TREND MICRO | research

The Sprawling Reach of Complex Threats

2019 Annual Security Roundup

Published by
Trend Micro Research

Stock image used under license from
Shutterstock.com

For Raimund Genes (1963-2017)

Contents

The 2010s saw a shift in the cybersecurity industry, as well as much of the rest of the IT landscape, from on-premise to cloud. This progression was occasioned by innovations in various technologies and in the ways the industry had adapted to a great many changes in the landscape. Unfortunately, it was also mirrored by the evolution of cyberthreats, which had gone a long way from basic and intermittent to complex and persistent. A testament to this was the high-profile threats that made their marks in the security landscape of the last year of the decade, which were notably diverse in terms of the entities and platforms they affected.

Ransomware operators zeroed in on government organizations, and deployed attacks that exhibited technical efficiency and were laced with next-level intimidation tactics. A popular office suite became even more favored among phishers, and cyberespionage campaigns showed an increasing inclination toward compromising mobile devices.

Vulnerabilities continued to set the alarm bells ringing, most blaringly with the disclosure of a “wormable” flaw in a widely used software protocol. In addition, the internet of things (IoT) remained fertile ground for botnets that exploited old and known weaknesses.

Supply chain attacks were in the spotlight thanks mainly to a notorious consortium of hacking groups that targeted e-commerce websites. Threats to software development tools and platforms, particularly those associated with the collaborative approach known as DevOps, became more prominent. And detection-evading “fileless” threats ironically made their presence more felt in the cases of different systems and platforms hit by malware that incorporated them.

Already, enterprises are faced with the challenging tasks of integrating and maintaining cloud, IoT, mobile, and other technologies into their infrastructures. But there is another task that enterprises would do well not to give short shrift to — that of securing their infrastructures at all layers, especially since the landscape is becoming increasingly riddled with complex and persistent threats that could have an impact on their operations, reputations, and bottom lines.

Our latest annual security roundup takes a deep dive into the most important issues that shaped the threat landscape of 2019, thereby providing enterprises with insights into the best practices and strategies for protecting their infrastructures from current and emerging threats.

Ransomware homes in on particular targets

Targeted ransomware plagues government sector

In 2019, ransomware operators' shift to a more targeted approach allowed them to orchestrate attacks where organizations' critical assets, systems, and services were sought after and compromised to bountiful effect.[1] This shift in strategy involved novel attack techniques that enabled them to perform actions such as swiftly moving laterally into the network and deploying as many pieces of malware as possible. One of the more notable techniques operators used in the past year involved compromising rarely targeted resources, such as domain controllers and active directories, in order to cause bigger disruptions and subsequently force affected organizations to give in to their demands.[2]

The effectiveness of the overall shift in strategy was tested and proved in ransomware attacks on the government sector, which became something of a global phenomenon in 2019.[3] This trend was particularly prominent in the U.S., where a number of high-profile ransomware attacks on government entities occurred.

In April, the U.S. Virgin Islands Police Department was hit by a ransomware attack that encrypted internal affairs records and citizen complaints.[4] In August, the city of Lodi, California, suffered from an attack that compromised its financial systems and critical phone lines.[5]

An incident involving the city of Pensacola, Florida, shone a light on a tactic not historically seen in previous ransomware cases. After compromising the city's email and phone services, the group behind the attack, known as Maze, deliberately released 2 GB of the 32 GB of stolen files to prove that it had in fact gotten ahold of the city's data besides encrypting the network. Maze had already leaked stolen data after its other victim organizations missed ransom payment deadlines. In the case of Pensacola, however, the group maintained that it made the move not to pressure city officials into paying the US$1 million ransom it had been asking, but merely to counter the media's claim that it had been stealing data of just a few files.[6]

The success of Maze's attack could be attributed to the capability of the deployed ransomware, also called Maze, to automatically copy all affected files to servers controlled by its operators. This capability results in an additional burden to victim entities: Not only would they have to deal with data encryption, but they would also have to reckon with the aftermath of a data breach. Security experts have remarked on the effect this could have on the implementation of incident response in organizations, seeing as the IT department would now have to coordinate with legal and other departments to plan additional recovery steps.[7]

Another important development seen in 2019 was the formation of alliances between ransomware groups, including at least two that targeted U.S. government organizations, and "access-as-a-service" providers, or entities that rent out or sell access to different company networks. The latter, which rely on network intrusion experts, price their services from US$3,000 to US$20,000, with their most expensive "package" including full access to a company's administrative panel, server hosts, and virtual private networks (VPNs).[8]

The operators behind Ryuk, who launched a ransomware attack on the Office of Technology Services of Louisiana in November,[9] were believed to have been working with access-as-a-service providers. They reportedly had been renting access-as-a-service malware such as Trickbot to gain unauthorized entry into systems of organizations whose networks had been infected with the malware.[10] Another group that is infamous for working with access-as-a-service providers is the one behind the Sodinokibi ransomware, aka Sodin or REvil. In August, the operators of Sodinokibi launched coordinated attacks on 22 local government units in Texas, demanding a combined US$2.5 million ransom. The ransomware was said to have been deployed through compromised third-party software that was shared by the victim municipalities.[11]

At least 110 state and municipal governments and agencies in the U.S. fell victim to ransomware attacks in 2019. Despite the unprecedented spate of attacks on government entities,[12] however, the healthcare sector remained the top ransomware target in the U.S., with more than 700 healthcare providers affected by ransomware in the past year. The U.S. education sector was not far behind the government sector, with over 80 universities, colleges, and school districts hit.[13] Ransomware operators target the healthcare, government, and education sectors because the damage they could exact extends beyond the victim organizations. Concerned individuals would also be affected since these sectors provide services that are essential to them. These sectors cannot afford to have their services taken offline or otherwise disrupted because of the far-reaching consequences.

Insurance coverage gains more prominent role in ransomware payouts

It could be surmised that ransomware operators increasingly targeted the government sector in 2019 because of the willingness of many victim organizations to pay the ransom. This trend could be a progression from previous attacks in the private sector where victim companies had shown a propensity to pay ransomware operators; in 2017, for example, about half of victim companies in the U.S. reportedly paid at least one ransom.[14] In their desire to cut losses from the disruption of their operations, victim organizations would rather negotiate with and subsequently pay ransomware operators than ignore their demands.[15]

In July, the government of LaPorte County, Indiana, found its systems paralyzed by ransomware whose operators had demanded US$250,000. It agreed to pay US$132,000 instead, US$100,000 of which was covered by its insurance provider. The county commission's president called the move an "economic decision," meant to curtail the time necessary to restore operations. In the same month, the city of New Bedford, Massachusetts, offered to pay attackers who had locked up its computers only US$400,000 instead of the US$5.3 million that they had asked for. The city mayor later revealed that while he was initially hesitant to offer payment, it would have been remiss of him not to consider the possibility of receiving the decryption key if the full cost of the ransom could be covered by the insurance provider.[16]

Evidently, insurance providers' coverage of a large portion of the payouts in ransomware attacks helps expedite the recovery of encrypted data and disabled systems. But victim organizations' increasing reliance on it is concerning in that it encourages cybercriminals to target more entities that may have insurance coverage.[17]

No less than the FBI remained firm on its stance against paying ransom. In September, the agency's Cyber Section chief advised victims to refuse paying ransomware operators because doing so does not guarantee that their data and systems will be restored. In one example he cited, a ransomware victim paid the operators in hopes of receiving a decryption key, but the key that was provided erased all of the victim's data.[18]

Notable ones emerge among relatively few new ransomware families

There was an uptick in our detections of ransomware-related threats (files, emails, and URLs) in 2019. The slight increase could be reflective not only of our proactive blocking of ransomware-related activities at the email and URL layers, but also of an overall improvement in security mechanisms that blocked ransomware past its download stage.

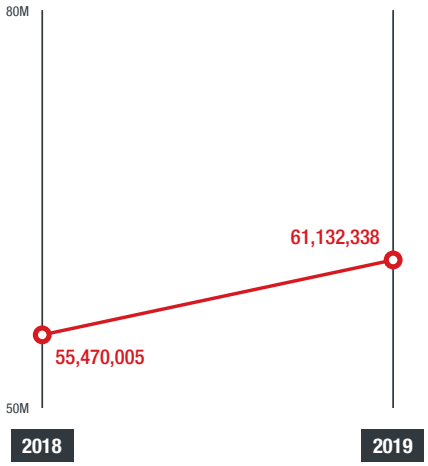

Figure 1. Ransomware-related threat components (files, emails, URLs) slightly increased:
Year-on-year comparison of the number of detections of ransomware-related threats

Source: Trend Micro™ Smart Protection Network™ infrastructure

The number of new ransomware families continued to decline from year to year, with just under a hundred detected in 2019 — fewer than half of the corresponding count in 2018. This could mean that threat actors had found a firmer footing in selective targeting than in creating new forms of ransomware.

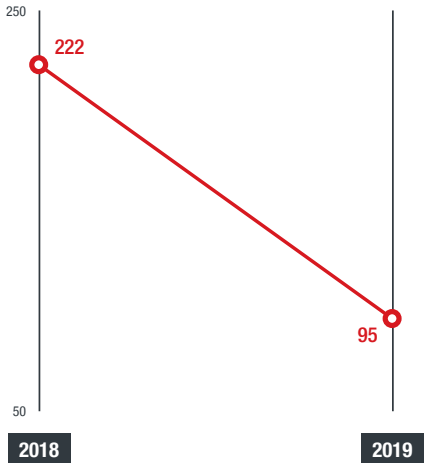

Figure 2. New ransomware families declined:
Year-on-year comparison of the number of detections of new ransomware families

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

Nevertheless, threat actors were able to spawn new ransomware families that can be considered impactful and notable in their technical capabilities. One of these was the Snatch ransomware, which was first spotted in October and had been used in attacks on organizations in the U.S., Canada, and several countries in Europe.[19] Snatch can force Windows machines to reboot into safe mode in order to bypass security software and encrypt files without being detected. This capability was crafted to take advantage of some security software that does not run in safe mode, which is meant for recovering a corrupt operating system and debugging.[20]

Ransomware family	How it can arrive and attack vectors used	How it can propagate	Notable characteristic
Maze[21]	Malicious spam, fake cryptocurrency websites, exploit kits	Compromised software, compromised frameworks (e.g., PowerShell), other malware variants	Exfiltrates files before encrypting machines and network shares
Snatch[22]	Exposed remote desktop ports	Compromised remote desktop services, domain controllers, compromised legitimate tools (e.g., PsExec)	Reboots infected machines into safe mode to evade detection
Zeppelin[23]	Compromised remote desktop control tools, malvertisements, compromised websites	Compromised frameworks (e.g., PowerShell)	Wraps its executables in three layers of obfuscation
LockerGoga[24]	Compromised credentials, compromised active directories[25]	System administration and possibly penetration testing and other hacking tools, valid certificates to evade detection and get into systems	Modifies passwords of infected systems' user accounts, prevents infected systems from being rebooted
Clop (CryptoMix)[26]	Compromised active directories[27]	Compromised remote desktop services	Uses executables with a valid digital signature for distribution

Table 1. Notable new ransomware families used varying and technically efficient methods: Comparison of the routines of notable ransomware families that emerged in 2019

Another new ransomware family of note was Zeppelin, which was first seen with compilation timestamps of no earlier than November and observed infecting companies in the U.S. and Europe. Samples of Zeppelin showed that it is highly configurable and can be deployed as a .dll or .exe file, or wrapped in a PowerShell loader. Aside from encrypting files, it is capable of terminating various processes. And its ransom notes have different versions, varying from generic messages to longer ones customized to its target organizations.[28]

Another new family that stood out was the aforementioned Maze ransomware, which can automatically copy all affected files to operator-controlled servers. The eponymous group behind Maze also used fake cryptocurrency sites, malicious spam campaigns, and even exploit kits to breach a network.[29] Maze's successful breach of its targets' networks has earned its operators a reputation for releasing stolen data if their victims decline or fail to meet their monetary demands.

Messaging threats remain viable for attackers

Phishing threats to Office 365 increase twofold

Phishing was the top threat to organizations in 2019, according to our latest Cyber Risk Index study, which surveyed more than a thousand organizations in the U.S.[30] But while phishing persisted in the past year, our detections of activities related to it dropped from the previous year. The instances of blocked access to non-unique phishing-related URLs decreased by 28% from 2018. And the number of users who would have been affected by phishing-related sites also declined; the instances of blocked access to phishing URLs by unique client IP address decreased by 38% from the previous year. The growing number of enterprise users of newer messaging platforms such as Slack as alternatives to email might have contributed to the drop in detections.

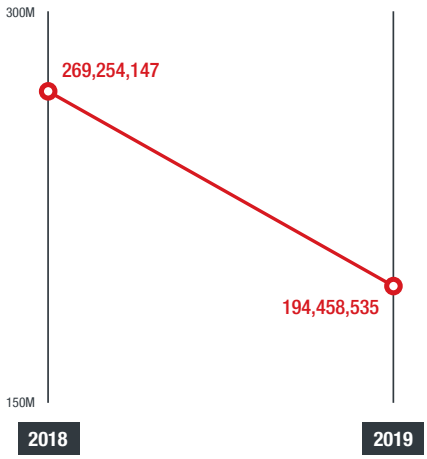

Figure 3. Detected attempts to visit phishing-related sites continued to decline:
Year-on-year comparison of the number of instances of blocked access to non-unique phishing URLs
(e.g., three instances of blocked access to the same URL counted as three)

Source: Trend Micro Smart Protection Network infrastructure

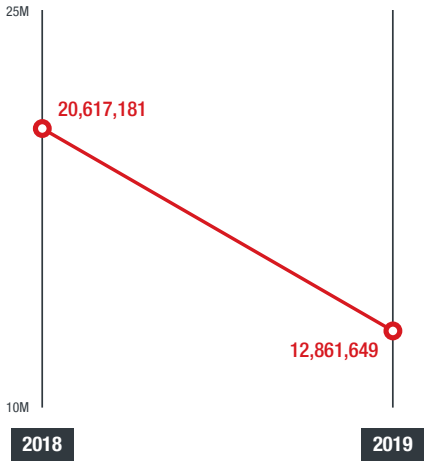

Figure 4. The number of users who would have been affected by phishing-related sites decreased: Year-on-year comparison of the number of instances of blocked access to phishing URLs by unique client IP address (e.g., one machine that attempted to access the same URL three times was counted as one)

Source: Trend Micro Smart Protection Network infrastructure

Despite the decrease in overall phishing activities, phishing URLs that spoofed Microsoft Office 365, particularly Outlook, continued on an upward trend. The number of blocked unique Office 365-related phishing URLs in 2019 doubled from the previous year.

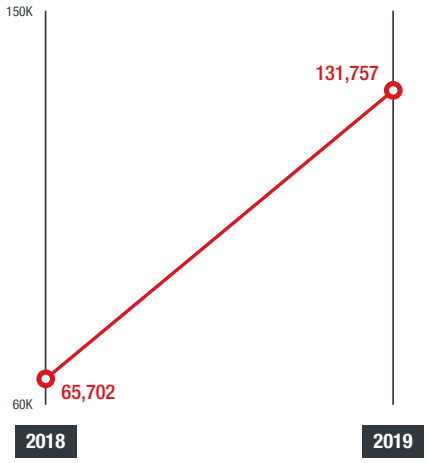

Figure 5. The number of blocked unique phishing URLs that spoofed Office 365 (including Outlook) doubled: Year-on-year comparison of the number of blocked unique Office 365-related phishing URLs

Source: Trend Micro Web Reputation Service

The widespread adoption of Office 365, which reached the 200 million monthly active users milestone in October,[31] is one reason for its sustained popularity as a prime target among cybercriminals. Another is the value of Office 365 accounts for spamming: Cybercriminals are inclined to abuse the Microsoft email architecture, which also includes Hotmail, Live Mail, and MSN Mail, because phishing emails coming

from Microsoft's email services are likely whitelisted or are more difficult for security solutions to block. In addition, a compromised Office 365 account could allow a cybercriminal to conduct internal phishing attacks in an organization without needing to spoof an email address, making it harder to spot the attacks.

Phishing scams pull new tricks

Cybercriminals had been continually refining their techniques to improve their chances of deceiving users of messaging tools such as email and SMS. This much was indicated by the advanced methods used by phishers in 2019.

In April, we reported on a campaign that carried out a new credential-phishing technique[32] through the abuse of SingleFile, a web extension for Google Chrome and Mozilla Firefox. Cybercriminals used the otherwise non-malicious extension to produce identical copies of legitimate login pages that could steal victims' login credentials.[33]

We also observed a credential-phishing technique capable of breaking two-factor authentication mechanisms by compromising one-time passwords (OTPs). This scheme, which was observed to have been prevalent in Japan in 2019, is directed toward online banking users. The phishing emails or SMS messages sent by the cybercriminals behind the scheme lead users to bogus online banking login pages. If a user logs in to a phishing page, the user's credentials are stolen and simultaneously used by the cybercriminals to log in to the actual online banking login page of the spoofed bank. This then prompts the bank to verify the user's identity through an OTP. Once the user receives the OTP and enters it into the phishing page, the cybercriminals are able to steal it as well and use it to successfully compromise the user's account.[34]

Cybercriminals had also managed to integrate the process of hijacking web search results for phishing. In 2019, they used poisoned Google search results to redirect phishing victims to an attacker-controlled page. To successfully do this, cybercriminals first funnel web traffic, which is hijacked from legitimate websites, to websites that they have control over. These websites then become the top Google search results for specific terms. The cybercriminals then send emails with links to the poisoned Google search results. Victims who click on the Google links and subsequently the top results are led to an attacker-controlled website before being redirected to a phishing website.[35]

Another notable technique seen in phishing campaigns in the past year was the use of custom "404 Not Found" pages. Instead of creating a single phishing website to redirect their victims to, cybercriminals register a domain and configure a custom "404 Not Found" page that poses as a login form to potential victims. Configuring a 404 error page allows cybercriminals to pair their domain with an infinite number of phishing landing pages.[36]

BEC operators expand from traditional targets

Business email compromise (BEC) — which includes CEO fraud, bogus invoice, and account compromise, among other schemes — is a form of cybercrime that relies on social engineering to trick members of a target organization into sending sensitive information and wiring funds to attackers.[37] According to the FBI's Internet Crime Complaint Center (IC3), BEC had been the internet crime type with the biggest gains for cybercriminals; in 2019 alone, BEC operators bilked organizations of nearly US$1.8 billion.[38]

A trend we observed in 2019 showed BEC operators expanding from their traditional enterprise victims. Religious,[39] educational,[40] and nonprofit[41] organizations were not spared from BEC attacks. And the public sector, particularly U.S. government entities, became frequent targets.

In June, the city of Griffin, Georgia, lost over US$800,000 to a BEC scam. BEC operators managed to trick city officials by posing as a longtime contractor and rerouting the stolen amounts in two separate transactions to a fraudulent bank account. One of the emails from the BEC operators requested a change in bank account information, which the recipient complied with. To make the scam appear more authentic, the scammers also used electronic invoices that contained information the city officials could verify.[42]

A similar scheme was employed by BEC operators in October against the town of Erie, Colorado. They inveigled town officials into wiring more than US$1 million to a fraudulent account by posing as a contractor that they were supposed to have been working with for a local bridge project.[43]

Our detections of BEC attempts, at around 13,000, registered only a 5% increase from the previous year. But this plateauing suggests that cybercriminals still recognized the high return on investment on BEC scams. Indeed, a single successful attempt could make for a lucrative yield, even factoring in the research and other efforts that went behind it.

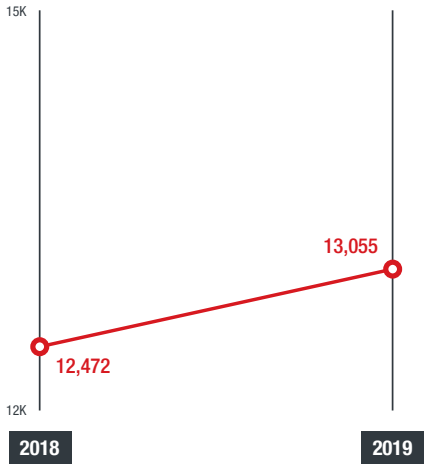

Figure 6. BEC attempts plateaued: Year-on-year comparison of the number of detections of BEC attempts

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

Source: Trend Micro Smart Protection Network infrastructure

The BEC attempts that we detected came from different countries, with most of them detected in the U.S., Australia, and the U.K. It should be noted that these countries are business hubs where headquarters of many multinational companies are based. Thus, while the number of attempts may be indicative of our customer user base distribution, it makes sense for a lot of these attempts to be directed toward them.

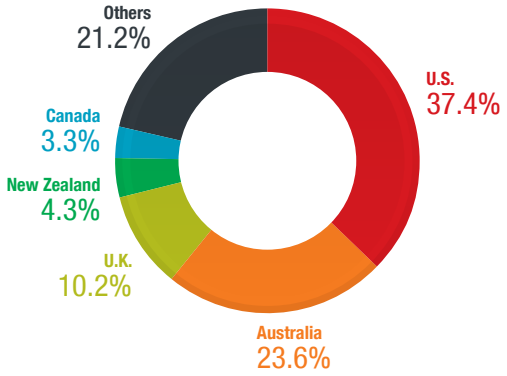

Figure 7. The majority of BEC attempts were detected in the U.S.:
Distribution of detections of BEC attempts by country

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

Source: Trend Micro Smart Protection Network infrastructure

Among the top five most targeted positions in BEC attempts that we detected were professor and accountant, supporting our security prediction for 2019 that, apart from high-ranking company members, BEC scammers would target employees several levels down the company hierarchy.[44] This appeared to be the case particularly in the education sector, where a number of BEC attacks were reported in the past year.[45]

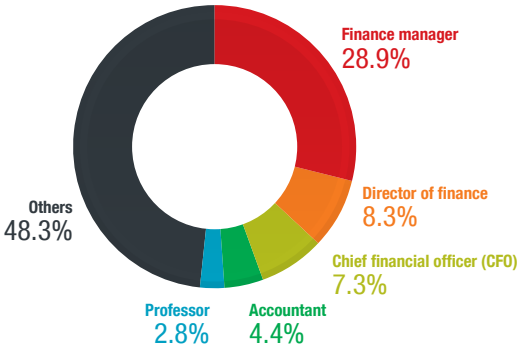

Figure 8. Positions other than high-ranking ones were among the top targeted positions in BEC attempts:
Distribution of targeted positions in BEC attempts detected in 2019

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

Source: Trend Micro Smart Protection Network infrastructure

In our detections, positions of high operating authority were, unsurprisingly, still the most spoofed by scammers, with the CEO impersonated in the majority of BEC attempts.

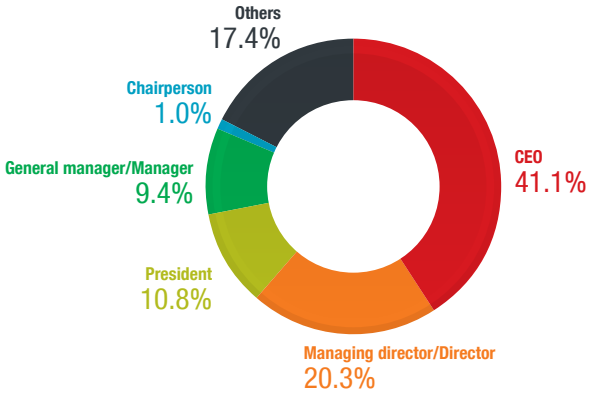

Figure 9. The CEO was still the most spoofed position in BEC attempts:
Distribution of spoofed positions in BEC attempts detected in 2019

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

Source: Trend Micro Smart Protection Network infrastructure

Critical vulnerabilities threaten old and new systems alike

BlueKeep vulnerability amplifies risks faced by legacy systems

The complexity of current and emerging threats has created a reality where a single unpatched vulnerability can put an entire organization at great risk. One need look no further than the damage caused by the WannaCry ransomware outbreak in 2017 due to unpatched systems: more than 230,000 computer systems infected in 150 countries and approximately US$4 billion in financial losses.[46] Organizations that use legacy systems are facing even more serious risks as computers that run on outdated operating systems are at peril of vulnerabilities that are no longer addressed by security fixes.

Threats to legacy systems, specifically those developed by Microsoft, were amplified anew in May when the company released a security guidance for BlueKeep (CVE-2019-0708), a vulnerability in its Remote Desktop Protocol (RDP). BlueKeep affects Windows 7, Windows 2003, Windows Server 2008 R2, Windows Server 2008, and Windows XP — legacy systems that a number of enterprises continue to use in their daily operations. If successfully exploited, the vulnerability can be used for remote code execution (RCE) attacks via the Remote Desktop Services component of Windows.[47]

BlueKeep was heavily covered in the media because of its potential damage to many systems, with almost a million reportedly affected by it. It was also deemed notable for its "wormability," akin to how the vulnerability used by the EternalBlue exploit was used to infect systems with the WannaCry, Petya, and Bad Rabbit ransomware.[48, 49] But despite experts' assertion of the severity of BlueKeep, more than 800,000 vulnerable systems remained unpatched two months after its disclosure.[50]

In September, threat actors started using BlueKeep in attacks to download and execute obfuscated PowerShell scripts, which installed and ensured the persistence of cryptocurrency miners. These attacks were a far cry from the scale of the outbreak caused by the aforementioned ransomware families, since missing in them was the self-propagating capability experts had warned about when BlueKeep first made

headlines. In November, however, Microsoft stated that it could not discount the possibility that future attacks abusing the RDP flaw would be more damaging.[51]

As early as 2018, the IC3, the FBI's center for internet crime complaints, had warned administrators of RDP's susceptibility to exploits. In a public service announcement, it noted that malicious activity concerning RDP had been increasing since mid-late 2016, citing the sale of RDP access in the cybercriminal underground.[52] Sure enough, threats that abuse RDP came into prominence when Microsoft issued its security guidance for BlueKeep in May 2019, and the disclosure of more RDP-related vulnerabilities ensued in the succeeding months.[53]

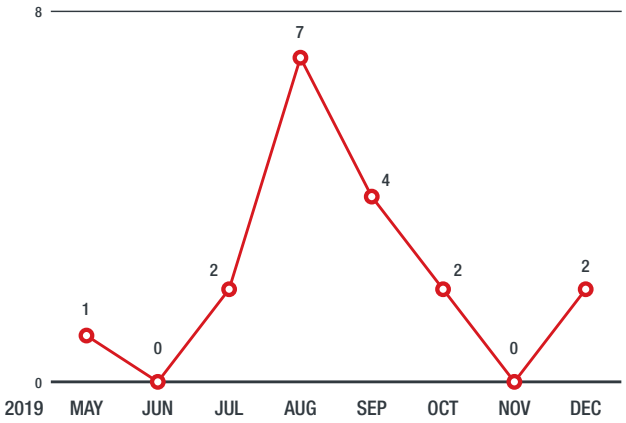

Figure 10. More vulnerabilities in RDP were disclosed in the wake of BlueKeep:
The number of disclosed RDP-related vulnerabilities from May to December 2019

Source: Microsoft

RDP is often used by out-of-office workers and IT teams outsourced by organizations for remote computer access. The protocol provides convenience for "anywhere working" collaboration and IT solution implementation, but it can also make for a convenient attack vector for threat actors.[54] Attacks that effectively abuse RDP allow threat actors to take over affected computers, enabling them to access, process, and use files from drives. Worse, they can be a launching pad for further attacks that can take over the entire network; an open and accessible connection via RDP can allow cybercriminals to compromise devices and other resources connected to it.

Organizations are therefore advised not only to refrain from delaying patches for vulnerable systems but also to upgrade outdated systems such as Windows 7, which accounted for about a third of the operating system market in 2019[55] and support for which was ended by Microsoft in January 2020.[56]

Disclosures of high-severity vulnerabilities more than double

In 2019, the Trend Micro™ Zero Day Initiative™ (ZDI) program published advisories covering 1,035 vulnerabilities, which were accumulated through collaboration efforts with independent researchers and vendors that released patches for the vulnerabilities ZDI reported to them.[57]

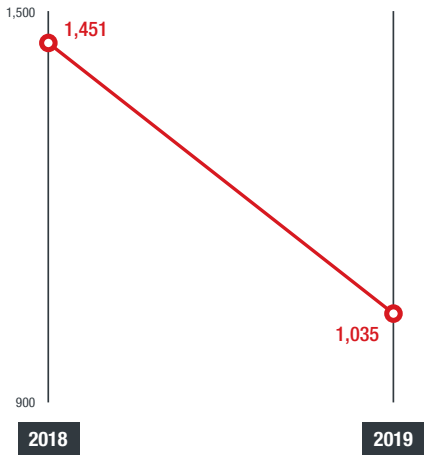

Figure 11. The number of published advisories decreased:
Year-on-year comparison of the number of vulnerabilities disclosed via our ZDI program

Source: Trend Micro™ Zero Day Initiative™ program

The number of reported vulnerabilities decreased by almost a third from the previous year. However, it should be noted that the ones recorded in 2019 were greater in potential impact: Vulnerabilities that were rated with high severity, based on the Common Vulnerability Scoring System (CVSS), increased by 171% from the previous year and made up more than half of the total. Critical-severity bugs, on the other hand, decreased by 64% from 2018 and accounted for only 9% of the published advisories.[58]

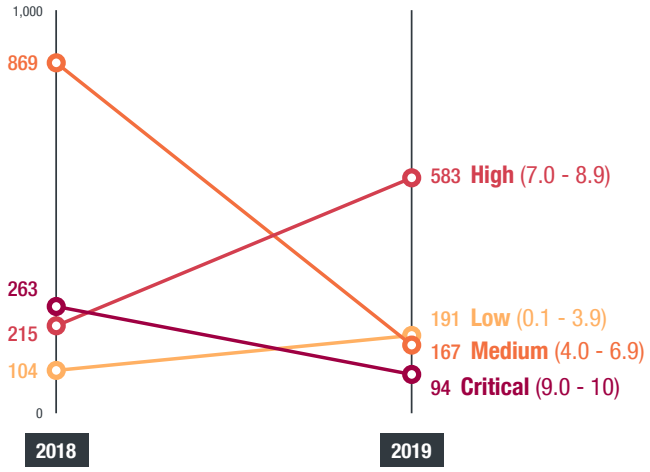

Figure 12. High-severity vulnerabilities increased more than twofold: Year-on-year comparison of the severity breakdown, based on the CVSS, of vulnerabilities disclosed via our ZDI program

Source: Trend Micro Zero Day Initiative program

Disclosed ICS software-related bugs decline

In 2019, based on disclosures made via our ZDI program, the number of zero-day vulnerabilities and that of known or non-zero-day (n-day) vulnerabilities in software used in industrial control systems (ICSs) dropped by 79% and 11%, respectively, from the previous year.

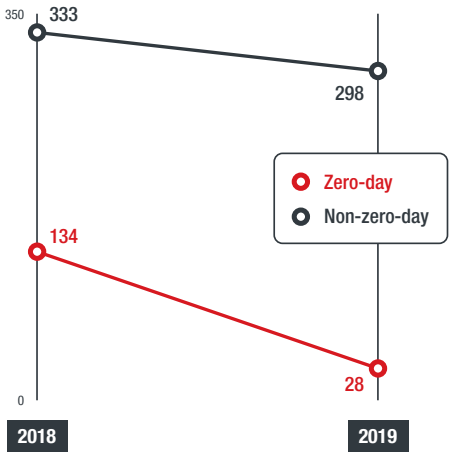

Figure 13. Disclosures of ICS software-related zero-day vulnerabilities decreased considerably: Year-on-year comparison of the number of ICS-related vulnerabilities disclosed via our ZDI program

Source: Trend Micro Zero Day Initiative program

Most of these flaws were found in human-machine interfaces (HMIs), which serve as hubs for managing critical infrastructures and monitoring different control systems that directly influence operations. As such, they can be abused by threat actors in attacks to cause disruptions.

Securing ICS environments is expected in the coming years to become an even more important imperative for enterprises that have them, as their adoption in the era of the industrial internet of things (IIoT) continues to widen.[59] For one thing, the market for supervisory control and data acquisition (SCADA), a subset of ICSs, is forecast to grow to US$15.2 billion by 2024.[60]

Multiple botnet attacks exploit common IoT device flaws

The number of IoT devices is expected to grow to 22 billion by 2025.[61] The prevalence of these devices in homes, offices, and cities has afforded people opportunities to take advantage of one of the most important technologies of the modern era. But as with any widely used technology, cybercriminals have also turned the IoT into a platform for conducting attacks.

Cybercriminals turn to IoT devices to take advantage of their often vulnerable state. Because patching them can be slow and problematic, IoT devices tend to be vulnerable for longer than traditional computing systems. This reality paved the way for the repeated use of old and known IoT device vulnerabilities by multiple botnets in 2019.

In April, for instance, we reported on a variant of the notorious Mirai malware (detected by Trend Micro as Trojan.Linux.MIRAI.SMMR1) that uses multiple exploits to target various routers and other IoT devices.[62] A month later, we highlighted another Mirai variant (Backdoor.Linux.MIRAI.VWIPT), which exploits some of the flaws abused by the former, including an arbitrary command execution vulnerability (CVE-2017-17215) in Huawei HG532 routers.[63]

This latter Mirai variant also notably exploited a remote arbitrary command execution vulnerability (CVE-2016-6277) in Netgear R6400 and R7000 routers. This vulnerability, in turn, is also part of the exploit arsenal of an Echobot botnet variant that uses more than 50 exploits and targets routers, network-attached storage devices, security cameras, smart home hubs, and other devices.[64]

Another pair of botnet variants that was found exploiting a common exploit was Neko and Momentum, which we reported in July and December, respectively, to have exploited a command execution vulnerability (CVE-2014-8361) in Realtek SDK-based routers.[65, 66]

Cybercriminals are also known to use brute-force attacks, in which they try out a large number of consecutive login credential guesses to gain access to unsecure devices. They typically use leaked, common, or even default usernames and passwords for their brute-force attempts, taking advantage of many IoT adopters' failure to change and update their devices' credentials. Based on our telemetry, which included feedback from third-party routers, the number of events involving brute-force logins in 2019 was nearly triple the corresponding count in 2018.

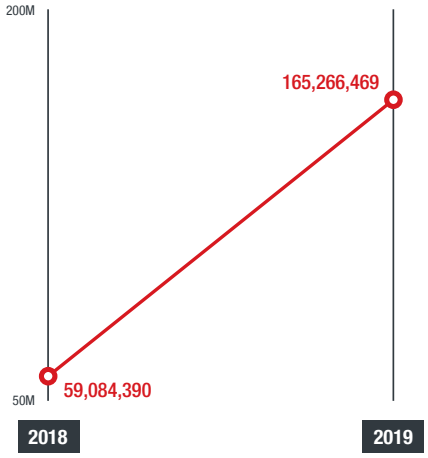

Figure 14. Brute-force logins surged:
Year-on-year comparison of the number of triggered inbound and outbound events involving brute-force logins

Source: Trend Micro™ Smart Home Network solution

Threats seep through gaps in supply chains and development pipelines

Magecart supply chain attacks hit e-commerce websites

The past year saw a rise in cases of supply chain attacks, or attacks that compromise a service or organization through an external partner or third-party provider that has access to its data or systems. And nowhere was this observation more evident than in the attacks tied to Magecart, a consortium of hacking groups that compromise e-commerce websites usually by going after their third-party shopping cart systems, such as Magento or OpenCart, to steal customer payment card information. As of October, Magecart had already compromised, either via supply chain attacks or directly, more than two million sites.[67]

Among the Magecart campaigns we observed in 2019, two operations stood out. One of these was a campaign launched by Magecart Group 12. In January, we found that Magecart Group 12 had infected 277 e-commerce sites — including ticketing, touring, and flight booking sites, and online stores of apparel, cosmetic, and healthcare brands — by compromising their third-party advertising service. The group injected skimming code into the service's JavaScript library, enabling the group to steal the payment information entered by users on the sites.[68]

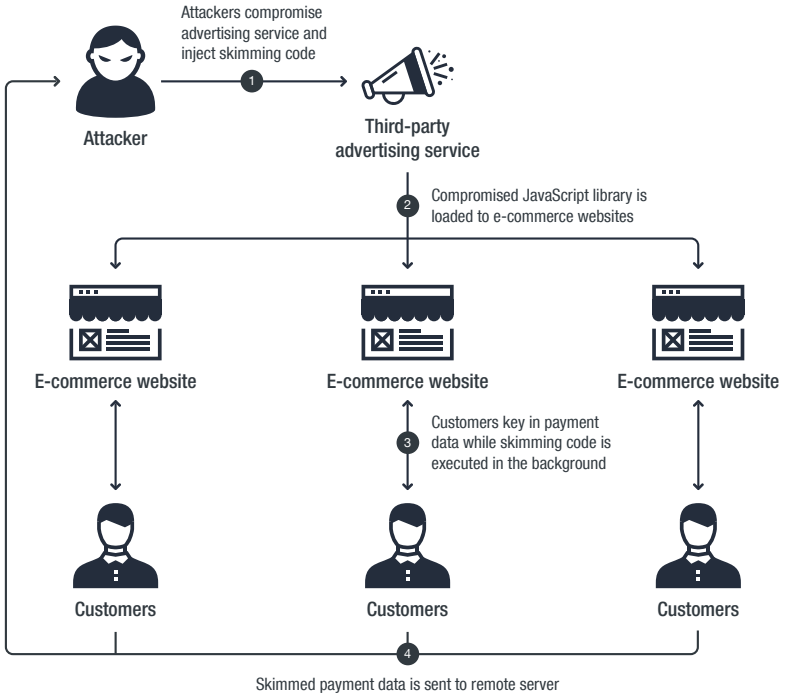

Figure 15. Magecart Group 12 compromised e-commerce sites by breaching a third-party advertising service: The infection chain of Magecart Group 12's campaign

The other notable card-skimming operation was one that we believe was launched by FIN6. From September to October, the campaign operated on 3,126 online shops hosted on one of the top e-commerce platforms in the market. The group injected malicious code into a JavaScript library provided by the e-commerce platform to their client shops, and this was followed by the loading of another JavaScript file stored on a cloud storage service. The loaded script was almost an exact replica of a normal JavaScript library but was subtly integrated with a credit card skimmer. Customers who visited the infected websites, most of whom were from the U.S., unknowingly submitted their credit card details to an exfiltration server.[69]

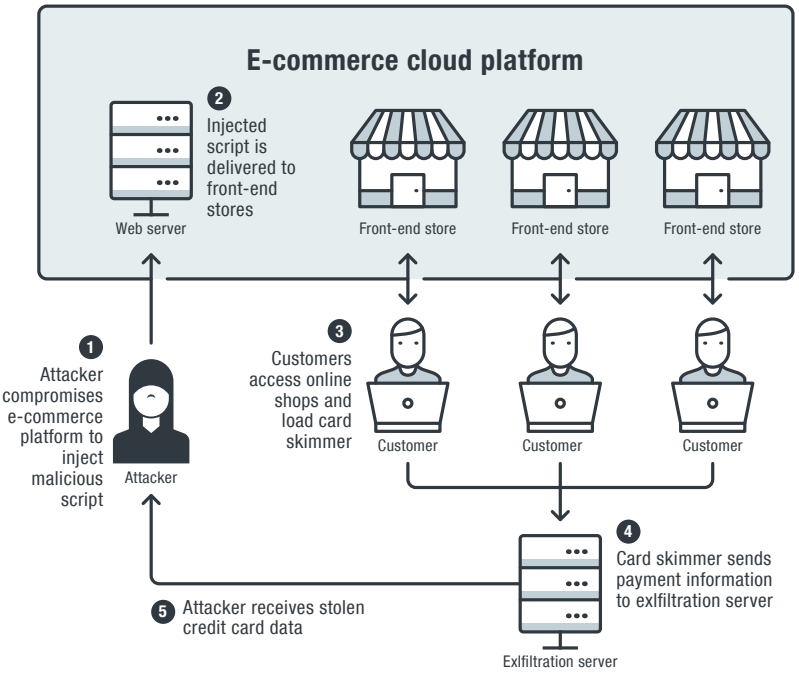

Figure 16. FIN6 compromised sites hosted on one of the top e-commerce platforms in the market: The infection chain of FIN6's campaign

The prevalence of supply chain attacks on e-commerce sites underlines the need for website owners to closely monitor security gaps in the platforms and services that they use and to implement stronger authentication mechanisms. For their part, users should keep an eye out for red flags when visiting e-commerce sites, especially since the number of reported cases of victims keeps on growing; in Japan, the pervasiveness of card skimming in e-commerce sites prompted the government to issue a warning to users in 2019.[70]

Threats to software development tools and platforms rise

DevOps is a range of tools and cultural philosophies for streamlining software or application release cycles. This approach has been helpful for organizations that want improved quality, security, and scalability for software development.[71] But while DevOps has given organizations an option for a faster and more efficient development process, the security aspect of it is sometimes overlooked, allowing threat actors to take advantage of components in the process with exploits and malicious code. For instance, there can be a tendency not to hold external parties to the same security standards implemented by the organizations themselves, which can lead to attacks such as code tampering, a technique often used in supply chain attacks.[72] The process DevOps practitioners are operating in should take this and other security issues into account to avoid system compromise. Threat actors can undermine the development pipeline of an

enterprise by interfering with a part of its software supply chain, and gaps in DevOps tools and platforms — such as those observed in 2019 — could enable them to that end.

In June, we spotted an API misconfiguration in the open-source version of the popular DevOps tool Docker Engine – Community that could allow attackers to compromise containers and run AESDDoS, a Linux botnet malware variant. The execution of the malware enables attackers to take over the host and gain remote access to servers and hardware resources.[73] Also in the same month, the developers of the widely used container orchestration system Kubernetes disclosed a high-severity vulnerability (CVE-2019-11246) in its command-line interface. Successfully exploiting the flaw could result in a directory traversal, enabling an attacker to use a malicious container to create or replace files in an affected workstation.[74]

In July, we discovered security weaknesses in Jenkins, an automation server also used by practitioners, that could subject it to attacks. We observed that a user account with insufficient privileges could gain administrator rights over Jenkins, potentially allowing an attacker to perform RCE on its master machine. This risk stems from the improper configuration of the automation server's security settings.[75] In August, we also reported about four vulnerabilities that affect Jenkins plugins whose successful exploitation could lead to the theft of sensitive user credentials.[76]

Unsecure Docker hosts were also subjected to a variety of attacks in the past year, including one that involved cryptocurrency-mining malware, which was uncovered in October. Targeted hosts that lacked authentication measures were infected with the malware. This incident resulted in the infection of more than 2,000 Docker hosts by a worm that discreetly used them to mine Monero.[77]

Poor software development practices can allow attackers to compromise DevOps tools and platforms, with the potential damage extending to organizations' physical, virtual, cloud, and container environments. As illustrated by two of the aforementioned examples, improper configuration of security settings could lead to system compromise. In addition, attackers could infect systems if the integrity of the source code, compiler libraries, and binaries, among others, are not properly maintained and cross-validated.[78]

Threat actors enhance stealth with crafty components

Fileless threats become common occurrence

Threats that abuse fileless components differ from traditional malware because in their case malicious software or executables are not a prerequisite for infecting a system. Rather, these threats rely on legitimate system administration or penetration testing tools, such as PowerShell, Windows Management Instrumentation (WMI), AutoHotKey, and PsExec, to remain under the radar. Be that as it may, we are able to detect fileless threat-related activities by tracking non-file-based indicators and through technologies like endpoint investigation and response, which can monitor events and analyze what processes or events are triggering malicious activity.[79]

In the past year, we blocked more than 1.4 million fileless events. This large number affirmed our prediction for 2019 that threat actors would increasingly "live off the land," or take advantage of a machine's built-in applications and tools for their attacks to evade detection.[80]

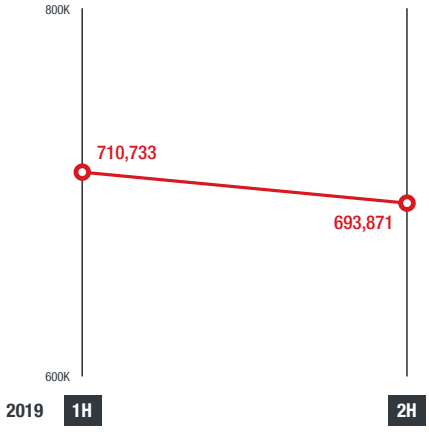

Figure 17. More than 1.4 million fileless events were blocked:
Half-year comparison of the number of fileless events blocked in 2019

Source: Trend Micro Smart Protection Network infrastructure

This was hardly surprising, especially since numerous malware campaigns were observed using fileless components in their attacks. These campaigns used fileless components in evasion methods, persistence mechanisms, and payload downloading and execution, among other stages of their attack chains.

In March, a campaign targeted three Brazilian banks to access users' banking accounts and steal personally identifiable information gathered from their visited websites and recorded machine credentials, which can be further abused or sold. The campaign used PowerShell to download a banking trojan.[81]

In August, we uncovered GhostMiner, a fileless cryptocurrency-mining malware variant that weaponized WMI objects for its fileless persistence, payload mechanisms, and antivirus-evasion capabilities. Previously, the variant was observed exploiting multiple flaws in Microsoft SQL Server, phpMyAdmin, and Oracle WebLogic Server to compromise vulnerable servers.[82]

The following month, Emotet reemerged after a brief hiatus and targeted English-, German-, Italian-, and Polish-speaking users with a spate of spam emails. These emails came with Microsoft Word document attachments embedded with a macro that, if enabled, runs a PowerShell script that downloads the Emotet malware from compromised websites.[83] In the same month, we reported on the Purple Fox downloader malware, which we observed abusing PowerShell — its first recorded use of the framework — for its fileless infection capabilities.[84]

Another notable campaign that integrated fileless components into its attacks was KovCoreG. In October, we observed the campaign running a PowerShell script to disable Windows Defender and Windows Update processes. PowerShell was also used by KovCoreG to filelessly execute Novter, which performed anti-debugging and anti-analysis checks, among other backdoor commands.[85]

Targeted attacks intensify use of complex routines

In targeted attacks, threat actor groups actively pursue and compromise their target entities' infrastructures while remaining unnoticed. Threat actor groups accomplish this by employing tactics, techniques, and procedures (TTPs) that allow them to ensure their attacks continue beyond initial network penetration.

In 2019, we observed a pair of notable threat actor groups that used complex TTPs for cyberespionage: Tick and APT33. For its "Operation Endtrade," Tick deployed attacks on industries that deal with highly classified information, particularly defense, aerospace, chemical, and satellite industries with head offices in Japan and subsidiaries in China. Our analysis revealed that the group was still using compromised legitimate email accounts, previously deployed malware, and tools for obfuscation. However, Tick turned out to have improved its arsenal by including new malware families capable of detection and termination of antivirus products, scanning of operating system code pages to check if they use the language Tick

was targeting, escalation of administrative privileges for succeeding attacks, and collection of proprietary information and classified data.[86, 87]

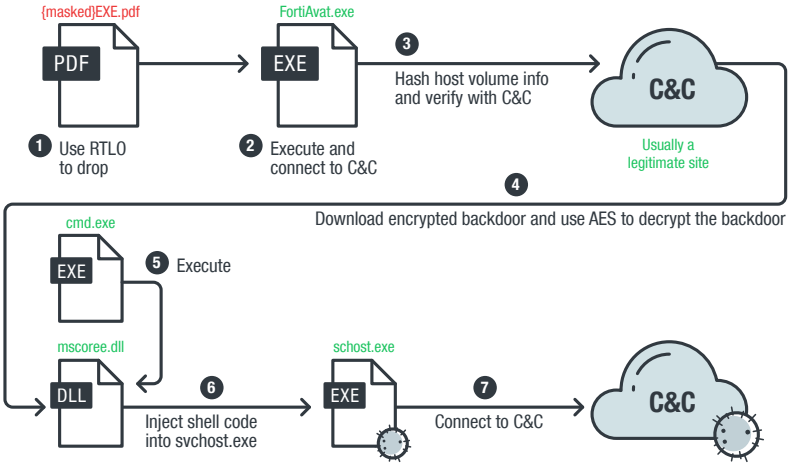

Figure 18. Tick used malware variants that terminated antivirus products: Attack chain of ABK and BBK, downloaders used by Tick

Note: TICK's complete attack chain, mapped using the MITRE ATT&CK™ framework, is included in the "Threat Landscape in Review" section of this report.

As for APT33, we observed the group using about a dozen live command-and-control (C&C) servers for extremely narrow targeting. APT33 put up multiple obfuscation layers to run these C&C servers in hopes of deploying malware campaigns against organizations based in Asia, the Middle East, and the U.S. Our analysis indicated that APT33 took a great deal of care to cover their trails. The C&C domains were usually hosted on cloud hosted proxies, and these proxies relayed URL requests from infected bots to back-ends at shared web servers that might host thousands of legitimate domains. The back-ends reported data back to an aggregator and a bot control server that was on a dedicated IP address. APT33 connected to these aggregators using a VPN with exit nodes that were changed frequently, and used the VPN connections to issue commands to and collect data from the bots.[88]

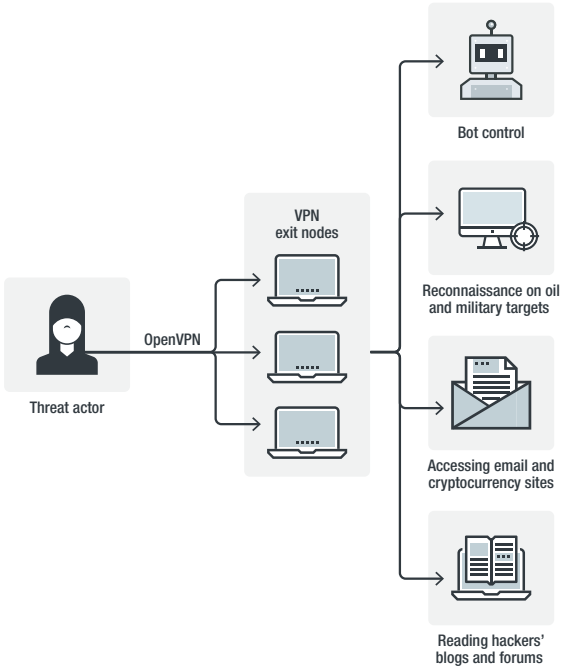

Figure 19. APT33 used a VPN with frequently changed exit nodes: How APT33 used a VPN

Note: APT33's complete attack chain, mapped using the MITRE ATT&CK framework, is included in the "Threat Landscape in Review" section of this report.

Malicious actors continue branching out into mobile and other platforms

Android malware blights official app store

Mobile devices, specifically those running on the Android operating system, remained dependable targets for threat actors in 2019. While the number of malicious Android apps that we blocked decreased from the first half of the year to the second, the total for 2019 was still sizable, at nearly 60 million. This further emphasized cybercriminals' reliance on attacking mobile devices for stealing credentials, deploying malicious advertisements, and cyberespionage, among others.

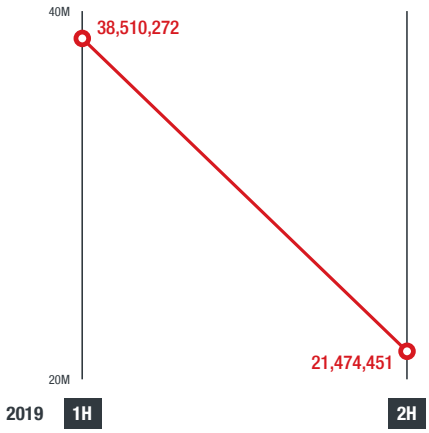

Figure 20. Nearly 60 million malicious Android apps were blocked:
Half-year comparison of the number of malicious Android apps blocked in 2019

Source: Trend Micro Mobile App Reputation Service

One of our biggest mobile threat stories in 2019 involved several malicious Android apps that had been downloaded by users a million times. These apps, which posed as beauty camera apps on the official Google Play app store, were found capable of accessing remote ad configuration servers, which could

then be used for malicious purposes. In our analysis of malicious samples, we found that it was difficult to see red flags in the apps. One of the samples created a shortcut after being launched, but it managed to hide its icon from the app list. This technique made it all but impossible for users to uninstall the app, especially since they would not be able to find it, let alone delete it.[89]

Another interesting development that we observed in 2019 was the rising number of mobile cyberespionage campaigns, signifying that threat actor groups had also been turning their attention to attacking mobile devices. In the past year, we counted 30 such campaigns, including ones carried out by Poison Carp,[90] Rana,[91] and, most notably, MuddyWater, a notorious cyberespionage group with a history of targeting organizations in Middle Eastern and Asian countries. Our analysis of MuddyWater activities, in particular, led to the discovery of its connections to four Android malware variants that posed as legitimate apps,[92] which were found equipped with information-stealing capabilities.[93]

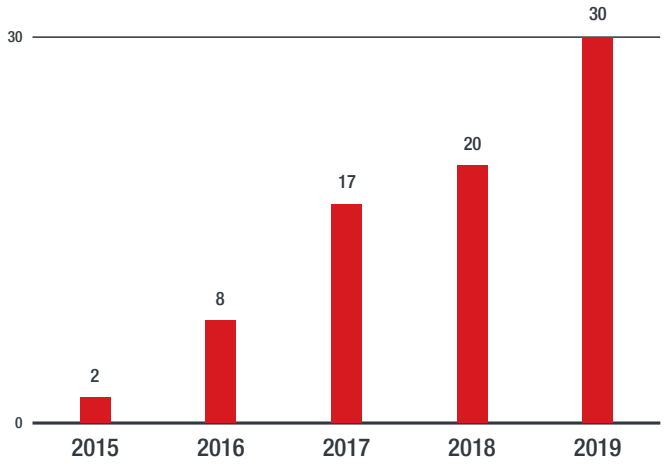

Figure 21. Mobile cyberespionage campaigns continuously increased over the last five years: The number of mobile cyberespionage campaigns from 2015 to 2019

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

Threats break into iOS and macOS

Apple's operating systems — iOS for its smartphones and tablets, and macOS for its desktop and laptop computers — have long been considered highly secure, with the company making continuous efforts to introduce new system protections.[94, 95] However, malicious actors have also been relentless in breaking the security of these devices, churning out threats in 2019 to help them accomplish that goal.

Last year, we found the operators of XLoader, a predominantly Android-targeting malware variant, deploying a scheme that tricked users into installing a malicious iOS configuration profile to steal data from iPhone and iPad devices.[96] We also observed threat actors using an iOS URL scheme that could subject users to privacy violation, bill fraud, and exposure to pop-up ads.[97]

Another of our key iOS threat discoveries involved hundreds of gambling apps that were cloaked in legitimate-sounding names to get past the review process for inclusion in Apple's App Store. Interestingly, some of the apps ranked in the top 100 list of the App Store, including ones that had been rated more than 100,000 times.[98]

The macOS threats we uncovered involved vulnerabilities and malware variants. CVE-2019-8519, a vulnerability in the graphic drivers installed in macOS Mojave 10.14.3, could allow access to restricted information since it leads to a buffer overflow or segmentation fault.[99] CVE-2019-8635, meanwhile, could enable an attacker to implement privilege escalation and execute malicious code on a macOS device with root privileges.[100]

We also spotted a macOS malware variant that spoofed trading apps to lure victims and steal their personal data.[101] And we discovered a macOS backdoor, attributed to the cybercriminal group Lazarus, that had been deployed against Korean-speaking users through macro-embedded Microsoft Excel spreadsheets. The backdoor was found capable of uploading and downloading files, among other malicious functions.[102]

Another notable macOS malware from 2019 was Shlayer, which uses steganography — the practice of hiding code within non-secret text or data — in using low-level manipulation of an image file to conceal a script code that downloads adware.[103] Shlayer was also discovered being dropped alongside another macOS malware variant, Tarmac, in a scheme that tricked users into downloading bogus software updates.[104]

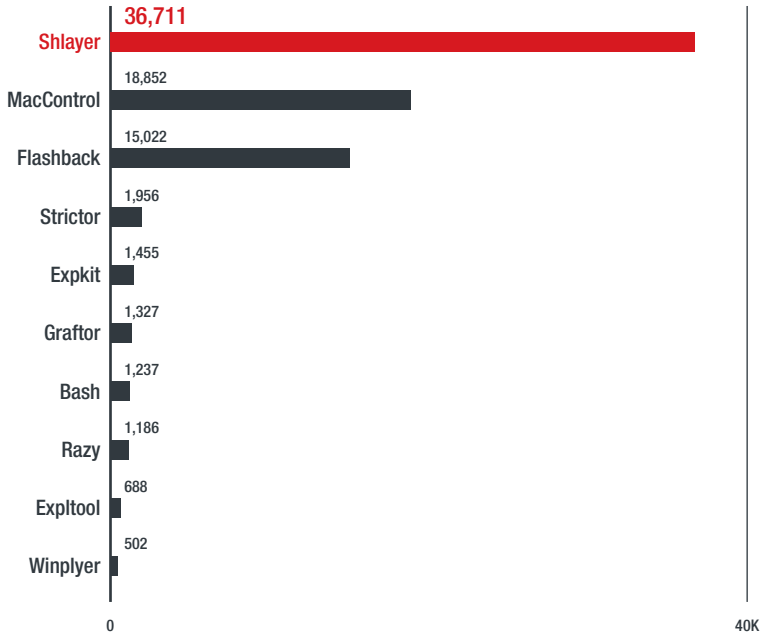

Figure 22. Shlayer was the most detected macOS malware family: Distribution of the top macOS malware families detected in 2019

Source: Trend Micro macOS sample database

Based on our in-house database where macOS samples are processed and analyzed, Shlayer was the top macOS malware family in 2019, with more than 36,000 unique detections, nearly 30,000 of which were in the U.S.

Multilayered security remains most effective defense against threats

Complex and persistent threats have pervaded the cybersecurity landscape. Collectively, these threats are remarkably industry-, platform-, and device-agnostic, and can effectively take advantage of gaps in new as well as old systems. Enterprises, in particular, must therefore reexamine how they implement cybersecurity and fortify their defenses accordingly.

An approach that puts forth a multilayered security strategy is best suited for enterprises dealing with threats that could result in operational disruption, reputational damage, and financial loss. A wide range of security technologies that are functional, innovative, convenient, and cost-efficient can help address the different needs of enterprises. Enterprises should choose solutions that can detect malicious activities in gateways, networks, servers, and endpoints using a mix of detection technologies, such as machine learning, behavioral monitoring, sandboxing, and intrusion prevention. An integrative, attack-centric detection and response solution can also be of great help.[105]

Enterprises should couple their use of multilayered security with industry best practices. Enterprises can stay protected from ransomware attacks by adopting a set of practices that includes creating an effective backup strategy, implementing network segmentation to prevent attackers from accessing parts of the network and corresponding assets in the event of an attack, and monitoring and auditing network traffic for any anomalies or suspicious behaviors.

To reduce the risk of falling victim to messaging threats like phishing and BEC, enterprises should regularly implement security awareness programs. Inculcating members of the organization with habits such as checking emails for grammatical errors and spelling mistakes, examining the email sender's display name, and verifying emails that request sensitive information and fund transfers can go a long way toward thwarting messaging threats.

Enterprises should also monitor vulnerabilities and misconfigurations not only in their own platforms and frameworks but also in their third-party providers'. Regularly checking systems across the board for flaws and errors can help keep enterprises safeguarded from threats that exploit external partners. Enterprises should also ensure that their systems and applications are updated to the latest versions to forestall threats that rely on critical vulnerabilities. For a more efficient patch management process, enterprises should consider adopting virtual patching, which can provide protection against threats that exploit vulnerabilities in outdated operating systems that are no longer being provided with security fixes.

Further, enterprises should keep a regular check on high-privilege software, particularly development tools. To protect these tools from abuse, administrators should always update and strengthen their credentials. Using multi-factor authentication and implementing the principle of least privilege are just a couple of the practices that can shield networks from attacks that rely on compromised tools. Such practices should also be adopted by users for their own computers, smartphones, tablets, and other connected devices.

Threat Landscape in Review

In 2019, the Trend Micro™ Smart Protection Network™ infrastructure blocked more than 52 billion threats, effectively protecting enterprises and users from a multitude of email, file, and URL threat components.

52,265,509,014

Overall threats blocked in 2019

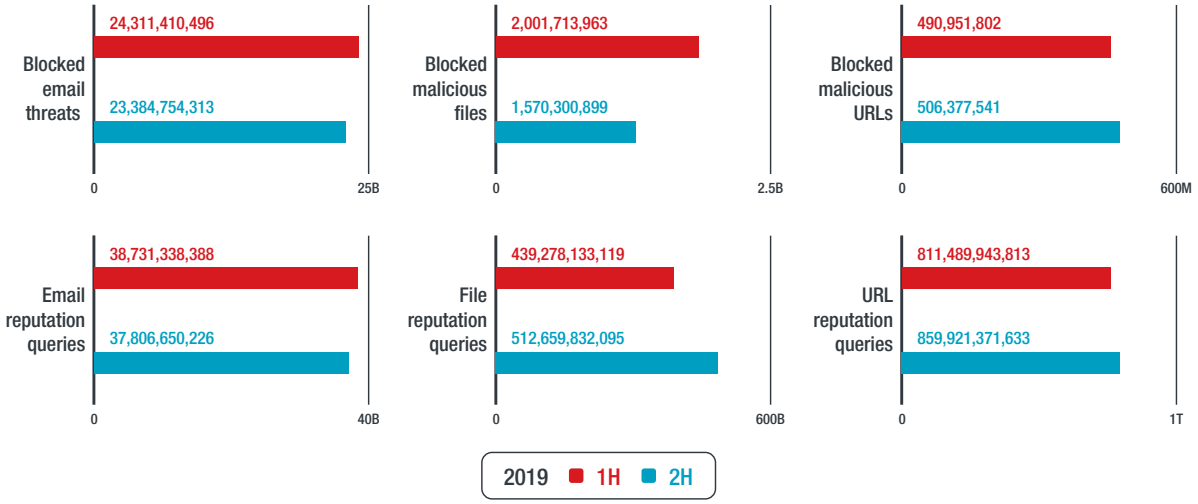

Figure 23. Blocked malicious URLs slightly increased, while blocked email threats and malicious files dropped: Half-year comparison of the numbers of email, file, and URL threats blocked in 2019

Source: Trend Micro Smart Protection Network infrastructure

Despite their relatively low number, the new ransomware families detected in the past year included several that exhibited fine-tuned capabilities from their predecessors or entirely new behaviors.

ANATOVA	BIGBORB	BITLOCKED	BLACKROUTER	BLUEAGLE
BONE	BROWEC	BURAN	BXCODE	CHATER
CLOP	CONTI	CORTEX	COSAKOS	CRAZYCRYPT
CRAZYZIP	CRYPONY	CRYPROTO	CRYPSPORT	CRYPTGO
CRYTEM	CYMRANSOM	DEATHRANSOM	DEMOCRY	DMR
DOGOJOKER	ECHORAIX	EKANS	ENTSCRYPT	ERIS
EXPBOOT	FAKEWCRY	FCRYPT	FREEZING	FTCODE
GOJDUE	GOLANG	GOLDENAXE	GOOD	GORGON
HERMES	HILDA	HOLA	IMSORRY	IRANSOM

JAMPER	JCRY	JUWON	LILOCKED	LOCKERGOGA
LOOCIPHER*	LOOCIPHER*	MAILTO	MAOLOA	MAZE
MEDUSALOCKER	MESPINOZA	MONGOLOCK	MONSTERRAT	MZREVENGE
NEMTY	PAPJ	PHOBOS	PONY	PURELOCKER
RABBIT	RANNOH	RAPID	REDKEEPER	ROBINHOOD
SATANA	SAVEQUEEN	SEEDLOCKER	SENJO	SEON
SHADOWCRYPTOR	SNATCH	SODINOKIBI*	SODINOKIBI*	SPARTCRYPT
SYRK	TELUDEPAS	TFLOWER	TIONE	TREE
TUNCA	VEGA	VIGRA	XCRY	YATRON
YFISNIFFER	ZARLOCK	ZEOTICUS	ZEPPELIN	ZILLA

Table 2. 95 new ransomware families were seen: New ransomware families detected in 2019

**Note: A different ransomware family has the same name.*

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

PDF was the most used file type for spam attachments in our dataset, followed immediately by XLS. Notably, PDF was just behind XLS in 2018.

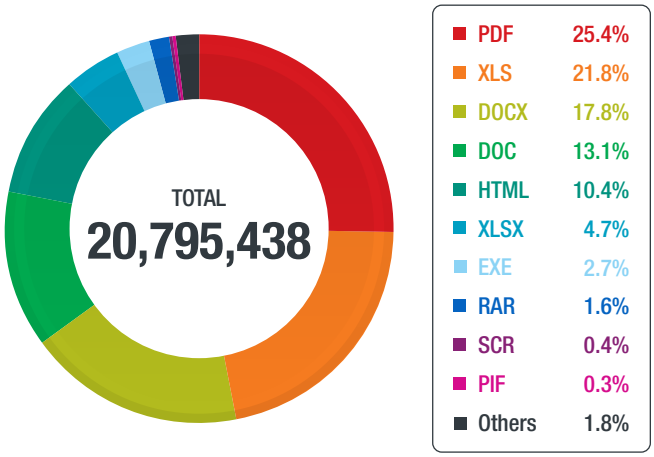

Figure 24. A quarter of the attachments in detected email threats were PDFs: Distribution of file types used as attachments in spam emails detected in 2019

Source: Trend Micro Smart Protection Network infrastructure

One of our security predictions for 2019 forecast an increase in digital extortion schemes, particularly sextortion.[106] The substantial number of sextortion-related spam emails we detected in 2019 — more than 14 million — supported this prediction.

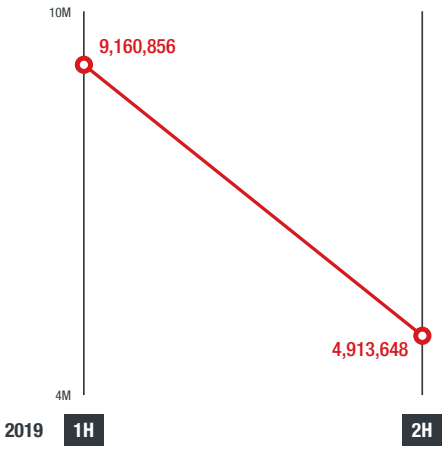

Figure 25. The number of sextortion-related spam emails decreased from the first half of the year to the second, but the total exceeded 14 million: Half-year comparison of the number of detections of sextortion-related spam emails in 2019

Source: Trend Micro Smart Protection Network infrastructure

We observed a 52% increase in exploit kit activities in 2019, suggesting that exploit kits were still being actively used by threat actors.

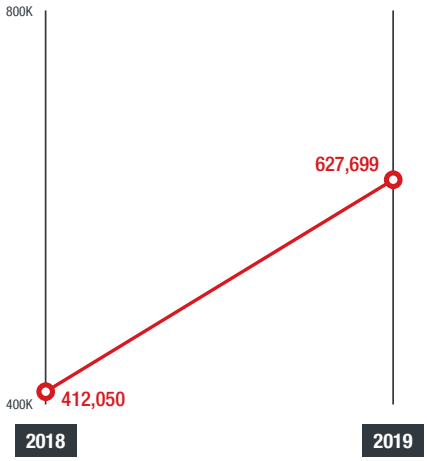

Figure 26. Exploit kit activities increased:
Year-on-year comparison of the number of instances of blocked access to URLs hosting exploit kits

Source: Trend Micro Smart Protection Network infrastructure

GrandSoft was the most detected exploit kit in 2019, with more than 280,000 detections, accounting for nearly half of the total. It overtook Rig, which was the most detected exploit kit in the previous year.

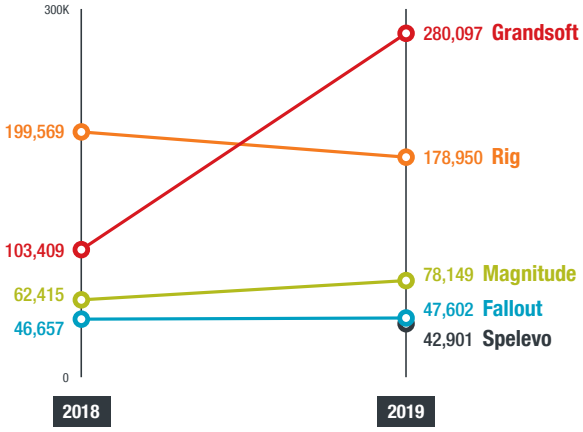

Figure 27. Grandsoft overtook Rig to become the most detected exploit kit:
Year-on-year comparison of instances of blocked access to URLs hosting specific exploit kits

Source: Trend Micro Smart Protection Network infrastructure

Exploit kits still abused old and known vulnerabilities to deliver their payloads, highlighting the need for organizations to regularly patch and update their systems.

Exploit kit	Vulnerabilities exploited	Ransomware delivered
GrandSoft	CVE-2018-4878 CVE-2018-8174	
Rig	CVE-2018-4878 CVE-2018-8174	Aurora, Buran, Crysis, Dharma, Eris, GandCrab, GetCrypt, Nemty, Paradise, Sodinokibi, VegaLocker
Magnitude	CVE-2019-0752 CVE-2018-4878 CVE-2018-8174	Magniber
Fallout	CVE-2018-15982 CVE-2018-4878 CVE-2018-8174	GandCrab, Hermes, Maze, Medusa, Paradise, Sodinokibi
Spelevo	CVE-2018-15982 CVE-2018-8174	Crysis, Maze, Shade, Troldash

Table 3. Exploit kits continued to abuse old and known vulnerabilities:
The top five exploit kits in 2019, the vulnerabilities they exploited, and the ransomware they delivered

Source: Trend Micro Smart Protection Network infrastructure

The number of disclosed vendor vulnerabilities dropped by 29% from the previous year. Microsoft was the vendor with the most reported vulnerabilities, totaling 190, with Adobe not far behind, with 166. Foxit, Apple, and Google had 70, 60, and 4 vulnerabilities, respectively.

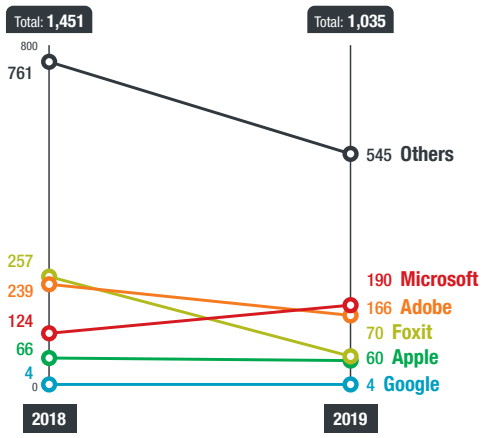

Figure 28. Disclosed vendor vulnerabilities decreased:
Year-on-year comparison of the numbers of disclosed vulnerabilities of selected software vendors

Source: Trend Micro Zero Day Initiative program

Botnets continued to be active in 2019, with our detections of botnet connections totaling just under 1.7 million, a figure that is virtually the same as the corresponding count from the previous year. The number of botnet C&C servers we detected practically did not change from the previous year as well, at nearly 15,000.

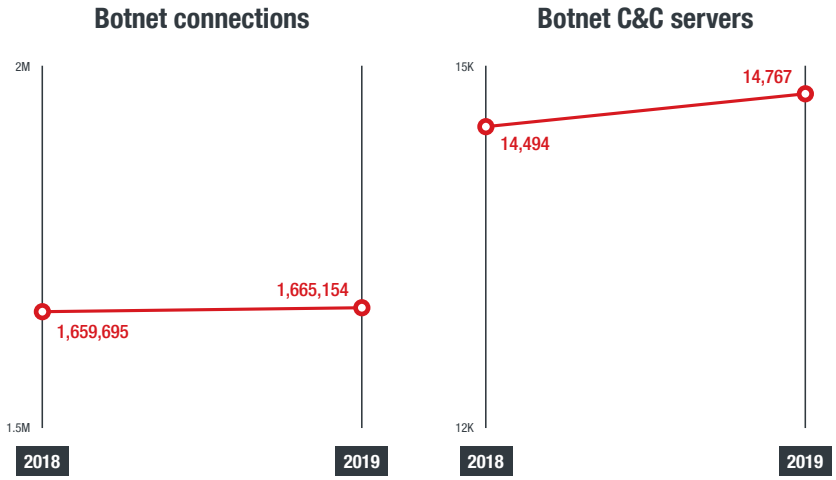

Figure 29. Botnet connections and C&C servers plateaued:
Year-on-year comparison of the numbers of detections of botnet connections and botnet C&C servers

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

Source: Trend Micro Smart Protection Network infrastructure

Telnet default password login remained the most triggered event in 2019, yielding close to 600 million counts. The persistence of this event further highlighted the need for changing, updating, and strengthening device credentials.

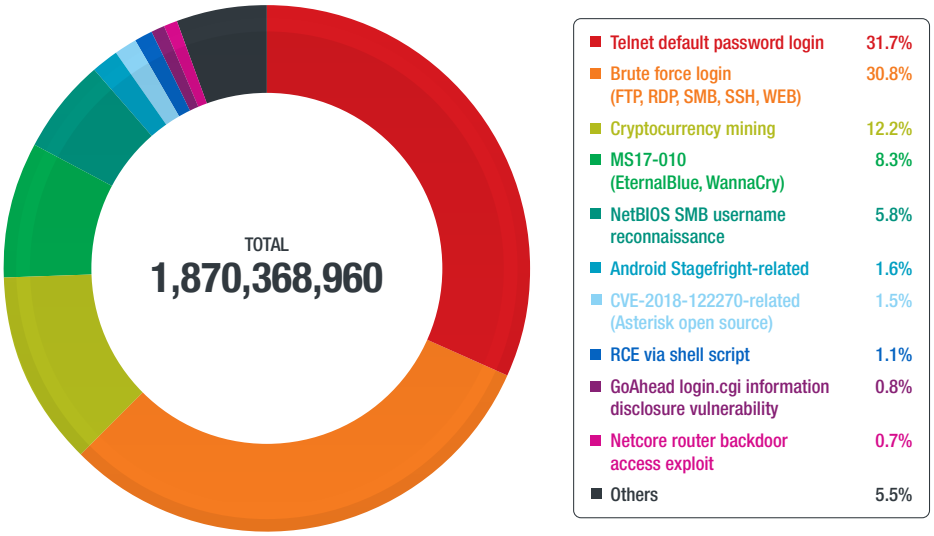

Figure 30. Telnet default password login remained the most triggered event: Distribution of top inbound and outbound events in smart home networks in 2019

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

Source: Trend Micro Smart Home Network solution

Attacks that attempted to exploit old vulnerabilities still posed significant risks to users and enterprises.

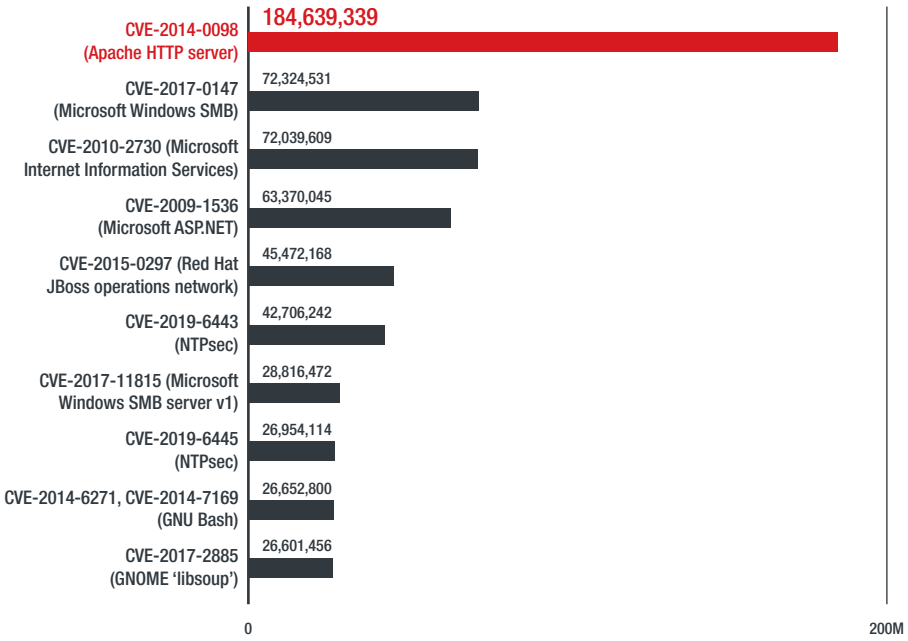

Figure 31. Old vulnerabilities for which patches had long been issued continued to pose security risks to organizations: Distribution of the top filters triggered in 2019 based on feedback from the Trend Micro™ Deep Security™ solution

Note: Filters were triggered when intrusion attempts exploiting the corresponding vulnerabilities were blocked.

Source: Trend Micro™ Deep Security™ solution

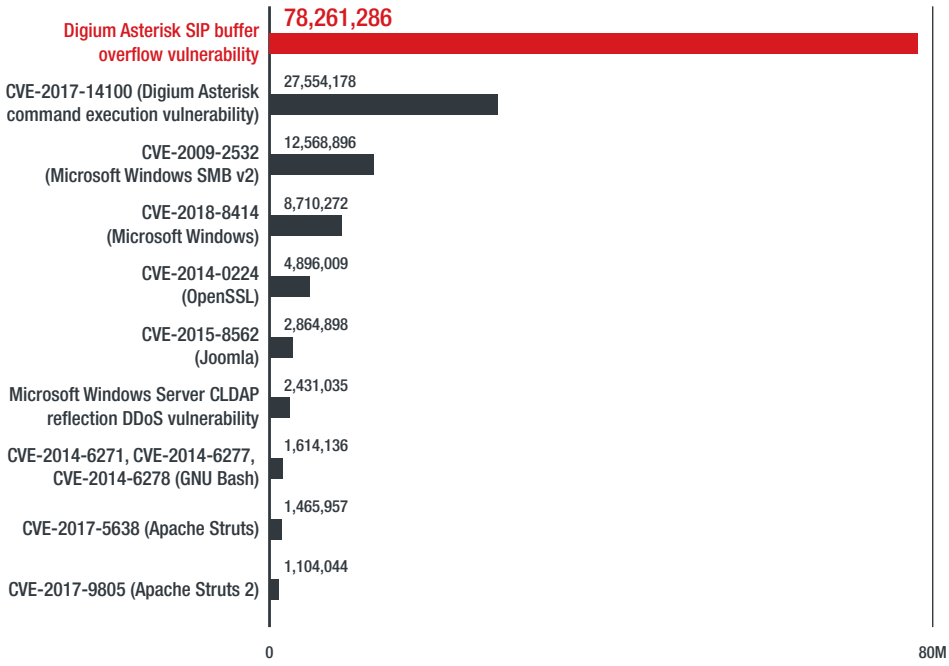

Figure 32. The filter for a buffer overflow vulnerability was the most triggered: Distribution of the top filters triggered in 2019 based on feedback from the Trend Micro TippingPoint® Threat Protection System solution

Note: Filters were triggered when intrusion attempts exploiting the corresponding vulnerabilities were blocked.

Source: Trend Micro TippingPoint® Threat Protection System solution

Our research on Operation Endtrade showed the sophistication of Tick's TTPs against organizations in China and Japan.

Tactic	Technique	ID	Description
Initial access	Spear-phishing attachment	T1193	Used to deliver first-stage malware
	Supply chain compromise	T1195	Used for initial intrusion on subsidiaries
Execution	Exploitation for client execution	T1203	Used to exploit CVE-2018-0802 and CVE-2018-0798
	Command-line interface	T1059	Used by some modified tools for command-line interface
	Scheduled task	T1053	Used to execute malware
	Scripting	T1064	Used VBScript
	Signed binary proxy execution	T1218	Used to execute malicious files and evade antivirus detection
	Third-party software	T1072	Used publicly available tools during attacks such as RAR
	User execution	T1204	Used for initial infection

Tactic	Technique	ID	Description
Persistence	Registry run keys/Startup folder	T1060	Used to add themselves to registry run key
Privilege escalation	User Account Control (UAC) bypassing	T1088	Used UAC bypassing tool for Windows 10
Defense evasion	Binary padding	T1009	Used to add junk data and expand the file size
	UAC bypassing	T1088	Used UAC bypassing tool for Windows 10
	Disabling security tools	T1089	Used to attempt termination of antivirus process
	Deobfuscation/Decoding of files or information	T1140	Used TSPY_LOADVBS to execute encoded command
	File deletion	T1107	Used to delete files after use
	Masquerading	T1036	Used right-to-left override (RTLO) technique
	Process injection	T1055	Used by Casper to inject backdoor's shell code
	Scripting	T1064	Used VBScript
Credential access	Credential dumping	T1003	Used Mimikatz
Discovery	Account discovery	T1087	Used net utility for internal reconnaissance
	File and directory discovery	T1083	Accessed shared folders to find confidential information
	Software discovery	T1518	Enumerated installed software
	System information discovery	T1082	Used to collect volume serial ID and other system information
	System service discovery	T1007	Used TROJ_GETVERSION to discover system service
Lateral movement	Remote file copy	T1105	Copied malware to remote desktop via Windows admin shares
	Windows admin shares	T1077	Copied malware to remote desktop via Windows admin shares
Collection	Automated collection	T1119	Used a trojan to perform series of discovery techniques and save it to a text file
	Data from local system	T1005	Collected data from both local and network shared drives
	Data from network shared drive	T1039	Collected data from both local and network shared drives
	Screen capture	T1113	Possibly stolen RAR file contained desktop screen capture image

Tactic	Technique	ID	Description
Command and control	Commonly used port	T1043	Used ports 80 or 443
	Custom cryptographic protocol	T1024	Used for downloaded/sent-back data
	Data encoding	T1132	Used for downloaded/sent-back data
	Data obfuscation	T1001	Used for downloaded/sent-back data
	Remote access tools	T1219	Used various RAT families
	Remote file copy	T1105	Used to download files in C&C server
	Standard application layer protocol	T1071	Used to communicate with remote C&C server
	Standard cryptographic protocol	T1032	Used AES
	Web service	T1102	Used to compromise legitimate web sites as C&C servers
Exfiltration	Exfiltration over command-and-control channel	T1041	Possibly sent collected data to attacker via C&C channel
	Data compression	T1002	Used password-protected RAR
	Data encryption	T1022	Used password-protected RAR

Table 4. Tick employed a sophisticated attack chain: Tactics and techniques used in Tick's Operation Endtrade, plotted on the MITRE ATT&CK™ for Enterprise matrix[107]

APT33, another threat actor group that we observed in 2019, launched attacks on organizations across three continents that were notable for obfuscating multiple botnets to cover its tracks.

Tactic	Technique	ID	Description
Initial access	Spear-phishing link	T1192	Sent spear-phishing emails containing links to HTA files
	Valid accounts	T1078	Used valid accounts for initial access and privilege escalation
Execution	Exploitation for client execution	T1203	Attempted to exploit a known vulnerability in WinRAR (CVE-2018-20250)
	PowerShell	T1086	Used PowerShell to download files from the C&C server and run various scripts
	User execution	T1204	Lured users to click links to malicious HTML applications delivered via spear-phishing emails

Tactic	Technique	ID	Description
Persistence	Registry run keys/Startup folder	T1060	Deployed several malware variants using both registry run keys and startup folder of victims
Privilege escalation	Scheduled task	T1053	Created a scheduled task to execute a VBE file multiple times a day
Defense evasion	Execution guardrails	T1480	Used kill dates in their malware to guardrail execution
	Obfuscated files or information	T1027	Used Base64 to encode payloads
Credential access	Brute force	T1110	Used password spraying to gain access to target systems
	Credential dumping	T1003	Used a variety of publicly available tools, such as LaZagne, Mimikatz, Gpppassword, SniffPass, and ProcDump, to dump credentials
Discovery	Network sniffing	T1040	Used SniffPass to collect credentials by sniffing network traffic
Lateral movement	Remote file copy	T1105	Downloaded additional files and programs from the C&C server
Command and control	Commonly used port	T1043	Used port 443 for C&C
	Data encoding	T1132	Used Base64 to encode C&C traffic
	Standard application layer protocol	T1071	Used HTTP for C&C
	Standard cryptographic protocol	T1032	Used AES for encryption of C&C traffic
	Uncommonly used port	T1065	Used ports 808 and 880 for C&C
Exfiltration	Data compression	T1002	Used WinRAR to compress data prior to exfiltration
	Exfiltration over alternative protocol	T1048	Used FTP to exfiltrate files (separately from the C&C channel)

Table 5. APT33 used multiple C&C-related techniques: Tactics and techniques used by APT33, plotted on the MITRE ATT&CK for Enterprise matrix[108]

Trend Micro Research remained at the forefront of discovering new threat techniques and developing innovative cybersecurity technologies in 2019. One of our most compelling discoveries came from our analysis of vulnerabilities in radio frequency (RF) remote controllers, which are widely used in manufacturing, construction, transportation, and other industrial applications. Our research revealed that RF remote controllers made by several popular vendors lacked security features, and their exploitation could lead to theft, extortion, sabotage, and injury, among other consequences.[109]

We also developed tools that examined data and case studies on Twitter to see how social media could aid in the gathering of actionable threat intelligence. In our study, we proved that the vast amount of information on social media makes it a viable platform for acquiring strategic and operational threat intelligence.[110]

We also emphasized the importance of the application of machine learning in threat detection with our research on the technology. In two studies conducted with researchers from Federation University Australia, we demonstrated the use of machine learning, specifically the generative adversarial autoencoder model, in the detection and analysis of malware given a small dataset or even only a single malware sample.[111, 112] Further, we demonstrated our innovative use of machine learning through the development of a model that uses two training phases to improve detection rates and reduce false positives. Called TrendX Hybrid Model, this model not only identifies malware variants but also predicts their behavior.[113]

References

1 Trend Micro. (27 August 2019). *Trend Micro*. "2019 Midyear Roundup: Evasive Threats, Pervasive Effects." Last accessed on 12 February 2020 at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/evasive-threats-pervasive-effects.

2 Janus Agcaoili and Miguel Ang. (6 June 2019). *Trend Micro*. "Narrowed Sights, Bigger Payoffs: Ransomware in 2019." Last accessed on 12 February 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/narrowed-sights-bigger-payoffs-ransomware-in-2019.

3 Trend Micro. (5 November 2019). *Trend Micro*. "Ransomware Attacks Hit Spanish Companies, Paralyzes Government Services in Canadian Territory of Nunavut." Last accessed on 6 February 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-attacks-hit-spanish-companies-paralyzes-government-services-in-canadian-territory-of-nunavut.

4 Trend Micro. (4 July 2019). *Trend Micro*. "Ransomware, BEC Attacks Strike Government Offices in the US Virgin Islands" Last accessed on 25 January 2020 at https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/ransomware-bec-attacks-strike-government-offices-in-the-us-virgin-islands.

5 Trend Micro. (2 August 2019). *Trend Micro*. "California City Confirms Phone Line and Financial Data System Disruptions Caused by Ransomware." Last accessed on 25 January 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/california-city-confirms-phone-line-and-financial-data-system-disruptions-caused-by-ransomware.

6 Lawrence Abrams. (24 December 2019). *Bleeping Computer*. "Maze Ransomware Releases Files Stolen from City of Pensacola." Last accessed on 25 January 2020 at https://www.bleepingcomputer.com/news/security/maze-ransomware-releases-files-stolen-from-city-of-pensacola/.

7 Fahmida Y. Rashid. (11 December 2019). *Decipher*. "Maze Turns Ransomware Into Data Breaches." Last accessed on 25 January 2020 at https://duo.com/decipher/maze-turns-ransomware-incidents-into-data-breaches.

8 Trend Micro. (21 October 2019). *Trend Micro*. "Underground Intrusion Specialists Team Up With Ransomware Groups." Last accessed on 30 January 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/underground-intrusion-specialists-team-up-with-ransomware-groups.

9 Sean Gallagher. (22 November 2019). *Ars Technica*. "Louisiana was hit by Ryuk, triggering another cyber-emergency." Last accessed on 12 February 2020 at https://arstechnica.com/information-technology/2019/11/louisiana-was-hit-by-ryuk-triggering-another-cyber-emergency/.

10 Lawrence Abrams. (12 January 2019). *Bleeping Computer*. "Ryuk Ransomware Partners with TrickBot to Gain Access to Infected Networks." Last accessed on 12 February 2020 at https://www.bleepingcomputer.com/news/security/ryuk-ransomware-partners-with-trickbot-to-gain-access-to-infected-networks/.

11 Trend Micro. (10 September 2019). *Trend Micro*. "Texas Municipalities Hit by REvil/Sodinokibi Paid No Ransom, Over Half Resume Operations." Last accessed on 25 January 2020 at https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/texas-municipalities-hit-by-revil-sodinokibi-paid-no-ransom-over-half-resume-operations.

12 Matthew Rosenberg, Nicole Perlroth, and David E. Sanger. (10 January 2020). *The New York Times*. "'Chaos Is the Point': Russian Hackers and Trolls Grow Stealthier in 2020." Last accessed on 7 February 2020 at https://www.nytimes.com/2020/01/10/us/politics/russia-hacking-disinformation-election.html.

13 Emsisoft Malware Lab. (12 December 2019). *Emsisoft Blog*. "The State of Ransomware in the US: Report and Statistics 2019." Last accessed on 25 January 2020 at https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/.

14 SentinelOne. (27 March 2018). *SentinelOne*. "SentinelOne: Global Ransomware Study 2018." Last 31 January 2020 at https://go.sentinelone.com/rs/327-MNM-087/images/Ransomware%20Research%20Data%20Summary%202018.pdf.

15 Kathleen Foody. (20 September 2019). *AP News*. "Payouts from insurance policies may fuel ransomware attacks." Last accessed on 25 January 2020 at https://apnews.com/234360e2e36b424b8849e51e57fe53c5.

16 Kathleen Foody. (20 September 2019). *AP News*. "Payouts from insurance policies may fuel ransomware attacks." Last accessed on 25 January 2020 at https://apnews.com/234360e2e36b424b8849e51e57fe53c5.

17 Kathleen Foody. (20 September 2019). *AP News*. "Payouts from insurance policies may fuel ransomware attacks." Last accessed on 25 January 2020 at https://apnews.com/234360e2e36b424b8849e51e57fe53c5.

18 James Leggate. (3 September 2019). *Fox Business*. “Hit by ransomware? Here’s what the FBI says you should do” Last accessed on 25 January 2020 at https://www.foxbusiness.com/technology/ransomware-fbi-paying-cyber-criminals.

19 Andrew Brandt. (9 December 2019). *Sophos News*. “Snatch ransomware reboots PCs into Safe Mode to bypass protection.” Last accessed on 25 January 2020 at https://news.sophos.com/en-us/2019/12/09/snatch-ransomware-reboots-pcs-into-safe-mode-to-bypass-protection/.

20 Trend Micro. (12 December 2019). *Trend Micro*. “Ransomware Recap: Snatch and Zeppelin Ransomware.” Last accessed on 25 January 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-snatch-and-zeppelin-ransomware.

21 Trend Micro. (6 January 2020). *Trend Micro*. “Ransomware Recap: Clop, DeathRansom, and Maze Ransomware.” Last accessed on 10 February 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-clop-deathransom-and-maze-ransomware.

22 Andrew Brandt. (9 December 2019). *Sophos News.* “Snatch ransomware reboots PCs into Safe Mode to bypass protection.” Last accessed on 10 February 2020 at https://news.sophos.com/en-us/2019/12/09/snatch-ransomware-reboots-pcs-into-safe-mode-to-bypass-protection/.

23 Alon Groisman. (18 December 2019). *Morphisec*. “ConnectWise Control Abused Again to Deliver Zeppelin Ransomware.” Last accessed on 10 February 2020 at https://blog.morphisec.com/connectwise-control-abused-again-to-deliver-zeppelin-ransomware/.

24 Trend Micro. (20 March 2019). *Trend Micro*. “What You Need to Know About the LockerGoga Ransomware.” Last accessed on 12 February 2020 at https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware/.

25 Andy Greenberg. (25 March 2019). *Wired*. “A Guide to LockerGoga, the Ransomware Crippling Industrial Firms.” Last accessed on 12 February 2020 at https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms/.

26 Lawrence Abrams. (5 March 2019). *Bleeping Computer*. “CryptoMix Clop Ransomware Says It’s Targeting Networks, Not Computers.” Last accessed on 10 February 2020 at https://www.bleepingcomputer.com/news/security/cryptomix-clop-ransomware-says-its-targeting-networks-not-computers/.

27 Lee Tae-woo, Kim Byoung-jae, Kim Dong-wook, Ryu So-joon, Shim Jae-hong, and Eunju Pak. (n.d.). *Korea Internet & Security Agency*. “Analysis on Cases of Distribution of Internal Network Ransomware through Exploiting AD Server.” Last accessed on 12 February 2020 at https://www.boho.or.kr/filedownload.do?attach_file_seq=2235&attach_file_id=EpF2235.pdf.

28 Trend Micro. (12 December 2019). *Trend Micro*. “Ransomware Recap: Snatch and Zeppelin Ransomware.” Last accessed on 25 January 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-snatch-and-zeppelin-ransomware.

29 Trend Micro. (6 January 2020). *Trend Micro*. “Ransomware Recap: Clop, DeathRansom, and Maze Ransomware.” Last accessed on 25 January 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-clop-deathransom-and-maze-ransomware.

30 Business Wire. (19 December 2019). *Business Wire*. “Trend Micro Cyber Risk Index Increased in 2019.” Last accessed on 25 January 2020 at https://www.businesswire.com/news/home/20191219005130/en/Trend-Micro-Cyber-Risk-Index-Increased-2019.

31 Tony Redmond. (24 October 2019). *Office 365 for IT Pros*. “Office 365 Hits 200 Million Monthly Active Users.” Last accessed on 6 February 2020 at https://office365itpros.com/2019/10/24/office-365-hits-200-million-monthly-active-users/.

32 Trend Micro. (4 March 2019). *Trend Micro*. “Trend Micro Cloud App Security Report 2018: Advanced Defenses for Advanced Email Threats.” Last accessed on 25 January 2020 at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/advanced-defenses-for-advanced-email-threats.

33 Samuel P Wang. (4 April 2019). *Trend Micro Security Intelligence Blog*. “Phishing Attack Uses Browser Extension Tool SingleFile to Obfuscate Malicious Log-in Pages.” Last accessed on 25 January 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/phishing-attack-uses-browser-extension-tool-singlefile-to-obfuscate-malicious-log-in-pages/.

34 Katsuyuki Okamoto. (24 October 2019). トレンドマイクロ セキュリティブログ. “国内ネットバンキングの二要素認証を狙うフィッシングが激化.” Last accessed on 30 January 2020 at https://blog.trendmicro.co.jp/archives/22696.

35 Office 365 Threat Research Team. (11 December 2019). *Microsoft Security*. “The quiet evolution of phishing.” Last accessed on 25 January 2020 at https://www.microsoft.com/security/blog/2019/12/11/the-quiet-evolution-of-phishing/.

36 Office 365 Threat Research Team. (11 December 2019). *Microsoft Security*. "The quiet evolution of phishing." Last accessed on 25 January 2020 at https://www.microsoft.com/security/blog/2019/12/11/the-quiet-evolution-of-phishing/.

37 Trend Micro. (18 January 2018). *Trend Micro*. "Delving into the World of Business Email Compromise (BEC)." Last accessed on 25 January 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/delving-into-the-world-of-business-email-compromise-bec.

38 Federal Bureau of Investigation Internet Crime Complaint Center (IC3). (n.d.). *Federal Bureau of Investigation Internet Crime Complaint Center (IC3)*. "2019 Internet Crime Report." Last accessed on 20 February 2020 at https://pdf.ic3.gov/2019_IC3Report.pdf.

39 Trend Micro. (2 May 2019). *Trend Micro*. "BEC Scammers Steal US$1.75 Million From an Ohio Church." Last accessed on 25 January 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/bec-scammers-steal-us-1-75-million-from-an-ohio-church.

40 Oregon Live. (19 August 2019). *Oregon Live*. "Portland Public Schools nearly scammed out of $2.9 million." Last accessed on 6 February 2020 at https://www.oregonlive.com/education/2019/08/portland-public-schools-nearly-scammed-out-of-29-million.html.

41 Trend Micro. (16 April 2019). *Trend Micro*. "New Business Email Compromise Scheme Reroutes Paycheck by Direct Deposit." Last accessed on 25 January 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/new-business-email-compromise-scheme-reroutes-paycheck-by-direct-deposit.

42 Trend Micro. (12 July 2019). *Trend Micro*. "Fake Invoices Used by BEC Scammers to Defraud Griffin City, Georgia of Over US$800,000." Last accessed on 25 January 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fake-invoices-used-by-bec-scammers-to-defraud-griffin-georgia-us-800-000.

43 Sergiu Gatlan. (3 January 2020). *Bleeping Computer*. "Colorado Town Wires Over $1 Million to BEC Scammers." Last accessed on 25 January 2020 at https://www.bleepingcomputer.com/news/security/colorado-town-wires-over-1-million-to-bec-scammers/.

44 Trend Micro. (11 December 2018). *Trend Micro*. "Mapping the Future: Dealing With Pervasive and Persistent Threats." Last accessed on 7 February 2020 at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2019.

45 Lindsey O'Donnell. (5 March 2019). *Threatpost*. "RSA Conference 2019: BEC Scammer Gang Takes Aim at Boy Scouts, Other Nonprofts." Last accessed on 7 February 2020 at https://threatpost.com/rsac-2019-bec-scammer-gang-takes-aim-at-boy-scouts-other-nonprofts/142302/.

46 Charles Cooper. (16 May 2018). *Symantec Blogs*. "WannaCry: Lessons Learned 1 Year Later." Last accessed on 25 January 2020 at https://www.symantec.com/blogs/feature-stories/wannacry-lessons-learned-1-year-later.

47 Microsoft. (14 May 2019). *Microsoft MSRC*. "CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability." Last accessed on 25 January 2020 at https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708.

48 Trend Micro. (29 May 2019). *Trend Micro*. "Nearly 1 Million Systems Affected By 'Wormable' BlueKeep Vulnerability (CVE-2019-0708)." Last accessed on 6 February 2020 at https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/nearly-1-million-systems-affected-by-wormable-bluekeep-vulnerability-cve-2019-0708.

49 Danny Palmer. (27 October 2017). *ZDNet*. "Bad Rabbit ransomware spread using leaked NSA EternalRomance exploit, researchers confirm." Last accessed on 7 February 2020 at https://www.zdnet.com/article/bad-rabbit-ransomware-spread-using-leaked-nsa-eternalromance-exploit-researchers-confirm/.

50 Rob Wright. (17 July 2019). *SearchSecurity*. "BlueKeep blues: More than 800,000 systems still unpatched." Last accessed on 25 January 2020 at https://searchsecurity.techtarget.com/news/252466932/BlueKeep-blues-More-than-800000-systems-still-unpatched.

51 Microsoft Defender ATP Research Team. (7 November 2019). *Microsoft Security*. "Microsoft works with researchers to detect and protect against new RDP exploits." Last accessed on 25 January 2020 at https://www.microsoft.com/security/blog/2019/11/07/the-new-cve-2019-0708-rdp-exploit-attacks-explained/.

52 Federal Bureau of Investigation Internet Crime Complaint Center (IC3). (27 September 2018). *Federal Bureau of Investigation Internet Crime Complaint Center (IC3)*. "Cyber Actors Increasingly Exploit the Remote Desktop Protocol to Conduct Malicious Activity." Last accessed on 25 January 2020 at https://www.ic3.gov/media/2018/180927.aspx.

53 Microsoft. (n.d.). *Microsoft MSRC*. "Security Update Guide." Last accessed on 29 January 2020 at https://portal.msrc.microsoft.com/en-us/security-guidance.

54 Trend Micro. (31 October 2018). *Trend Micro*. "InfoSec Guide: Remote Desktop Protocol (RDP)." Last accessed on 25 January 2020 at https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/infosec-guide-remote-desktop-protocol-rdp.

55 Net Market Share. (n.d.). *Net Market Share*. "Operating System Share by Version." Last accessed on 25 January 2020 at https://netmarketshare.com/operating-system-market-share.aspx?id=platformsDesktopVersions.

56 Microsoft. (14 Jan 2020). *Microsoft*. "Windows 7 support ended on January 14, 2020." Last accessed on 25 January 2020 at https://support.microsoft.com/en-us/help/4057281/windows-7-support-ended-on-january-14-2020.

57 Brian Gorenc. (30 January 2020). *Zero Day Initiative*. "LOOKING BACK AT THE ZERO DAY INITIATIVE IN 2019." Last accessed on 3 February 2020 at https://www.zerodayinitiative.com/blog/2020/1/30/looking-back-at-the-zero-day-initiative-in-2019.

58 Brian Gorenc. (30 January 2020). *Zero Day Initiative*. "LOOKING BACK AT THE ZERO DAY INITIATIVE IN 2019." Last accessed on 3 February 2020 at https://www.zerodayinitiative.com/blog/2020/1/30/looking-back-at-the-zero-day-initiative-in-2019.

59 Trend Micro. (27 June 2019). *Trend Micro*. "The IIoT Attack Surface: Threats and Security Solutions." Last accessed on 6 February 2020 at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/-the-iiot-attack-surface-threats-and-security-solutions.

60 Markets and Markets. (April 2019). *Markets and Markets*. "SCADA Market." Last accessed on 25 January 2020 at https://www.marketsandmarkets.com/Market-Reports/scada-market-19487518.html.

61 Randal Kenworthy. (18 November 2019). *Forbes*. "The 5G And IoT Revolution Is Coming: Here's What To Expect." Last accessed on 25 January 2020 at https://www.forbes.com/sites/forbestechcouncil/2019/11/18/the-5g-iot-revolution-is-coming-heres-what-to-expect/#7cc557756abf.

62 Trend Micro. (4 April 2019). *Trend Micro*. "Mirai Variant Spotted Using Multiple Exploits, Targets Various Routers." Last accessed on 25 January 2020 at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/mirai-variant-spotted-using-multiple-exploits-targets-various-routers.

63 Augusto Remillano II and Jakub Urbanec. (23 May 2019). *Trend Micro Security Intelligence Blog*. "New Mirai Variant Uses Multiple Exploits to Target Routers and Other Devices." Last accessed on 25 January 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/new-mirai-variant-uses-multiple-exploits-to-target-routers-and-other-devices/.

64 Trend Micro. (8 August 2019). *Trend Micro*. "Mirai Spawn Echobot Found Using Over 50 Different Exploits." Last accessed on 25 January 2020 at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/mirai-spawn-echobot-found-using-over-50-different-exploits.

65 Augusto Remillano II and Jakub Urbanec. (13 August 2019). *Trend Micro Security Intelligence Blog*. "Back-to-Back Campaigns: Neko, Mirai, and Bashlite Malware Variants Use Various Exploits to Target Several Routers, Devices." Last accessed on 25 January 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/back-to-back-campaigns-neko-mirai-and-bashlite-malware-variants-use-various-exploits-to-target-several-routers-devices/.

66 Aliakbar Zahravi. (16 December 2019). *Trend Micro Security Intelligence Blog*. "DDoS Attacks and IoT Exploits: New Activity from Momentum Botnet." Last accessed on 25 January 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/ddos-attacks-and-iot-exploits-new-activity-from-momentum-botnet/.

67 Dark Reading Staff. (7 October 2019). *Dark Reading*. "Magecart Skimmers Spotted on 2M Websites." Last accessed on 25 January 2020 at https://www.darkreading.com/endpoint/magecart-skimmers-spotted-on-2m-websites/d/d-id/1336011.

68 Chaoying Liu and Joseph C. Chen. (16 January 2019). *Trend Micro Security Intelligence Blog*. "New Magecart Attack Delivered Through Compromised Advertising Supply Chain." Last accessed on 30 January 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/new-magecart-attack-delivered-through-compromised-advertising-supply-chain/.

69 Joseph C. Chen. (9 October 2019). *Trend Micro Security Intelligence Blog*. "FIN6 Compromised E-commerce Platform via Magecart to Inject Credit Card Skimmers Into Thousands of Online Shops." Last accessed on 25 January 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/fin6-compromised-e-commerce-platform-via-magecart-to-inject-credit-card-skimmers-into-thousands-of-online-shops/.

70 Katsuyuki Okamoto. (10 January 2020). トレンドマイクロ セキュリティブログ. “2019年「法人」と「個人」のサイバー脅威動向：サイバー犯罪が覆す「安全」の常識.” Last accessed on 25 January 2020 at https://blog.trendmicro.co.jp/archives/23409.

71 Trend Micro. (n.d.). *Trend Micro*. “DevOps.” Last accessed on 6 February 2020 at https://www.trendmicro.com/vinfo/us/security/definition/devops.

72 Tony Bradely. (1 August 2018). *Forbes*. “Supply Chain Attacks Increase As Cybercriminals Focus On Exploiting Weak Links.” Last accessed on 5 February 2020 at https://www.forbes.com/sites/tonybradley/2018/08/01/supply-chain-attacks-increase-as-cybercriminals-focus-on-exploiting-weak-links/#2661edfd3519.

73 David Fiser, Jakub Urbanec, and Jaromir Horejsi. (14 June 2019). *Trend Micro Security Intelligence Blog*. “AESDDoS Botnet Malware Infiltrates Containers via Exposed Docker APIs.” Last accessed on 5 February 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/aesddos-botnet-malware-infiltrates-containers-via-exposed-docker-apis/.

74 Trend Micro. (26 June 2019). *Trend Micro*. “Kubernetes Vulnerability CVE-2019-11246 Discovered Due to Incomplete Updates from a Previous Flaw.” Last accessed on 25 January 2020 at https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/kubernetes-vulnerability-cve-2019-11246-discovered-due-to-incomplete-updates-from-a-previous-flaw.

75 David Fiser. (17 June 2019). *Trend Micro Security Intelligence Blog*. “Jenkins Admins: Relying on Default Settings Could Put Master at Risk of Remote Code Execution Attacks.” Last accessed on 25 January 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/jenkins-admins-relying-on-default-settings-could-put-master-at-risk-of-remote-code-execution-attacks/.

76 David Fiser. (30 August 2019). *Trend Micro Security Intelligence Blog*. “Hiding in Plain Text: Jenkins Plugin Vulnerabilities.” Last accessed on 25 January 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/hiding-in-plain-text-jenkins-plugin-vulnerabilities/.

77 Trend Micro. (17 October 2019). *Trend Micro*. “Monero-mining Worm Infects Over 2,000 Unsecure Docker Hosts.” Last accessed on 25 January 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/monero-mining-worm-infects-over-2-000-unsecure-docker-hosts.

78 Mohamad Mokbel. (22 April 2019). *Trend Micro Security Intelligence Blog*. “Analyzing C/C++ Runtime Library Code Tampering in Software Supply Chain Attacks.” Last accessed on 5 February 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/analyzing-c-c-runtime-library-code-tampering-in-software-supply-chain-attacks/.

79 Trend Micro. (29 July 2019). *Trend Micro*. “Risks Under the Radar: Understanding Fileless Threats.” Last accessed on 25 January 2020 at https://www.trendmicro.com/vinfo/us/security/news/security-technology/risks-under-the-radar-understanding-fileless-threats.

80 Trend Micro. (11 December 2018). *Trend Micro*. “Mapping the Future: Dealing With Pervasive and Persistent Threats.” Last accessed on 7 February 2020 at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2019.

81 Henry Alarcon, Jr. and Raphael Centeno. (4 March 2019). *Trend Micro Security Intelligence Blog*. “Fileless Banking Trojan Targeting Brazilian Banks Downloads Possible Botnet Capability, Info Stealers.” Last accessed on 25 January 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/fileless-banking-trojan-targeting-brazilian-banks-downloads-possible-botnet-capability-info-stealers/.

82 Carl Maverick Pascual. (19 September 2019). *Trend Micro Security Intelligence Blog*. “Fileless Cryptocurrency-Miner GhostMiner Weaponizes WMI Objects, Kills Other Cryptocurrency-Mining Payloads.” Last accessed on 25 January 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/fileless-cryptocurrency-miner-ghostminer-weaponizes-wmi-objects-kills-other-cryptocurrency-mining-payloads/.

83 Trend Micro. (18 September 2019). *Trend Micro*. “Emotet Ends Hiatus with New Spam Campaigns.” Last accessed on 25 January 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/emotet-ends-hiatus-with-new-spam-campaigns.

84 Johnlery Triunfante and Earle Earnshaw. (9 September 2019). *Trend Micro Security Intelligence Blog*. “‘Purple Fox’ Fileless Malware with Rookit Component Delivered by Rig Exploit Kit Now Abuses PowerShell.” Last accessed on 25 January 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/purple-fox-fileless-malware-with-rookit-component-delivered-by-rig-exploit-kit-now-abuses-powershell/.

85 Jaromir Horejsi and Joseph C. Chen. (1 October 2019). *Trend Micro Security Intelligence Blog*. “New Fileless Botnet Novter Distributed by KovCoreG Malvertising Campaign.” Last accessed on 25 January 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/new-fileless-botnet-novter-distributed-by-kovcoreg-malvertising-campaign/.

86 Joey Chen, Hiroyuki Kakara, and Masaoki Shoji. (29 November 2019). *Trend Micro Security Intelligence Blog*. "Operation ENDTRADE: Finding Multi-Stage Backdoors that TICK." Last accessed on 25 January 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/operation-endtrade-finding-multi-stage-backdoors-that-tick/.

87 Joey Chen, Hiroyuki Kakara, and Masaoki Shoji. (2019). *Trend Micro*. "Operation ENDTRADE: TICK's Multi-Stage Backdoors for Attacking Industries and Stealing Classified Data." Last accessed on 6 February 2020 at https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf.

88 Feike Hacquebord, Cedric Pernet, and Kenney Lu. (12 December 2019). *Trend Micro Security Intelligence Blog*. "More than a Dozen Obfuscated APT33 Botnets Used for Extreme Narrow Targeting." Last accessed on 25 January 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/more-than-a-dozen-obfuscated-apt33-botnets-used-for-extreme-narrow-targeting/.

89 Lorin Wu. (30 January 2019). *Trend Micro Security Intelligence Blog*. "Various Google Play 'Beauty Camera' Apps Send Users Pornographic Content, Redirect Them to Phishing Websites and Collect Their Pictures." Last accessed on 25 January 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/various-google-play-beauty-camera-apps-sends-users-pornographic-content-redirects-them-to-phishing-websites-and-collects-their-pictures/.

90 Bill Marczak, Adam Hulcoop, Etienne Maynier, Bahr Abdul Razzak, Masashi Crete-Nishihata, John Scott-Railton, and Ron Deibert. (24 September 2019). *The Citizen Lab*. "Missing Link: Tibetan Groups Targeted with 1-Click Mobile Exploits." Last accessed on 13 February 2020 at https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/.

91 ClearSky Cybersecurity. (May 2019). *ClearSky Cyber Security*. "Iranian Nation-State APT Groups 'Black Box' Leak." Last accessed on 13 February 2020 at https://www.clearskysec.com/wp-content/uploads/2019/05/Iranian-Nation-State-APT-Leak-Analysis-and-Overview.pdf.

92 Daniel Lunghi and Jaromir Horejsi. (10 June 2019). *Trend Micro Security Intelligence Blog*. "MuddyWater Resurfaces, Uses Multi-Stage Backdoor POWERSTATS V3 and New Post-Exploitation Tools." Last accessed on 25 January 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/muddywater-resurfaces-uses-multi-stage-backdoor-powerstats-v3-and-new-post-exploitation-tools/.

93 Daniel Lunghi and Jaromir Horejsi. (2019). *Trend Micro Security Intelligence Blog*. "New MuddyWater Activities Uncovered: Threat Actors Used Multi-Stage Backdoors, New PostExploitation Tools, Android Malware, and More." Last accessed on 7 February 2020 at https://documents.trendmicro.com/assets/white_papers/wp_new_muddywater_findings_uncovered.pdf.

94 Kari Paul. (6 January 2019). *MarketWatch*. "Apple or Android? Here is the most secure phone you can get." Last accessed on 25 January 2020 at https://www.marketwatch.com/story/apple-or-android-here-is-the-most-secure-phone-you-can-get-2018-10-10.

95 Eric Zeman. (29 September 2018). *Fortune*. "Apple iOS 12 Fortifies Your iPhone's Security. Here's How." Last accessed on 25 January 2020 at https://fortune.com/2018/09/29/apple-ios-12-iphone-security/.

96 Hara Hiroaki, Lilang Wu, and Lorin Wu. (2 April 2019). *Trend Micro Security Intelligence Blog*. "New Version of XLoader That Disguises as Android Apps and an iOS Profile Holds New Links to FakeSpy." Last accessed on 25 January 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/new-version-of-xloader-that-disguises-as-android-apps-and-an-ios-profile-holds-new-links-to-fakespy/.

97 Lilang Wu, Yuchen Zhou, and Moony Li. (12 July 2019). *Trend Micro Security Intelligence Blog*. "iOS URL Scheme Susceptible to Hijacking." Last accessed on 25 January 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/ios-url-scheme-susceptible-to-hijacking/.

98 Mobile Threat Response Team. (26 September 2019). *Trend Micro Security Intelligence Blog*. "Gambling Apps Sneak into Top 100: How Hundreds of Fake Apps Spread on iOS App Store and Google Play." Last accessed on 25 January 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/gambling-apps-sneak-top-100-hundreds-fake-apps-spread-app-store-google-play/.

99 Juwei Lin. (8 April 2019). *Trend Micro Security Intelligence Blog*. "Patch With March macOS Updates: Vulnerabilities May Expose Restricted Information, Enable Arbitrary Code Execution." Last accessed on 25 January 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/patch-with-march-macos-updates-vulnerabilities-may-expose-restricted-information-enable-arbitrary-code-execution/.

100 Moony Li and Lilang Wu. (21 June 2019). *Trend Micro Security Intelligence Blog*. "CVE-2019-8635: Double Free Vulnerability in Apple macOS Lets Attackers Escalate System Privileges and Execute Arbitrary Code." Last accessed on 25 January 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/cve-2019-8635-double-free-vulnerability-in-apple-macos-lets-attackers-escalate-system-privileges-and-execute-arbitrary-code/.

101 Luis Magisa. (20 September 2019). *Trend Micro Security Intelligence Blog*. "Mac Malware that Spoofs Trading App Steals User Information, Uploads it to Website." Last accessed on 25 January 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/mac-malware-that-spoofs-trading-app-steals-user-information-uploads-it-to-website/.

102 Gabrielle Joyce Mabutas. (20 November 2019). *Trend Micro Security Intelligence Blog*. "Mac Backdoor Linked to Lazarus Targets Korean Users." Last accessed on 25 January 2020 at https://blog.trendmicro.com/trendlabs-security-intelligence/mac-backdoor-linked-to-lazarus-targets-korean-users/.

103 Eliya Stein. (24 January 2019). *Confiant*. "Confiant & Malwarebytes Uncover Steganography Based Ad Payload That Drops Shlayer Trojan On Mac Users." Last accessed on 30 January 2020 at https://blog.confiant.com/confiant-malwarebytes-uncover-steganography-based-ad-payload-that-drops-shlayer-trojan-on-mac-cd31e885c202.

104 Taha Karim. (25 September 2019). *Confiant*. "OSX/Shlayer new Shurprise.. unveiling OSX/Tarmac." Last accessed on 31 January 2020 at https://blog.confiant.com/osx-shlayer-new-shurprise-unveiling-osx-tarmac-f965a32de887.

105 Greg Young. (8 August 2019). *Trend Micro Simply Security*. "Why XDR Is A Big Deal, and Is Different from SIEM and Platforms." Last accessed on 25 January 2020 at https://blog.trendmicro.com/why-xdr-is-a-big-deal-and-is-different-from-siem-and-platforms/.

106 Trend Micro. (11 December 2018). *Trend Micro*. "Mapping the Future: Dealing With Pervasive and Persistent Threats. Last accessed on 7 February 2020 at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2019.

107 Joey Chen, Hiroyuki Kakara, and Masaoki Shoji. (2019). *Trend Micro*. "Operation ENDTRADE: TICK's Multi-Stage Backdoors for Attacking Industries and Stealing Classified Data." Last accessed on 7 February 2020 at https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf.

108 MITRE ATT&CK. (18 April 2018). *MITRE ATT&CK*. "APT33."Last accessed on 7 February 2020 at https://attack.mitre.org/groups/G0064/.

109 Jonathan Andersson, Marco Balduzzi, Stephen Hilt, Philippe Lin, Federico Maggi, Akira Urano, and Rainer Vosseler. (2019). *Trend Micro*. "A Security Analysis of Radio Remote Controllers for Industrial Applications." Last accessed on 30 January 2020 at https://documents.trendmicro.com/assets/white_papers/wp-a-security-analysis-of-radio-remote-controllers.pdf.

110 Vladimir Kropotov and Fyodor Yarochkin. (30 July 2019). *Trend Micro*. "Hunting Threats on Twitter: How Social Media Can Be Used to Gather Actionable Threat Intelligence." Last accessed on 30 January 2020 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hunting-threats-on-twitter.

111 Sean Park, Iqbal Gondal, Joarder Kamruzzaman, and Jon Oliver. (2019). *Trend Micro*. "Generative Malware Outbreak Detection." Last accessed on 30 January 2020 at https://documents.trendmicro.com/assets/white_papers/GenerativeMalwareOutbreakDetection.pdf.

112 Sean Park, Iqbal Gondal, Joarder Kamruzzaman, and Leo Zhang. (2019). *Trend Micro*. "One-Shot Malware Outbreak Detection Using Spatio-Temporal Isomorphic Dynamic Features." Last accessed on 30 January 2020 at https://documents.trendmicro.com/assets/white_papers/one-shot-malware-outbreak-detection-using-spatio-temporal-isomorphic-dynamic-features.pdf.

113 Dr. Spark Tsao. (8 November 2019). *Trend Micro*. "Faster and More Accurate Malware Detection Through Predictive Machine Learning: Correlating Static and Behavioral Features." Last accessed on 30 January 2020 at https://www.trendmicro.com/vinfo/us/security/news/security-technology/faster-and-more-accurate-malware-detection-through-predictive-machine-learning-correlating-static-and-behavioral-features.

TREND MICRO™ RESEARCH

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

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

www.trendmicro.com

TREND MICRO™ | research