



2019 Midyear Security Roundup

# Evasive Threats, Pervasive Effects



#### **TREND MICRO LEGAL DISCLAIMER**

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

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

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

Published by  
**Trend Micro Research**

Stock images used under license from  
Shutterstock.com

# Contents

**04**

Ransomware remains widespread,  
with costly consequences

**09**

Threats increasingly 'live off the land'

**14**

Targeted attacks employ more  
tried-and-tested techniques than new ones

**15**

Illicit actors continue to bank on  
cryptocurrency mining

**19**

Messaging threats further diversify

**25**

Pervasive vulnerabilities make patching  
even more important

**29**

IoT and IIoT security remains  
a significant issue

**31**

Multilayered defense helps address  
today's multifaceted threats

**32**

Threat Landscape in Review



A woman with long blonde hair is seen from the side, working on a laptop. The background is a blurred office environment. The text is overlaid on a dark, semi-transparent rectangular area.

In an ever-evolving threat landscape, cybersecurity is no longer just about safeguarding sensitive data and other digital assets by merely keeping cybercriminals and other threat actors out of networks, systems, devices, and underlying technologies. Now it is also about having to proactively stop them in their tracks before they even gain a foothold in their spheres of operation.

The notable threats in the first half of 2019 drove this point home, what with the prevalence of so-called fileless threats that “lived off the land” — abusing legitimate and typically whitelisted system tools to do their malicious bidding — and the presence of malware and phishing campaigns that took advantage of security lapses and diversified in the ways they counted on the still unpatched flaw that was human vulnerability.

Ransomware operators distinctly set their sights on organizations, with crippling ramifications: Their attacks proved they could strike with such severity that some victims were even strong-armed into acquiescing to the cybercriminals’ exorbitant demands. For many cryptocurrency-mining threats, servers and cloud-based environments, having far more computing resources than endpoints, became their new frontier. Messaging platforms — the bedrock underpinning many business transactions — were inundated with a range of threats, including business email compromise scams, sextortion schemes, and phishing incidents that did not rely on hacking human behavior alone.

Over the course of the half-year, many threat actors seemed to be hedging their bets, in light of their broad and multiplatform targeted attack campaigns, an apparent stir in their use of exploit kits, and their persistent attacks on routers and other internet-of-things devices. And a number of threats used multistage or multilayered infection chains. To be sure, the tactics, techniques, and procedures used by these threats might not be groundbreaking, but that they were employed as fail-safe mechanisms was worthy of attention.

Vulnerabilities remained a cause for concern, in the form of both the software sort that had been a perpetual bane of cybersecurity and the hardware-level class that had been gaining pointed relevance of late. In particular, the disclosure of pervasive vulnerabilities, such as those found in popular desktop services and container platforms, highlighted the extent of the impact that security flaws could have if left unpatched.

Ensuring that networks, systems, devices, and technologies are properly configured or patched in a timely manner can be an arduous task for enterprises and their security administrators — to say nothing of taking steps to reduce the attack surface and actively monitoring and thwarting attempts at compromise at each stage or layer of an attack. But if accomplished, it is a challenge whose potential benefits far outweigh the effort required to bring it to fruition, especially given the value of what is at stake, in terms of not only cybersecurity but also physical safety.

Our midyear report reexamines the security landscape of the first half of 2019 — the threats that made their mark and their attendant risks and issues — to enable enterprises with insights that can help them tackle the aforementioned challenge throughout the rest of the year and beyond.

# Ransomware remains widespread, with costly consequences

## High-profile attacks exact high-value losses

Toward the end of the first half of 2019, after having earned more than US\$2 billion, the operators of GandCrab announced their retirement on a hacking forum where they peddled their ransomware as a service (RaaS).<sup>1</sup> GandCrab was notable for its business model: Cybercriminals, regardless of their technical know-how, could pay for a subscription to access custom builds. They could then distribute their own versions of GandCrab through their preferred means, such as spam and exploit kits. While ransomware operators had been largely known for using the spray-and-pray approach and selling their malware to would-be affiliates,<sup>2</sup> casting a wider net of business partners and potential victims increased their earning potential.

However, the half-year showed a change in their tack. Cybercriminals perhaps considered that they could consistently earn as much, or even more, by zeroing in on multinationals, large enterprises, and even government organizations. Their modus operandi entailed reconnoitering their target, sending its employees tailored phishing emails, and searching for security gaps that they could exploit to gain access to and laterally move within its networks and systems.

This was exemplified when — less than two weeks after a ransomware attack hit Riviera Beach in the same state and compelled the city's officials to pay US\$600,000<sup>3</sup> — the Ryuk ransomware struck Lake City, Florida, in June. With the systems used to provide public services having been taken hostage, the city's officials were coerced into paying the US\$460,000 ransom.<sup>4</sup>

Given such a large amount, it should come as no surprise that Ryuk was cited as one of the threats attributed with the higher ransom payouts observed so far this year.<sup>5</sup> The ransomware was reported in January to have earned over 705 bitcoins (at least US\$3.7 million at the time) since first emerging in August last year.<sup>6</sup> Its notoriety was reflected by its prevalence, as it was one of the top ransomware families detected in the first half of 2019, based on feedback from the Trend Micro™ Smart Protection Network™ infrastructure.

These remarkably high payouts were congruous with the 77% uptick, from the second half of 2018 to the first half of 2019, that we observed in our detections of ransomware-related threats (files, emails, and URLs) – notwithstanding the 55% decline in new ransomware families. The increase could be reflective not only of how we proactively blocked 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. The heightened activities were also indicative of the targeted ransomware attacks reported in the half-year, which made strong impressions with the considerable degree of damage left in their trail.

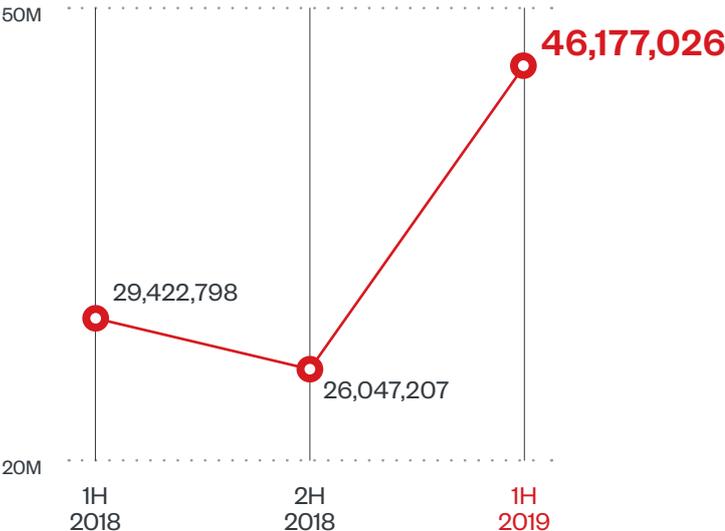


Figure 1. Detections of ransomware-related threats significantly increased: Half-year comparison of detections of ransomware-related threat components (files, emails, and URLs)

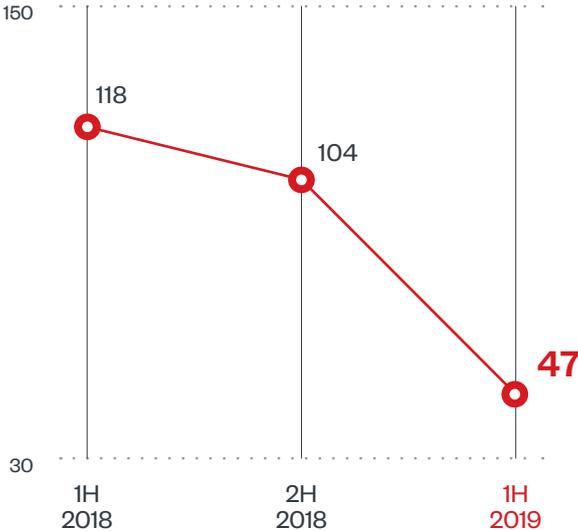


Figure 2. New ransomware families further declined: Half-year comparison of new ransomware families

In March, the LockerGoga ransomware struck a Norwegian manufacturing company and halted production in several of its plants, forcing the other plants to switch to manual operations.<sup>7</sup> When the dust had settled three months later,<sup>8</sup> the financial losses had exceeded US\$55 million.<sup>9</sup> Considerably less — but still substantial, at over US\$5.3 million — had been incurred by the city of Baltimore, Maryland, to recover from an attack involving the RobbinHood ransomware in May.<sup>10</sup> RobbinHood was also the culprit behind the ransomware attack that hit Greenville, North Carolina, in April, resulting in the prolonged shutdown of the city’s infected systems.<sup>11</sup>

Ransomware family	How it can arrive and attack vectors used	How it can propagate	Other notable behaviors
Clop (CryptoMix)	Compromised active directory in the network <sup>12</sup>	Hacked remote desktop services <sup>13</sup>	Distributed via executables with a valid digital signature to evade detection
Dharma <sup>14</sup> aka Crysis <sup>15</sup>	Spam emails	Brute-forced remote desktops (Crysis) <sup>16</sup>	Uses antivirus installation processes as distraction
NamPoHyu Virus aka MegaLocker Virus <sup>17</sup>	Exposed Samba servers	Brute-forced Samba servers	Its previous iteration encrypts network-attached storage (NAS) devices.
GandCrab	Spam emails, exploit kits, malvertisements, compromised websites, exposed databases, <sup>18</sup> vulnerable software <sup>19</sup>	Depends on the affiliate’s customizations	Uses the RaaS business model
MongoLock <sup>20</sup>	Exposed or poorly secured MongoDB databases	Scanning for exposed or poorly secured MongoDB servers via services like Shodan	Deletes databases rather than encrypting them, formats backup drives if available <sup>21</sup>
Ryuk <sup>22</sup>	Spam emails	Compromised routers, Trickbot and Emotet (as loader malware), <sup>23</sup> EternalBlue	Can render infected systems unbootable <sup>24</sup>
LockerGoga <sup>25</sup>	Compromised credentials	System administration and possibly penetration testing and other hacking tools, <sup>26</sup> valid certificates to evade detection and get into systems	Modifies passwords of infected systems’ user accounts, prevents infected systems from being rebooted
Nozelesn <sup>27</sup>	Spam emails with malicious attachments	Emotet malware (copying itself into other machines in the network via administrative shares)	Its trojan downloader, Nymaim, uses fileless techniques to load the ransomware.
RobbinHood <sup>28</sup>	Compromised or unsecure remote desktops, trojan loaders	Domain controllers or frameworks (e.g., Empire PowerShell and PsExec)	Encrypts each file with a unique key
BitPaymer <sup>29</sup>	Compromised accounts with administrator privileges, emails containing Dridex <sup>30</sup>	Dridex (to steal network information), supply chain attacks, <sup>31</sup> compromised remote desktop servers <sup>32</sup>	Abuses PsExec tool
MegaCortex <sup>33</sup>	Compromised domain controllers	Renamed PsExec tool	Disables certain processes

Table 1. The half-year’s notable ransomware attacks used techniques beyond file encryption: Comparison of the routines of notable ransomware families seen in the first half of 2019

These incidents showed how ransomware operators furthered their strong-arm schemes by compromising mission-critical systems and hence the affected organizations’ operations and bottom lines. The emboldened attacks and higher ransom demands could have also been spurred by their malware’s having been outfitted with destructive routines beyond file encryption, serving as fail-safes to maximize impact. With foolproof mechanisms that could lessen the chances for victims to recover their systems or files, ransomware operators could be further motivated into intimidating and demanding heftier ransom payments from their victims.

## WannaCry still reigns supreme

Feedback from the Trend Micro Smart Protection Network infrastructure indicated various active ransomware families in the first half of 2019. The organizations we saw that were most affected were in manufacturing, government, education, and healthcare industries, but we also saw affected organizations in finance, technology, energy, food and beverage, and oil and gas industries.

Offering further proof of its endurance, the notorious WannaCry, which left significant damage across a number of countries in the wake of its initial outbreak in May 2017,<sup>34</sup> was still the most detected ransomware family throughout the period — its numbers even exceeded, by wide margins, those of the other ransomware families combined. As in last year, the majority of WannaCry detections were from systems running Microsoft Windows 7. Evidently, bridging security gaps in vulnerable systems remained a challenge especially for enterprises, given that the vulnerability exploited by WannaCry had been patched since 2017 and that support for Windows 7 had been set to end in January 2020.<sup>35</sup>

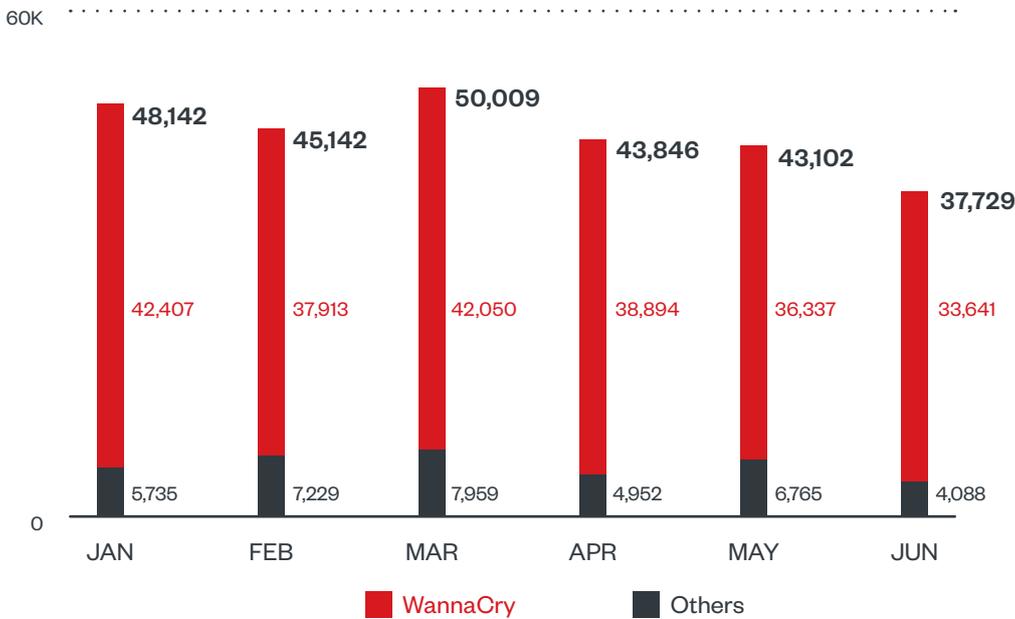


Figure 3. WannaCry still accounted for the majority of ransomware detections: Monthly comparison between detections of WannaCry and combined detections of the other ransomware families in the first half of 2019



Figure 4. Over 90% of WannaCry detections were from systems running Windows 7:  
Distribution of WannaCry detections in the first half of 2019 by operating system

Despite the continued decrease in new ransomware families, their apparently newfound lucrativeness meant they would remain a perennial threat, especially to enterprises. In fact, a budding player, Sodinokibi (aka Sodin or REvil), seemed to have already taken the reins from GandCrab with its use of similar distribution methods.<sup>36,37</sup>

The many approaches and attack surfaces that cybercriminals can use to get inside organizations' online premises means securing just the endpoint is no longer enough. Employing multilayered threat defense solutions — from the gateways, servers, and networks to endpoints — can help thwart ransomware at each layer of their online infrastructures.

# Threats increasingly 'live off the land'

## Fileless events are 18% more than in the whole of 2018; macro malware persists

The significant surge in fileless events we detected in the first half of 2019 — 18% more than in the whole of 2018 — reflected what we noted in our security predictions for this year: Cybercriminals and other threat actors would increasingly “live off the land,”<sup>38</sup> abusing or repurposing legitimate system administration or penetration testing tools to blend in.

Compared to traditional malware that writes to a machine’s disk, threats that live off the land, such as fileless threats, are not as visible since they can be executed in a system’s memory, reside in the registry, or abuse normally whitelisted tools like PowerShell, PsExec, Windows Management Instrumentation,<sup>39</sup> and AutoHotKey.<sup>40</sup> Nevertheless, we are able to detect fileless threat-related activities by tracking non-file based indicators, such as specific execution events or behaviors.

In some ways, many of the notable threats we uncovered in the half-year used fileless techniques to either drop or execute the payload — typically in the form of cryptocurrency-mining malware<sup>41</sup> and ransomware,<sup>42</sup> and in some cases, in the form of banking trojans.<sup>43</sup> These threats had something in common: PowerShell abuse. While a convenient and flexible tool for system administrators, PowerShell could be potent in cybercriminal hands.

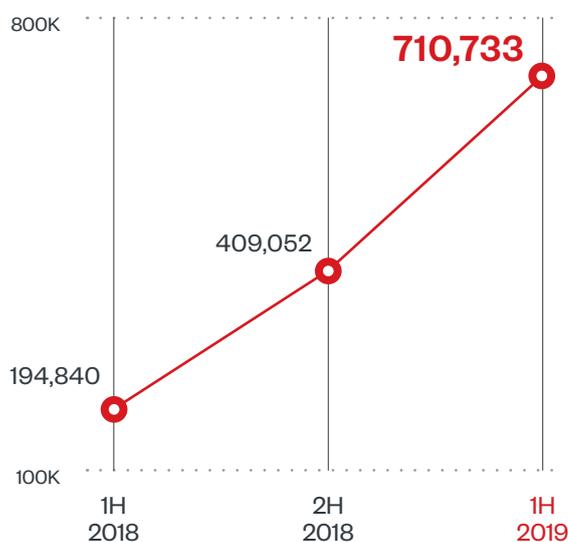


Figure 5. Fileless events were 18% more than in the whole of 2018: Half-year comparison of fileless events blocked

Despite a slight decrease in its detections compared to the second half of 2018, macro malware still persisted. As in last year, the detections for macro-based threats were due to the prevalence of Powload, mainly in spam emails.

Apart from the variety of payloads it delivers, such as the Ursnif and Bebloh information stealers, Powload itself has evolved over the years. Among other developments, it has begun using steganography – the practice of hiding code within an image – and singling out its targets by imitating and using region-specific brands or vocabulary. Powload’s abuse of PowerShell is also notable, as this is often combined with macro malware, which serves as another layer in the infection chain that can further hide malicious activity.<sup>44</sup>

Beyond Powload, we also saw macro malware used in spam campaigns that delivered information stealers like Trickbot<sup>45</sup> and even in connection with malware used for cyberespionage.<sup>46</sup>

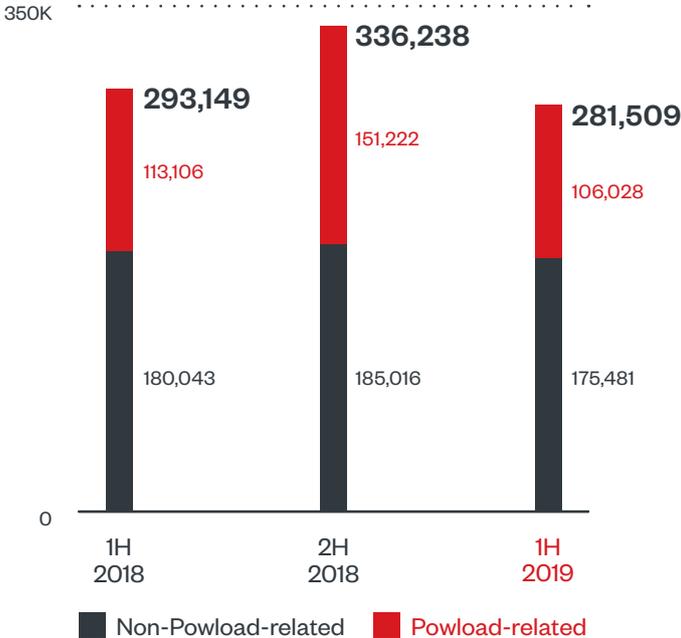


Figure 6. The majority of macro malware was still due to Powload: Half-year comparison of detections of non-Powload-related macro malware and Powload-related macro malware

## Multiple stages and layers used as fail-safes

If the use of fileless techniques and macro malware was not deterrent enough, several notable threats we saw in the half-year not only employed a combination of these but also used multistage or multilayered infection chains.

Staging the delivery of malware helps lessen the chances of its getting blocked altogether. The first stage of a malware's infection chain would often be unexacting, e.g., retrieving a second-stage script, so that it would seem innocuous. Embedding a large piece of malware in a Microsoft Office document, for instance, would raise suspicion. For threat actors, multistage delivery can be their fail-safe way to bypass security measures. We saw such a strategy in a cryptocurrency-mining campaign whose infection chain involved three stages of retrieving and executing PowerShell scripts until it downloaded the payload and propagated to other machines.<sup>47</sup>

Multilayered attacks, on the other hand, give malware more chances of getting into systems. Even if an attack does not use new malware or a groundbreaking technique, cramming in as many exploits as possible, for example, increases its opportunity to infect a system. The cryptocurrency-mining BlackSquid malware did just that, employing eight exploits to propagate, drop and run the payload, and give attackers the capability to execute remote code.<sup>48</sup> Even more exploits were used by a variant of Mirai: 13 exploits in a single attack, employed by the malware to spread to routers and other devices associated with the internet of things (IoT). And as if that was not enough, it also had capabilities for brute-forcing these devices using a list of commonly used credentials.<sup>49</sup>

Multistage and multilayered malware infections are difficult to detect, as they can find refuge within routinely used files or programs and can thus be easily overlooked, especially if a security mechanism is limited to only inspecting a specific malicious routine. It does not help that as more of these advanced and stealthy threats crop up, fewer people are available to tackle them — to the extent that according to a survey we commissioned and published in March, nearly 50% of organizations are contending with a cybersecurity skills shortage.<sup>50</sup>

Another interesting and related trend we saw was mobile ransomware's periodic shifts between file encryption and information theft. Anubis, for example, had ransomware-like capabilities<sup>51</sup> but could also serve as banking malware.<sup>52</sup> Its latest iterations actually retained both routines, but its operators seemed to be focusing on one depending on their campaigns or targets — or perhaps they were just going where the money was.<sup>53</sup> After all, old ransomware families like SMSLocker and Svpeng had also operated as banking malware.<sup>54</sup>

## Exploit kits remain a credible threat

After a period of subdued activity, the ShadowGate campaign resurfaced in June to deliver cryptocurrency miners using an upgraded version of the Greenflash Sundown exploit kit that was now capable of living off the land, that is, using an updated PowerShell loader to filelessly execute the payload. Its last notable activity was in April 2018, when it used the exploit kit to briefly spread cryptocurrency-mining malware across servers in East Asia.<sup>55</sup>

Greenflash Sundown’s resurgence in particular is a sign of things to come in the exploit kit landscape. Users and enterprises, therefore, should not allow themselves to be lulled into complacency by such factors as threat actors’ lack of access to zero-day exploits and the curtailed reliance on platforms that exploit kits capitalize on.

Telemetry from the Trend Micro Smart Protection Network showed that exploit kit-related activities rose in the first half of 2019, continuing the increase seen in 2018. The further rise, though, was still a far cry from several years ago, when exploit kits were at their peak and the instances of blocked access to sites that hosted them were on the order of millions.<sup>56</sup> Be that as it may, the observed increase suggested that exploit kits were still having some success despite exploiting old vulnerabilities, likely reinforced by the various payloads and proofs of concept that they could incorporate.

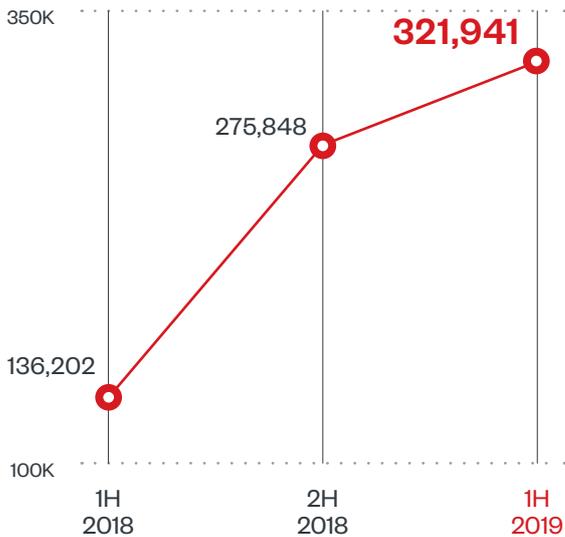


Figure 7. Despite an erratic presence, exploit kit activities were still significant: Half-year comparison of instances of blocked access to URLs hosting exploit kits

## Social media and networking platforms abused to hide cybercriminal trails

Social media certainly had been no stranger to abuse. Our 2017 research on fake news showed how it could be misused to help instigate protests, discredit journalists, and even manipulate national policies or influence elections.<sup>57</sup> But the notable trend we observed in the first half of 2019 was the abuse of social media channels along with collaboration platforms and networks, including those widely used by developers and information security professionals, as part of a threat’s kill chain or other schemes.

The Slub backdoor, for example, abused Slack and Github: the former, a popular web-based collaboration and messaging platform, as an intermediary between the malicious actors and their victims, and the latter, a web-based collaboration and version-control platform for developers, as a repository for malicious code.<sup>58</sup> There was also a hacking group whose modus operandi was to steal popular profiles on Instagram through phishing, and then drawing the attention of the true owners by defacing the stolen accounts and extorting money or nude images from them.<sup>59</sup>

Twitter, another popular social media site, also figured in the strategy of the operators of the XLoader Android malware, who concealed their command-and-control (C&C) servers by encoding the C&C addresses in Twitter account names.<sup>60</sup> Tech support scams also caught on, as they were seen using social media channels to bait unfortunate users into handing out personally identifiable information (PII), downloading questionable software, or even being charged for fake services.<sup>61</sup>

Social media provides feature- and content-rich platforms that can serve as additional avenues for information security professionals to gather actionable threat intelligence.<sup>62</sup> But as these incidents have shown, it can also be abused by malicious actors to obfuscate their activities. Therefore, as enterprises use social media to promote their brands and expand their reach, they should extend their cybersecurity strategies to their social media channels, given the security and privacy risks — data breach, impersonation, and phishing, among others.

# Targeted attacks employ more tried-and-tested techniques than new ones

Targeted attacks had been considered to be at the forefront of innovating tactics, techniques, and procedures (TTPs). But the notable campaigns we saw in the first half of 2019 indicated otherwise. The more noticeable use of relatively old and established TTPs was perhaps due to their efficiency — after all, creating malware with new routines took time and resources. Moreover, targeted attacks could accomplish their cyberespionage-driven goals by living off the land.

The Bouncing Golf campaign, for example, used the known technique of repackaging legitimate apps. The apps' distribution was notable, however, as they were hosted on neither official nor third-party app marketplaces, but rather were hosted on a website that was promoted on social media.<sup>63</sup> The TA505 cybercriminal group also did not have to rope in novel techniques to its campaigns. It had an arsenal of tried-and-tested mechanisms at its disposal: hacking tools, macro malware (including malicious macros embedded in Microsoft Excel 4.0), trojans, downloaders, and backdoors.<sup>64,65</sup> By deploying large-scale spam campaigns and regularly revamping its distribution methods, it remained a persistent threat to enterprises.

The MuddyWater cyberespionage campaign banked on known techniques too: spear-phishing emails, watering hole, macro malware, and PowerShell abuse.<sup>66</sup> Its attacks might not be using zero-day exploits or sophisticated malware, but they managed to affect their targets by persistently luring victims into downloading and opening their backdoor-embedded documents.<sup>67</sup> Most recently, the campaign was seen using a multistage PowerShell-based backdoor called Powerstats v3 and 13 open-source post-exploitation tools to further carry out routines like dumping credentials or gaining administration rights after compromising a system.<sup>68</sup>

That these campaigns' apparently old tricks still proved effective against their targets only highlighted the need for enterprises to reexamine or renew their cybersecurity strategies — from improving awareness among employees and patching vulnerable systems to assigning only the necessary privileges across the whole network infrastructure.

# Illicit actors continue to bank on cryptocurrency mining

## Cryptocurrency-mining malware is still the most detected threat

Despite a decrease in detections that continued from 2018, data from the Trend Micro Smart Protection Network infrastructure showed that cryptocurrency-mining malware was still the most detected threat in the first half of 2019 in terms of file-based threat components.

Signs of strength of and upbeat sentiment toward cryptocurrencies perhaps were driving cybercriminals into engaging in illicit cryptocurrency mining (aka cryptojacking). For one thing, the value of bitcoin, arguably the best-known cryptocurrency in the world, increased over the last several months, peaking at around US\$12,000 in late June — triple its value at the start of the year.<sup>69</sup>

Monero also tripled in value from the start of the year to late June, albeit reaching its highest point at just US\$117.<sup>70</sup> Still, it continued to be quite popular among cybercriminals, even becoming their preferred cryptocurrency for mining malware.<sup>71</sup> That Monero had been cybercriminals' cryptocurrency of choice was no surprise, considering that Monero had been known to provide near-total anonymity.<sup>72</sup> Monero could also be viably mined without using dedicated hardware or custom rigs, like those used in bitcoin mining.<sup>73</sup>

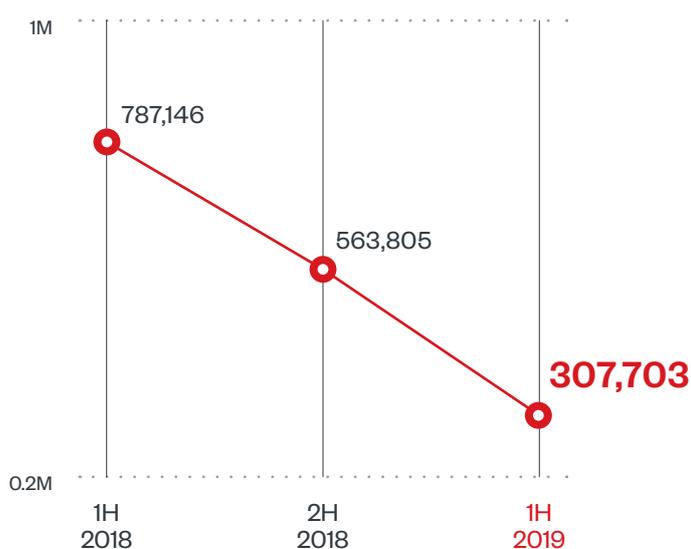


Figure 8. Despite the downward trend, cryptocurrency-mining malware was still the most detected threat in terms of file-based threat components: Half-year comparison of detections of file-based cryptocurrency-mining malware-related threat components

## Cryptocurrency-mining threats further evolve with complex routines

Cryptocurrency-mining threats also acquired some degree of maturity. Many of them were seen using advanced hacking tools, modular malware, and intricate infection chains typically associated with targeted attacks or information theft campaigns.

In February, we reported on an apparent Korkerds copycat Linux threat that removed cryptocurrency miners from affected systems and installed its own cryptocurrency-mining malware.<sup>74</sup> In the same month, we also shared our findings on a cryptocurrency-mining threat that used the hacking tools Radmin and Mimikatz to harvest credentials and gain administrator rights — and even took pains to hide its trails by concealing its activities under randomly named files and mounting its attacks during holidays (when companies would be unlikely to make the necessary detections).<sup>75</sup>

As we reported in April, we also discovered a campaign that employed multiple propagation techniques to execute the PCastle script, which in turn dropped a Monero miner onto victimized systems.<sup>76</sup> While we detected this campaign across a handful of countries, its ensuing spate of attacks, which we first observed in May, reverted to its initial target: systems based in China. This time, however, it used a multilayered fileless approach to execute PCastle.<sup>77</sup>

Several cryptocurrency-mining threats manifestly took advantage of security gaps. A vulnerability in the widely used Confluence collaboration software was exploited to deliver a cryptocurrency miner that contained a rootkit designed to hide its activities.<sup>78</sup> There were also cryptocurrency-mining botnet malware variants that used open ports as entry points to spread to other Android devices<sup>79</sup> and incorporated a Perl-based backdoor component that was capable of launching distributed denial-of-service (DDoS) attacks.<sup>80</sup> Yet another evolution we observed was the use of malware written in the open-source programming language Go (aka Golang) that scanned machines running vulnerable software to spread its cryptocurrency miner payload.<sup>81</sup>

## Malicious cryptocurrency mining cashes in on servers and cloud environments

If in 2017 and 2018 malicious cryptocurrency-mining activities were largely occupied with techniques to get their malware into systems, the first half of 2019 showed a noticeable incidence of cryptocurrency-mining malware deployed on servers and, as we predicted, in cloud environments.<sup>82</sup> Cryptocurrency-mining threats to cloud infrastructures continued to gain traction among illicit actors, entailing the abuse of compromised container platforms and the use of malicious Docker images, among other vectors.<sup>83</sup>

As we reported in March, a Docker Control API was being abused by a service that had a Monero miner as its payload. The service's malicious activities involved searching for an exposed or misconfigured container image, which then enabled the attacker to abuse the API to execute commands, such as creating new containers with an attacker-specified image.<sup>84</sup> We reported a similar incident in May: We discovered that a publicly accessible Docker Hub repository was hosting images that included cryptocurrency-mining software binaries and a script that was probably used to look for more API-exposed Docker hosts to infect.<sup>85</sup>

Also in May, a cryptocurrency-mining campaign was reported to have been exploiting a vulnerability in the web framework used by the Jenkins automation server to execute the Kerberods malware, which in turn deployed Monero-mining malware on affected systems.<sup>86</sup> A Jenkins vulnerability was also exploited in a prior incident, reported in early 2018, involving the JenkinsMiner malware, which was said to have earned its operators over 10,800 Monero, or at least US\$3 million at the time of its discovery.<sup>87</sup>

The shift was driven by several factors. One was that endpoint security had moved ahead in terms of detecting and blocking cybercriminals' cryptocurrency-mining threats running on individual machines. Another was the shutdown in March of Coinhive,<sup>88</sup> an otherwise popular service that let users mine cryptocurrency by embedding scripts on websites, which meant a significant loss to the cybercriminals' toolkit.

Servers and cloud-based platforms are more than just viable alternatives. Public cloud infrastructures, for instance, are an attractive target. Even a multitude of devices or endpoints cannot deliver the same dedicated and nearly unlimited resources a cloud infrastructure can provide. For cybercriminals, it is a gold mine — one that may be unguarded or unsecured at that. And they are only too willing to take advantage of gaps such as those brought about by misconfiguration to deploy and spread their malware.

Cryptojacking may not be as destructive as ransomware. But its impact on enterprises goes beyond the stealthy theft of computing power or issues of system performance. For cloud deployments, in particular, it can translate to higher usage bills, especially if usage quotas are exceeded. And it can mean wear and tear of hardware and higher electric energy consumption for on-premise servers or data centers. Moreover, the availability, integrity, and stability of systems used to schedule or run specific tasks can be undermined when cryptocurrency miners are deployed in them.<sup>89</sup>

Malicious actors want their cryptocurrency-mining malware on as many systems as possible while staying under the radar. The longer their activities are hidden, the more money they can make. Given their threats' increased sophistication of routines and broadening scale of deployment, having greater visibility and control over systems can help organizations better identify the activities and processes running in their online infrastructures.

## Exposed and unsecure cloud environments show their ripple effect

Threats to cloud environments, including those initiated by malicious actors engaged in illicit cryptocurrency mining, usually take advantage of misconfiguration and weakly secured credentials — oft-overlooked security risks that are, in fact, a major concern particularly in application components and APIs.<sup>90</sup> Misconfigurations have a ripple effect beyond their immediate impact: An unsecure API, for example, can invite threat actors who are constantly looking, through network-scanning tools and the like, for vulnerable or misconfigured APIs that they can abuse.

In a cloud-based environment, misconfiguration means that a cloud instance is set up in such a way that it becomes susceptible to breaches. In the first half of 2019, for example, cloud-based infrastructures storing sensitive data were discovered to have been lacking password protection<sup>91</sup> or found with neither authentication nor firewall security.<sup>92</sup>

While misconfiguration may sound easy to fix, setting up a cloud instance, let alone an entire cloud infrastructure, is actually a complex task that requires specialized knowledge. And if the task is not done properly, any security mechanism running within the cloud environment will not be able to fully deter attackers from hacking into it. This is particularly true for organizations adopting DevOps, an approach and set of practices focusing on agile development and release life cycles,<sup>93</sup> which are compelled to quickly create and deliver their applications or products while also complying with auditing, monitoring, and data privacy regulations such as the General Data Protection and Regulation (GDPR) of the European Union (EU).<sup>94</sup>

# Messaging threats further diversify

## Phishing sites spoofing Office 365 markedly increase

Phishing activities decreased in the first half of 2019, based on data from the Trend Micro Smart Protection Network infrastructure. Taking into account our numbers from the second half of 2018, we noted a 9% drop in instances of blocked access to non-unique phishing-related URLs — which counted all detected attempts to visit the sites — and an 18% decline in instances of blocked access to phishing URLs by unique client IP address — which indicated the number of users who would otherwise have been affected.

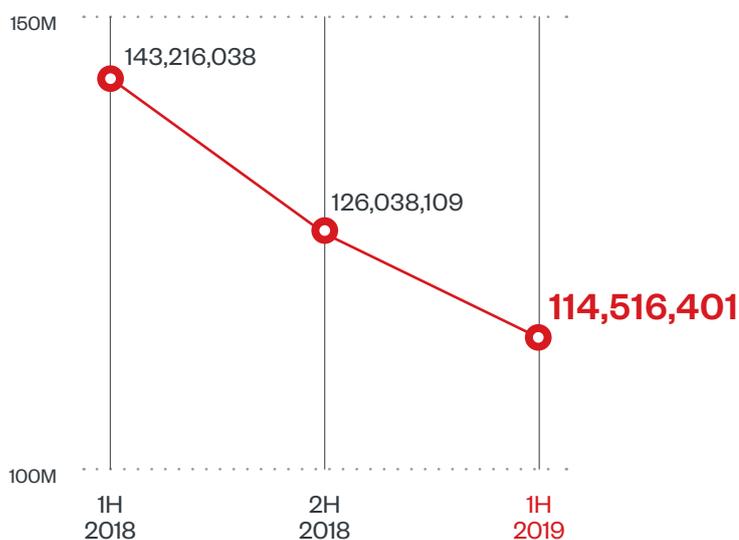


Figure 9. Detected attempts to visit phishing-related sites continued to decline: Half-year comparison of instances of blocked access to non-unique phishing URLs (e.g., three instances of blocked access to the same URL counted as three)

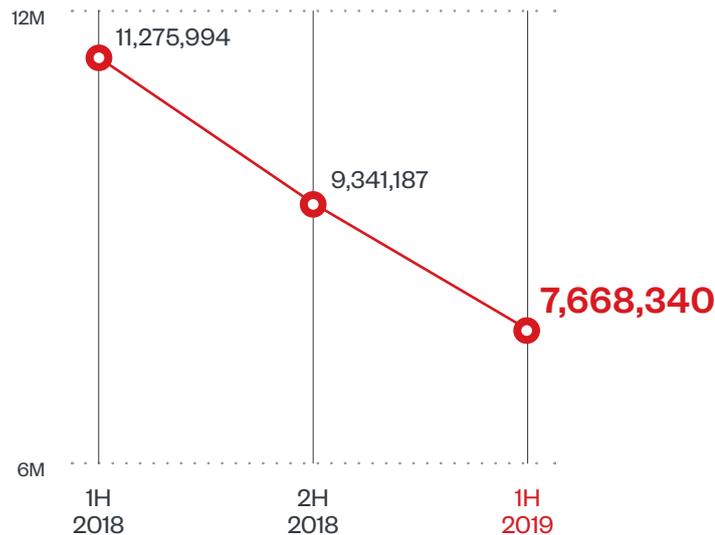


Figure 10. The number of users who would have been affected by phishing-related sites further decreased:  
 Half-year comparison of instances of blocked access to phishing URLs by unique client IP address  
 (e.g., one machine that attempted to access a URL three times was counted as one)

The downturn could have certain dynamics at play, such as improved user awareness on phishing scams. Interestingly, though, comparing our data from the second half of 2018 and the first half of 2019, we saw a 76% increase in the number of blocked unique phishing URLs that spoofed Microsoft Office 365, particularly Outlook. An apparent corroboration of this trend could be found in a research that determined that 29% of organizations had their Office 365 accounts compromised in March, resulting in more than 1.5 million malicious spam emails sent from the hacked accounts in that month alone.<sup>95</sup> This trend was possibly buoyed by cybercriminals who found and favored cloud-based or mobile platforms such as Office 365 as avenues for scamming users and enterprises.

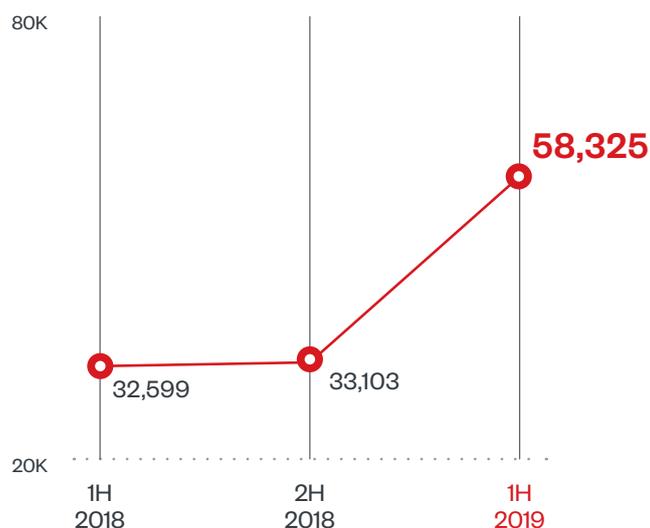


Figure 11. The number of blocked unique phishing URLs that spoofed Office 365 (including Outlook) increased by 76%: Half-year comparison of unique Office 365-related phishing URLs blocked

For cybercriminals, this pronounced refocus meant diversifying into polymorphic and multiplatform social engineering threats.<sup>96</sup> As we reported in January, some Android apps promised unwitting users to enable them to spruce up their photos but instead redirected them to phishing sites and stole the photos they were trying to beautify.<sup>97</sup> In March, we discovered a phishing campaign that used the watering hole technique — performing reconnaissance to compromise a target’s website — to put up fake login forms designed to pilfer user credentials.<sup>98</sup> And in another campaign, which we reported on in April, phishers abused SingleFile, an extension for Google Chrome and Mozilla Firefox, to obfuscate their fraudulent login pages, including one that spoofed a popular payment processing website.<sup>99</sup>

Also in March, the Oregon Department of Human Services announced that the personal health information of more than 350,000 clients were exposed after a phishing attack that most likely gave hackers access to employees’ email accounts.<sup>100</sup> And cybercriminals continued to deliver malware by hijacking existing email threads, as exemplified by an evolution of Emotet reported on in April<sup>101</sup> — the trick was previously seen last year being pulled by a campaign that delivered the Ursnif malware.<sup>102</sup>

By hijacking existing email threads, malicious actors can make their scams more believable to unwitting recipients, as opposed to creating new emails that can be more easily flagged as fraudulent. By turning an organization’s own data or assets against its own employees, they can carry out their attacks without anyone suspecting that something is amiss. These attacks can be further complicated by techniques such as employing uncommonly used files<sup>103</sup> and abusing legacy<sup>104</sup> or even supposedly secure protocols.<sup>105</sup>

## **Business email compromise scams continue to thrive**

Scams that rely on business email compromise (BEC) may be far simpler than the technically advanced malware involved in phishing or targeted attacks: At the very least, BEC scams need only exhibit familiarity and mimic well-established business interactions. But they do rely quite heavily on social engineering techniques, such as pretending to be a high-level executive — typically the CEO — and prodding the recipients — usually employees who can conduct wire transfers — with a sense of urgency. And if the FBI’s recent report is any indication, falling prey to them has become costlier than ever.

The figures released by the FBI’s Internet Crime Complaint Center (IC3) showed that BEC schemes had been very lucrative for the scammers behind them. The agency determined that companies in the U.S. lost over US\$1.2 billion to BEC or email account compromise (EAC) scams in 2018, based on the more than 20,000 related complaints that it received throughout the year.<sup>106</sup>

Based on our data, BEC attempts thrived well into the first half of 2019, increasing by 52% from the second half of 2018. And as in the previous half-year, businesses in the U.S., Australia, and the U.K. encountered the most BEC attempts. While they might be reflective of the distribution of our customer base, these countries had been home to many large enterprises and multinational headquarters, and thus made sense as locations for scammers to direct their BEC attempts at.

Unsurprisingly, the CEO remained the most spoofed position in BEC scams, far ahead of other figures of authority within companies.

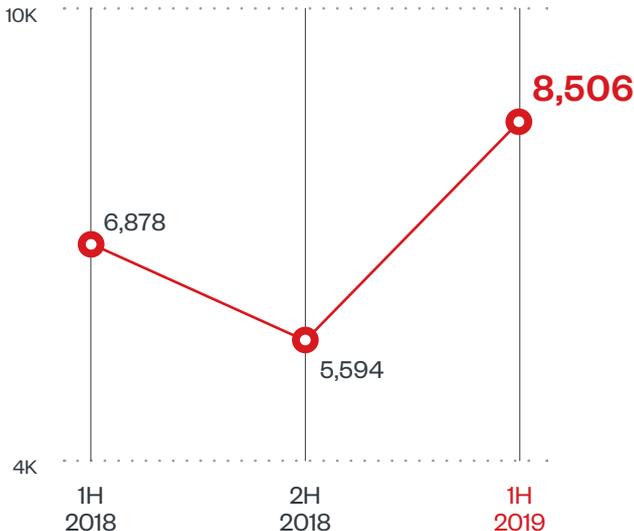


Figure 12. BEC attempts increased: Half-year comparison of BEC attempts

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.



Figure 13. More BEC attempts were seen in countries considered as business hubs:  
Distribution of BEC attempts in the first half of 2019 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.



Figure 14. The CEO was still the most spoofed position in BEC attempts:  
Distribution of spoofed positions in BEC attempts in the first half of 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.*

BEC scammers started out with relatively simple methods, which usually involved just hacking or spoofing the email accounts of C-level executives to fraudulently wire money. But they have since broadened their horizons, as illustrated by a number of incidents in the first half of 2019 — including ones that affected a public relations agency,<sup>107</sup> the regional office of a multinational,<sup>108</sup> and even a school district.<sup>109</sup>

The London Blue group, most notably, have over the years targeted other employees such as finance controllers and executive assistants,<sup>110</sup> while other fraudsters have targeted human resource personnel<sup>111</sup> — a trend foretold by our prediction that BEC attempts would be targeting positions several levels down the organizational hierarchy.<sup>112</sup> There has also been a noticeable shift in targets from traditional enterprises toward nonprofit and religious organizations, as evidenced by a BEC scam in April that cost a church in Ohio US\$1.75 million; the scammers managed to compromise the email accounts of a couple of employees, which they then used to dupe other members of the organization into transferring funds into an account claiming to be that of a contractor.<sup>113</sup>

## Sextortion schemes via spam surge

In April,<sup>114</sup> the FBI reported that sextortion constituted the majority of extortion-related complaints it received in 2018.<sup>115</sup> Toward the end of last year, we issued a prediction that in 2019 there would be an increased incidence in digital extortion schemes, particularly sextortion.<sup>116</sup> Sure enough, data from the Trend Micro Smart Protection Network infrastructure showed a whopping 319% increase, from the second half of 2018 to the first half of 2019, in detections of sextortion-related spam emails.

A notable example of sextortion in the first half of 2019 was a spam campaign we saw in April that mainly targeted Italian-speaking users, threatening them with the prospect of sending compromising videos to their contacts unless they sent their payments in time.<sup>117</sup>

The use of fear and the sensitive nature of sextortion schemes can intimidate victims into giving in to sextortionists' demands. These schemes will not be going away anytime soon, and may even see further significant activity, if their recent numbers are anything to go by.

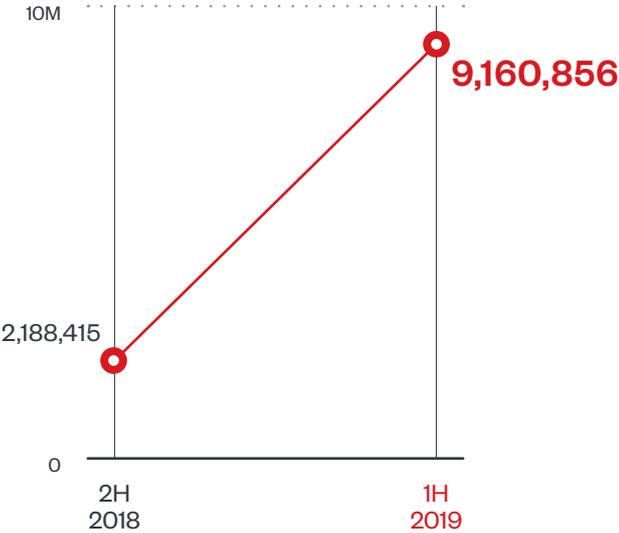


Figure 15. Sextortion schemes via spam more than quadrupled:  
Half-year comparison of detections of sextortion-related spam emails

# Pervasive vulnerabilities make patching even more important

## More hardware-level vulnerabilities disclosed

The disclosure, at the start of 2018, of Meltdown and Spectre — security flaws related to the speculative execution of CPU instructions in certain microprocessors<sup>118</sup> — added a new dimension to the challenges of mitigating and patching vulnerabilities. Indeed, even devices fitted with processors from as early as 1995 could be affected,<sup>119</sup> making the potential impact of the vulnerabilities pervasive. Seemingly out of the blue, hardware-level vulnerabilities gained some relevance in the predominantly software-based cybersecurity landscape, which saw the disclosure of even more such flaws.

In February of this year, researchers showed a proof of concept that could enable hackers to conceal their malware from antivirus solutions by using enclaves in Intel's Software Guard Extensions (SGX), a set of instructions found in Intel's Core and Xeon CPUs. Designed to protect and restrict access to data in them, enclaves could be abused by hackers by putting malicious code in them and embedding them in applications that could then be unwittingly installed by users.<sup>120</sup>

In May, researchers disclosed several microarchitectural data sampling vulnerabilities in modern Intel processors. Their impact was demonstrated through the side-channel attacks ZombieLoad, Fallout, and Rogue In-Flight Data Load (RIDL), with methods similar to those of Meltdown and Spectre. These side-channel attacks could enable hackers to execute code or exfiltrate data that were otherwise protected by the processors' architectural mechanisms.<sup>121</sup>

## Disclosure of high-impact vulnerabilities is more pronounced

Ubiquity characterized the vulnerabilities disclosed during the first half of 2019, given how pervasive their impact could be. Indeed, the majority of the vulnerabilities reported through our Zero Day Initiative (ZDI) program were rated high in severity.

One of the most notable was BlueKeep (CVE-2019-0708), a critical vulnerability in remote desktop services, which made headlines in May due to its “wormability” — its successful exploitation could let malware propagate in a way similar to how WannaCry used EternalBlue.<sup>122</sup> The risk it posed was so significant that Microsoft even rolled out patches for the out-of-support operating systems Windows 2003 and Windows XP.<sup>123</sup>

Separately, also in May, a security researcher, going by the handle SandboxEscaper, published exploit code for a then-zero-day vulnerability (CVE-2019-1069) in Windows 10’s Task Scheduler. Affecting 32- and 64-bit Windows 10, Windows Server 2016 and 2019, and even Windows 8, the vulnerability could let attackers escalate their privileges to access normally protected files.<sup>124</sup>

None (0.0)	Low (0.1-3.9)	Medium (4.0-6.9)	High (7.0-8.9)	Critical (9.0-10.0)
0	107	101	335	40

Table 2. While there might be relatively few vulnerabilities that were rated critical, many of the reported vulnerabilities had pervasive impact: Severity breakdown, based on Common Vulnerability Scoring System (CVSS) v3.0, of vulnerabilities disclosed in the first half of 2019 through our ZDI program

The disclosure of vulnerabilities in container platforms and in tools especially used by DevOps professionals was also more pronounced. It was not unexpected, given the increased adoption of these kinds of software. But the risks the vulnerabilities posed also highlighted the importance of incorporating security into workflows or development life cycles as early as possible.

Among the most notable was CVE-2019-5736, a vulnerability in runC, a runtime component used for container platforms such as Docker and Kubernetes. The successful exploitation of this vulnerability could give attackers full control of the host running the container and allow them to deploy a malicious container in the production environment.<sup>125</sup> Another was CVE-2019-1002101, a vulnerability in Kubernetes’ command-line interface for running commands and managing resources that was actually derived from an earlier vulnerability (CVE-2018-1002100).<sup>126</sup> Its successful exploitation could enable hackers to lure users into downloading a malicious container image, or, by chaining it with another vulnerability, illicitly access a container.<sup>127</sup>

A vulnerability (CVE-2019-9580) was also found in StackStorm, a workflow automation tool widely used by DevOps teams. It could allow attackers to gain unauthorized access to and carry out arbitrary commands on exposed servers.<sup>128</sup>

## Microsoft has the most vulnerabilities disclosed; ICS security advisories decline

Based on our data, which included input from more than 3,500 independent researchers who contribute to our ZDI program, Microsoft issued the most advisories among home and office software vendors in the first half of 2019; many of these were related to Windows, Office, and Internet Explorer. But the majority of the vulnerabilities disclosed in the half-year were related to software used in industrial control systems (ICSs).

Compared to the second half of 2018, however, there was a 36% decrease in ICS software-related vulnerabilities disclosed in the first half of 2019. The decrease could be due to several factors: overall improvement in cybersecurity awareness, patching ecosystems, and timely and responsible disclosures presumably in compliance with regulations and directives such as the Network and Information Service (NIS) Directive, which had been requiring operators of critical infrastructures in the EU to improve their security posture.<sup>129</sup>

Interestingly, nearly half of the ICS software-related vulnerabilities, including those in supervisory control and data acquisition (SCADA) environments, were found in LAquis SCADA software and Advantech WebAccess. The former software product includes human-machine interfaces (HMIs) and the latter is a web-based HMI solution. In SCADA environments, HMIs are essentially hubs that manage critical infrastructures and monitor different control systems that directly influence operations. As such, they have become high-value targets for threat actors looking to disrupt business operations. The trouble is that they can be challenging to secure since they are used not only to manage operational technology (OT) infrastructures, but also to connect to devices associated with the industrial internet of things (IIoT) and even to traditional information technology (IT) systems — which can broaden a critical infrastructure's attack surface.

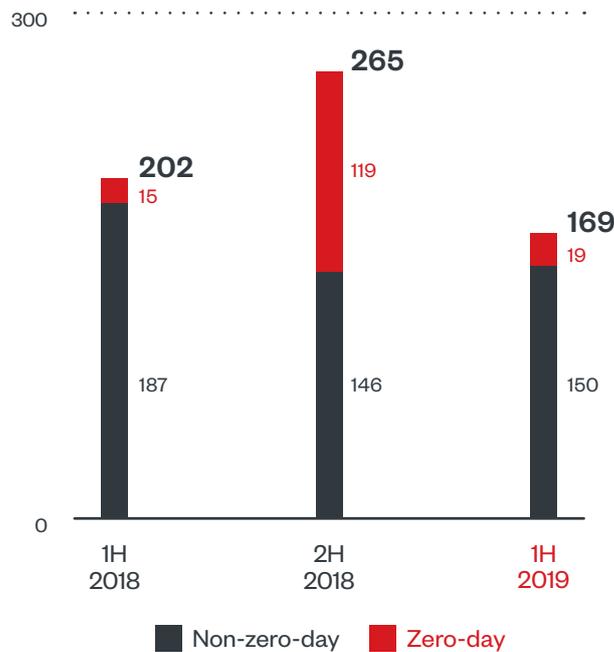


Figure 16. Disclosures of ICS software-related vulnerabilities decreased: Half-year comparison of ICS-related vulnerabilities disclosed via our ZDI program

Vulnerabilities — be they unknown, known (n-day), or found in legacy systems or software — are a reminder that organizations should not be complacent. There is practically nothing stopping malicious actors from, say, repurposing exploits for old vulnerabilities, as they can still take advantage of windows of exposure. In April, for instance, attackers were already exploiting a zero-day vulnerability in Oracle WebLogic (CVE-2019-2725) even before Oracle released a patch for it. And with the likes of BlueKeep and the critical vulnerability that SandboxEscaper divulged, it could take only a single vulnerable system to affect many others.

Immediately patching zero-day and even n-day vulnerabilities is a good practice, but it is not as easy as it sounds. In fact, according to a survey published in April, the majority of companies postpone it to avoid downtime.<sup>130</sup> This is further complicated by legacy and embedded systems, such as those used in ICSs, for which patches may no longer be issued.<sup>131</sup> Apart from employing additional mechanisms that can help bridge security gaps, such as virtual patching, it is important for enterprises to have a good grasp of the vulnerabilities that may affect their systems in terms of exploitability<sup>132</sup> and real-world risk and impact,<sup>133</sup> so that they may better assess which ones warrant urgent attention.

# IoT and IIoT security remains a significant issue

## IoT becomes battleground in incipient botnet and worm wars

It is estimated that the number of IoT devices in use will reach 25 billion by 2021.<sup>134</sup> It is not surprising, then, that attackers have been taking advantage of them too.

Indeed, the first half of 2019 was marked by a glut of malware whose capabilities abused such devices. Threat actors capitalized on improper configuration and other forms of weak security in these devices. In fact, based on telemetry from the Trend Micro™ Smart Home Network solution, the number of routers involved in possible inbound attacks (from the internet to the routers and devices connected to them) remained steady compared to the second half of 2018, at well over half a million.

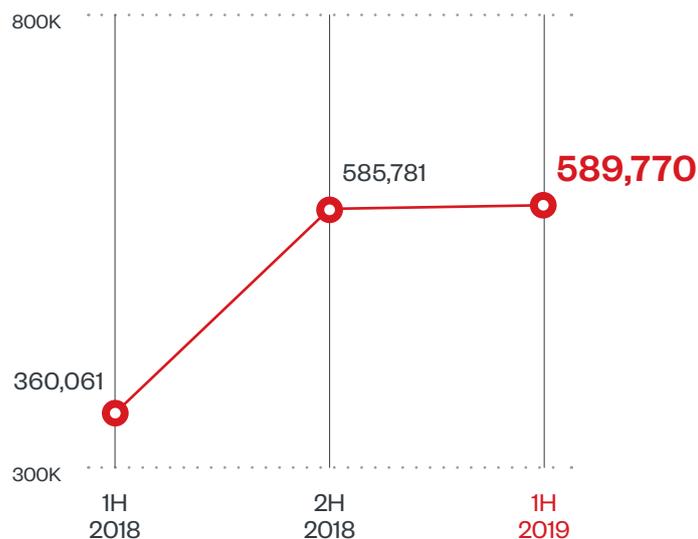


Figure 17. Activities on routers, including possible attacks, remained steady: Half-year comparison of routers identified to have been involved in possible inbound attacks

*Note: Possible attacks were detected as high-risk events closely related to threat activity.*

And as we predicted,<sup>135</sup> the IoT landscape had become a battleground of botnets and worms vying for control over their infected devices. The players in these IoT botnet and worm wars — including Bashlite<sup>136</sup> as well as several Mirai variants,<sup>137,138</sup> such as Omni,<sup>139</sup> Hakai, and Yowai<sup>140</sup> — had this routine in common: scanning the infected device for any competing malware or payload already in the device, deleting it, and embedding their own. Another trend we noted among some of these warring IoT threats was that they also further monetized the zombified devices by illicitly turning them into cryptocurrency miners.<sup>141</sup>

Other IoT threats deviated from these clashes and instead made a mark on their own. In May, for example, the HiddenWasp malware was discovered being used as a second-stage targeted attack on already compromised systems.<sup>142</sup> And a month later, Silex was discovered, having managed to brick thousands of IoT devices and render them unusable unless their firmware was reinstalled.<sup>143</sup>

IoT security has become a major concern given the ubiquity of the IoT across homes,<sup>144</sup> workplaces,<sup>145</sup> and entire industries<sup>146</sup> — from food production<sup>147</sup> and manufacturing<sup>148</sup> to telecommunications<sup>149</sup> and healthcare.<sup>150</sup> And the security risks to IoT devices will persist as long as their users and manufacturers continue to forgo something as simple as changing or updating device credentials.

## **Real-world attacks on critical infrastructures highlight importance of IIoT security**

The IIoT has transformed how industrial facilities and critical infrastructures operate.<sup>151</sup> Bringing OT and IT together has enabled enterprises to streamline, automate, and gain more visibility into their operations — so much so that the IIoT market is poised to reach US\$123 billion by 2021.<sup>152</sup>

This convergence, however, can introduce security risks. IIoT devices often spread across multiple facilities, share data across different regions, access data from readily shared infrastructures, and be managed by consoles connected to the corporate network and even traditional IT systems. These intricacies can introduce security gaps that threat actors are more than willing to exploit. In fact, according to a survey published in March, 50% of organizations already experienced an attack on their critical infrastructures in the past two years.<sup>153</sup>

A key example of IIoT malware is Triton, which was used against facilities in oil and gas industries in 2017. Also known as Trisis, it can access and modify a facility's safety instrumented system (SIS), which acts as a countermeasure that puts systems undergoing operational problems into "safe mode." If a SIS is tampered with, an attack can disrupt operations and even cause physical harm.<sup>154</sup> In April, the group behind Triton was discovered to have targeted another critical infrastructure facility.<sup>155</sup> And in June, the same group, called Xenotime, was seen probing the ICSs of power grids in the U.S. and Asia-Pacific region.<sup>156</sup>

Critical infrastructures use the IIoT to ensure smooth and safe operations, which is why upholding its security is of paramount importance — from implementing stringent patching policies, particularly in legacy systems, to enforcing authentication and authorization mechanisms, and securing the channels traversed by data between devices used in industrial facilities.<sup>157</sup>

# Multilayered defense helps address today's multifaceted threats

The notable threats seen in the first half of 2019 were persistent, stealthy, and intent on taking advantage of weaknesses in technologies, processes, and people.

For threats that live off the land or introduce additional security risks, a multilayered or defense-in-depth approach can help organizations thwart and mitigate them — from gateways, networks, and servers to endpoints. Fileless threats that abuse PowerShell and use macro malware, for example, can be tackled through mechanisms such as behavior monitoring, which blocks malware-associated routines; sandboxing, which quarantines suspicious scripts; and intrusion detection and prevention systems, which can deter suspicious traffic like C&C communication or data exfiltration. However, actively monitoring for even the subtlest anomalies or signs of malware infection in networks and endpoints, while also triaging alerts and patches, can overwhelm system administrators. To address this complication, enterprises can look into solutions that suitably combine human expertise and security technologies that can better detect, correlate, respond to, and remediate threats.

Organizations moving toward digital transformation, especially those adopting DevOps, are being driven to migrate many of their operations into or incorporate their systems with newfangled technologies or some form of cloud infrastructure. This, though, can introduce security risks. Cloud infrastructures are dynamic by nature, and hardening their security can be an iteratively demanding task. This is compounded by the relative ease with which their underlying systems and networks can be accessed or modified when misconfiguration, little or no authentication, and integration with legacy infrastructures are at play. Enterprises should therefore bake security into the technologies, workflows, and development life cycles they use, or implement it as early as possible in order to mitigate security and privacy risks down the line.

Dealing with social engineering should also be an important part of organizations' cybersecurity strategies. Security solutions arrayed at the email gateway, such as machine learning-powered technologies that help detect suspicious content in emails, can significantly deter threats. But fostering a culture of cybersecurity, which includes increasing members' awareness of typical red flags in malicious emails and regularly conducting phishing simulations, helps just as much in combating malware and cybercriminals' attempts to steal PII and money.

Enterprises and individual users alike can also benefit from security technologies that can secure their devices, especially if they are used in "bring your own device" (BYOD) environments. They should as a matter of course still follow basic security hygiene practices, such as enabling authentication features, strengthening passwords, securing routers, and not clicking links or downloading applications of dubious intent or value — if a message, product, service, or proposition sounds too good (or bad or urgent) to be true, it most probably is.

## Threat Landscape in Review

In the first half of 2019, the Trend Micro Smart Protection Network infrastructure was able to protect users from more than 26.8 billion threats — a multitude of email, file, and URL threat components.

# 26,804,076,261

Overall threats blocked in the first half of 2019

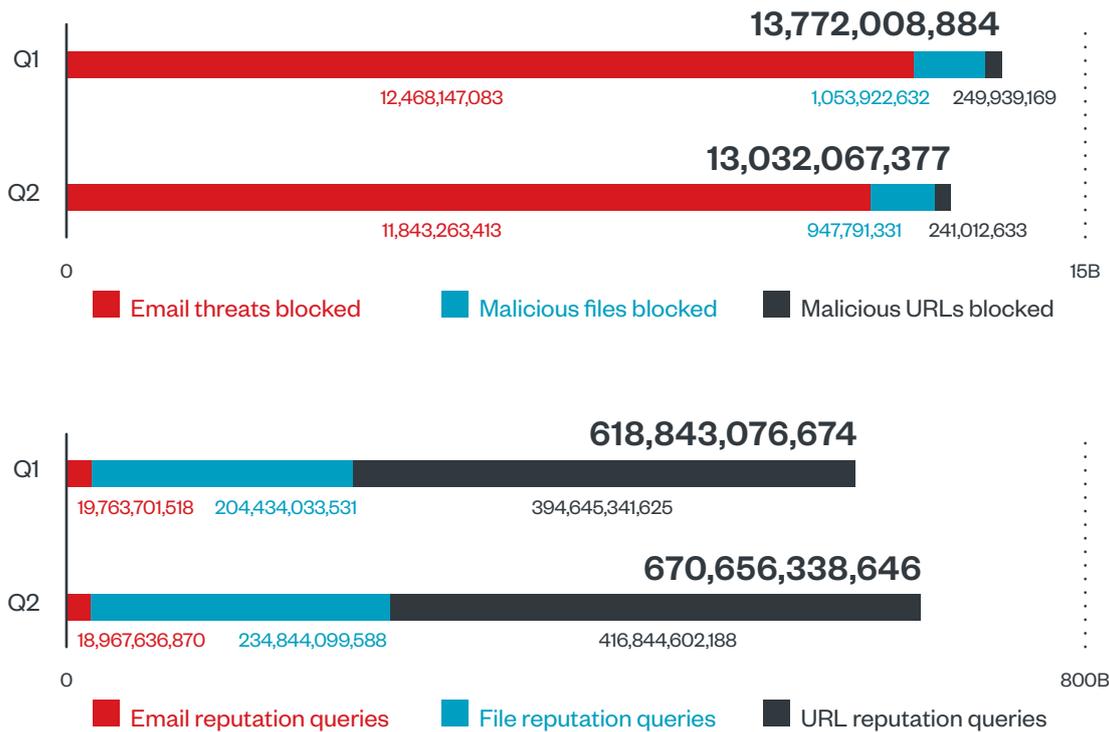


Figure 18. Email, file, and URL threats blocked decreased slightly in the second quarter of the year: Quarterly comparison of blocked email, file, and URL threats and of email, file, and URL reputation queries in the first half of 2019

Cybercriminals and fraudsters continued to take advantage of the ubiquity of the Android mobile platform. Based on data from the Trend Micro Mobile App Reputation Service, the number of blocked malicious Android apps, which included malicious apps and potentially unwanted applications (PUAs), decreased from the first quarter to the second quarter of 2019, but the overall number for the half-year was still substantial.

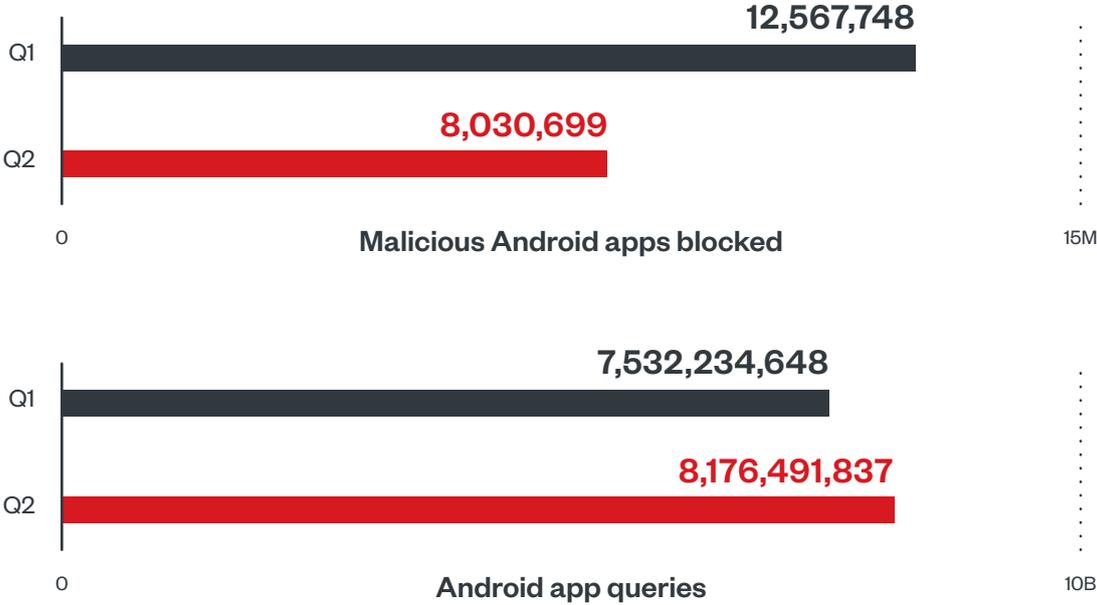


Figure 19. Android-based threats decreased in the second quarter of the year: Quarterly comparison of malicious Android apps blocked and Android app queries in the first half of 2019, based on data from the Trend Micro Mobile App Reputation Service

Despite the decrease from the second half of 2018 in the number of new ransomware families, the notable incidents in the first half of 2019 suggested that ransomware would still be a staple in the threat landscape.

New Ransomware Families					
ANATOVA	CLOP	DOGOJOKER	JUWON	RABBIT	TIONE
BIGBORB	CORTEX	FCRYPT	LOCKERGOGA	RANNOH	TREE
BITLOCKED	CRAZYCRYPT	FREEZING	LOOCIPHER	RAPID	TUNCA
BLACKROUTER	CRAZYZIP	GOLDENAXE	MAOLOA	REDKEEPER	VEGA
BLUEEAGLE	CRYPONY	GORGON	MONGOLOCK	ROBBINHOOD	XCRY
BONE	CRYPTO	HOLA	PAPJ	SEEDLOCKER	YATRON
BROWEC	CRYPTGO	JAMPER	PHOBOS	SEON	YFISNIFFER
CHATER	CYMRANSOM	JCRY	PONY	SODINOKIBI	

Table 3. 47 new ransomware families were seen: New ransomware families in the first half of 2019

In the first half of 2019, PDF was the most used file type for spam email attachments in our dataset, barely eclipsing XLS (Microsoft Excel), which was the most prevalent in 2018.

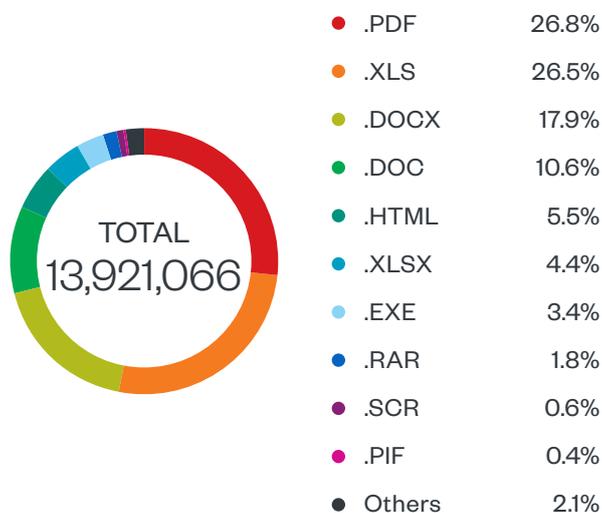


Figure 20. PDF barely overtook XLS as the most common file type in spam email attachments:  
Distribution of file types used as attachments in spam emails in the first half of 2019

Amid an increase in activity, exploit kits still used exploits for old vulnerabilities to deliver their payloads, further reinforcing the need to keep systems regularly patched and updated.

Exploit kit	Vulnerabilities exploited	Ransomware delivered	Botnet malware delivered
<b>Magnitude</b>	CVE-2018-8174 (Internet Explorer) CVE-2018-4878 (Adobe Flash Player)	Magniber	
<b>Rig</b>	CVE-2018-8174 CVE-2018-4878	GandCrab Paradise Sodinokibi GetCrypt Buran VegaLocker	Amadey AZORult KPOT Predator the Thief PurpleFox SmokeLoader Vidar
<b>GrandSoft</b>	CVE-2018-15982 (Adobe Flash Player) CVE-2018-4878		Ramnit
<b>GreenFlash Sundown</b>	CVE-2018-15982 CVE-2018-8174 CVE-2018-4878	Seon	
<b>Fallout</b>	CVE-2018-15982 CVE-2018-8174 CVE-2018-4878	GandCrab Paradise Maze	Amadey AZORult KPOT SmokeLoader Vidar
<b>Spelevo</b>	CVE-2018-15982 CVE-2018-8174	Shade Troidash	Amadey IcedID PsiXBot Vidar

Table 4. Amid a stir in activity, exploit kits still banked on old vulnerabilities: Notable exploit kits in the first half of 2019, the vulnerabilities they exploited, and the ransomware and botnet malware they delivered

The prevalence of botnet malware in the first half of 2019 was further exemplified by the 91% increase in our detections of botnet connections from the first quarter to the second quarter of the year. Botnet-related activities involved compromised and hijacked computers and devices, which connected to hacker-owned C&C servers.

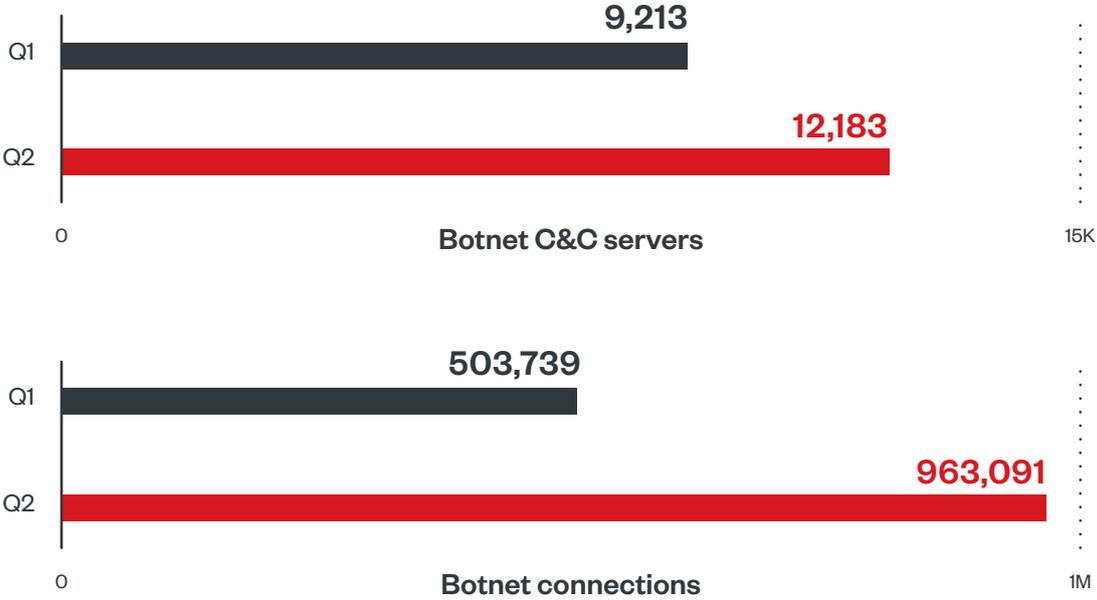


Figure 21. Botnet-related activities continued to have an upward trend:  
Quarterly comparison of C&C servers used by botnets and of botnet connections detected in the first half of 2019  
*Note: Botnet C&C servers were unique and active C&C servers that endpoints queried or connected to, while botnet connections were unique endpoints that queried or connected to C&C servers.*

As in last year, the Telnet default password login event was the most triggered event rule, based on feedback from the Trend Micro Smart Home Network solution — further reflecting the ever-important need to change, update, and strengthen credentials. Also of note was the pervasiveness of EternalBlue- and WannaCry-related events — indicating that the Server Message Block (SMB) vulnerability exploited by EternalBlue and addressed by Microsoft with its MS17-010 security bulletin was still a persistent security risk, exposing users to threats like WannaCry.

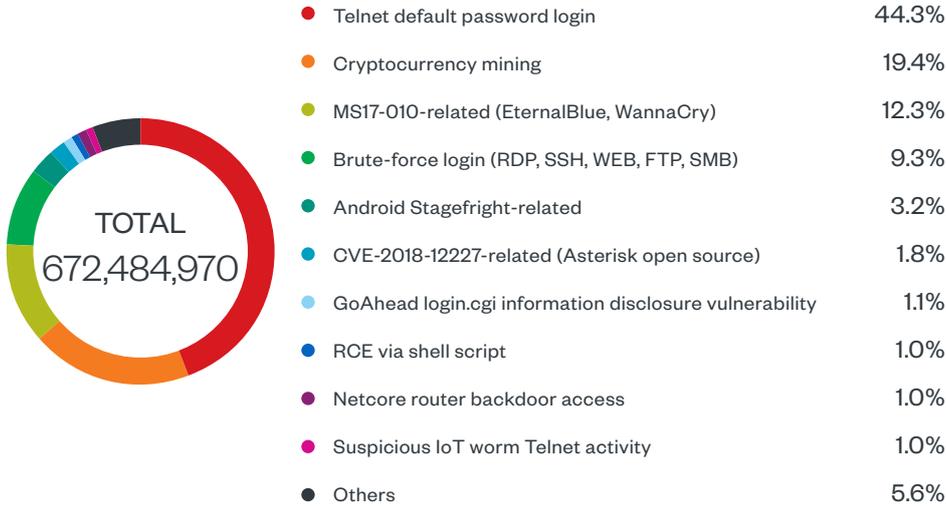


Figure 22. Telnet default password logins, cryptocurrency mining activities, and SMB vulnerability-exploiting attacks were still prevalent: Distribution of top inbound and outbound events in smart home networks in the first half of 2019, based on feedback from the Trend Micro Smart Home Network solution

*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.*

Feedback from the Trend Micro™ Deep Security™ and Trend Micro TippingPoint® Threat Protection System solutions indicated that known (n-day) vulnerabilities were still significant security issues. Attacks that exploited SMB vulnerabilities that were also used by the notorious EternalBlue and EternalChampion exploits were among the most prevalent.

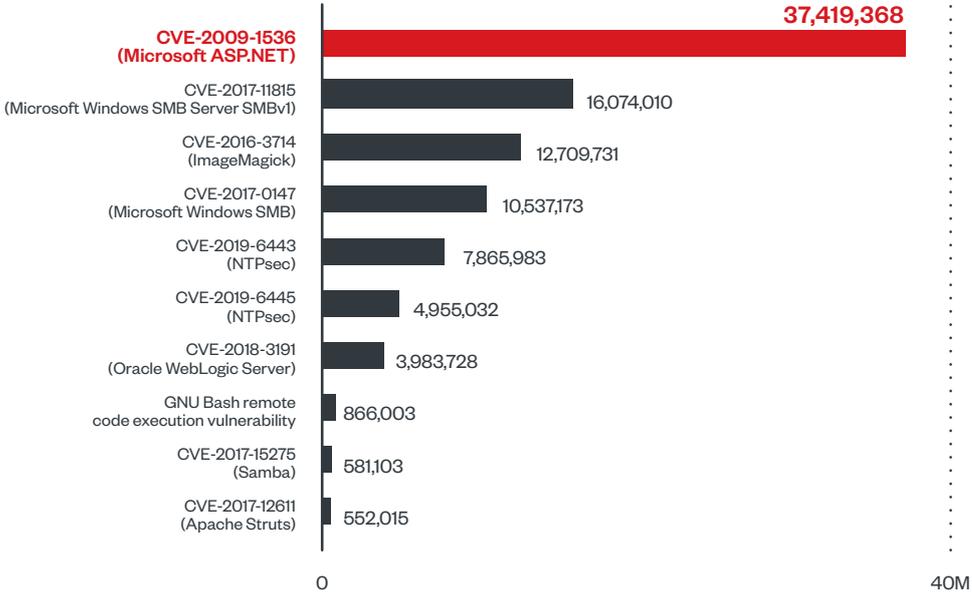


Figure 23. Old vulnerabilities for which patches had long been issued continued to pose security risks to organizations: Distribution of the top filters triggered in the first half of 2019, based on feedback from the Trend Micro Deep Security solution

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

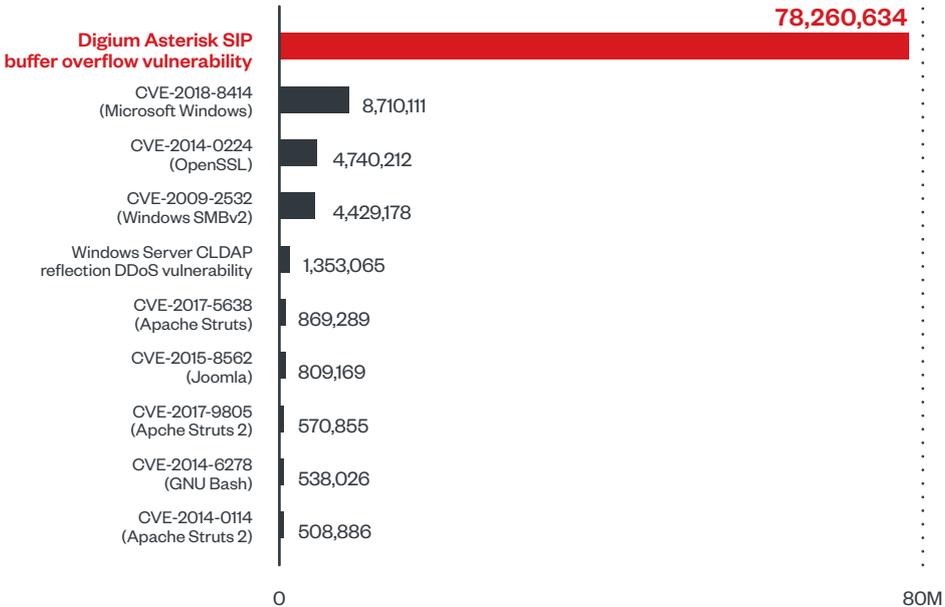


Figure 24. Intrusions or attacks that exploited old vulnerabilities for which patches had already been issued were still rampant: Distribution of the top filters triggered in the first half of 2019, based on feedback from the Trend Micro TippingPoint Threat Protection System solution

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

## References

- 1 Catalin Cimpanu. (1 June 2019). *ZDNet*. "GandCrab ransomware operation says it's shutting down." Last accessed on 24 July 2019 at <https://www.zdnet.com/article/gandcrab-ransomware-operation-says-its-shutting-down/>.
- 2 Trend Micro. (7 September 2016). *Trend Micro Security News*. "Ransomware as a Service Offered in the Deep Web: What This Means for Enterprises." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-what-this-means-for-enterprises>.
- 3 Patricia Mazzei. (19 June 2019). *The New York Times*. "Hit by Ransomware Attack, Florida City Agrees to Pay Hackers \$600,000." Last accessed on 24 July 2019 at <https://www.nytimes.com/2019/06/19/us/florida-riviera-beach-hacking-ransom.html>.
- 4 Patricia Mazzei. (27 June 2019). *The New York Times*. "Another Hacked Florida City Pays a Ransom, This Time for \$460,000." Last accessed on 24 July 2019 at <https://www.nytimes.com/2019/06/27/us/lake-city-florida-ransom-cyberattack.html>.
- 5 Coveware. (15 July 2019). *Coveware*. "Ransomware Amounts Rise 3x in Q2 as Ryuk & Sodinokibi Spread." Last accessed on 24 July 2019 at <https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread>.
- 6 Alexander Hanel. (10 January 2019). *CrowdStrike Blog*. "Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware." Last accessed on 24 July 2019 at <https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/>.
- 7 Trend Micro. (20 March 2019). *Trend Micro Security News*. "What You Need to Know About the LockerGoga Ransomware." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware>.
- 8 Joe Tidy. (25 June 2019). *BBC News*. "How a ransomware attack cost one firm £45m." Last accessed on 1 August 2019 at <https://www.bbc.com/news/business-48661152>.
- 9 Pound Sterling Live. (n.d.). *Pound Sterling Live*. "Historical Rates for the GBP/USD currency conversion on 25 June 2019 (25/06/2019)." Last accessed on 1 August 2019 at <https://www.poundsterlinglive.com/best-exchange-rates/british-pound-to-us-dollar-exchange-rate-on-2019-06-25>.
- 10 Manny Fernandez, David E. Sanger, and Marina Trahan Martinez. (22 August 2019). *The New York Times*. "Ransomware Attacks Are Testing Resolve of Cities Across America." Last accessed on 23 August 2019 at <https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html>.
- 11 Doug Olenick. (26 April 2019). *SC Media*. "Greenville in recovery phase from Robbinhood ransomware attack." Last accessed on 13 August 2019 at <https://www.scmagazine.com/home/security-news/ransomware/greenville-in-recovery-phase-from-robbinhood-ransomware-attack/>.
- 12 Janus Agcaoil and Miguel Ang. (6 June 2019). *Trend Micro Security News*. "Narrowed Sights, Bigger Payoffs: Ransomware in 2019." Last accessed on 2 August 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/narrowed-sights-bigger-payoffs-ransomware-in-2019>.
- 13 Lawrence Abrams. (5 March 2019). *BleepingComputer*. "CryptoMix Clop Ransomware Says It's Targeting Networks, Not Computers." Last accessed on 24 July 2019 at <https://www.bleepingcomputer.com/news/security/cryptomix-clop-ransomware-says-its-targeting-networks-not-computers/>.
- 14 Raphael Centeno. (8 May 2019). *TrendLabs Security Intelligence Blog*. "Dharma Ransomware Uses AV Tool to Distract from Malicious Activities." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/dharma-ransomware-uses-av-tool-to-distract-from-malicious-activities/>.
- 15 Trend Micro. (9 May 2019). *Trend Micro Security News*. "Ransomware Recap: Still in Development, Found in the Wild." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-still-in-development-found-in-the-wild/>.
- 16 Jon Oliver. (19 September 2016). *TrendLabs Security Intelligence Blog*. "A Show of (Brute) Force: Crysis Ransomware Found Targeting Australian and New Zealand Businesses." Last accessed on 1 August 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/crysis-targeting-businesses-in-australia-new-zealand-via-brute-forced-rdps/>.
- 17 Trend Micro. (18 April 2019). *Trend Micro Security News*. "NamPoHyu aka MegaLocker Virus Ransomware Found Remotely Encrypting Samba Servers." Last accessed on 2 August 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/nampohyu-aka-megalocker-virus-ransomware-found-remotely-encrypting-samba-servers>.

- 18 Trend Micro. (27 May 2019). *Trend Micro Security News*. "GandCrab Ransomware Found Targeting MySQL Databases." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/gandcrab-ransomware-found-targeting-mysql-databases/>.
- 19 Augusto Remillano II and Robert Malagad. (7 May 2019). *TrendLabs Security Intelligence Blog*. "CVE-2019-3396 Redux: Confluence Vulnerability Exploited to Deliver Cryptocurrency Miner With Rootkit." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/cve-2019-3396-redux-confluence-vulnerability-exploited-to-deliver-cryptocurrency-miner-with-rootkit/>.
- 20 Lawrence Abrams. (11 September 2018). *BleepingComputer*. "Mongo Lock Attack Ransoming Deleted MongoDB Databases." Last accessed on 2 August 2019 at <https://www.bleepingcomputer.com/news/security/mongo-lock-attack-ransoming-deleted-mongodb-databases/>.
- 21 Trend Micro. (8 January 2019). *Trend Micro Security News*. "Ransomware MongoLock Immediately Deletes Files, Formats Backup Drives." Last accessed on 2 August 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-mongolock-immediately-deletes-files-formats-backup-drives/>.
- 22 Buddy Tancio, Ryan Maglaque, Cenen Enalbes, and Jay Yaneza. (14 March 2019). *Trend Micro Security News*. "Examining Ryuk Ransomware Through the Lens of Managed Detection and Response." Last accessed on 2 August 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/examining-ryuk-ransomware-through-the-lens-of-managed-detection-and-response/>.
- 23 Trend Micro. (21 May 2019). *Trend Micro Security News*. "Ryuk Ransomware Shows Diversity in Targets, Consistency in Higher Payouts." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ryuk-ransomware-shows-diversity-in-targets-consistency-in-higher-payouts/>.
- 24 Alexander Hanel. (10 January 2019). *CrowdStrike Blog*. "Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware." Last accessed on 24 July 2019 at <https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/>.
- 25 Trend Micro. (20 March 2019). *Trend Micro Security News*. "What You Need to Know About the LockerGoga Ransomware." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware/>.
- 26 Kevin Beaumont. (22 March 2019). *Double Pulsar*. "How Lockergoga took down Hydro — ransomware used in targeted attacks aimed at big business." Last accessed on 2 August 2019 at <https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880>.
- 27 Erika Mendoza, Jay Yaneza, Gilbert Sison, Anjali Patil, Julie Cabuhat, and Joelson Soares. (29 March 2019). *TrendLabs Security Intelligence Blog*. "Emotet-Distributed Ransomware Loader for Nozelesn Found via Managed Detection and Response." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/emotet-distributed-ransomware-loader-for-nozelesn-found-via-managed-detection-and-response/>.
- 28 Lawrence Abrams. (26 April 2019). *BleepingComputer*. "A Closer Look at the RobbinHood Ransomware." Last accessed on 24 July 2019 at <https://www.bleepingcomputer.com/news/security/a-closer-look-at-the-robbinhood-ransomware/>.
- 29 Gilbert Sison and Ryan Maglaque. (15 April 2019). *TrendLabs Security Intelligence Blog*. "Account With Admin Privileges Abused to Install BitPaymer Ransomware via PsExec." Last accessed on 2 August 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/account-with-admin-privileges-abused-to-install-bitpaymer-ransomware-via-psexec/>.
- 30 NJCCIC. (29 August 2017). *NJCCIC*. "Bit Paymer." Last accessed on 24 July 2019 at <https://www.cyber.nj.gov/threat-profiles/ransomware-variants/bitpaymer/>.
- 31 Arnold Osipov. (18 July 2019). *Morphisec*. "Bitpaymer Ransomware Leveraging New Custom Packer Framework Against Targets Across the U.S." Last accessed on 24 July 2019 at <http://blog.morphisec.com/bitpaymer-ransomware-with-new-custom-packer-framework>.
- 32 Threat Team. (13 August 2018). *BluVector*. "BitPaymer Ransomware Freezes the PGA and an Alaskan Town." Last accessed on 24 July 2019 at <https://www.bluvector.io/threat-report-bitpaymer-ransomware-freezes-the-pga-and-an-alaskan-town/>.
- 33 Trend Micro. (7 May 2019). *Trend Micro Security News*. "MegaCortex Ransomware Spotted Attacking Enterprise Networks." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/megacortex-ransomware-spotted-attacking-enterprise-networks/>.
- 34 Trend Micro. (12 May 2017). *TrendLabs Security Intelligence Blog*. "Massive WannaCry/Wcry Ransomware Attack Hits Various Countries." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/massive-wannacrywcry-ransomware-attack-hits-various-countries/>.
- 35 Microsoft. (3 August 2019). *Windows Help*. "Windows 7 support will end on January 14, 2020." Last accessed on 1 August 2019 at <https://support.microsoft.com/en-us/help/4057281/windows-7-support-will-end-on-january-14-2020>.
- 36 Lawrence Abrams. (24 June 2019). *BleepingComputer*. "Sodinokibi Ransomware Now Pushed by Exploit Kits and Malvertising." Last accessed on 24 July 2019 at <https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-now-pushed-by-exploit-kits-and-malvertising/>.
- 37 Brian Krebs. (15 July 2019). *Krebs on Security*. "Is 'REvil' the New GandCrab Ransomware?" Last accessed on 24 July 2019 at <https://krebsonsecurity.com/2019/07/is-revil-the-new-gandcrab-ransomware/>.
- 38 Trend Micro Research. (2018). *Trend Micro*. "Mapping the Future: Dealing With Pervasive and Persistent Threats." Last accessed on 24 July 2019 at <https://documents.trendmicro.com/assets/rpt/rpt-mapping-the-future.pdf>.
- 39 Trend Micro. (29 July 2019). *Trend Micro Security News*. "Risks Under the Radar: Understanding Fileless Threats." Last accessed on 2 August 2019 at <https://www.trendmicro.com/vinfo/us/security/news/security-technology/risks-under-the-radar-understanding-fileless-threats/>.

- 40 Hiroyuki Kakara and Kazuki Fujisawa. (17 April 2019). *TrendLabs Security Intelligence Blog*. "Potential Targeted Attack Uses AutoHotkey and Malicious Script Embedded in Excel File to Avoid Detection." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/potential-targeted-attack-uses-autohotkey-and-malicious-script-embedded-in-excel-file-to-avoid-detection/>.
- 41 Augusto Remillano II and Arvin Macaraeg. (12 April 2019). *TrendLabs Security Intelligence Blog*. "Miner Malware Spreads Beyond China, Uses Multiple Propagation Methods Including EternalBlue, Powershell Abuse." Last accessed on 2 August 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/miner-malware-spreads-beyond-china-uses-multiple-propagation-methods-including-eternalblue-powershell-abuse/>.
- 42 Erika Mendoza, Jay Yaneza, Gilbert Sison, Anjali Patil, Julie Cabuhat, and Joelson Soares. (29 March 2019). *TrendLabs Security Intelligence Blog*. "Emotet-Distributed Ransomware Loader for Nozelesn Found via Managed Detection and Response." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/emotet-distributed-ransomware-loader-for-nozelesn-found-via-managed-detection-and-response/>.
- 43 Henry Alarcon, Jr. and Raphael Centeno. (4 March 2019). *TrendLabs Security Intelligence Blog*. "Fileless Banking Trojan Targeting Brazilian Banks Downloads Possible Botnet Capability, Info Stealers." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/fileless-banking-trojan-targeting-brazilian-banks-downloads-possible-botnet-capability-info-stealers/>.
- 44 Augusto Remillano II and Kiyoshi Obuchi. (12 March 2019). *TrendLabs Security Intelligence Blog*. "From Fileless Techniques to Using Steganography: Examining Powload's Evolution." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/from-fileless-techniques-to-using-steganography-examining-powloads-evolution/>.
- 45 Miguel Ang. (20 May 2019). *TrendLabs Security Intelligence Blog*. "Trickbot Watch: Arrival via Redirection URL in Spam." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/trickbot-watch-arrival-via-redirection-url-in-spam/>.
- 46 Hiroyuki Kakara and Kazuki Fujisawa. (17 April 2019). *TrendLabs Security Intelligence Blog*. "Potential Targeted Attack Uses AutoHotkey and Malicious Script Embedded in Excel File to Avoid Detection." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/potential-targeted-attack-uses-autohotkey-and-malicious-script-embedded-in-excel-file-to-avoid-detection/>.
- 47 Janus Agcaoil. (5 June 2019). *TrendLabs Security Intelligence Blog*. "Monero-Mining Malware PCASTLE Zeroes Back In on China, Now Uses Multilayered Fileless Arrival Techniques." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-malware-pcastle-zeroes-back-in-on-china-now-uses-multilayered-fileless-arrival-techniques/>.
- 48 Johnlery Triunfante. (3 June 2019). *TrendLabs Security Intelligence Blog*. "BlackSquid Slithers Into Servers and Drives With 8 Notorious Exploits to Drop XMRig Miner." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/blacksquid-slithers-into-servers-and-drives-with-8-notorious-exploits-to-drop-xmrig-miner/>.
- 49 Augusto Remillano II and Jakub Urbanec. (23 May 2019). *TrendLabs Security Intelligence Blog*. "New Mirai Variant Uses Multiple Exploits to Target Routers and Other Devices." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/new-mirai-variant-uses-multiple-exploits-to-target-routers-and-other-devices/>.
- 50 Trend Micro. (25 March 2019). *Trend Micro Security News*. "Cybersecurity Skills Shortage a Problem for Nearly 50 Percent of Organizations." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cybersecurity-skills-shortage-a-problem-for-nearly-50-percent-of-organizations/>.
- 51 Trend Micro. (5 March 2019). *Trend Micro Security News*. "2018 Mobile Threat Landscape." Last accessed on 2 August 2019 at <https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/2018-mobile-threat-landscape>.
- 52 Kevin Sun. (17 January 2019). *TrendLabs Security Intelligence Blog*. "Google Play Apps Drop Anubis Banking Malware, Use Motion-based Evasion Tactics." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/google-play-apps-drop-anubis-banking-malware-use-motion-based-evasion-tactics/>.
- 53 Tony Bao. (8 July 2019). *TrendLabs Security Intelligence Blog*. "Anubis Android Malware Returns with Over 17,000 Samples." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/anubis-android-malware-returns-with-over-17000-samples/>.
- 54 Mobile Threat Response Team. (18 January 2017). *TrendLabs Security Intelligence Blog*. "In Review: 2016's Mobile Threat Landscape Brings Diversity, Scale, and Scope." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/2016-mobile-threat-landscape/>.
- 55 Joseph C. Chen. (27 June 2019). *TrendLabs Security Intelligence Blog*. "ShadowGate Returns to Worldwide Operations With Evolved Greenflash Sundown Exploit Kit." Last accessed on 24 July 2019 <https://blog.trendmicro.com/trendlabs-security-intelligence/shadowgate-returns-to-worldwide-operations-with-evolved-greenflash-sundown-exploit-kit/>.
- 56 Trend Micro. (2016). *Trend Micro*. "Setting the Stage: Landscape Shifts Dictate Future Threat Response Strategies." Last accessed on 1 August 2019 at <https://documents.trendmicro.com/assets/rpt/rpt-setting-the-stage.pdf>.
- 57 Lion Gu, Vladimir Kropotov, and Fyodor Yarochkin. (13 June 2017). *Trend Micro Security News*. "Fake News and Cyber Propaganda: The Use and Abuse of Social Media." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media/>.
- 58 Cedric Pernet, Daniel Lunghi, Jaromir Horejsi, and Joseph C. Chen. (7 March 2019). *TrendLabs Security Intelligence Blog*. "New SLUB Backdoor Uses GitHub, Communicates via Slack." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/new-slub-backdoor-uses-github-communicates-via-slack/>.
- 59 Jindrich Karasek and Cedric Pernet. (28 February 2019). *TrendLabs Security Intelligence Blog*. "How a Hacking Group is Stealing Popular Instagram Profiles." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/how-a-hacking-group-is-stealing-popular-instagram-profiles/>.

- 60 Hara Hiroaki, Lilang Wu, and Lorin Wu. (2 April 2019). *TrendLabs Security Intelligence Blog*. “New Version of XLoader That Disguises as Android Apps and an iOS Profile Holds New Links to FakeSpy.” Last accessed on 24 July 2019 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/>.
- 61 Trend Micro. (28 February 2019). *TrendLabs Security Intelligence Blog*. “Shifting Strategies: Using Social Media, SEO in Tech Support Scams.” Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/shifting-strategies-using-social-media-seo-in-tech-support-scams/>.
- 62 Vladimir Kropotov and Fyodor Yarochkin. (30 July 2019). *Trend Micro Security News*. “Hunting Threats on Twitter: How Social Media Can Be Used to Gather Actionable Threat Intelligence.” Last accessed on 2 August 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hunting-threats-on-twitter/>.
- 63 Ecular Xu and Grey Guo. (18 June 2019). *TrendLabs Security Intelligence Blog*. “Mobile Cyberespionage Campaign ‘Bouncing Golf’ Affects Middle East.” Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/mobile-cyberespionage-campaign-bouncing-golf-affects-middle-east/>.
- 64 Hara Hiroaki and Loseway Lu. (12 June 2019). *TrendLabs Security Intelligence Blog*. “Shifting Tactics: Breaking Down TA505 Group’s Use of HTML, RATs and Other Techniques in Latest Campaigns.” Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/shifting-tactics-breaking-down-ta505-groups-use-of-html-rats-and-other-techniques-in-latest-campaigns/>.
- 65 Hara Hiroaki and Loseway Lu. (4 July 2019). *TrendLabs Security Intelligence Blog*. “Latest Spam Campaigns from TA505 Now Using New Malware Tools Gelup and FlowerPippi.” Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/latest-spam-campaigns-from-ta505-now-using-new-malware-tools-gelup-and-flowerpippi/>.
- 66 Jaromir Horejsi. (12 March 2018). *TrendLabs Security Intelligence Blog*. “Campaign Possibly Connected to ‘MuddyWater’ Surfaces in the Middle East and Central Asia.” Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/campaign-possibly-connected-muddywater-surfaces-middle-east-central-asia/>.
- 67 Jaromir Horejsi and Daniel Lunghi. (30 November 2018). *TrendLabs Security Intelligence Blog*. “New PowerShell-based Backdoor Found in Turkey, Strikingly Similar to MuddyWater Tools.” Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/new-powershell-based-backdoor-found-in-turkey-strikingly-similar-to-muddywater-tools/>.
- 68 Daniel Lunghi and Jaromir Horejsi. (10 June 2019). *TrendLabs Security Intelligence Blog*. “MuddyWater Resurfaces, Uses Multi-Stage Backdoor POWERSTATS V3 and New Post-Exploitation Tools.” Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/muddywater-resurfaces-uses-multi-stage-backdoor-powerstats-v3-and-new-post-exploitation-tools/>.
- 69 CoinDesk. (n.d.). *CoinDesk*. “Bitcoin Price Index — Real-time Bitcoin Price Charts.” Last accessed on 24 July 2019 at <https://www.coindesk.com/price/bitcoin/>.
- 70 CoinDesk. (n.d.). *CoinDesk*. “Monero Price Index — Real-time Monero (XMR) Price Charts.” Last accessed on 24 July 2019 at <https://www.coindesk.com/price/monero/>.
- 71 Sergio Pastrana and Guillermo Suarez-Tangil. (3 January 2019). *ArXiv*. “A First Look at the Crypto-Mining Malware Ecosystem: A Decade of Unrestricted Wealth.” Last accessed on 2 August 2019 at <https://arxiv.org/pdf/1901.00846.pdf>.
- 72 Tom Wilson. (15 May 2019). *Reuters*. “Explainer: ‘Privacy coin’ Monero offers near total anonymity.” Last accessed on 2 August 2019 at <https://www.reuters.com/article/us-crypto-currencies-altcoins-explainer/explainer-privacy-coin-monero-offers-near-total-anonymity-idUSKCN1SL0F0>.
- 73 Danny Palmer. (20 February 2018). *ZDNet*. “Cyber attackers are cashing in on cryptocurrency mining - but here’s why they’re avoiding bitcoin.” Last accessed on 2 August 2019 at <https://www.zdnet.com/article/cyber-attackers-are-cashing-in-on-cryptocurrency-mining-but-heres-why-theyre-avoiding-bitcoin/>.
- 74 Augusto Remillano II and Jakub Urbanec. (8 February 2019). *TrendLabs Security Intelligence Blog*. “Linux Coin Miner Copied Scripts From KORKERDS, Removes All Other Malware and Miners.” Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/linux-coin-miner-copied-scripts-from-korkerds-removes-all-other-malware-and-miners/>.
- 75 Don Ovid Ladores, Michael Jhon Ofiaza, and Gilbert Sison. (20 February 2019). *TrendLabs Security Intelligence Blog*. “Monero Miner-Malware Uses RADMIN, MIMIKATZ to Infect, Propagate via Vulnerability.” Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/monero-miner-malware-uses-radmin-mimikatz-to-infect-propagate-via-vulnerability/>.
- 76 Augusto Remillano II and Arvin Macaraeg. (12 April 2019). *TrendLabs Security Intelligence Blog*. “Miner Malware Spreads Beyond China, Uses Multiple Propagation Methods Including EternalBlue, Powershell Abuse.” Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/miner-malware-spreads-beyond-china-uses-multiple-propagation-methods-including-eternalblue-powershell-abuse/>.
- 77 Janus Agcaoili. (5 June 2019). *TrendLabs Security Intelligence Blog*. “Monero-Mining Malware PCASTLE Zeroes Back In on China, Now Uses Multilayered Fileless Arrival Techniques.” Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-malware-pcastle-zeroes-back-in-on-china-now-uses-multilayered-fileless-arrival-techniques/>.
- 78 Augusto II Remillano and Robert Malagad. (7 May 2019). *TrendLabs Security Intelligence Blog*. “CVE-2019-3396 Redux: Confluence Vulnerability Exploited to Deliver Cryptocurrency Miner With Rootkit.” Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/cve-2019-3396-redux-confluence-vulnerability-exploited-to-deliver-cryptocurrency-miner-with-rootkit/>.
- 79 Jindrich Karasek. (20 June 2019). *TrendLabs Security Intelligence Blog*. “Cryptocurrency-Mining Botnet Malware Arrives Through ADB and Spreads Through SSH.” Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-mining-botnet-arrives-through-adb-and-spreads-through-ssh/>.

- 80 Augusto Remillano II. (13 June 2019). *TrendLabs Security Intelligence Blog*. "Outlaw Hacking Group's Botnet Observed Spreading Miner, Perl-Based Backdoor." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/outlaw-hacking-groups-botnet-observed-spreading-miner-perl-based-backdoor/>.
- 81 Augusto Remillano II and Mark Vicente. (28 June 2019). *TrendLabs Security Intelligence Blog*. "Golang-based Spreader Used in a Cryptocurrency-Mining Malware Campaign." Last accessed on 24 July 2019 <https://blog.trendmicro.com/trendlabs-security-intelligence/golang-based-spreader-used-in-a-cryptocurrency-mining-malware-campaign/>.
- 82 Trend Micro Research. (2018). *Trend Micro*. "Mapping the Future: Dealing With Pervasive and Persistent Threats." Last accessed on 24 July 2019 at <https://documents.trendmicro.com/assets/rpt/rpt-mapping-the-future.pdf>.
- 83 Chris Doman and Tom Hegel. (14 March 2019). *AT&T Cybersecurity*. "Making it Rain - Cryptocurrency Mining Attacks in the Cloud." Last accessed on 24 July 2019 at <https://www.alienvault.com/blogs/labs-research/making-it-rain-cryptocurrency-mining-attacks-in-the-cloud/>.
- 84 Alfredo Oliveira. (1 March 2019). *TrendLabs Security Intelligence Blog*. "Exposed Docker Control API and Community Image Abused to Deliver Cryptocurrency-Mining Malware." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/exposed-docker-control-api-and-community-image-abused-to-deliver-cryptocurrency-mining-malware/>.
- 85 Alfredo Oliveira. (30 May 2019). *TrendLabs Security Intelligence Blog*. "Infected Cryptocurrency-Mining Containers Target Docker Hosts With Exposed APIs, Use Shodan to Find Additional Victims." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/infected-cryptocurrency-mining-containers-target-docker-hosts-with-exposed-apis-use-shodan-to-find-additional-victims/>.
- 86 Trend Micro. (10 May 2019). *Trend Micro Security News*. "Jenkins Vulnerability Exploited to Drop Kerberods Malware and Launch Monero Miner." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/jenkins-vulnerability-exploited-to-drop-kerberods-malware-and-launch-monero-miner/>.
- 87 Check Point Research. (15 February 2018). *Check Point Research*. "Jenkins Miner: One of the Biggest Mining Operations Ever Discovered." Last accessed on 24 July 2019 at <https://research.checkpoint.com/jenkins-miner-one-biggest-mining-operations-ever-discovered/>.
- 88 Jon Porter. (28 February 2019). *The Verge*. "Popular 'cryptojacking' service Coinhive will shut down next week." Last accessed on 24 July 2019 at <https://www.theverge.com/2019/2/28/18244636/coinhive-cryptojacking-cryptocurrency-mining-shut-down-monero-date/>.
- 89 Radiflow. (8 February 2018). *Radiflow*. "Radiflow Reveals First Documented Cryptocurrency Malware Attack on a SCADA Network." Last accessed on 24 July 2019 at <https://radiflow.com/news/radiflow-reveals-first-documented-cryptocurrency-malware-attack-on-a-scada-network/>.
- 90 Dave Shackelford. (30 April 2019). *SANS Institute*. "SANS 2019 Cloud Security Survey." Last accessed on 24 July 2019 at <https://www.sans.org/reading-room/whitepapers/analyst/2019-cloud-security-survey-38940/>.
- 91 Trend Micro. (2 April 2019). *Trend Micro Security News*. "More than 13,000 Misconfigured iSCSI Storage Clusters Accessible via the Public Internet." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/more-than-13-000-misconfigured-iscsi-storage-clusters-accessible-via-the-public-internet/>.
- 92 Trend Micro. (14 May 2019). *Trend Micro Security News*. "Unsecured Server Leaks PII of Almost 90% of Panama Residents." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/online-privacy/unsecured-server-leaks-pii-of-almost-90-of-panama-residents/>.
- 93 Trend Micro. (n.d.). *Trend Micro Security News*. "DevOps." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/definition/devops/>.
- 94 Trend Micro. (n.d.). *Trend Micro Security News*. "EU General Data Protection Regulation (GDPR)." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/definition/eu-general-data-protection-regulation-gdpr/>.
- 95 Asaf Cidon. (2 May 2019). *Barracuda Journey Notes*. "Threat Spotlight: Account Takeover." Last accessed on 24 July 2019 at <https://blog.barracuda.com/2019/05/02/threat-spotlight-account-takeover/>.
- 96 Abhishek Agrawal, David Fantham, Debraj Ghosh, Diana Kelley, Elia Florio, Eric Avena, Eric Douglas, et al. (2019). *Microsoft Corporation*. "Microsoft Security Intelligence Report, Volume 24, January – December 2018." Last accessed on 24 July 2019 at <https://clouddamcdnprodep.azureedge.net/gdc/gdc09FrGq/original>.
- 97 Lorin Wu. (30 January 2019). *TrendLabs 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 24 July 2019 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/>.
- 98 Joseph C. Chen. (28 March 2019). *TrendLabs Security Intelligence Blog*. "Desktop, Mobile Phishing Campaign Targets South Korean Websites, Steals Credentials Via Watering Hole." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/desktop-mobile-phishing-campaign-targets-south-korean-websites-steals-credentials-via-watering-hole/>.
- 99 Samuel P. Wang. (4 April 2019). *TrendLabs Security Intelligence Blog*. "Phishing Attack Uses Browser Extension Tool SingleFile to Obfuscate Malicious Log-in Pages." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/phishing-attack-uses-browser-extension-tool-singlefile-to-obfuscate-malicious-log-in-pages/>.
- 100 Trend Micro. (29 March 2019). *Trend Micro Security News*. "Health Information of 350,000 Oregon DHS Clients Exposed After Phishing Attack." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/health-information-of-350-000-oregon-dhs-clients-exposed-after-phishing-attack/>.
- 101 Catalin Cimpanu. (11 April 2019). *ZDNet*. "Emotet hijacks email conversation threads to insert links to malware." Last accessed on 24 July 2019 at <https://www.zdnet.com/article/emotet-hijacks-email-conversation-threads-to-insert-links-to-malware/>.

- 102 Erika Mendoza, Anjali Patil, and Jay Yaneza. (9 October 2018). *TrendLabs Security Intelligence Blog*. "Phishing Campaign uses Hijacked Emails to Deliver URSNIF by Replying to Ongoing Threads." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/phishing-campaign-uses-hijacked-emails-to-deliver-ursnif-by-replying-to-ongoing-threads/>.
- 103 Miguel Ang and Donald Castillo. (29 October 2018). *TrendLabs Security Intelligence Blog*. "Same Old yet Brand-new: New File Types Emerge in Malware Spam Attachments." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/same-old-yet-brand-new-new-file-types-emerge-in-malware-spam-attachments/>.
- 104 Proofpoint Information Protection Research Team. (14 March 2019). *Proofpoint*. "Threat actors leverage credential dumps, phishing, and legacy email protocols to bypass MFA and breach cloud accounts worldwide." Last accessed on 24 July 2019 at <https://www.proofpoint.com/us/threat-insight/post/threat-actors-leverage-credential-dumps-phishing-and-legacy-email-protocols/>.
- 105 APWG. (15 May 2019). *APWG*. "Phishing Activity Trends Report, 1st Quarter 2019." Last accessed on 24 July 2019 at [https://docs.apwg.org/reports/apwg\\_trends\\_report\\_q1\\_2019.pdf](https://docs.apwg.org/reports/apwg_trends_report_q1_2019.pdf).
- 106 Trend Micro. (25 April 2019). *Trend Micro Security News*. "IC3: BEC Cost Organizations US\$1.2 Billion in 2018." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ic3-bec-cost-organizations-us-1-2-billion-in-2018/>.
- 107 Katia Moskvitch. (20 March 2019). *Wired UK*. "Cyber criminals are targeting HR departments to steal your salary." Last accessed on 1 August 2019 at <https://www.wired.co.uk/article/hr-email-scam-phishing-impersonating-employees>.
- 108 Sachin Dave. (10 January 2019). *The Economic Times*. "How Chinese hackers pulled off the Italian con job, a Rs 130-crore heist." Last accessed on 1 August 2019 at <https://economictimes.indiatimes.com/tech/internet/how-chinese-hackers-pulled-off-the-italian-con-job-a-rs-130-crore-heist/articleshow/67464588.cms>.
- 109 Nick Wooten. (8 January 2019). *Shreveport Times*. "Update: Some of \$1M scammed from Caddo schools has been found." Last accessed on 1 August 2019 at <https://www.shreveporttimes.com/story/news/2019/01/08/scammer-get-nearly-1-million-meant-caddo-charter-school/2514083002/>.
- 110 Trend Micro. (10 April 2019). *Trend Micro Security News*. "London Blue Group Using Evolving BEC Techniques in Attacks." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/london-blue-group-using-evolving-bec-techniques-in-their-attacks/>.
- 111 Trend Micro. (16 April 2019). *Trend Micro Security News*. "New Business Email Compromise Scheme Reroutes Paycheck by Direct Deposit." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/new-business-email-compromise-scheme-reroutes-paycheck-by-direct-deposit/>.
- 112 Trend Micro Research. (2018). *Trend Micro*. "Mapping the Future: Dealing With Pervasive and Persistent Threats." Last accessed on 24 July 2019 at <https://documents.trendmicro.com/assets/rpt/rpt-mapping-the-future.pdf>.
- 113 Trend Micro. (2 May 2019). *Trend Micro Security News*. "BEC Scammers Steal US\$1.75 Million From an Ohio Church." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/bec-scammers-steal-us-1-75-million-from-an-ohio-church/>.
- 114 FBI National Press Office. (22 April 2019). *FBI*. "FBI Releases the Internet Crime Complaint Center 2018 Internet Crime Report." Last accessed on 13 August 2019 at <https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2018-internet-crime-report>.
- 115 Federal Bureau of Investigation Internet Crime Complaint Center. (n.d.). *Federal Bureau of Investigation Internet Crime Complaint Center (IC3)*. "2018 Internet Crime Report." Last accessed on 24 July 2019 at [https://pdf.ic3.gov/2018\\_IC3Report.pdf](https://pdf.ic3.gov/2018_IC3Report.pdf).
- 116 Trend Micro Research. (2018). *Trend Micro*. "Mapping the Future: Dealing With Pervasive and Persistent Threats." Last accessed on 24 July 2019 at <https://documents.trendmicro.com/assets/rpt/rpt-mapping-the-future.pdf>.
- 117 Trend Micro. (24 April 2019). *Trend Micro Security News*. "New Sextortion Scheme Demands Payment in Bitcoin Cash." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/new-sextortion-scheme-demands-payment-in-bitcoin-cash/>.
- 118 Vit Sembera. (5 January 2018). *TrendLabs Security Intelligence Blog*. "When Speculation Is Risky: Understanding Meltdown and Spectre." Last accessed on 1 August 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/speculation-risky-understanding-meltdown-spectre/>.
- 119 Graz University of Technology. (2018). *Graz University of Technology*. "Meltdown and Spectre." Last accessed on 1 August 2019 at <https://meltdownattack.com/>.
- 120 Trend Micro. (14 February 2019). *Trend Micro Security News*. "Proof of Concept Shows How Malware Can Hide From AV Solutions via Intel's SGX Enclaves." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/proof-of-concept-shows-how-malware-can-hide-from-av-solutions-via-intel-s-sgx-enclaves/>.
- 121 Trend Micro. (15 May 2019). *Trend Micro Security News*. "Side-Channel Attacks RIDL, Fallout, and ZombieLoad Affect Millions of Vulnerable Intel Processors." Last accessed on 1 August 2019 at <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/side-channel-attacks-ridl-fallout-and-zombieload-affects-millions-of-vulnerable-intel-processors/>.
- 122 Trend Micro. (29 May 2019). *Trend Micro Security News*. "Nearly 1 Million Systems Affected By 'Wormable' BlueKeep Vulnerability (CVE-2019-0708)." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/nearly-1-million-systems-affected-by-wormable-bluekeep-vulnerability-cve-2019-0708/>.
- 123 Simon Pope. (14 May 2019). *Microsoft Security Response Center*. "Prevent a worm by updating Remote Desktop Services (CVE-2019-0708)." Last accessed on 24 July 2019 at <https://msrc-blog.microsoft.com/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/>.

- 124 Trend Micro. (31 May 2019). *Trend Micro Security News*. "SandboxEscaper Releases Exploit for Zero-Day Vulnerability in Task Scheduler." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/sandboxescaper-releases-exploit-for-zero-day-vulnerability-in-task-scheduler/>.
- 125 Trend Micro. (28 February 2019). *Trend Micro Security News*. "CVE-2019-5736: RunC Container Escape Vulnerability Provides Root Access to the Target Machine." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/cve-2019-5736-runc-container-escape-vulnerability-provides-root-access-to-the-target-machine/>.
- 126 Trend Micro. (4 April 2019). *Trend Micro Security News*. "Previously Patched, Still Potentially Critical: Kubernetes' Path Traversal Vulnerability." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/previously-patched-still-potentially-critical-kubernetes-path-traversal-vulnerability/>.
- 127 Ariel Zelivansky. (28 March 2019). *Twistlock*. "Disclosing a directory traversal vulnerability in Kubernetes copy – CVE-2019-1002101." Last accessed on 24 July 2019 at <https://www.twistlock.com/labs-blog/disclosing-directory-traversal-vulnerability-kubernetes-copy-cve-2019-1002101/>.
- 128 Trend Micro. (12 March 2019). *Trend Micro Security News*. "StackStorm DevOps Software Vulnerability CVE-2019-9580 Allows Remote Code Execution." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/stackstorm-devops-software-vulnerability-cve-2019-9580-allows-remote-code-execution/>.
- 129 Trend Micro. (n.d.). *Trend Micro Security News*. "Network and Information Security (NIS) Directive." Last accessed on 1 August 2019 at [https://www.trendmicro.com/vinfo/us/security/definition/network-and-information-security-\(nis\)-directive/](https://www.trendmicro.com/vinfo/us/security/definition/network-and-information-security-(nis)-directive/).
- 130 Keumars Affi-Sabet. (4 April 2019). *IT Pro*. "IT chiefs are compromising security for smoother business operations." Last accessed on 24 July 2019 at <https://www.itpro.co.uk/security/33384/it-chiefs-are-compromising-security-for-smoother-business-operations>.
- 131 Trend Micro. (25 June 2019). *Trend Micro Security News*. "Security 101: Virtual Patching." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/security-technology/security-101-virtual-patching>.
- 132 John Simpson. (29 May 2019). *TrendLabs Security Intelligence Blog*. "CVE-2019-0725: An Analysis of Its Exploitability." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/cve-2019-0725-an-analysis-of-its-exploitability/>.
- 133 John Simpson. (24 May 2019). *TrendLabs Security Intelligence Blog*. "CVE-2019-11815: A Cautionary Tale About CVSS Scores." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/cve-2019-11815-a-cautionary-tale-about-cvss-scores/>.
- 134 Gartner. (7 November 2018). *Gartner*. "Gartner Identifies Top 10 Strategic IoT Technologies and Trends." Last accessed on 24 July 2019 at <https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends/>.
- 135 Trend Micro Research. (2018). *Trend Micro*. "Mapping the Future: Dealing With Pervasive and Persistent Threats." Last accessed on 24 July 2019 at <https://documents.trendmicro.com/assets/rpt/rpt-mapping-the-future.pdf>.
- 136 Mark Vicente, Byron Galera, and Augusto Remillano. (3 April 2019). *TrendLabs Security Intelligence Blog*. "Bashlite IoT Malware Updated with Mining and Backdoor Commands, Targets WeMo Devices." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/bashlite-iot-malware-updated-with-mining-and-backdoor-commands-targets-wemo-devices/>.
- 137 Trend Micro. (4 April 2019). *Trend Micro Security News*. "Mirai Variant Spotted Using Multiple Exploits, Targets Various Routers." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/mirai-variant-spotted-using-multiple-exploits-targets-various-routers/>.
- 138 Augusto Remillano II and Jakub Urbanec. (23 May 2019). *TrendLabs Security Intelligence Blog*. "New Mirai Variant Uses Multiple Exploits to Target Routers and Other Devices." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/new-mirai-variant-uses-multiple-exploits-to-target-routers-and-other-devices/>.
- 139 Ruchna Nigam. (20 July 2018). *Unit 42*. "Unit 42 Finds New Mirai and Gafgyt IoT/Linux Botnet Campaigns." Last accessed on 1 August 2019 at <https://unit42.paloaltonetworks.com/unit42-finds-new-mirai-gafgyt-iotlinux-botnet-campaigns/>.
- 140 Augusto Remillano II. (25 January 2019). *TrendLabs Security Intelligence Blog*. "ThinkPHP Vulnerability Abused by Botnets Hakai and Yowai." Last accessed on 24 July 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/thinkphp-vulnerability-abused-by-botnets-hakai-and-yowai/>.
- 141 Augusto Remillano II. (26 April 2019). *TrendLabs Security Intelligence Blog*. "AESDDoS Botnet Malware Exploits CVE-2019-3396 to Perform Remote Code Execution, DDoS Attacks, and Cryptocurrency Mining." Last accessed on 1 August 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/aesddos-botnet-malware-exploits-cve-2019-3396-to-perform-remote-code-execution-ddos-attacks-and-cryptocurrency-mining/>.
- 142 Trend Micro. (31 May 2019). *Trend Micro Security News*. "HiddenWasp Malware Targets Linux Systems, Borrows Code from Mirai, Winnti." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/hiddenwasp-malware-targets-linux-systems-borrows-code-from-mirai-winnti/>.
- 143 Trend Micro. (27 June 2019). *Trend Micro Security News*. "Silex Malware Bricks IoT Devices with Weak Passwords." Last accessed on 1 August 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/silex-malware-bricks-iot-devices-with-weak-passwords/>.
- 144 Trend Micro Research. (5 March 2019). *Trend Micro Security News*. "Cybersecurity Risks in Complex IoT Environments: Threats to Smart Homes, Buildings and Other Structures." Last accessed on 1 August 2019 at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/threats-and-risks-to-complex-iot-environments/>.

- 145 Trend Micro. (2 May 2019). *Trend Micro Security News*. "IoT Devices in the Workplace: Security Risks and Threats to BYOD Environments." Last accessed on 1 August 2019 at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-devices-in-the-workplace-security-risks-and-threats-to-byod-environments/>.
- 146 Trend Micro. (n.d.). *Trend Micro Security News*. "Industrial Internet of Things (IIoT)." Last accessed on 1 August 2019 at <https://www.trendmicro.com/vinfo/us/security/definition/industrial-internet-of-things-iiot/>.
- 147 Ryan Flores, Stephen Hilt, and Akira Urano. (6 March 2019). *Trend Micro Security News*. "Cultivating Security in the Food Production Industry: Nipping IoT Risks and Threats in the Bud." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/cultivating-security-in-the-food-production-industry/>.
- 148 Trend Micro Research. (3 April 2019). *Trend Micro Security News*. "Security in the Era of Industry 4.0: Dealing With Threats to Smart Manufacturing Environments." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/security-in-the-era-of-industry-4-dealing-with-threats-to-smart-manufacturing-environments>.
- 149 Trend Micro. (4 April 2019). *Trend Micro Security News*. "Securing Enterprises for 5G Connectivity." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/securing-enterprises-for-5g-connectivity>.
- 150 Trend Micro. (5 April 2018). *Trend Micro Security News*. "Exposed Devices and Supply Chain Attacks: Overlooked Risks in Healthcare Networks." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/exposed-medical-devices-and-supply-chain-attacks-in-connected-hospitals>.
- 151 Trend Micro. (27 June 2019). *Trend Micro Security News*. "The IIoT Attack Surface: Threats and Security Solutions." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/-the-iiot-attack-surface-threats-and-security-solutions/>.
- 152 Louis Columbus. (6 June 2018). *Forbes*. "10 Charts That Will Challenge Your Perspective Of IoT's Growth." Last accessed on 24 July 2019 at <https://www.forbes.com/sites/louiscolombus/2018/06/06/10-charts-that-will-challenge-your-perspective-of-iots-growth/>.
- 153 Ponemon Institute. (March 2019). *Tenable*. "Cybersecurity in Operational Technology: 7 Insights You Need to Know." Last accessed on 24 July 2019 at [https://static.tenable.com/marketing/research-reports/PonemonReport-Cybersecurity\\_in\\_Operational\\_Technology.pdf](https://static.tenable.com/marketing/research-reports/PonemonReport-Cybersecurity_in_Operational_Technology.pdf).
- 154 Trend Micro. (22 December 2017). *Trend Micro Security News*. "TRITON Wielding Its Trident – New Malware Tampering with Industrial Safety Systems." Last accessed on 1 August 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/triton-wielding-its-trident-new-malware-tampering-with-industrial-safety-systems/>.
- 155 Trend Micro. (11 April 2019). *Trend Micro Security News*. "New Critical Infrastructure Facility Hit by Group Behind TRITON." Last accessed on 1 August 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/new-critical-infrastructure-facility-hit-by-group-behind-triton/>.
- 156 Trend Micro. (17 June 2019). *Trend Micro Security News*. "Xenotime, Hacking Group Behind Triton, Found Probing Industrial Control Systems of Power Grids in the US." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/xenotime-hacking-group-behind-triton-found-probing-industrial-control-systems-of-power-grids-in-the-us>.
- 157 Trend Micro. (27 June 2019). *Trend Micro Security News*. "The IIoT Attack Surface: Threats and Security Solutions." Last accessed on 24 July 2019 at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/-the-iiot-attack-surface-threats-and-security-solutions/>.



## 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 threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

[www.trendmicro.com](http://www.trendmicro.com)

