via appropriate HTTP query strings, HTML form values, and cookies, and to execute web shell commands through a specific HTTP request format.³⁴

Covid-19 and Remote Work Cause Major Shifts in Cybersecurity

Malicious Actors Take Advantage of Global Pandemic and Other Significant Events

Malicious actors notably capitalized on the 2020 US elections, specifically the presidential election, to prey on people's desires to get involved by setting up election-related scams.³⁵ And it was not just run-of-the-mill cybercriminals who were active during the runup to the elections either. Even several major advanced persistent threat (APT) groups were reported to have been participating in campaigns targeting individuals and groups associated with major presidential candidates and with general political and advocacy groups.³⁶

Of course, it would be difficult, if not impossible, to talk about cybersecurity in 2020 without discussing how it was affected by the global Covid-19 pandemic. As we covered in our 2020 midyear cybersecurity report, malicious actors began taking advantage of the situation to hatch up a slew of Covid-19-themed threats.³⁷

In 2020, we detected more than 16 million Covid-19-related threats, consisting of malicious URLs, spam, and malware. Nearly 90% of these detections were malicious spam, indicating that spam emails were the preferred avenue for malicious actors, likely because of their accessibility and simplicity relative to malicious URLs and malware, which require some technical knowledge and planning. The bulk of these detections came from the US, Germany, and France, which were also among the countries that had been hit hardest by the pandemic.

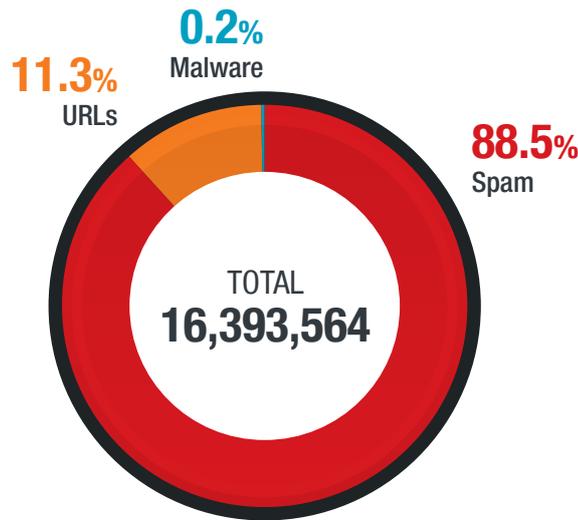


Figure 11. Nearly 90% of detections of Covid-19-related threats were malicious spam:
The distribution of detections of Covid-19-related threats in 2020 by type

Source: Trend Micro Smart Protection Network infrastructure

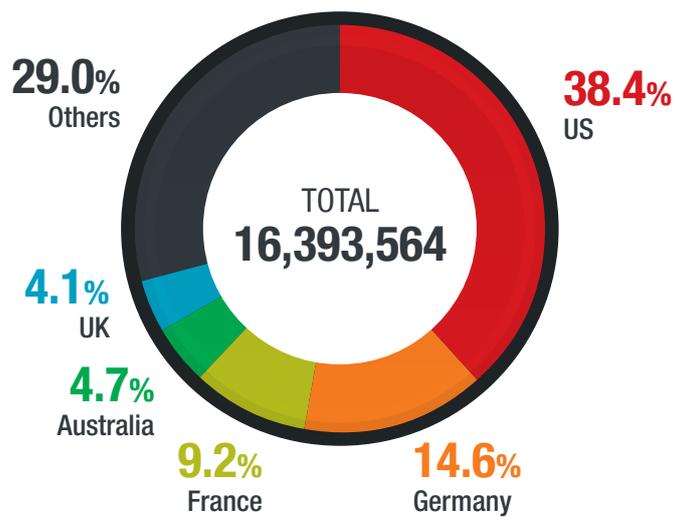


Figure 12. The bulk of detections of Covid-19-related threats came from the US, Germany, and France:
The distribution of detections of Covid-19-related threats in 2020 by country

Source: Trend Micro Smart Protection Network infrastructure

In the first half of the year, Covid-19-based threats focused on either causing alarm to recipients or allegedly providing information about the pandemic. For instance, many of the early spam emails discussed symptoms of the viral disease.³⁸

The scammers behind these threats tailored their techniques to whatever new and current information was available. For example, with the benefits of the original Covid-19 stimulus package provided by the

US government nearing its expiry date,³⁹ malicious actors took advantage of the time-bound situation by sending text messages to potential victims stating that they had received a certain amount as part of the package. Included in the text was a link to a phishing page designed to steal personal and financial information.⁴⁰

Another major development was the initial rollout of Covid-19 vaccines from different drug companies in the second half of the year. As expected, cybercriminals promptly followed suit with their own doses of vaccine-related scams. Some offered fake vaccines for varying amounts, even setting up domains (some of which included malware) to fool their victims.⁴¹ Other scammers resorted to phishing emails, sent not just to the general populace but also to people involved in the vaccine supply chain.⁴²

Unsurprisingly, business email compromise (BEC) scammers also banked on the pandemic, as Covid-19-related subject lines made up the highest number among the BEC samples we detected. Many of the subject lines were vague, with some even referring to unrelated topics such as invoice or payment requests. However, even these emails found a way to use the terms “Covid” or “Covid-19,” likely as a way to garner their victims’ attention.

“Re: COVID-19”
“Re: Covid-19 update”
“COVID-19 QUICK REPLY”
“Important Message on COVID-19”
“COVID-19...Fwd: April Invoices”
“COVID-19 Shut down”
“COVID-19 issue”
“COVID-19...Fwd: May Invoices”
“Fwd: Covid-19 update”
“Re: Covid positive donors”
“COVID-19 RESPOND”
“COVID-19/FluA+B Antigen Combo Rapid Test”
“Covid Task Force”

Table 3. Examples of the subject lines we encountered in BEC attempts that referenced Covid-19 in 2020

Overall, however, the number of BEC attempts we detected in 2020 decreased by 17% year on year from 2019.

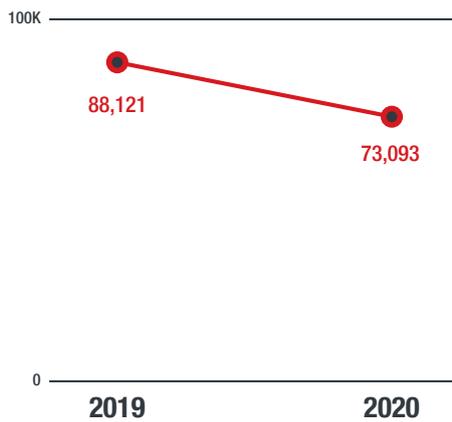


Figure 13. While the overall number of BEC attempts declined, BEC scammers were able to capitalize on the Covid-19 pandemic: A comparison of the numbers of detected BEC attempts in 2019 and 2020

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

The CEO and the managing director/director continued to be the positions most spoofed by BEC scammers, accounting for more than half of all spoofed positions. Meanwhile, finance managers and directors of finance remained the most targeted; they were targeted in nearly a third of BEC attempts. Professors were the third most common target of BEC attempts, showing that scams on educational institutions continued to be rampant.

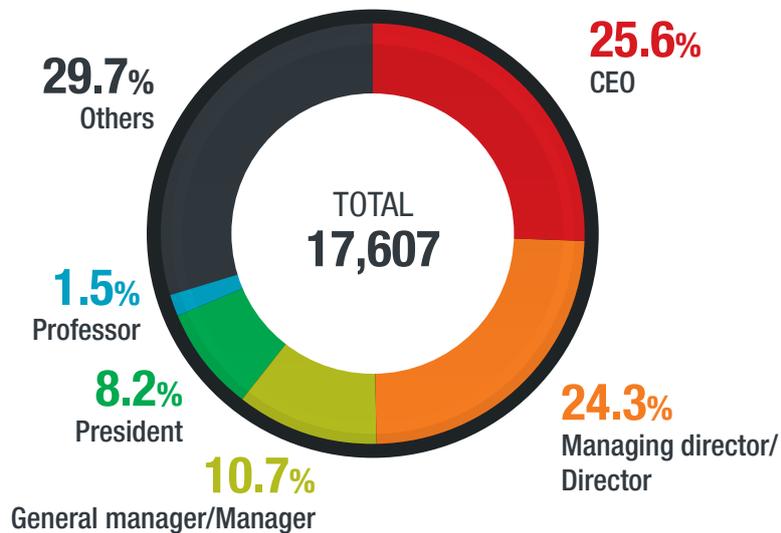


Figure 14. The CEO remained the most spoofed position in BEC attempts, closely followed by the managing director/director: The distribution of spoofed organizational positions in detected BEC attempts in 2020

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

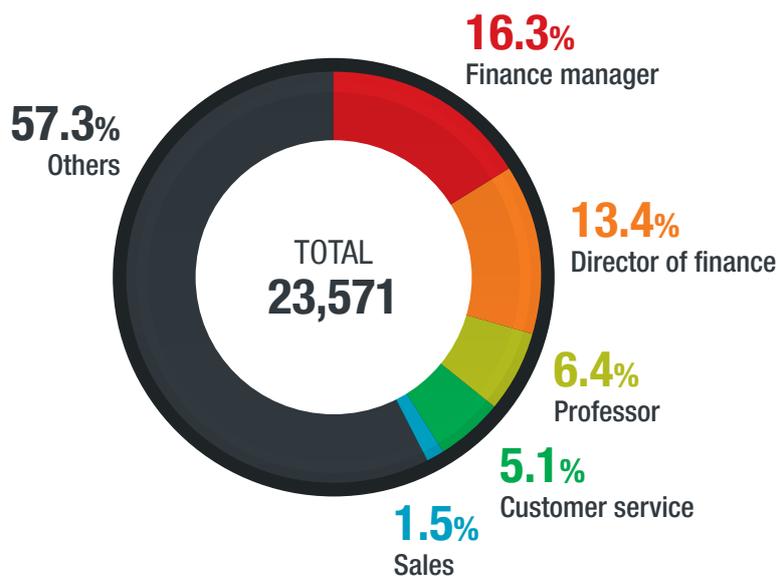


Figure 15. Finance managers, directors of finance, and professors were the most frequently targeted positions in BEC attempts: The distribution of targeted positions in detected BEC attempts in 2020

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

One of the hallmarks of BEC attacks is that its perpetrators do not need to have a complex infrastructure to pull off successful attacks. Scammers can even use public cloud infrastructure, as we observed in the Water Nue BEC campaigns. This series of campaigns, which started in March, targeted senior executives in the US and Canada to obtain account credentials for further malicious activities. Once compromised, these accounts were used to send fund transfer requests to lower-ranking staff. The fraudsters behind Water Nue used legitimate cloud-based email services such as SendGrid to deliver their emails. While this might sound like a typical BEC attack pattern, with no noteworthy characteristics other than the use of the cloud service, the Water Nue campaigns had collected more than 800 credentials at the time of our analysis, showing that even seemingly ordinary BEC campaigns could still have the potential to do damage.⁴³

We also encountered a new modus operandi in 2020 aimed at French companies wherein cybercriminals used fake tax fraud emails — apparently from the French tax system itself — to gather information about their victims. The PDF letter (built from an actual PDF file used by the tax system) included in the email looked quite convincing, while the email address used to send the email was very similar to the official email address of the French tax system. After obtaining the information they needed, the scammers behind the scheme would then send bogus emails to their target’s customers requesting banking account reference changes in favor of an account presumably controlled by the scammers.⁴⁴

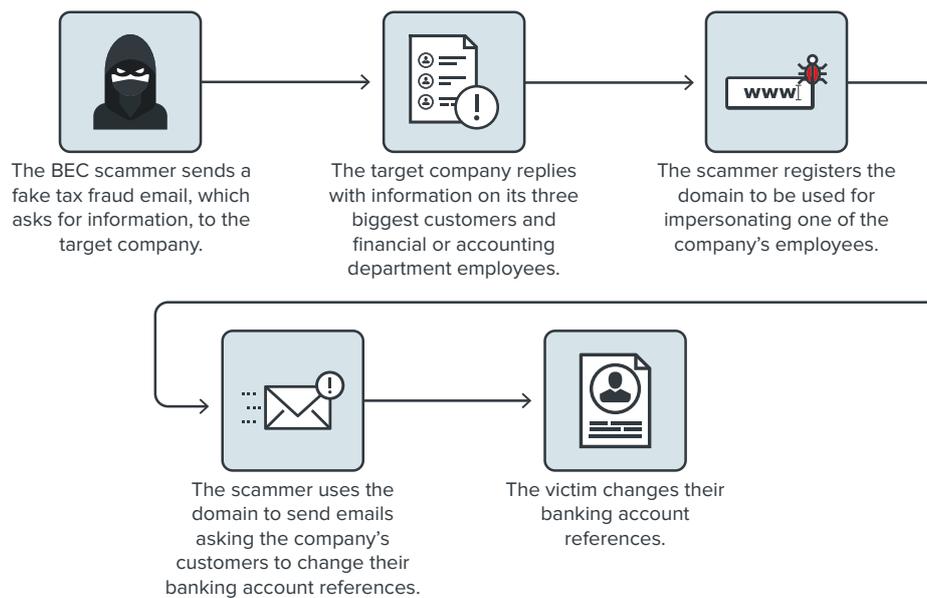


Figure 16. The method used by BEC scammers in the French BEC campaign in 2020

Remote Work Presents Challenges for Organizations

The pandemic forced a shift away from the traditional office structure toward a work-from-home (WFH) setup for a large number of organizations. While it provided certain benefits for organizations and employees alike, such as less expense on infrastructure and reduced costs for travel, remote work was not without its own set of challenges, especially from a cybersecurity perspective.

While some organizations might have already had some form of remote work option in place for employees before the pandemic, migrating the majority of workers to the same setup meant having to stress-test critical systems to ensure that they would operate effectively even under heavy loads.⁴⁵ Furthermore, organizations also had to ensure that their employees were provided all the support and training they needed to work effectively from home. There was also a need to look beyond infrastructure. To help close security gaps, enterprises needed to introduce or reinforce policies that focused on security and that would help remote workers secure their own home workspace.

To that end, virtual private networks (VPNs) became indispensable tools for organizations in protecting network connections from external threats. In fact, bolstered by the WFH arrangements implemented by organizations around the world, usage of VPNs reached an all-time high in 2020.⁴⁶

It is important to note, however, that VPNs are not the be-all and end-all of security technology. They can be and are abused by malicious actors for cyberattacks. Like any software, VPN solutions could also be host to various vulnerabilities, which, if exploited, could provide attackers ways to compromise their targets' systems.

One of the most notable and widespread VPN vulnerabilities is CVE-2019-11510, a critical arbitrary file disclosure flaw in the VPN product Pulse Connect Secure that could allow remote attackers to obtain usernames and plain-text passwords from affected machines.⁴⁷ Despite being relatively new, CVE-2019-11510 already accounted for nearly 800,000 detections in 2020 alone. It had already been involved in actual attacks, including ones in 2020 where it was exploited to deliver the Sodinokibi ransomware.⁴⁸

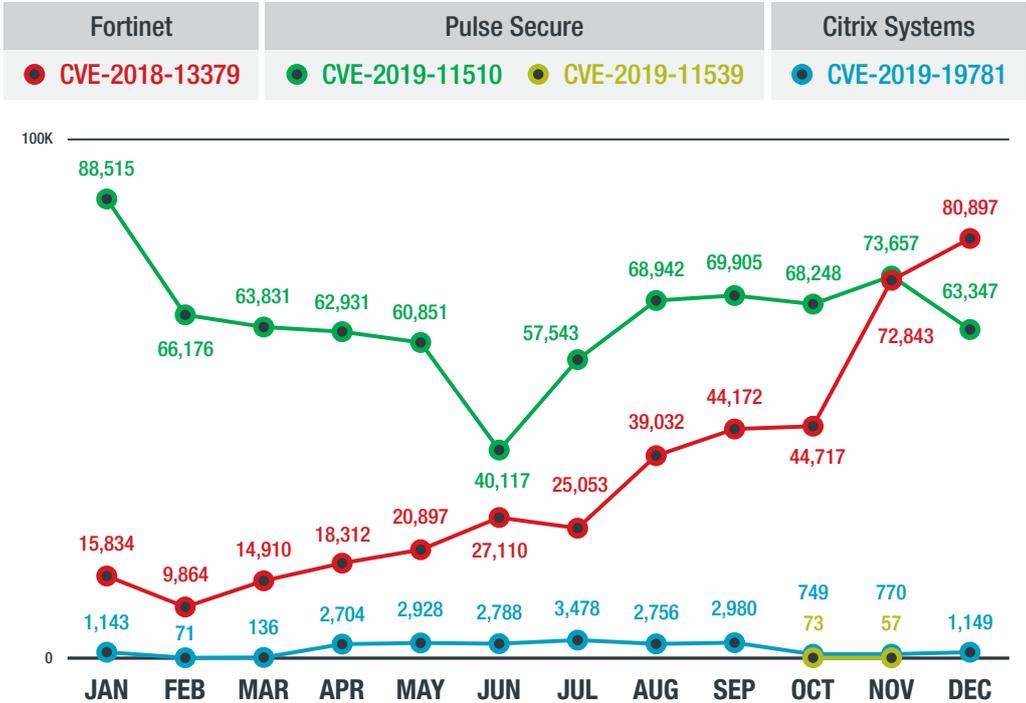


Figure 17. The detections for CVE-2018-13379 rose sharply in the fourth quarter, while the opposite occurred for CVE-2019-19781; detections for the Pulse Secure vulnerability CVE-2019-11510 remained fairly consistent on a per-month basis: A monthly comparison of the detection counts of notable VPN vulnerabilities in 2020

Source: Trend Micro Digital Vaccine filters

Malicious actors also found other ways to incorporate VPNs in their attacks. In September, we published our analysis of an instance where an attacker bundled a VPN installer with the Bladabindi backdoor, which could be used to gather information from infected machines.⁴⁹ Cases like this show that, in addition to updating their VPN software regularly to ensure that existing vulnerabilities are addressed, VPN users should be mindful of where they download their software.

The transition to remote work also led to increased reliance on communication tools such as Zoom, Slack, and Discord. This, in turn, led to an increase in attacks that targeted or used these applications.⁵⁰

“Zoombombing,” in which unwanted users would intrude on ongoing Zoom meetings, was one of the more common methods of communication app abuse. And while it could be highly disruptive at times, ultimately most instances of Zoombombing amounted to nothing more than harmless, if annoying, pranks. Other types of Zoom-related attacks, though, were more damaging. Some malicious actors resorted to using Zoom installers — either legitimate ones bundled with malware or malware disguised as installers — to trick users into installing various payloads on their machines.⁵¹

Slack and Discord were also incorporated by cybercriminals into their attacks. One of these involved Crypren, a ransomware variant that had a unique method of reporting its victims’ encryption status back to the command-and-control (C&C) server: via Slack webhooks. We also found samples showing how Discord was used in an email spam campaign that delivered malware to its victims’ machines.⁵²

Organizations Face Threats in Cloud, IoT, and Mobile Environments

Cloud Misconfiguration Is Still a Problem for Many Organizations

In 2020, the cloud became an even more integral part of the operations of many organizations. According to the 2020 Cyber Risk Index, the area of cloud computing infrastructure and providers was ranked as one of the chief areas of concern for organizations.⁵³

The cloud has indeed become critical to a properly functioning enterprise, even more so in a remote working environment. Cloud-based services offer many benefits to enterprises, especially with regard to cost efficiency, agility, and scalability. However, it would be a mistake to consider the cloud as a turnkey solution that organizations should not have to worry about in terms of security. Securing the cloud is not without its own set of challenges.⁵⁴ One aspect of cloud infrastructure that is often overlooked is the proper configuration of cloud assets and services, leading to misconfiguration remaining a major risk in cloud environments, as seen in the various incidents in 2020 that were primarily caused by misconfigured cloud software and infrastructure.

Traditionally, malicious actors use vulnerability exploitation to execute remote code, a crucial step in gaining a foothold in a target system. However, some of the incidents we observed in the past year instead involved attackers looking for open APIs to exploit. In April, it was reported that attackers had dropped cryptocurrency miners on misconfigured Docker daemon API ports via the Golang-based Kinsing malware. One notable characteristic of Kinsing is its ability to hide the presence of malicious components through the use of a rootkit, making its activities even more difficult to detect for affected users.⁵⁵

A month later, we analyzed a bot from the threat actor group TeamTNT that was designed to mine cryptocurrency and perform distributed denial-of-service attacks.⁵⁶ The main target of this bot was, again,

open Docker daemon ports. And toward the end of the year, we observed more malicious activities from the group as it evolved its attacks further. Its December attack saw the group adding propagation functionalities and the ability to steal Amazon Web Services (AWS) Secure Shell (SSH) credentials.⁵⁷ However, none of these attacks would have been possible without some form of misconfiguration or security gap in the infected system. In these cases, the group needed to perform remote code execution on the system by taking advantage of instances of misconfiguration, weak or stolen credentials, or vulnerabilities.

In October, we also reported on a unique attack on exposed Docker APIs that involved the use of the Metasploit Framework (MSF) shellcode as a payload — the first time we observed the use of such a technique.⁵⁸ This is notable since a typical attack on exposed Docker APIs involves cryptocurrency miners.

Cybercriminals Take Advantage of Underground Cloud Infrastructure

Ironically, it is not just enterprises that benefited from cloud services in 2020, as we found in our extensive research into how malicious actors used the cloud in the past year.

In the cybercriminal underground, malicious actors regularly interact and deal with one another. There are even cases where cybercriminals work with one another to perform various tasks — for example, one group or individual can be responsible for accessing a victim’s system, while another group provides the C&C infrastructure — essentially commodifying underground services. There is also an extensive list of cloud-based services being peddled in the underground. These range from simple dedicated hosting services to more niche offerings such as mobile workspaces and telecommunication-related services, all of which could help malicious actors with their activities.⁵⁹

In recent times, we have seen a number of attacks where data is stolen by cybercriminals. Often the amount of stolen data is such that individual cybercrime groups are unable to fully use all the information even if they want to. As a result, some underground elements have resorted to renting out their “clouds of logs” to other cybercriminals.⁶⁰

Some of these offerings even have pricing models, depending on the level of access they provide. The data found in these sets also varies, with the typical contents being personally identifiable information (PII), user credentials for various cloud services, and credit card information.



Figure 18. A dataset being sold in the underground at varying prices, including a US\$900 “lifetime membership”

One of the primary advantages provided by these types of services is that they give malicious actors the ability to process and manage enormous amounts of data without the need to have complex infrastructure. The easy access to this information means that attacks can occur faster and more efficiently. This is especially useful in targeted attacks, where threat actors could find the information that they need without having to spend substantial time and effort in gathering it.

As participants continue to refine and evolve this underground market, we can expect to see organizations at greater risk from their data being stolen, especially since the use of services sold in this space means that the gap between the theft and the actual attack becomes much shorter.

Attacks on IoT Devices Increased

In addition to the cloud, the IoT also played a key role in many organizations’ shift to remote work — and sure enough, malicious actors also took notice.

As we noted in our security predictions for 2021, malicious actors will increasingly focus on home networks as they try to find ways into their targets’ systems.⁶¹ Compromised home networks and devices could serve as launching points for attackers before they jump to other devices with the eventual goal of gaining access to the corporate networks the devices are connected to. Routers are particularly vulnerable

to remote attacks, especially since the security at an employee’s home is not as robust as that at an enterprise workplace.

Based on our detections, inbound attacks possibly occurred on 15.5% of routers while 5.1% of routers were possibly used for outbound attacks in 2020.



Figure 19. In 2020, 15.5% of routers were possibly victimized while 5.1% were possibly compromised.

Note: Data is based on the percentages of detected inbound attacks (routers as victims) and outbound attacks (routers as attackers).

Source: Trend Micro™ Smart Home Network solution

In the past year, we also saw an uptick in the total number of inbound attack events, which was more than triple the 2019 tally, and in the total number of outbound attack events, which nearly doubled from 2019. Furthermore, the number of internet-connected devices on which we detected possible inbound attacks and the number of those that might have been used for possible outbound attacks both increased. We also saw more routers (which the internet-connected devices were connected to) being targeted by possible inbound attacks or being used for possible outbound attacks.

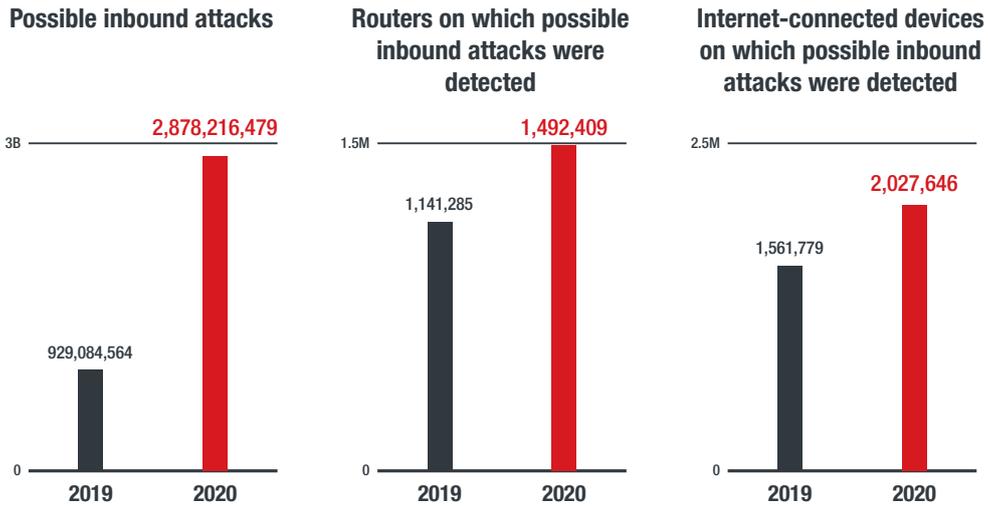


Figure 20. There was a significant increase in possible inbound attacks, and the numbers of internet-connected devices and routers on which possible inbound attacks were detected also increased: A comparison of the detection counts of possible inbound attacks and affected routers and devices in 2019 and 2020

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

Source: Trend Micro Smart Home Network solution

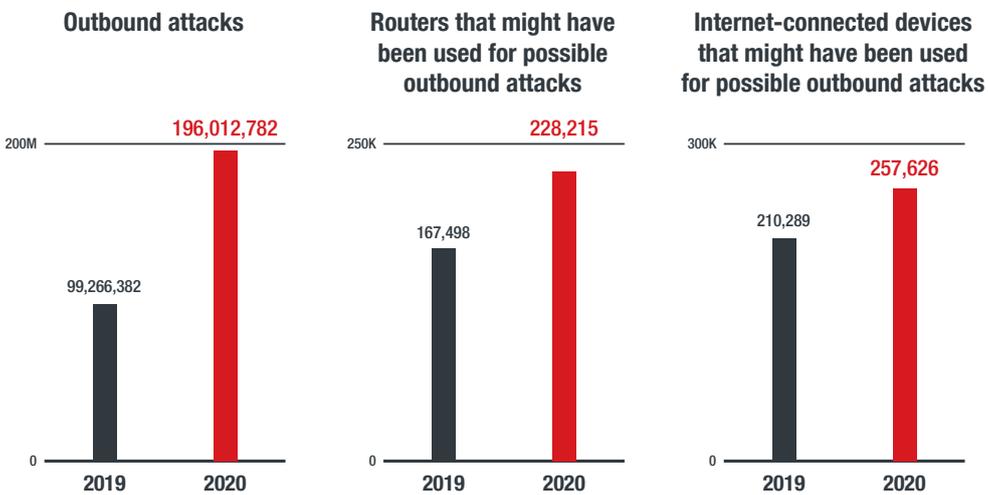


Figure 21. There were growths in the number of possible outbound attacks and the numbers of internet-connected devices and routers that might have been used for possible outbound: A comparison of the detection counts of possible outbound attacks and affected routers and devices in 2019 and 2020

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

Source: Trend Micro Smart Home Network solution

Brute-force attempts made up a significant portion of the inbound attacks, indicating that user credentials were attackers' most preferred target in 2020.

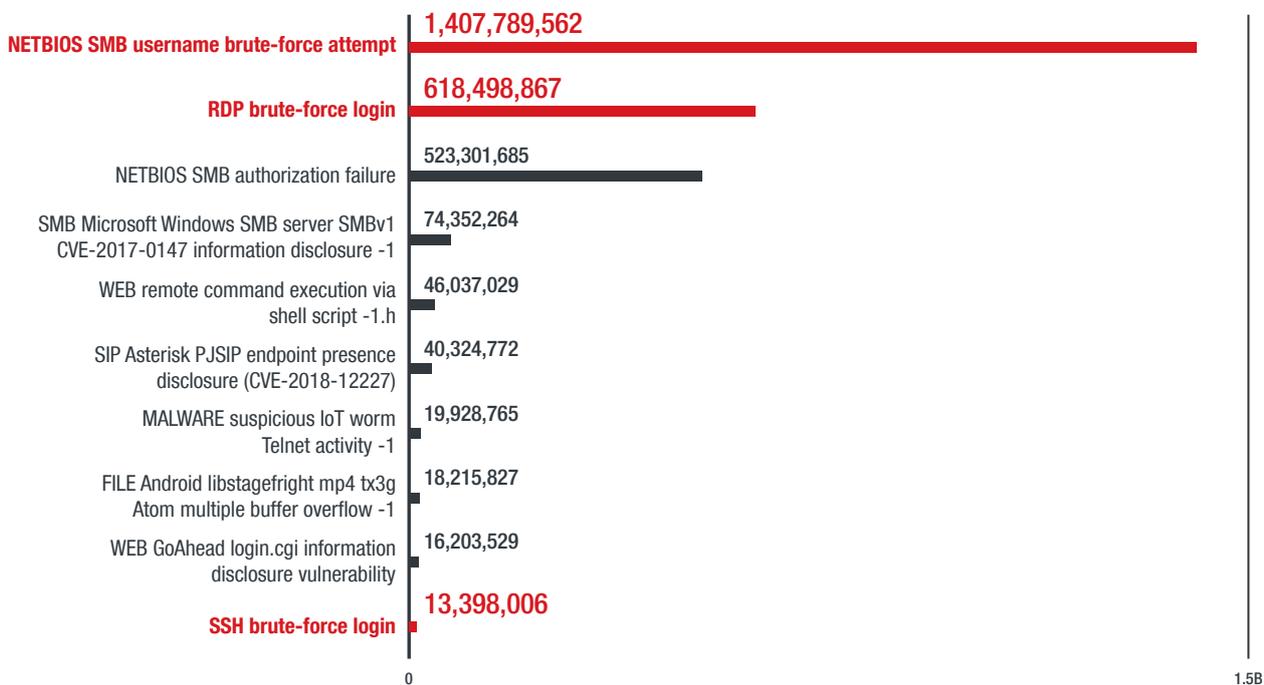


Figure 22. Brute-force login attempts were the top two inbound attack events:
A comparison of the detection counts of the top 10 event rules triggered by possible inbound attacks in 2020

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

Source: Trend Micro Smart Home Network solution

A similar story can be seen for outbound attacks, where NetBIOS Server Message Block (SMB) username brute-force attempts accounted for the highest number. Microsoft Windows SMB attacks, including exploitation of WannaCry vulnerabilities, were a close second.

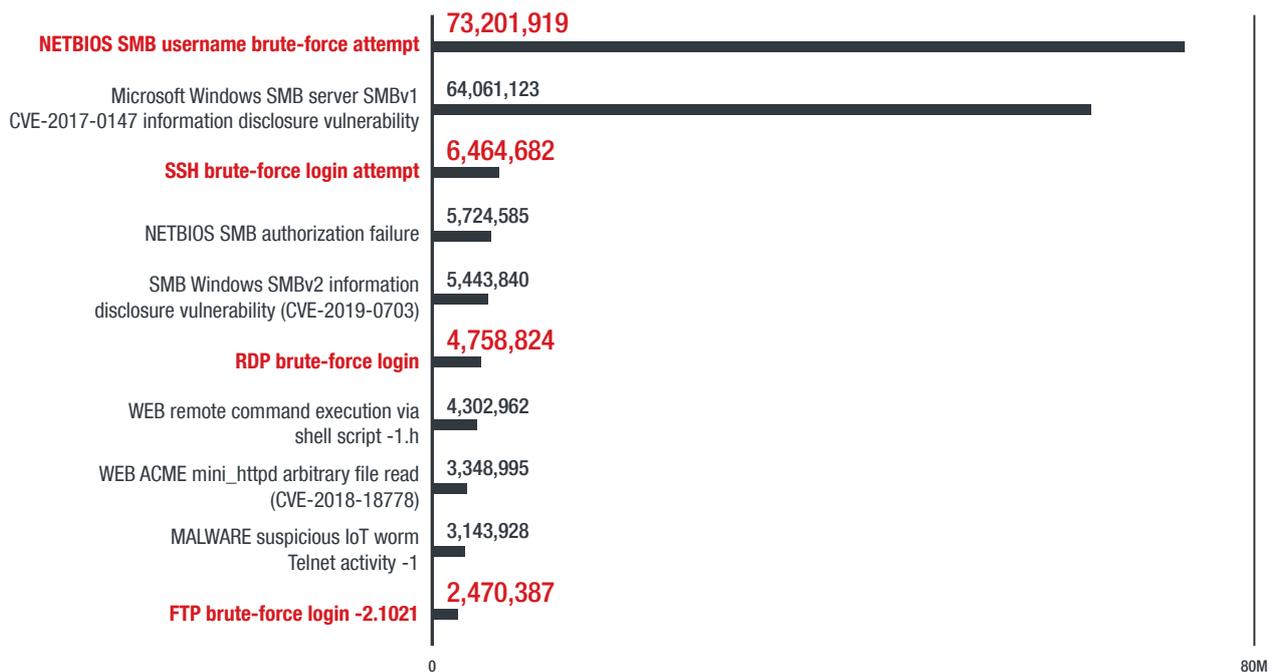


Figure 23. Brute-force login attempts were among the most common methods used in outbound attacks: A comparison of the detection counts of the top 10 event rules triggered by possible outbound attacks in 2020

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

Source: Trend Micro Smart Home Network solution

There were several noteworthy IoT incidents from the first half of the year, some of which, such as Urgent/11 and Ripple20, we had covered in our midyear cybersecurity report.⁶² In the second half of the year, researchers from Forescout disclosed Amnesia:33, a set of 33 vulnerabilities affecting open-source TCP/IP stacks deployed in a large number of IoT devices worldwide, including industrial internet-of-things (IIoT) devices. Exploitation of these vulnerabilities could enable attackers to take control of devices and abuse them for malicious activities such as creating an entry point to get into a network or for lateral movement.⁶³

What makes Amnesia:33 especially troubling is that the affected TCP/IP stacks — which include Nut/Net, FNET, picoTCP, and uIP — are not from a single company. Considering the number of devices from different companies that could be affected, the vulnerabilities could spread at a rapid rate. Furthermore, tracking the bugs and assessing their impact could prove difficult because of the scope of the vulnerabilities and because the potentially affected systems might be highly modular, lack any kind of documentation, or no longer even be supported.⁶⁴

Vulnerabilities like those found in Amnesia:33 could have significant impact, not just on the users of the affected devices but also on the supply chain as a whole. It is not difficult to imagine a situation similar to the SolarWinds attack where malicious actors gain access to their target via vulnerable devices from an organization that is part of the supply chain.

As for the more common IoT threats, among the most notable were the variants of the Mirai botnet malware, which had been accruing greater infamy since its discovery in 2016,⁶⁵ that we observed in the past year. In July, we reported on our discovery and analysis of a Mirai variant that exploited nine vulnerabilities, a mix of old and new, most notably CVE-2020-10173, a multiple authenticated command injection vulnerability in Comtrend VR-3033 routers.⁶⁶ Later that month, we reported on our examination of another Mirai variant, which exploited CVE-2020-5902, an F5 BIG-IP Traffic Management User Interface (TMUI) remote code execution vulnerability.⁶⁷

Mobile Malware Becomes Stealthier Despite Decrease in Malicious Apps

We saw a 41% decline in the number of mobile apps that we blocked in 2020, compared to the corresponding number from 2019. On the other hand, the number of mobile device-related malicious samples that we detected grew by 67% from the previous year. One possible reason for this discrepancy might be that malicious actors targeted mobile devices (either directly or indirectly) via methods that did not involve their apps, such as phishing pages or social media messages.

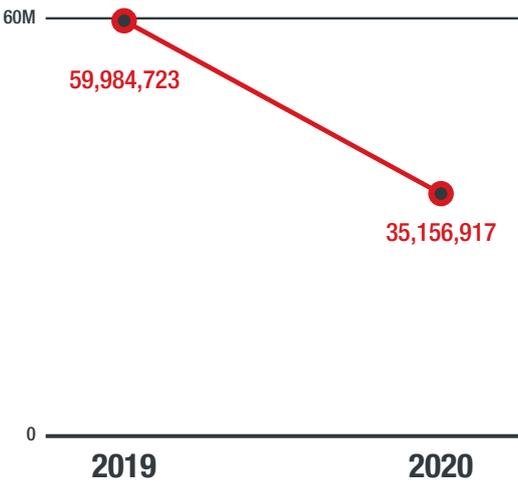


Figure 24. There was a 41% year-on-year decrease in blocked mobile apps, a possible indication that malicious actors did not focus too much on deploying malicious apps this year: A comparison of the numbers of blocked malicious Android apps in 2019 and 2020

Source: Trend Micro Mobile App Reputation Service

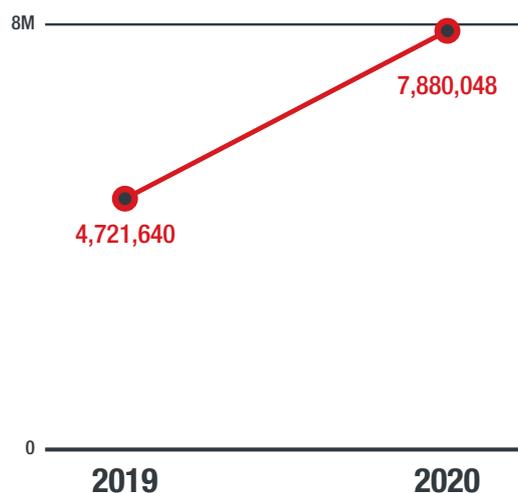


Figure 25. Despite the decrease in blocked mobile apps, mobile device-related malicious samples saw a 67% year-on-year increase, perhaps because malicious actors employed methods of infecting mobile devices other than malicious apps: A comparison of the numbers of detected mobile device-related malicious samples in 2019 and 2020

Source: Trend Micro Mobile App Reputation Service

Although mobile device attacks were overshadowed by other cybersecurity incidents, there were still several noteworthy mobile threat stories from the past year. In November, we examined a new variant of the Joker malware that was contained in a wallpaper app offering HD and 4K wallpapers. This Joker variant was notable for incorporating GitHub pages and repositories as a method of evading detection.⁶⁸

Instead of its past behavior of using application class and launcher activity, the new variant instead injects code into a new location. Furthermore, its use of GitHub serves a double purpose of facilitating stealthy malicious activity while also housing the payload. What makes this variant particularly nefarious is that it is contained in a functioning app, which, when combined with the variant's other obfuscation features, makes it difficult for victims to detect that they have already been infected.

We also looked into how Android malware obfuscation is evolving via an in-depth analysis of Geost and its multiple layers of obfuscation, noting that the malicious actors behind the malware are continuously investing in and improving it.⁶⁹ However, we also noted that the changes found in the code did not yet seem to have much of an impact on the actual quality of the obfuscation and, in turn, on the detection rate.

A Greater Number of Dangerous Vulnerabilities Threaten Organizations

More Risky Flaws Are Disclosed Even as Older Bugs Are Still Being Actively Exploited

In 2020, the Trend Micro™ Zero Day Initiative™ (ZDI) program published advisories on 1,453 vulnerabilities, a 40% increase from 2019. Of these, 173 were rated with critical severity and 983 with high severity, based on the Common Vulnerability Scoring System (CVSS).⁷⁰ The critical- and high-severity vulnerabilities saw significant spikes from the 2019 numbers. Because of the dangers they could pose to enterprises, critical- and high-severity vulnerabilities need to be patched as soon as possible, potentially adding to the workloads of IT teams.

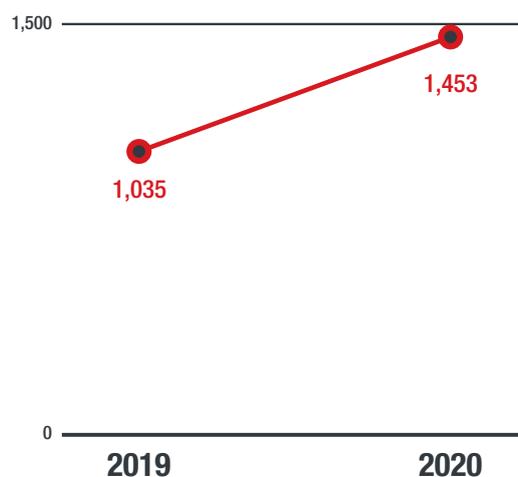


Figure 26. The number of published vulnerability advisories increased year on year by 40%:
A comparison of the numbers of disclosed vulnerabilities in 2019 and 2020

Source: Trend Micro™ Zero Day Initiative™ program

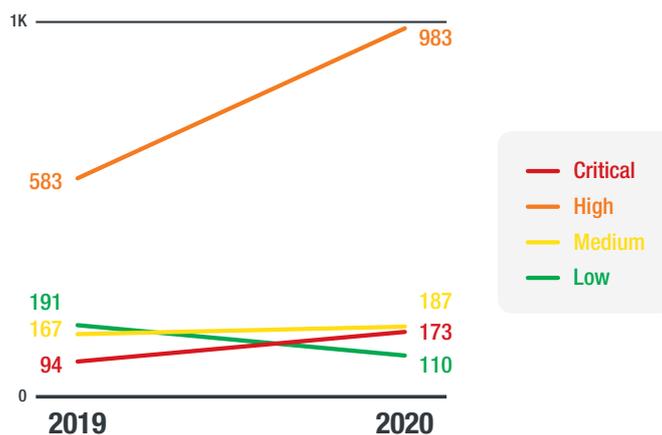


Figure 27. Critical- and high-severity vulnerabilities saw spikes in numbers, which could mean heavier workloads for IT teams due to patching issues: A comparison of the severity breakdown, based on the CVSS, of disclosed vulnerabilities in 2019 and 2020

Source: Trend Micro Zero Day Initiative program

Based on our data on the top exploited vulnerabilities from 2017 to 2020, vulnerabilities from as far back as 2005 were still being heavily exploited. What this signifies is that organizations should not assume that their systems are automatically safe from exploitation of old vulnerabilities and should always be vigilant in patching their software.

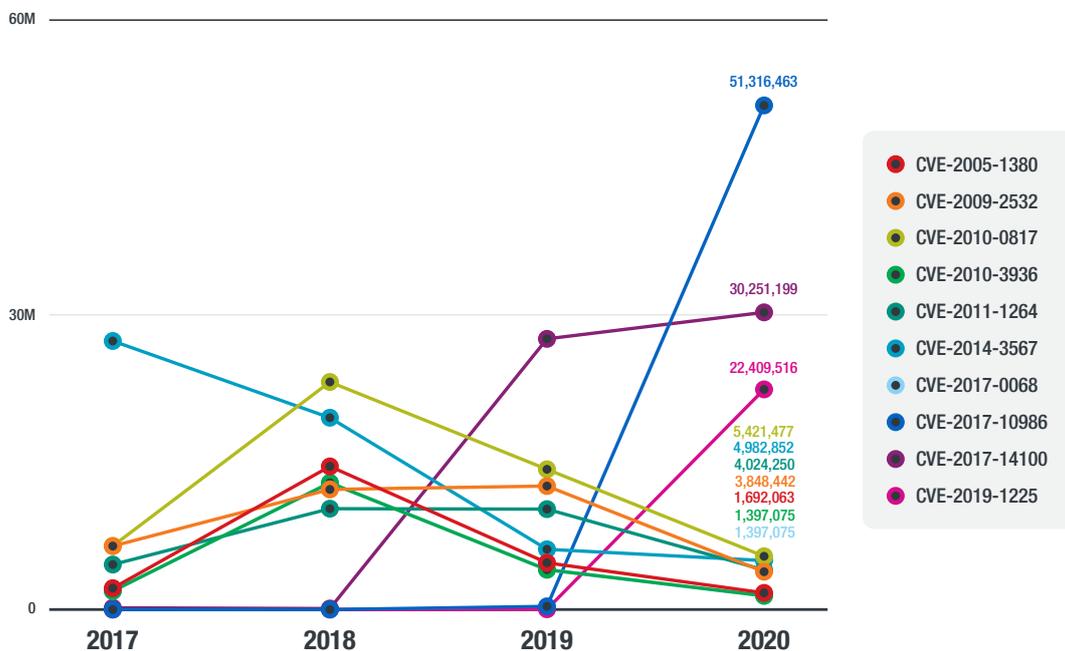


Figure 28. The age of vulnerabilities did not matter to malicious actors, as vulnerabilities from as far back as 2005 were still among the most exploited: A comparison of the detection counts of the 10 most exploited vulnerabilities from 2017 to 2020

Note: CVE-2010-3936 and CVE-2017-0068 use the same filter ID and therefore have the same numbers.

Source: Trend Micro Digital Vaccine filters

Zerologon Bug Emerges, Potentially Allowing Attackers to Take Over Entire Networks

One of the most prominent vulnerabilities discovered in 2020 was CVE-2020-1472.⁷¹ It was dubbed Zerologon because the flaw exists in the logon process for servers that use NT Lan Manager (NTLM): Ideally, the code behind the process should always be a random number, but in Zerologon's case, it contains four zeroes.⁷²

Zerologon is a dangerous bug with active proof-of-concept (POC) exploits; its severity is rated 10 out of 10 on the CVSS. It exploits a flaw in Microsoft's Active Directory (AD) Netlogon Remote Protocol (MS-NRPC) that gives users the ability to log on to servers that are using NTLM.⁷³ Given that MS-NRPC is also used to transmit account changes and passwords, it is clear to see why it could become problematic.

Zerologon could allow an attacker to take control of a domain controller by either changing or removing the password used for a service account on the controller, after which the attacker could perform malicious actions such as launching a denial-of-service attack or even taking over the entire network. By using the publicly available POC exploits, the attacker could perform even more damaging activities such as infecting the affected system with ransomware.⁷⁴

Microsoft released an initial patch for Zerologon in August 2020 and a second patch in February 2021.⁷⁵ The first update blocks domain controllers from using unsecured remote procedure call (RPC) communications, while the second update enables enforcement mode on domain controllers by default to block vulnerable connections from noncompliant devices.⁷⁶

Modern Threats Require Comprehensive Defense Strategies and Multilayered Security Technologies

Enterprises are facing major security risks from determined threat actors who do not shy away from using every tool and trick in their arsenal. This is compounded by the unique situation in which many organizations have found themselves in, having to secure both the physical and virtual workspaces amid a worldwide pandemic.

In today's complex working environment, where the lines between the home and the office have been blurred, the right technologies are essential for building a robust security profile. Instead of relying on single layers of protection, each of which covers only a portion of the overall infrastructure, organizations should consider a strong multilayered security. The solution should offer a wide range of capabilities — including detection, investigation, and response — and provide comprehensive protection throughout the whole system — from emails and endpoints to servers, networks, and even cloud workloads.

In addition to the technological factors and issues, the pandemic has had a significant effect on the performance of security operation centers (SOCs). Aside from having to ensure that the right technological pieces are in place for a secure working environment, security professionals also have to deal with increased workloads that could lead to burnout.⁷⁷ A proper multilayered security solution should give IT staff and security personnel the ability to gain insights into the nature of the threats they are facing. The use of technologies such as machine learning and behavior monitoring can help organizations focus on the most critical aspects of security without needing to go through a sizeable amount of data.

Enterprises should combine these technologies with the right security strategies and policies. Even with the emergence of increasingly complex attacks, phishing and social engineering remain to be common infection vectors for most malicious actors — from inexperienced amateurs to even the most skilled groups. Organizations should therefore consider investing in the training of their workforce with regard to identifying the most prevalent phishing and social engineering techniques.⁷⁸

Organizations should also conduct regular security audits to ensure that their physical and cloud infrastructures are free of instances of misconfiguration and other weak points. They should also perform periodic data sweeps to help detect early warning signs such as first-stage malware and tools that are usual precursors to the actual payloads.

Furthermore, given how supply-chain attacks are now being used regularly by malicious actors, it is important for companies to evaluate the security of their suppliers and other partners and, if possible, work with them to create strong defenses against these attacks.

The need for timely and efficient patch management cannot be stressed enough. Vulnerabilities such as Zerologon prove that the best time for updates is as soon as the updates become available. However, the reality is that patching is not as simple as it seems. It takes considerable time to update the whole system, and the existence of zero-day vulnerabilities further complicates matters. To help with this, enterprises can consider using technologies that offer virtual patching to bolster security while implementing updates or waiting for fixes to be rolled out.⁷⁹

For most organizations, the issue of migrating their workforce from the physical office to the home is something that has been dealt with in some manner. The pressing need for most enterprises now is the need to sustain their operations while taking into account the technologies, the importance of security, and the human point of view.

Threat Landscape in Review

In 2020, the Trend Micro™ Smart Protection Network™ infrastructure protected users from more than 62 billion threats consisting of email threats, malicious files, and malicious URLs.

62,637,731,995

blocked threats in 2020

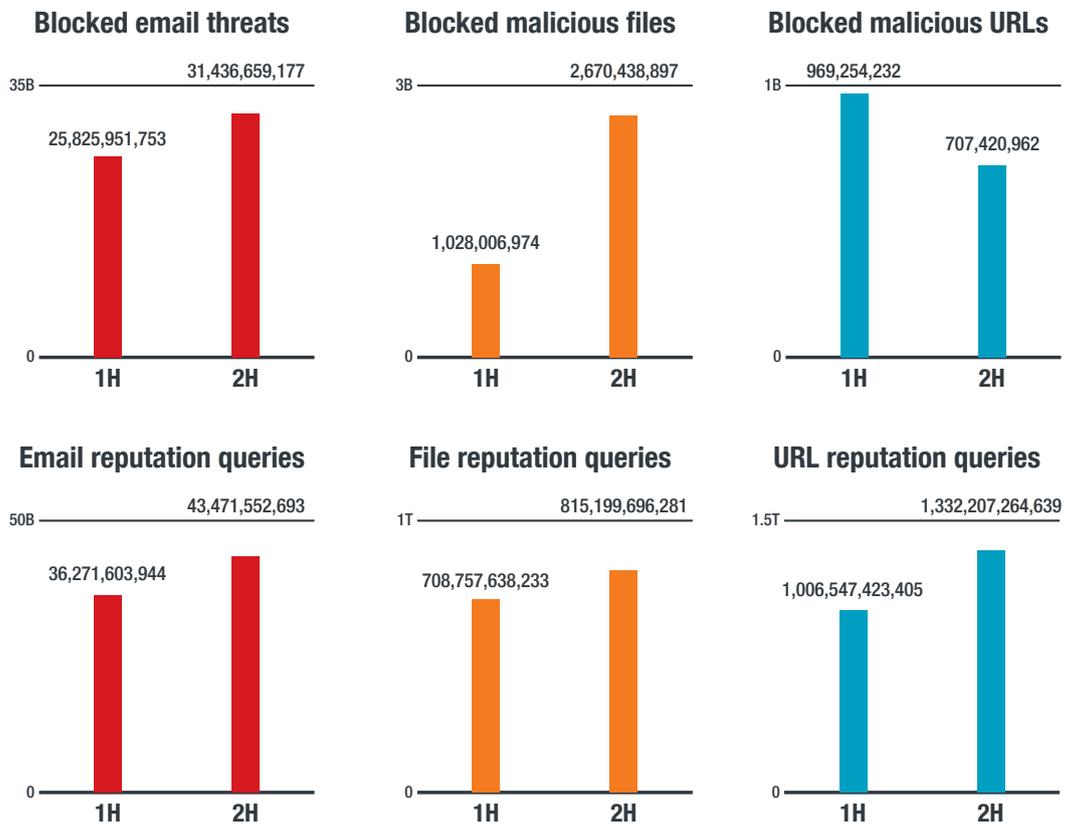


Figure 29. While nearly every metric for blocked threats and reputation queries increased from the first to the second half of the year, the increase in blocked malicious files was particularly substantial:

A comparison of the numbers of blocked email, file, and URL threats, and of email, file, and URL reputation queries in the first and second halves of 2020

Source: Trend Micro Smart Protection Network infrastructure

The top 10 malware families in terms of detections in 2020 included familiar names, with WannaCry, Coinminer, and Emotet making up the top three. WannaCry, aside from being the top malware family, is the only ransomware in the list. Cryptocurrency miners as a whole are in second place, showing how prevalent they had become. The majority of the top 10 are made up of older families that, despite their age, were still responsible for a large number of infections.

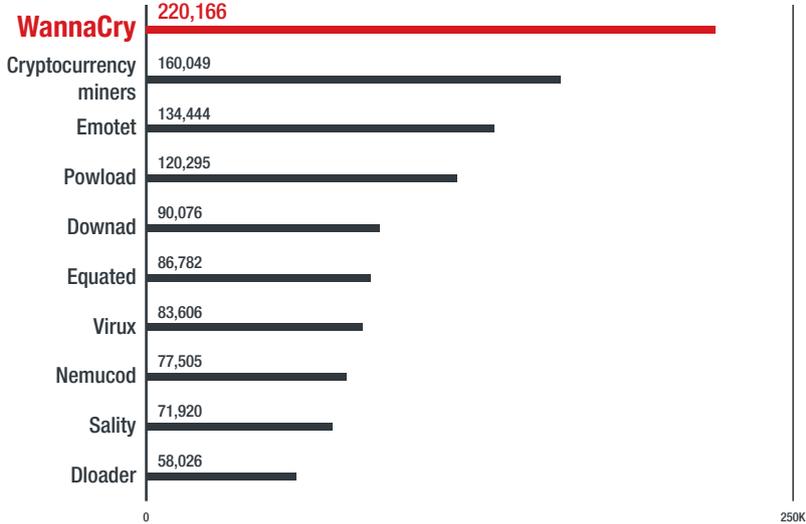


Figure 30. The WannaCry ransomware remained the top threat, with cryptocurrency miners as a whole in second place: The 10 most detected malware families in 2020

Source: Trend Micro Smart Protection Network infrastructure

Our data on the top cryptocurrency miners in 2020 reveals that the top three entries alone accounted for more than 120,000 detections.

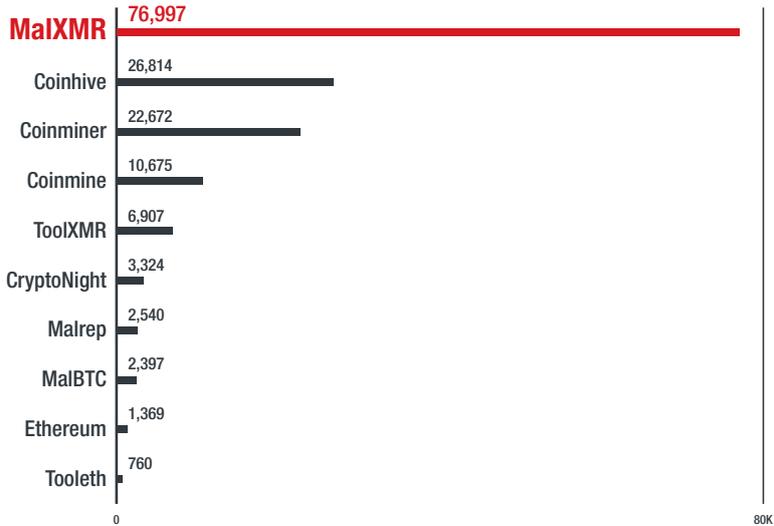


Figure 31. MalXMR, Coinhive, and Coinminer were the most detected cryptocurrency miners, accounting for more than 120,000 between the three of them: The 10 most detected cryptocurrency miners in 2020

Source: Trend Micro Smart Protection Network infrastructure

In 2020, we detected more than 2.3 million endpoints that connected to C&C servers, while we detected just over 100,000 botnet C&C servers. The large number of servers could be attributed either to malicious actors that were using C&C servers as part of their operations or to groups that were using increasingly complex C&C infrastructure. On the other hand, the number of botnet connections we detected from our sensors alone suggests that there could have been millions of potential victims.

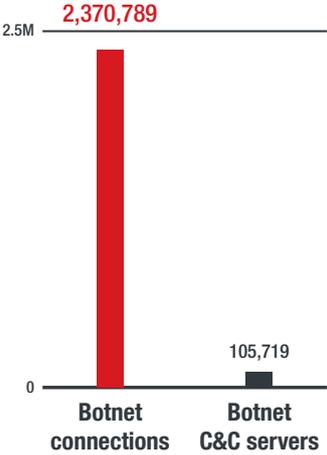


Figure 32. We detected over 2.3 million botnet connections and over 100,000 botnet C&C servers:
The numbers of detected botnet connections and botnet C&C servers in 2020

Note: Botnet connections were unique endpoints that queried or connected to C&C servers, while botnet C&C servers were unique and active C&C servers that endpoints queried or connected to.

Source: Trend Micro Smart Protection Network infrastructure

There were 127 new ransomware families discovered in 2020, a 34% increase from the 95 found in 2019.⁸⁰ Egregor, despite having its initial detection occur only in September, managed to rank in the top 10 ransomware families of 2020, as shown in Figure 1.

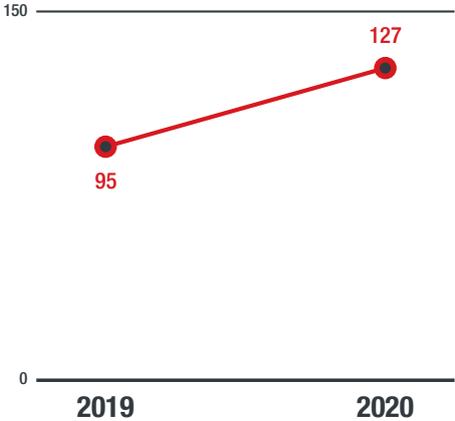


Figure 33. New ransomware families increased year on year by 34%:
A comparison of the numbers of new ransomware families in 2019 and 2020

Source: Trend Micro Smart Protection Network infrastructure

JAN	FEB	MAR	APR	MAY	JUN
AkoLocker	Antefrigus	BB	Ballistic	PonyFinal	Zorab
Avest	Balaclava	Corvina	BearCrypt	GonnaCry	WorldCry
BitPyLocker	Cai	Mado	Coronawinlocker	CoronaLock	SuchCrypt
Keslan	CrypenCode	Nefilim	Creepy	ColdLock	Sapphire
Zeoticus	Cryptopxj	Pysa	CryLock	BlueCheeser	QrnaLock
	Crytox	Triplem	Geminice		PowLock
	DemonCrypt	WannaRen	Jest		Locment
	FTCode		Lbkut		LickyAgent
	Ledif		OnaLocker		Krygo
	Makop		Ooglego		Funicorn
	Morrisbatchcrypt		Sadogo		Freefil
	OnyxLocker		Sfile2		Escal
	Ragnarok		Upper		CyberThanos
	Ranscrape		Void		Chimera
	Trsomware		Wreath		BlackMoon
	WannaCash				BlackKingdom
	WannaScream				BlackClaw
	Wilboy				Avaddon

JUL	AUG	SEP	OCT	NOV	DEC
Xinof	Tappif	Aidsnt	Doowtar	Hiddeneargdarmerie	AgeLocker
WhoLocker	SunCrypt	BitMiner	EyeCryLocker	RanzyLocker	Alol
Wastedlocker	Silvertor	BlackKnight	Hibuniel	WoodRat	BacuCrypt
ThiefQuest	RagnarLocker	BlackSquid	JarCrypt		Dusk
StrongPity	GiveMeTheKey	CoronaCryptor	LeakTheMall		Erica
Pojje	FlyingShip	DogeCrypt	Pay2Key		Godra
Panther	Exorcist	Egregor	RegretLocker		Hwru
Lolkek	DarkSide	Exx	SantaCrypt		RedRoman
JosephNull	CryptoLock	Gav			StingJar
EvilQuest	BigLock	HexaCrypt			Vaggen
CryCryptor		MountLocket			
Bead		ReadMan			
		Thanos			
		Vashsorena			
		Viluciware			
		Zhen			

Table 4. 127 new ransomware families were discovered: New ransomware families detected in 2020

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

Of our more than 11 million detections of file types used in spam email attachments in 2020, PDF accounted for nearly half. XLSX and HTML also had sizeable detection counts.

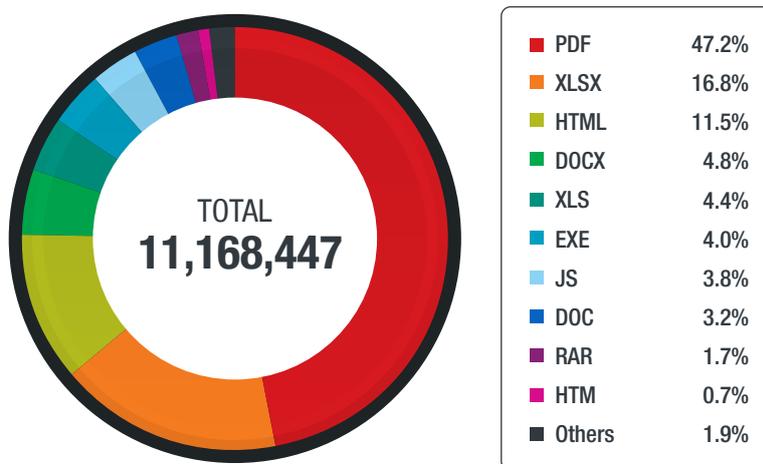


Figure 34. PDF files accounted for nearly half of spam email attachments:
The distribution of file types used in spam email attachments in 2020

Source: Trend Micro Email Reputation Services

While Windows-based operating systems still make up the majority of machines that were detected to have some form of malware infection, a sizeable number of macOS and Linux machines also suffered similarly.

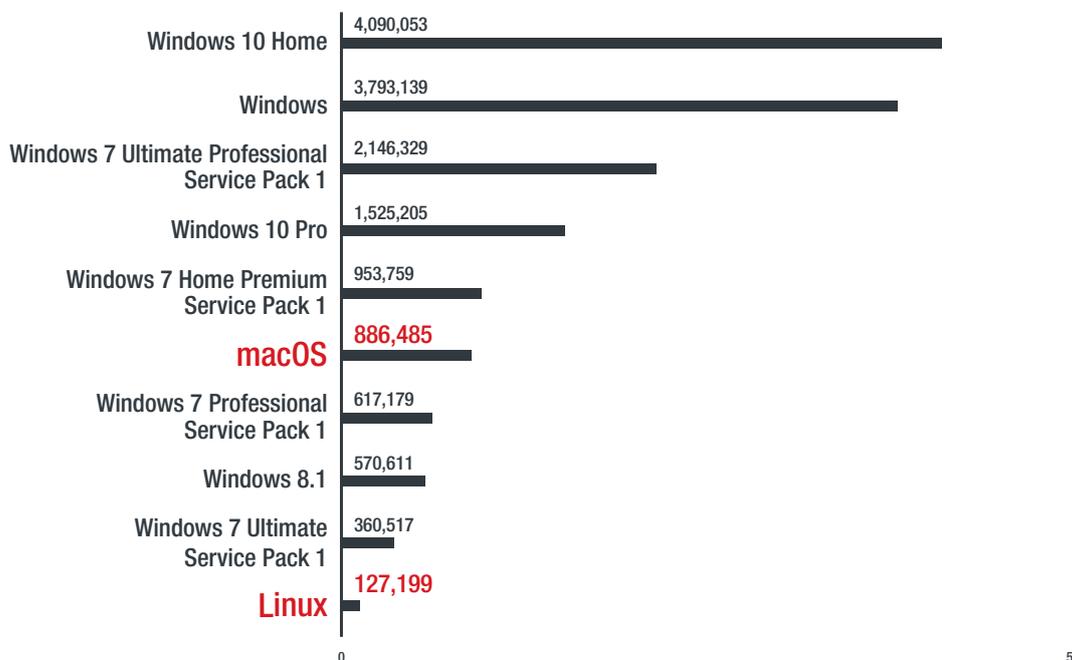


Figure 35. Both macOS and Linux accounted for fairly significant numbers of malware infections, with macOS ranking higher than certain versions of Windows: The top 10 operating systems based on malware infections detected on machines in 2020

Source: Trend Micro Smart Protection Network infrastructure

References

- 1 Trend Micro. (Sept. 15, 2020). *Trend Micro*. "Boosting Impact for Profit: Evolving Ransomware Techniques for Targeted Attacks." Accessed on Jan. 15, 2021, at https://www.trendmicro.com/en_us/research/20/i/boosting-impact-for-profit-evolving-ransomware-techniques-for-targeted-attacks.html.
- 2 Catalin Cimpanu. (April 21, 2020). *ZDNet*. "Here's a list of all the ransomware gangs who will steal and leak your data if you don't pay." Accessed on Jan. 15, 2021, at <https://www.zdnet.com/article/heres-a-list-of-all-the-ransomware-gangs-who-will-steal-and-leak-your-data-if-you-dont-pay>.
- 3 Coalition, Inc. (n.d.). *Coalition*. "Cyber Insurance Claims Report." Accessed on Jan. 15, 2021, at <https://info.coalitioninc.com/rs/566-KWJ-784/images/DLC-2020-09-Coalition-Cyber-Insurance-Claims-Report-2020.pdf>.
- 4 Trend Micro. (Feb. 4, 2020). *Trend Micro Security News*. "Ryuk Ransomware Infects US Government Contractor." Accessed on Jan. 15, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ryuk-ransomware-infects-us-government-contractor>.
- 5 Cybersecurity & Infrastructure Agency. (Nov. 2, 2020). *Cybersecurity & Infrastructure Agency*. "Ransomware Activity Targeting the Healthcare and Public Health Sector." Accessed on Jan. 15, 2021, at <https://us-cert.cisa.gov/ncas/alerts/aa20-302a>.
- 6 HHS Cybersecurity Program. (Nov. 11, 2020). *HHS Cybersecurity Program*. "TrickBot, Ryuk, and the HPH Sector." Accessed on Feb. 3, 2021, at <https://www.hhs.gov/sites/default/files/trickbot-ryuk-and-the-hph-sector.pdf>.
- 7 Greg Foss. (Oct. 30, 2020). *Carbon Black*. "TAU Threat Advisory: Imminent Ransomware threat to U.S. Healthcare and Public Health Sector." Accessed on Feb. 3, 2021, at <https://www.carbonblack.com/blog/tau-threat-advisory-imminent-ransomware-threat-to-u-s-healthcare-and-public-health-sector>.
- 8 Trend Micro. (March 14, 2019). *Trend Micro*. "Examining Ryuk Ransomware Through the Lens of Managed Detection and Response." Accessed on Feb. 3, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/examining-ryuk-ransomware-through-the-lens-of-managed-detection-and-response>.
- 9 Trend Micro. (Nov. 4, 2020). *Trend Micro*. "Ryuk 2020: Distributing Ransomware via TrickBot and BazarLoader." Accessed on Jan. 15, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ryuk-2020-distributing-ransomware-via-trickbot-and-bazarloader>.
- 10 Trend Micro. (Aug. 26, 2020). *Trend Micro*. "Securing the Pandemic-Disrupted Workplace." Accessed on Feb. 8, 2021, at <https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/securing-the-pandemic-disrupted-workplace-trend-micro-2020-midyear-cybersecurity-report>.
- 11 Trend Micro. (Dec. 14, 2020). *Trend Micro*. "Egregor Ransomware Launches String of High-Profile Attacks to End 2020." Accessed on Jan. 15, 2021, at https://www.trendmicro.com/en_us/research/20/l/egregor-ransomware-launches-string-of-high-profile-attacks-to-en.html.
- 12 Tomas Meskauskas. (Oct. 29, 2020). *Security Boulevard*. "Egregor: Sekhmet's Cousin." Accessed on Jan. 15, 2021, at <https://securityboulevard.com/2020/10/egregor-sekhmets-cousin>.
- 13 CISO Mag. (Nov. 3, 2020). *CISO Mag*. "Are We Really Out of the Maze? The Ransomware Gang Announces Retirement." Accessed on Feb. 8, 2021, at <https://cisomag.eccouncil.org/maze-ransomware-retires>.
- 14 Trend Micro. (Dec. 14, 2020). *Trend Micro*. "Egregor Ransomware Launches String of High-Profile Attacks to End 2020." Accessed on Jan. 15, 2021, at https://www.trendmicro.com/en_us/research/20/l/egregor-ransomware-launches-string-of-high-profile-attacks-to-en.html.
- 15 Trend Micro. (Jan. 5, 2020). *Trend Micro*. "An Overview of the DoppelPaymer Ransomware." Accessed on Jan. 15, 2021, at https://www.trendmicro.com/en_us/research/21/a/an-overview-of-the-doppelpaymer-ransomware.html.
- 16 Federal Bureau of Investigation, Cyber Division. (Dec. 10, 2020). *Internet Crime Complaint Center*. "DoppelPaymer Ransomware Attacks on Critical Infrastructure Impact Critical Services." Accessed on Jan. 15, 2021, at <https://www.ic3.gov/Media/News/2020/201215-1.pdf>.
- 17 Trend Micro. (Aug. 13, 2020). *Trend Micro*. "BitPaymer Malware Information." Last accessed on Jan. 24, 2021, at <https://success.trendmicro.com/solution/000261855>.
- 18 Process Hacker. (n.d.). *Process Hacker*. "Process Hacker." Accessed on Jan. 15, 2021, at <https://processhacker.sourceforge.io>.

- 19 Ryan Flores. (Dec. 1, 2020). *Trend Micro*. "The Impact of Modern Ransomware on Manufacturing Networks." Accessed on Jan. 19, 2021, at https://www.trendmicro.com/en_us/research/20/l/the-impact-of-modern-ransomware-on-manufacturing-networks.html.
- 20 Leandro Froes. (Jan. 6, 2021). *Trend Micro*. "Expanding Range and Improving Speed: A RansomExx Approach." Accessed on Feb. 4, 2021, at https://www.trendmicro.com/en_us/research/21/a/expanding-range-and-improving-speed-a-ransomexx-approach.html.
- 21 Nelson William Gamazo Sanchez et al. (Oct. 19, 2020). *Trend Micro*. "Operation Earth Kitsune: Tracking SLUB's Current Operations." Accessed on Jan. 15, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-earth-kitsune-tracking-slub-s-current-operations>.
- 22 Nelson William Gamazo Sanchez et al. (Oct. 28, 2020). *Trend Micro*. "Operation Earth Kitsune: A Dance of Two New Backdoors." Accessed on Jan. 15, 2021, at https://www.trendmicro.com/en_us/research/20/j/operation-earth-kitsune-a-dance-of-two-new-backdoors.html.
- 23 Trend Micro. (Jan. 5, 2021). *Trend Micro*. "Earth Wendigo Injects JavaScript Backdoor to Service Worker for Mailbox Exfiltration." Accessed on Jan. 15, 2021, at https://www.trendmicro.com/en_us/research/21/a/earth-wendigo-injects-javascript-backdoor-to-service-worker-for-.html.
- 24 Joseph C Chen, Jaromir Horejsi, and Ecular Xu. (Dec. 9, 2020). *Trend Micro*. "SideWinder Uses South Asian Issues for Spear Phishing, Mobile Attacks." Accessed on Jan. 15, 2021, at https://www.trendmicro.com/en_us/research/20/l/sidewinder-leverages-south-asian-territorial-issues-for-spear-ph.html.
- 25 Mayra Rosario Fuentes. (May 26, 2020). *Trend Micro*. "Shifts in Underground Markets." Accessed on Feb. 5, 2021, at https://documents.trendmicro.com/assets/white_papers/wp-shifts-in-the-underground.pdf.
- 26 Lawrence Abrams. (Jan. 12, 2019). *Bleeping Computer*. "Ryuk Ransomware Partners with TrickBot to Gain Access to Infected Networks." Accessed on Feb. 8, 2021, at <https://www.bleepingcomputer.com/news/security/ryuk-ransomware-partners-with-trickbot-to-gain-access-to-infected-networks/>.
- 27 Trend Micro. (Jan. 16, 2016). *Trend Micro*. "Operation Pawn Storm: Fast Facts and the Latest Developments." Accessed on Jan. 15, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-pawn-storm-fast-facts>.
- 28 Feike Hacquebord and Lord Alfred Remorin. (Dec. 17, 2020). *Trend Micro*. "Pawn Storm's Lack of Sophistication as a Strategy." Accessed on Jan. 18, 2021, at https://www.trendmicro.com/en_us/research/20/l/pawn-storm-lack-of-sophistication-as-a-strategy.html.
- 29 Paul Miguel Babon. (Sept. 3, 2020). *Trend Micro*. "Tricky 'Forms' of Phishing." Accessed on Jan. 18, 2021, at https://www.trendmicro.com/en_us/research/20/i/tricky-forms-of-phishing.html.
- 30 Catalin Cimpanu. (Feb. 10, 2020). *ZDNet*. "FBI warns about ongoing attacks against software supply chain companies." Accessed on Feb. 10, 2021, at <https://www.zdnet.com/article/fbi-warns-about-ongoing-attacks-against-software-supply-chain-companies/>.
- 31 Federal Bureau of Investigation, Cyber Division. (March 30, 2020). *SANS Internet Storm Center*. "Kwampirs Malware Employed in Ongoing Cyber Supply Chain Campaign Targeting Global Industries, including Healthcare Sector." Accessed on Feb. 10, 2021, at https://isc.sans.edu/diaryimages/Kwampirs_PIN_20200330-001.pdf.
- 32 Jake Williams. (Dec. 15, 2020). *SANS Institute*. "What You Need to Know About the SolarWinds Supply-Chain Attack." Accessed on Jan. 19, 2021, at <https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack>.
- 33 SolarWinds. (Dec. 31, 2020). *SolarWinds*. "SolarWinds Security Advisory." Accessed on Jan. 19, 2021, at <https://www.solarwinds.com/securityadvisory>.
- 34 Trend Micro. (Dec. 15, 2020). *Trend Micro*. "Overview of Recent Sunburst Targeted Attacks." Accessed on Jan. 19, 2021, at https://www.trendmicro.com/en_us/research/20/l/overview-of-recent-sunburst-targeted-attacks.html.
- 35 David Klepper. (Oct. 17, 2020). *Associated Press News*. "Scammers seize on US election, but it's not votes they want." Accessed on Jan. 19, 2021, at <https://apnews.com/article/election-2020-virus-outbreak-joe-biden-senate-elections-media-f32410451f45102ddd4a82ebec8ac746>.
- 36 Tom Burt. (Sept. 10, 2020). *Microsoft*. "New cyberattacks targeting U.S. elections." Accessed on Jan. 19, 2021, at <https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/>.
- 37 Trend Micro. (Aug. 26, 2020). *Trend Micro*. "Securing the Pandemic-Disrupted Workplace." Accessed on Jan. 19, 2021, at <https://documents.trendmicro.com/assets/rpt/rpt-securing-the-pandemic-disrupted-workplace.pdf>.

- 38 Trend Micro. (Nov. 11, 2020). *Trend Micro*. "Developing Story: COVID-19 Used in Malicious Campaigns." Accessed on Jan. 19, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains>.
- 39 Andrew Duehren and Kristina Peterson. (Nov. 25, 2020). *The Wall Street Journal*. "Covid-19 Aid and Stimulus: What's Expiring Soon and What's in the Works." Accessed on Jan. 19, 2021, at <https://www.wsj.com/articles/coronavirus-aid-whats-expiring-soon-and-whats-in-the-works-11606311697>.
- 40 Internal Revenue Service. (Dec. 8, 2020). *Internal Revenue Service*. "IRS warns people about a COVID-related text message scam." Accessed on Jan. 19, 2021, at <https://www.irs.gov/newsroom/irs-warns-people-about-a-covid-related-text-message-scam>.
- 41 Check Point. (Jan. 12, 2021). *Check Point*. "Covid-19 'Vaccines' Touted for Just \$250 on Darknet." Accessed on Jan. 19, 2021, at <https://blog.checkpoint.com/2020/12/11/covid-19-vaccines-touted-for-just-250-on-darknet/>.
- 42 Claire Zaboeva and Melissa Frydrych. (Dec. 3, 2020). *IBM Security Intelligence*. "IBM Uncovers Global Phishing Campaign Targeting the COVID-19 Vaccine Cold Chain." Accessed on Jan. 19, 2021, at <https://securityintelligence.com/posts/ibm-uncovers-global-phishing-covid-19-vaccine-cold-chain>.
- 43 Marshall Chen et al. (Aug. 6, 2020). *Trend Micro*. "Water Nue Phishing Targets Execs' Office 365 Accounts." Accessed on Jan. 22, 2021, at https://www.trendmicro.com/en_us/research/20/h/water-nue-phishing-targets-execs-office-365-accounts.html.
- 44 Cedric Pernet. (Oct. 6, 2020). *Trend Micro*. "French companies Under Attack from Clever BEC Scam." Accessed on Jan. 22, 2021, at https://www.trendmicro.com/en_us/research/20/j/french-companies-under-attack-from-clever-bec-scam.html.
- 45 Trend Micro. (Oct. 7, 2020). *Trend Micro*. "CSO Insights: DataBank's Mark Houpt on Looking Beyond Securing Infrastructures in the New Normal." Accessed on Jan. 19, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/security-technology/cso-insights-databank-mark-houpt-on-looking-beyond-securing-infrastructures-in-the-new-normal>.
- 46 Yahoo!. (Nov. 24, 2020). *Yahoo! Finance*. "Virtual Private Network (VPN) Market Report 2020: VPN Usage Spirals to an all Time High of 27.1% - Global Forecast to 2027." Accessed on Jan. 19, 2021, at <https://finance.yahoo.com/news/virtual-private-network-vpn-market-100300294.html>.
- 47 Common Vulnerabilities and Exposures. (n.d.). *Common Vulnerabilities and Exposures*. "CVE-2019-11510." Accessed on Jan. 19, 2021, at <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11510>.
- 48 Eduard Kovacs. (Jan. 6, 2020). *Security Week*. "Pulse Secure VPN Vulnerability Exploited to Deliver Ransomware." Accessed on Jan. 19, 2021, at <https://www.securityweek.com/pulse-secure-vpn-vulnerability-exploited-deliver-ransomware>.
- 49 Raphael Centeno. (Sept. 21, 2020). *Trend Micro*. "Cybercriminals Distribute Backdoor With VPN Installer." Accessed on Feb. 5, 2021, at https://www.trendmicro.com/en_us/research/20/i/cybercriminals-distribute-backdoor-with-vpn.html.
- 50 Trend Micro. (Nov. 16, 2020). *Trend Micro*. "Malicious Actors Target Comm Apps such as Zoom, Slack, Discord." Accessed on Jan. 19, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/malicious-actors-target-comm-apps-such-as-zoom-slack-discord>.
- 51 Raphael Centeno, Bren Matthew Ebriega, and Llalum Victoria. (May 21, 2020). *Trend Micro*. "Backdoor, Devil Shadow Botnet Hidden in Fake Zoom Installers." Accessed on Feb. 5, 2021, at https://www.trendmicro.com/en_us/research/20/e/backdoor-devil-shadow-botnet-hidden-in-fake-zoom-installers.html.
- 52 Trend Micro. (Nov. 16, 2020). *Trend Micro*. "Malicious Actors Target Comm Apps such as Zoom, Slack, Discord." Accessed on Jan. 19, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/malicious-actors-target-comm-apps-such-as-zoom-slack-discord>.
- 53 Trend Micro. (2020). *Trend Micro*. "The 2020 Cyber Risk Index Goes Global." Accessed on Jan. 20, 2021, at https://www.trendmicro.com/en_us/research/20/l/2020-cyber-risk-index-global.html.
- 54 Trend Micro. (May 14, 2020). *Trend Micro*. "Cloud Security: Key Concepts, Threats, and Solutions." Accessed on Jan. 20, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/cloud-security-key-concepts-threats-and-solutions>.
- 55 Trend Micro. (April 7, 2020). *Trend Micro*. "Misconfigured Docker Daemon API Ports Attacked for Kinsing Malware Campaign." Accessed on Feb. 5, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/misconfigured-docker-daemon-api-ports-attacked-for-kinsing-malware-campaign>.

- 56 Augusto Remillano II and Jemimah Molina. (May 6, 2020). *Trend Micro*. "Coinminer, DDoS Bot Attack Docker Daemon Ports." Accessed on Jan. 20, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/coinminer-ddos-bot-attack-docker-daemon-ports>.
- 57 David Fiser. (Dec. 18, 2020). *Trend Micro*. "TeamTNT Now Deploying DDoS-Capable IRC Bot TNTbotinger." Accessed on Jan. 20, 2021 at https://www.trendmicro.com/en_us/research/20/1/teamtnt-now-deploying-ddos-capable-irc-bot-tntbotinger.html.
- 58 Alfredo Oliveira and David Fiser. (Oct. 12, 2020). *Trend Micro*. "Metasploit Shellcodes Attack Exposed Docker APIs." Last accessed on Jan. 20, 2021, at https://www.trendmicro.com/en_us/research/20/j/metasploit-shellcodes-attack-exposed-docker-apis.html.
- 59 Vladimir Kropotov, Robert McArdle, and Fyodor Yarochkin. (Sept. 1, 2020). *Trend Micro*. "Commodified Cybercrime Infrastructure: Exploring the Underground Services Market for Cybercriminals." Accessed on Jan. 20, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/commodified-cybercrime-infrastructure-exploring-the-underground-services-market-for-cybercriminals>.
- 60 Vladimir Kropotov and Fyodor Yarochkin. (Nov. 16, 2020). *Trend Micro*. "Cybercriminal 'Cloud of Logs'." Accessed on Jan. 24, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cybercriminal-cloud-of-logs-the-emerging-underground-business-of-selling-access-to-stolen-data>.
- 61 Trend Micro. (Dec. 8, 2020). *Trend Micro*. "Turning the Tide: Trend Micro Security Predictions for 2021." Accessed on Jan. 22, 2021, at <https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2021>.
- 62 Trend Micro. (Aug. 26, 2020). *Trend Micro*. "Securing the Pandemic-Disrupted Workplace." Accessed on Jan. 21, 2021, at <https://documents.trendmicro.com/assets/rpt/rpt-securing-the-pandemic-disrupted-workplace.pdf>.
- 63 Amine Amri et al. (2020). *Forescout*. "AMNESIA:33 How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices." Accessed on Jan. 22, 2021, at <https://www.forescout.com/company/resources/amnesia33-how-tcp-ip-stacks-breed-critical-vulnerabilities-in-iot-ot-and-it-devices>.
- 64 Amine Amri et al. (2020). *Forescout*. "AMNESIA:33 How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices." Accessed on Jan. 22, 2021, at <https://www.forescout.com/company/resources/amnesia33-how-tcp-ip-stacks-breed-critical-vulnerabilities-in-iot-ot-and-it-devices>.
- 65 Trend Micro. (Sept. 13, 2016). *Trend Micro*. "Linux Security: A Closer Look at the Latest Linux Threats." Accessed on Feb. 9, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/linux-security-a-closer-look-at-the-latest-linux-threats>.
- 66 Augusto Remillano II and Jemimah Molina. (July 8, 2020). *Trend Micro*. "New Mirai Variant Expands, Exploits CVE-2020-1017." Accessed on Jan. 20, 2021, at https://www.trendmicro.com/en_us/research/20/g/new-mirai-variant-expands-arsenal-exploits-cve-2020-10173.html.
- 67 Fernando Merces, Augusto Remillano II, and Jemimah Molina. (July 28, 2020). *Trend Micro*. "Mirai Botnet Attack IoT Devices via CVE-2020-5902." Accessed on Jan. 20, 2021, at https://www.trendmicro.com/en_us/research/20/g/mirai-botnet-attack-iot-devices-via-cve-2020-5902.html.
- 68 Zhengyu Dong. (Nov. 9, 2020). *Trend Micro*. "An Old Joker's New Tricks: Using Github To Hide Its Payload." Accessed on Jan. 21, 2021, at https://www.trendmicro.com/en_us/research/20/k/an-old-jokers-new-tricks--using-github-to-hide-its-payload.html.
- 69 Vit Sembera. (Dec. 3, 2020). *Trend Micro*. "From Geost to Locker: Monitoring the Evolution of Android Malware Obfuscation." Accessed on Jan. 21, 2021, at https://www.trendmicro.com/en_us/research/20/l/from-geost-to-locker-monitoring-the-evolution.html.
- 70 National Institute of Standards and Technology. (n.d.). *National Vulnerability Database*. "Vulnerability Metrics." Accessed on Feb. 5, 2021, at <https://nvd.nist.gov/vuln-metrics/cvss>.
- 71 Common Vulnerabilities and Exposures. (n.d.). *Common Vulnerabilities and Exposures*. "CVE-2020-1472." Accessed on Jan. 22, 2021, at <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1472>.
- 72 Ophtek, LLC. (n.d.). *Ophtek*. "ZeroLogon is the Latest Microsoft Vulnerability." Accessed on Feb. 10, 2021, at <https://ophtek.com/zerologon-is-the-latest-microsoft-vulnerability>.
- 73 Trend Micro. (n.d.). *Trend Micro*. "What is ZeroLogon?." Accessed on Jan. 22, 2021, at https://www.trendmicro.com/en_us/what-is/zerologon.html.

- 74 Trend Micro. (n.d.). *Trend Micro*. "What is Zerologon?." Accessed on Jan. 22, 2021, at https://www.trendmicro.com/en_us/what-is/zerologon.html.
- 75 Microsoft. (Aug. 8, 2020). *Microsoft*. "Netlogon Elevation of Privilege Vulnerability (CVE-2020-1472)." Accessed on Jan. 22, 2021, at <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-1472>.
- 76 Lindsey O'Donnell. (Jan. 15, 2021). *Threatpost*. "Microsoft Implements Windows Zerologon Flaw 'Enforcement Mode'." Last accessed on Feb. 10, 2021, at <https://threatpost.com/microsoft-implements-windows-zerologon-flaw-enforcement-mode/163104/>.
- 77 FireEye, Inc and Ponemon Institute LLC. (2021). *Respond Software*. "Second Annual Study on the Economics of Security Operations Centers: What is the True Cost for Effective Results?" Accessed on Jan. 19, 2021, at <https://d53g0hkpcf8eh.cloudfront.net/wp-content/uploads/2021/01/Ponemon-Institute-FireEye-Second-Annual-Study-Economics-of-the-SOC-2021.pdf>.
- 78 Trend Micro. (Feb. 10, 2017). *Trend Micro*. "Best Practices: Identifying and Mitigating Phishing Attacks." Accessed on Jan. 24, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/best-practices-identifying-and-mitigating-phishing-attacks>.
- 79 Trend Micro. (Oct. 25, 2018). *Trend Micro*. "Virtual Patching: Patch Those Vulnerabilities before They Can Be Exploited." Accessed on Jan. 22, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/virtual-patching-patch-those-vulnerabilities-before-they-can-be-exploited>.
- 80 Trend Micro. (Feb. 25, 2020). *Trend Micro*. "The Sprawling Reach of Complex Threats." Accessed on Jan. 21, 2021, 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

