



TREND  
MICRO™

research



# Caught in the Net: Unraveling the Tangle of Old and New Threats

2018 Annual Security Roundup

#### 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

*For Raimund Genes (1963-2017)*

# Contents

## 04

Messaging threats increase,  
in various forms

## 10

Ransomware remains compelling  
despite decline in attacks

## 17

Critical vulnerabilities in hardware and  
the cloud are found, number of ICS bugs  
continue rising

## 23

IoT security incidents shed light on  
smart home insecurity

## 26

Mega breaches continue to pile up  
as privacy concerns and responses  
intensify

## 28

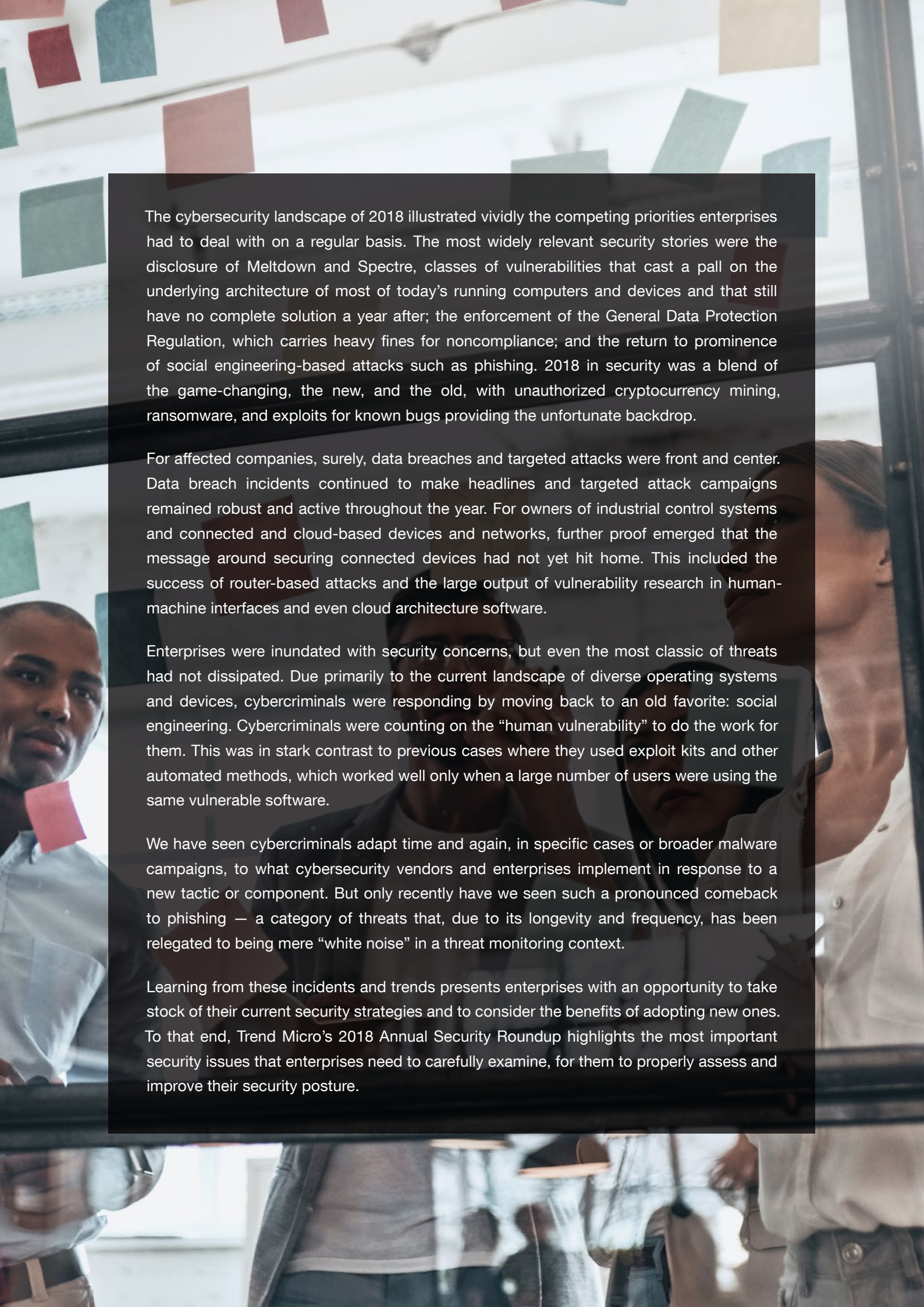
Further developments made in machine  
learning solutions, multisectoral research  
and law enforcement cooperation

## 31

Full-ranged multilayered solutions  
best suited to today's threat landscape

## 32

Threat Landscape in Review



The cybersecurity landscape of 2018 illustrated vividly the competing priorities enterprises had to deal with on a regular basis. The most widely relevant security stories were the disclosure of Meltdown and Spectre, classes of vulnerabilities that cast a pall on the underlying architecture of most of today's running computers and devices and that still have no complete solution a year after; the enforcement of the General Data Protection Regulation, which carries heavy fines for noncompliance; and the return to prominence of social engineering-based attacks such as phishing. 2018 in security was a blend of the game-changing, the new, and the old, with unauthorized cryptocurrency mining, ransomware, and exploits for known bugs providing the unfortunate backdrop.

For affected companies, surely, data breaches and targeted attacks were front and center. Data breach incidents continued to make headlines and targeted attack campaigns remained robust and active throughout the year. For owners of industrial control systems and connected and cloud-based devices and networks, further proof emerged that the message around securing connected devices had not yet hit home. This included the success of router-based attacks and the large output of vulnerability research in human-machine interfaces and even cloud architecture software.

Enterprises were inundated with security concerns, but even the most classic of threats had not dissipated. Due primarily to the current landscape of diverse operating systems and devices, cybercriminals were responding by moving back to an old favorite: social engineering. Cybercriminals were counting on the "human vulnerability" to do the work for them. This was in stark contrast to previous cases where they used exploit kits and other automated methods, which worked well only when a large number of users were using the same vulnerable software.

We have seen cybercriminals adapt time and again, in specific cases or broader malware campaigns, to what cybersecurity vendors and enterprises implement in response to a new tactic or component. But only recently have we seen such a pronounced comeback to phishing — a category of threats that, due to its longevity and frequency, has been relegated to being mere "white noise" in a threat monitoring context.

Learning from these incidents and trends presents enterprises with an opportunity to take stock of their current security strategies and to consider the benefits of adopting new ones. To that end, Trend Micro's 2018 Annual Security Roundup highlights the most important security issues that enterprises need to carefully examine, for them to properly assess and improve their security posture.

# Messaging threats increase, in various forms

Enterprises accomplish important communications inside and outside the organization through business email. This has made email a particularly attractive platform for cybercriminals and other threat actors to use in delivering various payloads or malicious calls to action. While email-based threats have been part of the threat landscape for decades, phishing attacks — identity theft via socially engineered email — have been among the top concerns of security professionals across the globe, as surveyed by Black Hat in 2018.<sup>1,2,3</sup> An unwanted email that slips through a company's gateway security can easily fool a recipient if the visual and content cues in the email matches what the recipient typically encounters in a business context. Logos, certain wording, and even the sender format can all be used to deceive the user.

## Cybercriminals cast wider phishing net

When phishing victims click on a link in an email, they invariably land on phishing websites as part of the overall attack chain. These sites are crafted to look as authentic as possible so users would have no qualms about entering whatever information the cybercriminals want to get.

As we noted in our security predictions for 2019, we saw that overall phishing activity ballooned in the first three quarters of 2018.<sup>4</sup> We continued to observe this increase toward the end of the year, with 269 million instances of blocked access to phishing URLs, for a 269-percent increase compared to 2017. Meanwhile, we observed an 82-percent increase in blocked access to phishing URLs by unique client IP address, an indicator of the number of users who would have been affected, compared to the previous year.

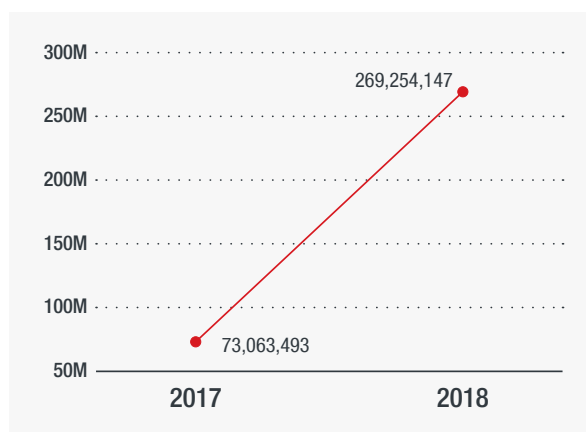


Figure 1. The instances of blocked access to phishing URLs increased by 269 percent compared to the previous year: Year-on-year comparison of blocked access to non-unique phishing URLs (e.g., three instances of blocked access to the same URL counted as three)

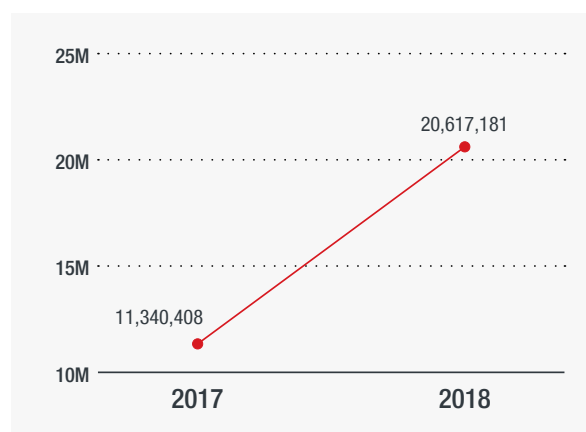


Figure 2. 82-percent increase in blocked access to phishing URLs by unique client IP address: Year-on-year comparison of blocked access to phishing URLs by unique client IP address (e.g., one machine that accessed a link three times was counted as one)

Since phishing attacks typically happen through email, this means cybercriminals intensified their efforts to send out more phishing emails. Phishing has been around for several decades and has even expanded to other modes of communication such as chat, SMS, and voice calls. The renewed focus on phishing attacks therefore reflects an important change in the computing landscape that cybercriminals are trying to navigate.

As recently as five years ago, there was a somewhat homogenous computing landscape: Almost 80 percent of operating systems in use were Microsoft Windows, albeit in different versions.<sup>5</sup> Since exploits could minimize the need for human interaction in the attack algorithm — unlike phishing attacks, which still required the victim to click a link — it thus made more sense for cybercriminals at the time to pay more attention to software exploits for widely used platforms and browsers.

However, that environment has significantly changed. Now, the kinds of connected devices have become more diverse. Versions of software operating systems that did not exist or were not commonplace five years ago are now part of the picture, and no single platform is being used by more than half of computer users. From the cybercriminal's point of view, therefore, the efficiency of attacks using exploit kits has started to go down. There is no longer a type of software version-dependent attack that will be effective against the majority. In fact, the numbers for exploit kit attacks, which rely heavily on being able to identify the user's specific version of the browser or other software in order to deploy the relevant exploit, plummeted in 2018 by 63 percent.

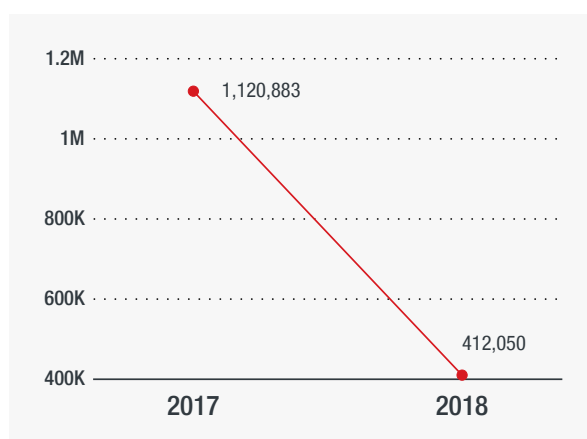


Figure 3. The number of instances of access to exploit kit sites decreased:  
Year-on-year comparison of access to exploit kits

The effort to continually refine attacks to address this reality is greater than simply re-strategizing and returning to exploiting the ever-present “vulnerability” that is human gullibility. Cybercriminals have thus begun increasing their efforts toward social engineering instead. Several data breaches in 2018 were directly attributable to phishing attacks, as when a school employee clicked on an email supposedly from a regional organization,<sup>6</sup> county workers were tricked via pay raise-related email,<sup>7</sup> or hospital staff members provided their sign-in credentials believing an email came from an executive inside their organization.<sup>8</sup> The impact of a single employee falling for a phishing attack is significant.

Some other interesting phishing attacks we saw in 2018 were the use of AES-encrypted sites to go after Apple IDs,<sup>9</sup> the use of the deceptive punycode technique for smishing (SMS-enabled phishing),<sup>10</sup> and the use of hijacked email accounts to respond to an existing email thread.<sup>11</sup>

This shift back is also exacerbated by the continued reliance of consumers on email as the keystone of their online personas; online services still require users to have an email address to send important account-related notifications and updates. On the enterprise front, the adoption of software-as-a-service (SaaS) office suites increases the value of login credentials in the eyes of cybercriminals, making these platforms viable targets for phishing. In fact, we saw a 319-percent increase in the number of blocked unique phishing URLs spoofing Microsoft Office 365 and Outlook.

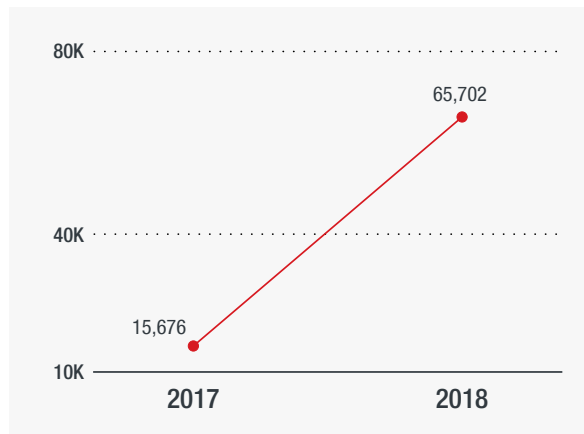


Figure 4. The number of blocked unique phishing URLs spoofing Office 365 and Outlook increased more than threefold: Year-on-year comparison of unique Office 365 and Outlook phishing URLs blocked

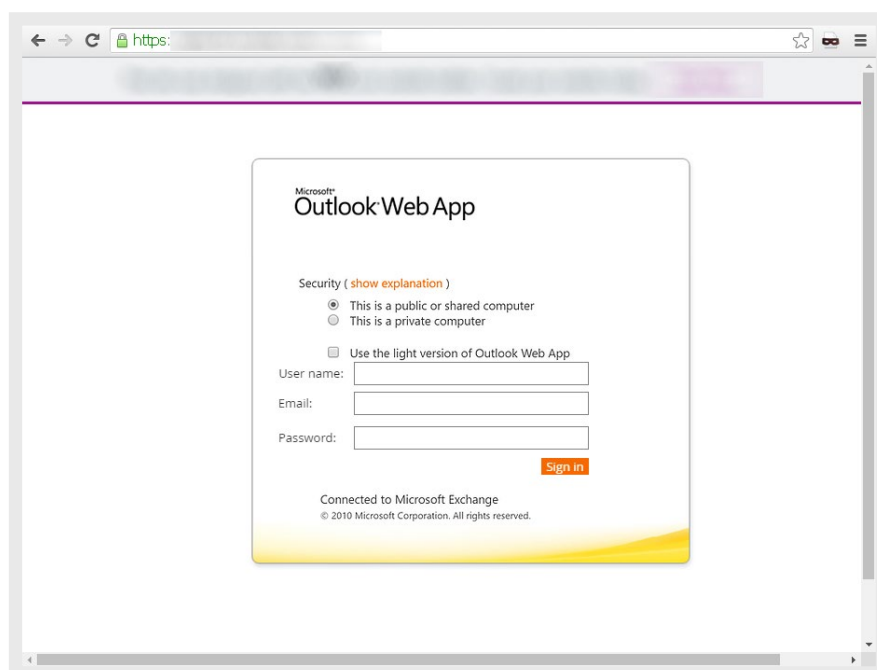


Figure 5. Cybercriminals attempt to harvest information from users of SaaS office suites via phishing sites: Sample screenshot of a phishing site posing as an Outlook Web App login page

# Cybercriminals go deep via BEC

Business email compromise (BEC), which includes CEO fraud, is another form of email-based threats. In a typical BEC attack, an attacker initiates or intercepts communication with someone in the company who has the decision-making power to release funds or conduct wire transfers as payment for services or as part of normal operations. In most cases, that would be the CEO, or an executive with similar powers.

BEC attempts showed no signs of abating as they continued to increase throughout 2018, registering a 28-percent increase from 2017. While the overall number of these email-based attacks was low, the danger lay in how effective each singular attempt could be. Whereas some phishing attacks are launched against a wide swath of possible victims, more research by the cybercriminal goes behind every BEC attack to increase the likelihood of user interaction.

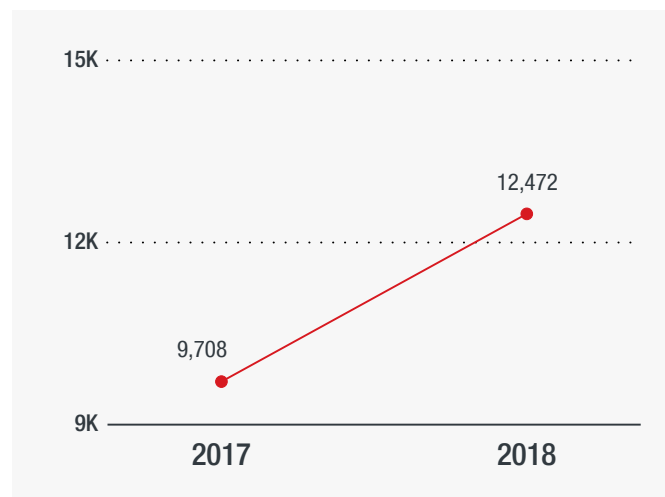


Figure 6. BEC attempts increased: Year-on-year comparison of BEC attempts

*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.*

Based on a sample set of our monitoring of BEC attempts in 2018, several figures of authority were being spoofed, with the top spoofed position being the CEO. This is not surprising as the CEO has the highest operating authority in most enterprises.

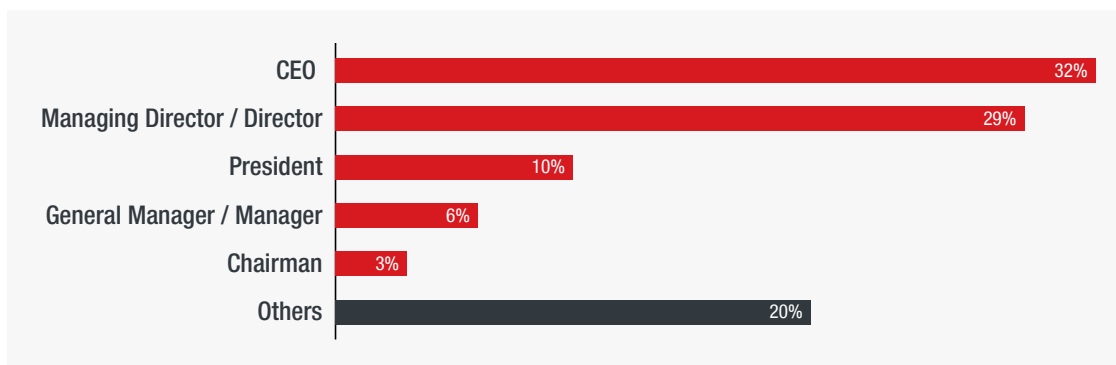


Figure 7. CEOs were the most spoofed position: Distribution of spoofed positions

*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.*

We saw numerous BEC attempts among our customers in Australia, the U.S., and the U.K. While the numbers may be suggestive of our customer user base distribution, these countries are business hubs where headquarters of many multinational companies are located. It makes sense, then, for a lot of these attempts to be directed toward them.

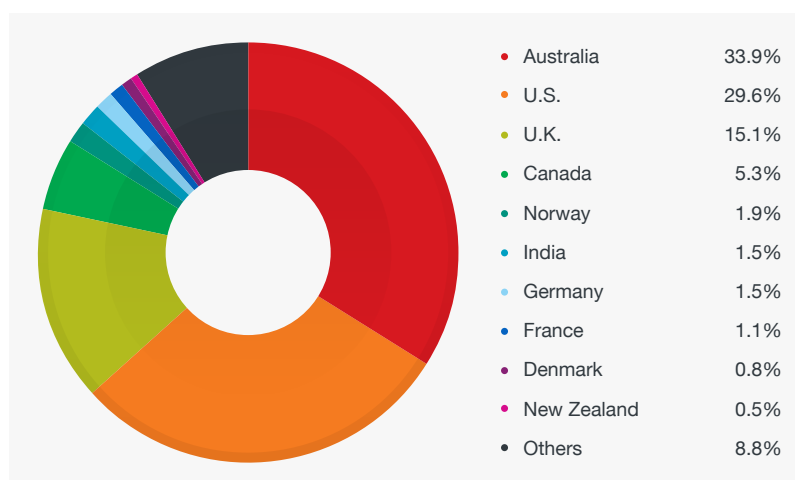


Figure 8. More BEC attempts were seen in countries considered as business hubs:  
Distribution of BEC attempts by country

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

Toward the end of the year, the FBI issued an advisory warning against a new ploy that uses the BEC model. In this scheme, called gift card fraud, an employee is ordered to purchase gift cards for the CEO to give away or to purchase items as gifts to employees. The ruse is convincing from a social engineering standpoint because of the timeliness and nature of the request. In the U.S. state of Arizona alone, the total losses due to gift card fraud came close to US\$90,000.<sup>12</sup>

# Ransomware remains compelling despite decline in attacks

## Overall ransomware threat detections drop while WannaCry maintains its hold

Despite the prevalence of ransomware incidents in the news, we observed a drastic 91-percent decrease in ransomware-related threat components. The decline was due to several reasons, including improved ransomware solutions, greater awareness about this specific extortion scheme, and to a certain extent, the recognized futility of succumbing to paying ransom to reclaim access to files held hostage by the threat.

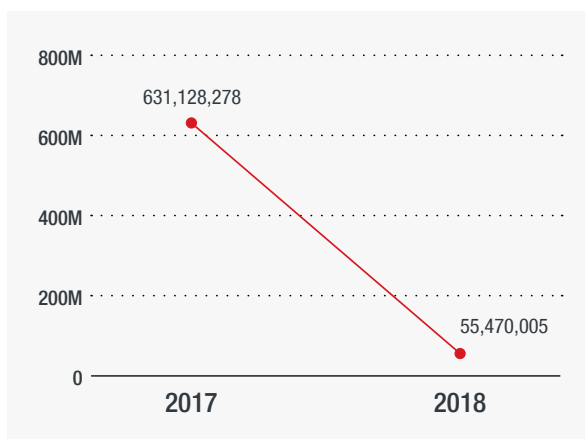


Figure 9. Ransomware-related threat components (files, emails, URLs) decreased:  
Year-on-year comparison of ransomware-related threats

There was also a corresponding decrease in new ransomware families.

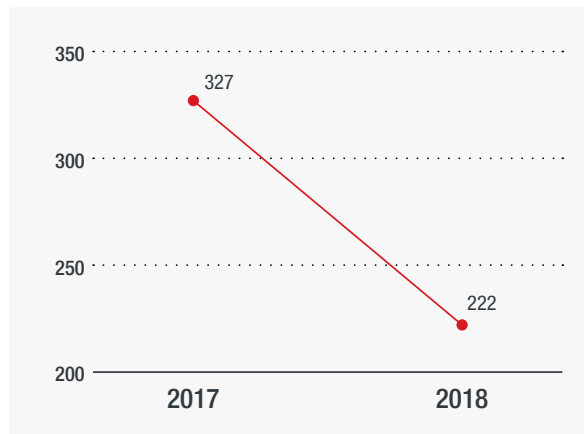


Figure 10. New ransomware families decreased:  
Year-on-year comparison of new ransomware families detected

However, the profits to be gained relative to the effort to be spent in launching an attack remained compelling, so we continued to see interesting, if not new, ransomware tactics. Among the different ransomware families, WannaCry, which first appeared in April 2017 and caused the infamous global infection outbreak of May 2017,<sup>13</sup> remained the top one at 616,399 detections in 2018. It overshadowed all the other ransomware families combined by a wide margin, despite being over a year old.

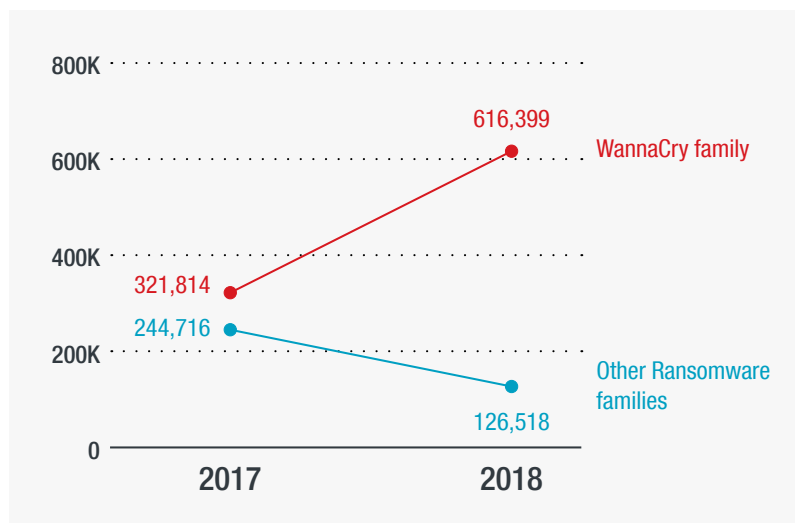


Figure 11. WannaCry accounted for more than half of ransomware detections for the second year:  
Year-on-year comparison of WannaCry detections versus other ransomware detections combined

WannaCry relies on a Microsoft Windows Server Message Block (SMB) vulnerability via an exploit called EternalBlue, which was leaked by the Shadow Brokers hacker group, to gain access to vulnerable systems.<sup>14</sup> It then spreads throughout networks via its worm capabilities. The number of WannaCry detections indicated that a great deal of computer users worldwide were still unable to deflect the malware via patching despite the availability of a solution for over a year.

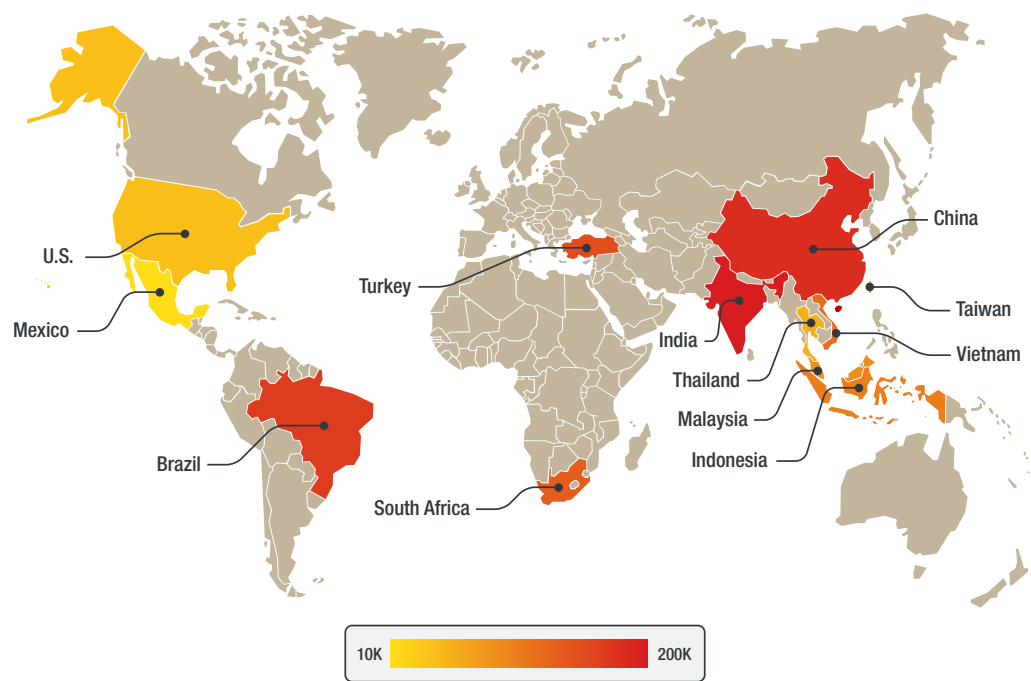


Figure 12. WannaCry continued to be detected all over the world:  
Heat map of countries with more than 10,000 WannaCry detections in 2018

Meanwhile, as was the case when the ransomware first came out in 2017,<sup>15</sup> an overwhelming majority of the WannaCry detections were from systems running Windows 7 operating system versions. This aligns broadly with the fact that the targeted vulnerability no longer exists in operating systems using SMB version 3, meaning Windows 8 and newer.<sup>16</sup> The patch had been available since 2017, but many users were still failing to apply it.

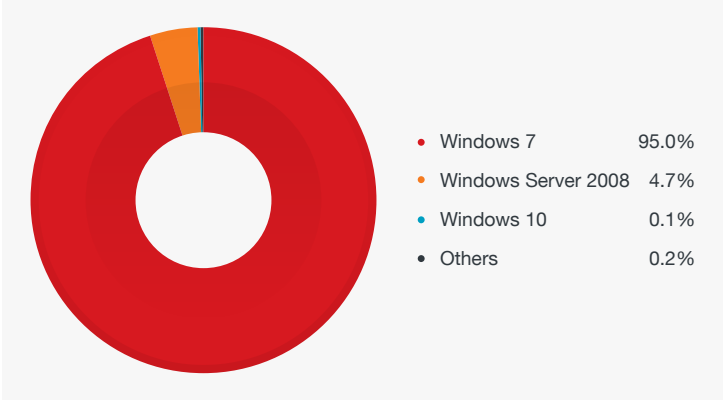


Figure 13. More than 90 percent of WannaCry detections came from systems running Windows 7:  
Distribution of WannaCry detections in 2018 by operating system

As for new developments, we observed a lot of activity from the GandCrab family of ransomware. It released several iterations of its ransomware throughout the year through various infection methods, including spam<sup>17</sup> and the Fallout exploit kit.<sup>18</sup> It was also found to append different file extensions to locked files or come with backdoors, worms, and malicious cryptocurrency miners. In line with the ransomware's tactics to tailor-fit targets, EGG compressed archive files were seen as carrying GandCrab in spam sent to users in South Korea.<sup>19</sup> In October, the developers reportedly teamed up with a crypter service to evade detection.<sup>20</sup>

Other pieces of ransomware continued to adapt as well. Cybercriminals set up fake software sharing sites and pop-up ads that pointed to them and that eventually led to ransomware<sup>21</sup> — an effective technique in side-stepping some users' learned apprehension of downloading executables or anything with a large file size. In another instance, cybercriminals bundled ransomware with legitimate software.<sup>22</sup> And in yet another, ransomware was programmed to send a copy of itself to an infected user's email contacts.<sup>23</sup> We also found evidence of ransomware evolving to have anti-machine learning capabilities, as in the case of PyLocky.<sup>24</sup> The operators of Princess Evolution, in particular, said in underground forums that they went on hiatus in order to improve their ransomware-as-a-service (RaaS), which used an affiliate program for ransom payments.<sup>25</sup>

## Cryptocurrency mining detections surpass 1 million

Cryptocurrency mining detections reached a new peak in 2018 at over 1 million detections, a 237-percent increase over the previous year. The numbers reflect the trend we have observed of a “gold rush” in terms of the flurry of various attack methods throughout the year: abused ad platforms,<sup>26, 27</sup> pop-up ads,<sup>28</sup> server exploits,<sup>29, 30</sup> malicious browser extensions,<sup>31</sup> mobile phones,<sup>32</sup> plug-ins,<sup>33</sup> botnets,<sup>34, 35</sup> bundling with legitimate software,<sup>36</sup> exploit kits,<sup>37</sup> and repurposed ransomware.<sup>38</sup>

Cybercriminal interest in cryptocurrency was apparent in attacks against the infrastructure.<sup>39</sup> It was also reflected in the types of posts that cropped up in cybercriminal underground forums. Tools and services related to two main methods of targeting cryptocurrency were often advertised: cryptocurrency-mining malware, where most of the aforementioned examples fall under, and cryptocurrency-stealing malware, which looks for wallets and intercepts transactions. Despite all evidence that smartphones, routers, and other internet-of-things (IoT) devices are not capable of much computing power (unlike regular computers), underground forums still continued to peddle wares related to mining activities that use these devices,<sup>40</sup> perhaps counting on volume to make the campaigns worth the effort.

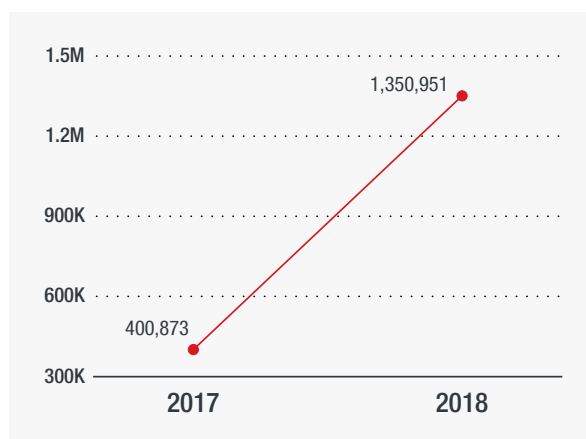


Figure 14. Cryptocurrency mining detections increased:  
Year-on-year comparison of cryptocurrency mining detections

## Fileless threats increase in fourth quarter

Another important development seen in 2018 was the upsurge of fileless threats, which are used increasingly by cybercriminals as another way to evade detection. Fileless threats are so named because they use no discrete binaries or executables. Nevertheless, they manage to run by injecting themselves into an existing application's memory or by running scripts within a legitimate application such as Windows Machine Instrumentation or PowerShell. In order to address the risk of a user simply restarting the computer to lose the malicious code since it resides only in memory, cybercriminals also make subtle changes to the system registry. However, we are able to detect fileless threat activities by tracking non-file-based indicators such as specific execution events or behaviors.

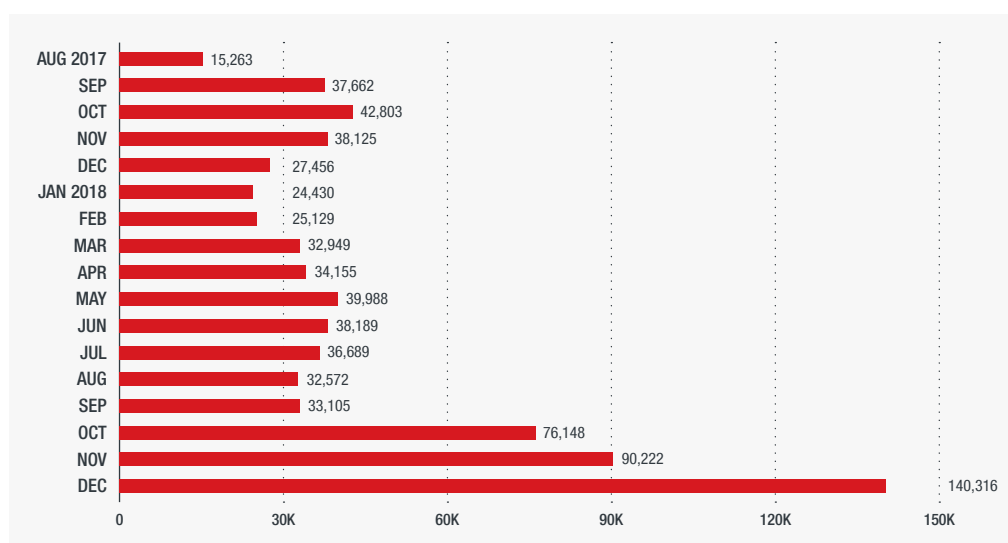


Figure 15. Fileless malware continued to be seen: Monthly comparison of fileless events blocked

Indicators of these threats can be detected via traffic and behavior monitoring, or sandboxing.<sup>41</sup> This means that conventional solutions that rely on the identification of malicious binaries are blind to these emerging threats. Fileless threats can be used toward whatever end cybercriminals envision; in the past couple of years, we saw it being used to deploy cryptocurrency miners,<sup>42</sup> ransomware,<sup>43</sup> and backdoors.<sup>44</sup>

## TinyPOS source code release triggers flurry of POS malware

In the first half of 2018, we observed an uptick in point-of-sale (POS) malware detections driven by the sudden proliferation of POS malware that we detect as TinyPOS. The TinyPOS malware family detection covers a certain strain of relatively older memory scrapers with the distinct characteristic of having a small file size, including the likes of PinkKite.

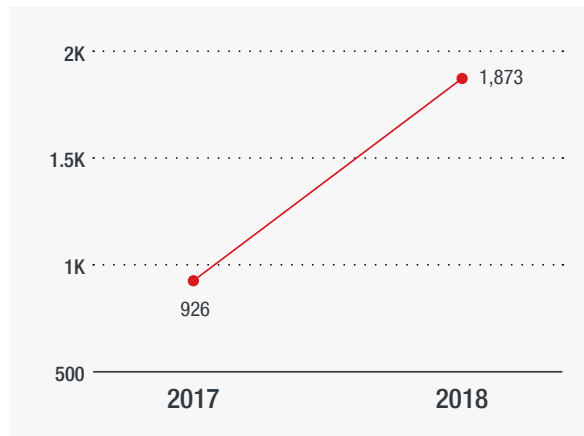


Figure 16. POS malware increased: Year-on-year comparison of POS malware detections

The spike, which occurred in May, was due to the release of the source code for the TreasureHunter POS malware.<sup>45</sup> Whenever cybercriminals share malware source code publicly or through forums, other cybercriminals are expected to study, use, improve on, and further weaponize the code. This in turn results in a surge in detections as tweaked versions are deployed, tested, and reviewed. We have seen similar scenarios happen after other malware source code leaks, as in the case of the Mirai-based Satori botnet<sup>46</sup> and even the well-intentioned but ill-advised release of the Hidden Tear ransomware code.<sup>47</sup>

# Misconfigured cloud containerization APIs lead to cryptocurrency miners

Cybercriminals have definitely begun looking to the cloud to expand their scopes of attack. In a recent case, we have seen cryptocurrency miners in the cloud as a result of exposed Docker APIs.<sup>48</sup> Docker is an open-source containerization software — a kind of virtualization done at the operating system rather than the application level.

Security features<sup>49</sup> have been put in place to empower users to secure their containers. As a basic security practice, since application program interfaces (APIs) allow remote manipulation of these cloud assets, they should never be open to external access. However, small misconfigurations in security settings can have repercussions for cloud administrators.

# Critical vulnerabilities in hardware and the cloud are found, number of ICS bugs continue rising

Several security-related discoveries served as vivid wakeup calls for the general computing population and cloud adopters, including those handling industrial control systems (ICSs).

## Meltdown and Spectre issues show no signs of fading

The year opened with the groundbreaking disclosure of two major processor-level vulnerability classes, Meltdown and Spectre, both of which relied on flaws in the speculative execution of CPU instructions. Rushed patches from some vendors in January triggered several complaints of blue screens of death (BSODs) and bricking (in which devices were rendered useless and unable to start up).<sup>50</sup> Over the following months, more specific variants of Meltdown and Spectre were found.<sup>51</sup>

Because Meltdown and Spectre are classes of flaws, the different ways by which microprocessors are designed make it challenging to determine the extent to which they are affected. This is why most mitigation guidance for Meltdown and Spectre comes in the form of long lists that include advisories from microprocessor, device, software, and cloud service vendors — as opposed to the usual straightforward advisories that can, at most, point to one patch per version of a piece of software.

By the end of the year, a clean resolution of these micro-architectural flaws was nowhere in sight, truly highlighting the watershed nature of their discovery and disclosure.<sup>52</sup> Unfortunately, this means that for several years, different devices under different circumstances will continue to harbor the risk of a practically undetectable data leak absent an overhaul of the foundational architecture.

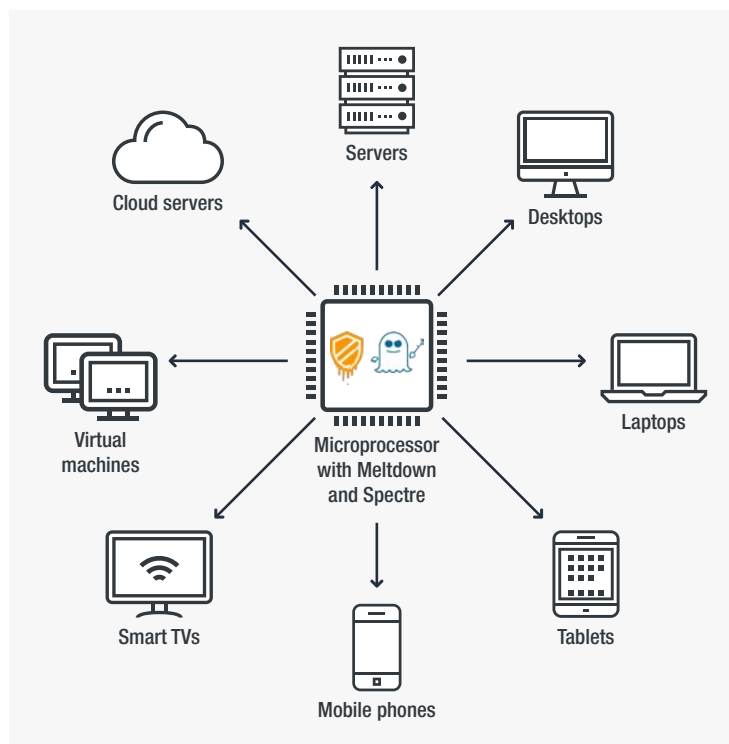


Figure 17. Meltdown and Spectre affected the underlying hardware in devices beyond desktop computers: Different device types affected by Meltdown and Spectre

## Critical cloud vulnerability allows back-end server access

Another unfortunate first was the discovery of a critical vulnerability in the open-source cloud orchestration software Kubernetes.<sup>53</sup> The vulnerability allows an attacker using a specially crafted network request to connect to a back-end server through the Kubernetes API server.<sup>54</sup> As a result, any command sent to the back-end will be executed because the request is considered authenticated for having passed through the API. While the vulnerability, unlike Meltdown and Spectre, was promptly fixed, it raises concerns about how important DevOps with security in mind (aka DevSecOps) will continue to be as new platforms and technologies are used to process data.

## Exploits for known and patched bugs increase in usage

It used to be that two or three major zero-day exploit attacks would mark a year. But recently there were either no widespread zero-day attacks or none that were identified as such. Rather, the ones that were discovered were in the context of attacks with limited scope.

Vulnerability ID	Zero-day exploit details
CVE-2018-4878	Flash zero-day exploit used in limited, targeted attacks in January <sup>55</sup>
CVE-2018-8120	Win32k component in May (no further details) <sup>56</sup>
CVE-2018-8174	Double Kill Internet Explorer zero-day exploit used in limited, targeted attacks in May <sup>57</sup>
CVE-2018-8341	Windows kernel in August <sup>58</sup>
CVE-2018-8373	Limited targeted attack using Microsoft VBScript in August <sup>59</sup>
CVE-2018-8414	Limited attacks against Windows Shell (also affects Adobe Acrobat) in August <sup>60</sup>
CVE-2018-8453	Limited active attacks against Windows kernel in October <sup>61</sup>
CVE-2018-8589	Limited active attacks against Windows kernel in November <sup>62</sup>

Table 1. Zero-day exploit incidents were not as widespread as in previous years:  
Notable zero-day exploit incidents

At the same time, we observed several cases of cybercriminals using exploits for vulnerabilities that had already been patched. These exploits for known bugs are also known as n-day or 1-day exploits.

Vulnerability ID	Details	Patch date	Attacks seen in 2018
CVE-2018-7602	Drupal vulnerability used to deliver cryptocurrency miners <sup>63</sup>	April 25, 2018	5 hours after release of patch <sup>64</sup>
CVE-2017-12635, CVE-2017-12636	Apache CouchDB vulnerabilities used to deliver cryptocurrency miners <sup>65</sup>	Nov. 14, 2017 <sup>66</sup>	Feb. 15, 2018 <sup>67</sup>
CVE-2017-10271	Oracle WebLogic WLS-WSAT vulnerability used for cryptocurrency mining	Oct. 16, 2017 <sup>68</sup>	Feb. 26, 2018, <sup>69</sup> and then again on May 11, 2018 <sup>70</sup>
CVE-2015-1805	Vulnerability that allows permanent rooting of Android phones <sup>71</sup> used in AndroRat <sup>72</sup>	March 16, 2016 <sup>73</sup>	Feb. 13, 2018 <sup>74</sup>

Table 2. Exploits for known and patched vulnerabilities were used in attacks hours up to years after patches were made available: Notable incidents involving n-day or 1-day exploits

This reverse strategy of first studying a disclosed vulnerability, even if it has been patched in the same advisory, then developing an exploit for it has become quite common over the years. But it appears that cybercriminals are correct in assuming that not all enterprises will be able to patch their systems in time, if at all. Notably, the number of vulnerabilities that were disclosed ballooned in 2017,<sup>75</sup> with the number further increasing in 2018.

Old exploits for bugs whose patches had been available, such as the Linux kernel privilege escalation vulnerability Dirty Cow (CVE-2016-5195) and the Windows SMB vulnerability exploited by EternalBlue (CVE-2017-0144), were still being used by cybercriminals to much effect. In the case of Dirty Cow, while it was immediately patched upon discovery of active exploitation in October 2016<sup>76</sup> — and then again in November 2017, when a flaw in the patch was found — researchers determined that attackers had used it to exploit a backdoor in Drupal web servers in October 2018.<sup>77</sup>

CVE-2017-0144, which was disclosed<sup>78</sup> and patched<sup>79</sup> in March 2017, caused much trouble as it was exploited by EternalBlue in the WannaCry ransomware outbreak in May 2017, and in several other malware campaigns soon after that. In 2018, as discussed in the malware section of this report, the WannaCry group of malware continued to be one of the top malware families we were able to block on systems worldwide, and EternalBlue-related connections were the top outbound attacks.

## Bugs still being found in PDF readers and managers

The continued exploitation of known and patched bugs makes it even more important for enterprises to pay attention to vulnerability trends in some widely used office software.

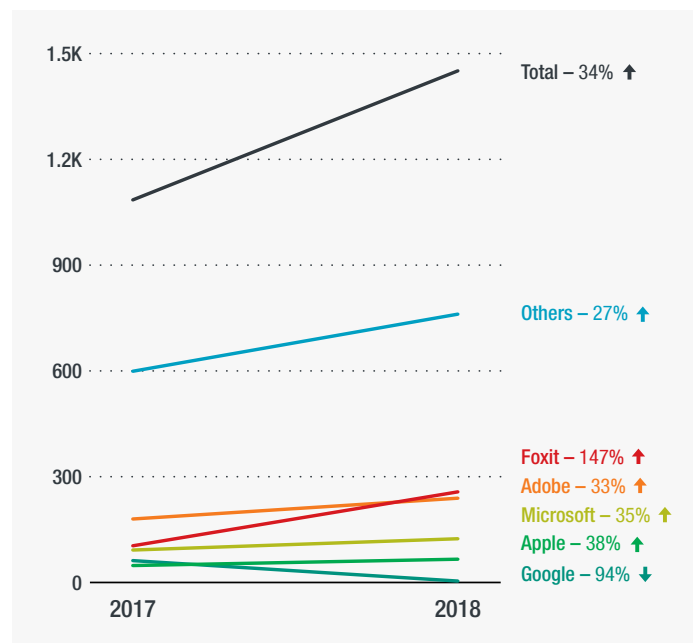


Figure 18. Discovered and reported vulnerabilities increased:  
Year-on-year comparison of vulnerabilities of selected software vendors

Based on our data, which included input from more than 3,500 independent researchers who contribute to our Zero Day Initiative (ZDI) program,<sup>80</sup> Foxit was the vendor with the most number of reported vulnerabilities, at 257, followed closely by Adobe with 239; both Adobe and Foxit are makers of tools for creating, modifying, and managing PDF files. The tech giants Microsoft, Apple, and Google had 124, 66, and 4 vulnerabilities, respectively.

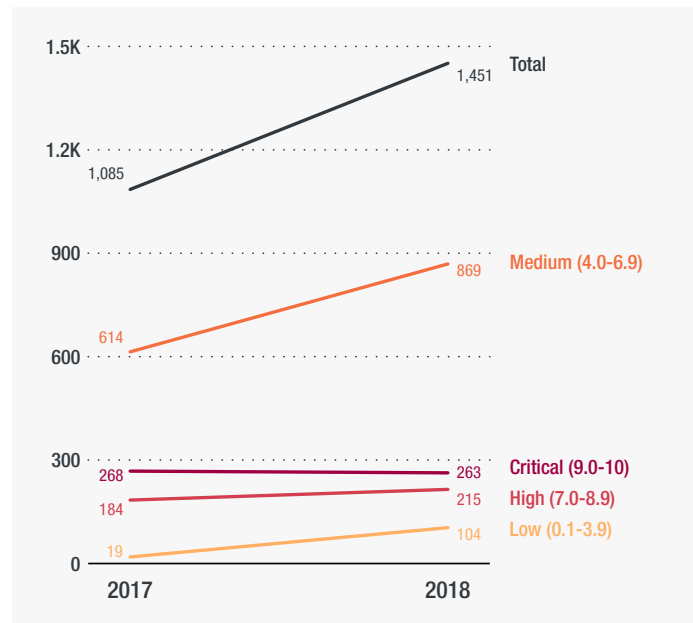


Figure 19. Critically rated vulnerabilities decreased from 25 percent to 18 percent of total:  
Year-on-year comparison of number of vulnerabilities by severity rating

Of the vulnerabilities disclosed in 2018, 60 percent were classified as medium, representing an increase of 3 percentage points from the number of medium-rated vulnerabilities in 2017. Fortunately, the distribution of critically rated vulnerabilities decreased from 25 percent in 2017 to 18 percent in 2018.

## Number of bugs in HMI for ICS still problematic

A considerable percentage of the reported vulnerabilities were found in software used in ICSs. Advantech and Wecon piled in over a hundred vulnerabilities each. The vulnerabilities were mostly in human-machine interface (HMI) software for ICSs and supervisory control and data acquisition (SCADA) environments. The HMI is the main hub for monitoring, managing, and implementing the states of different processes in facilities, a function that may be interpreted as not being able to directly affect equipment or devices. Unfortunately, however, apart from the value of information in a reconnaissance context for targeted attacks, it is also entirely possible to affect the function of physical components. This is especially true if a vulnerability allows an attacker to make modifications in the set points of particular equipment or devices.

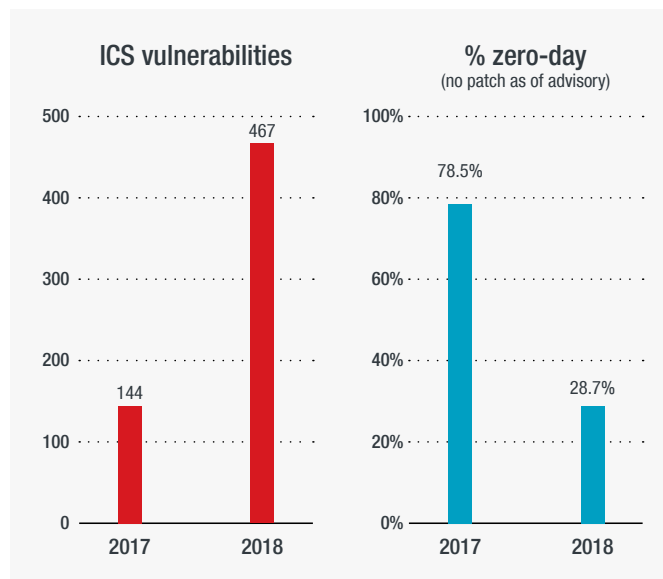


Figure 20. The number of ICS vulnerabilities increased but the percentage of vulnerabilities disclosed without patches decreased: Year-on-year comparison of ICS vulnerabilities

The overall response time from HMI vendors did not improve significantly compared to other software vendors either, as 85 percent of the total zero-day vulnerabilities reported in 2018 fell under the ICS category.<sup>81</sup>

# IoT security incidents shed light on smart home insecurity

While the creators of Mirai<sup>82</sup> and Satori<sup>83</sup> have suffered the consequences of designing code that converts vulnerable routers into weapons of distributed denial of service (DDoS), attacks against routers continued unabated. Routers were still being compromised using recycled Mirai code,<sup>84</sup> while VPNFilter, router malware that had increased functionalities including reconnaissance and persistence components, ushered in the abuse of routers beyond DDoS.<sup>85</sup> The trend of increasing functionalities of router-based attacks, which we noted in our midyear report,<sup>86</sup> continued as we found routers being used for cryptocurrency mining and pharming attacks.<sup>87</sup>

## Router weaknesses explored by cybercriminals

MikroTik routers in Brazil became vulnerable to cryptocurrency mining attacks because attackers exploited a then-patched security flaw in a remote management service software typically bundled in RouterOS, which is what MikroTik routers use. They injected malicious Coinhive script to mine Monero (XMR) cryptocurrency into every webpage visited by a user, but eventually resorted to loading it only when a user encountered an HTTP error to avoid immediate detection.<sup>88</sup> As previously noted, smart devices by themselves do not have much processing power to make a dent in cryptocurrency mining, but cybercriminals continue to target routers anyway.

We also investigated the workings of an exploit kit named Novidade.<sup>89</sup> It changes router Domain Name System (DNS) settings via cross-site request forgery (CSRF) so that subsequent access to the internet can get redirected to a server controlled by the attacker. For instance, a user with an infected router who wants to access a bank to conduct a transaction will instead land on a fake banking page. Unless the user is especially cautious, the user may proceed to log in, thereby giving up login and password details to the malicious server, which are all it takes to effectively take over the bank account.

# SMB vulnerability-related events dominate outbound router connections

Based on smart home network feedback from the Trend Micro™ Smart Home Network solution, which included feedback from third-party routers, the following were the top events (including legitimate connections) and their distribution. The Telnet default password login event reflected the unsecure practice on the part of users of not changing the passwords provided by the vendors. This practice is akin to buying locks for keeping valuable assets safe but using them without first setting new number combinations — a boon for thieves.

We also found the prevalence of the Microsoft Windows SMB attack via EternalBlue.

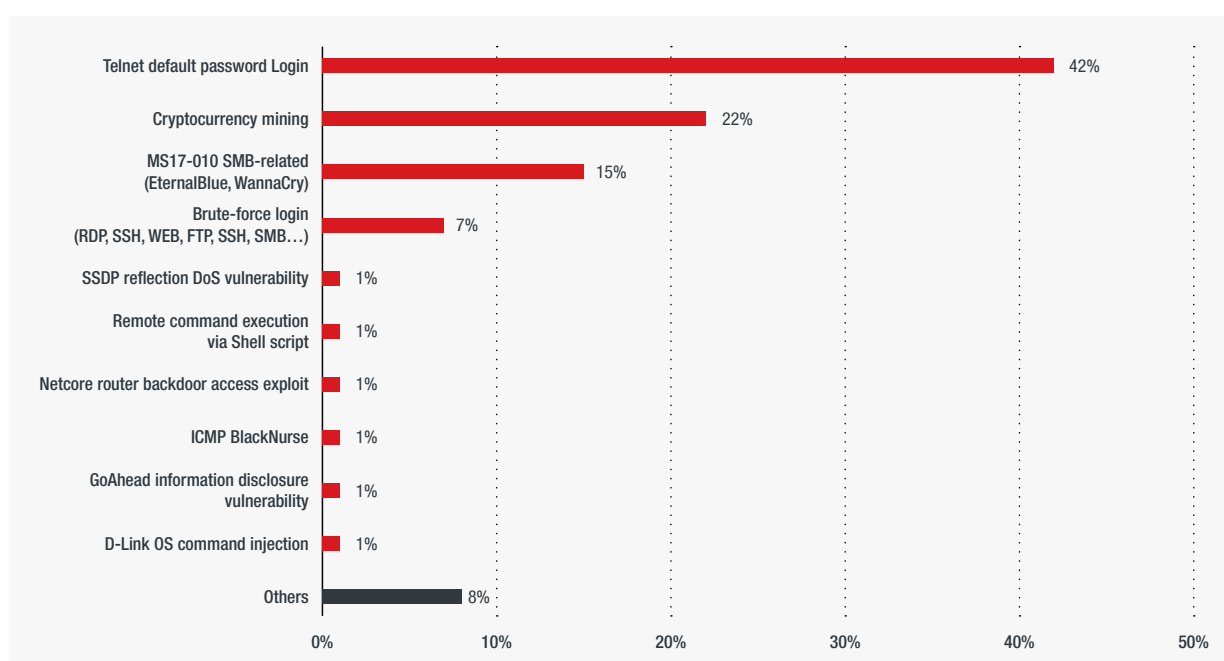


Figure 21. Telnet default password logins were the top event triggered:  
Distribution of event rules triggered in 2018

We dug deeper by looking only at outbound events, which might indicate the likelihood that a malicious attack had successfully compromised a router and was now “phoning home” to the attacker. And we found that possible WannaCry-related events accounted for more than half of the outbound communications, with the other events attributed to different types of flooding attacks (ICMP and TCP SYN) and brute-force attempts, among others. This also reflected the trend discussed in the ransomware discussion where WannaCry maintained its hold over vulnerable computers despite being easily addressed by an available patch.

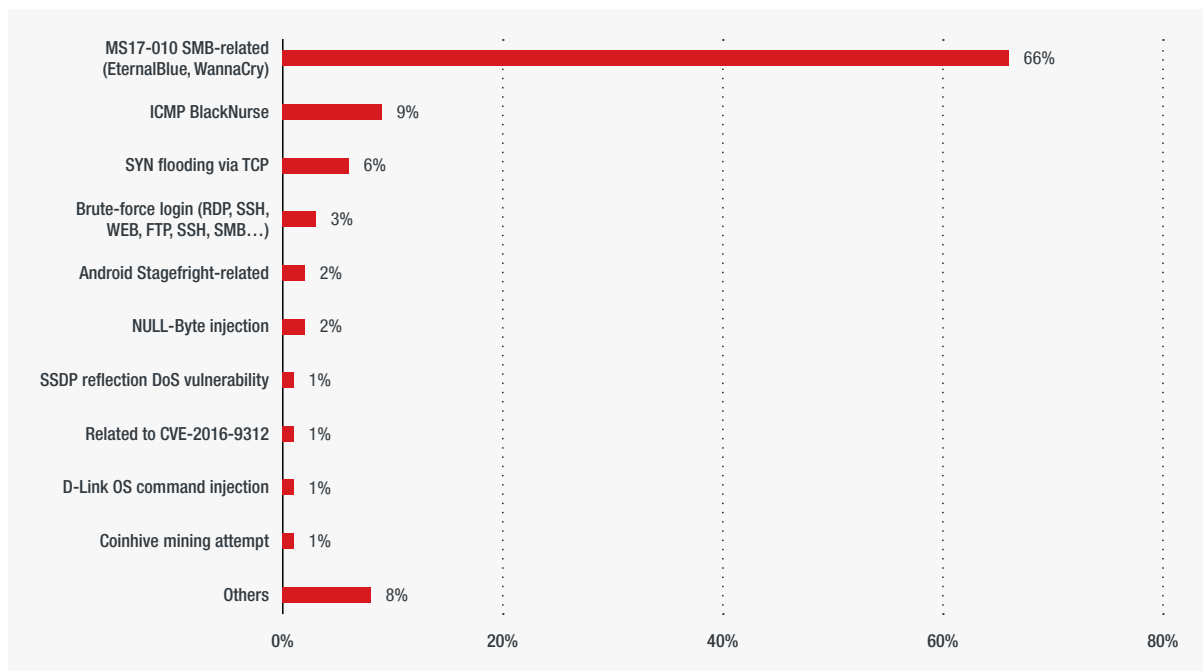


Figure 22. WannaCry-related events were the top outbound event rules triggered:  
Distribution of outbound events in 2018

The said connections came from different countries, with most of the events coming from countries in Asia.

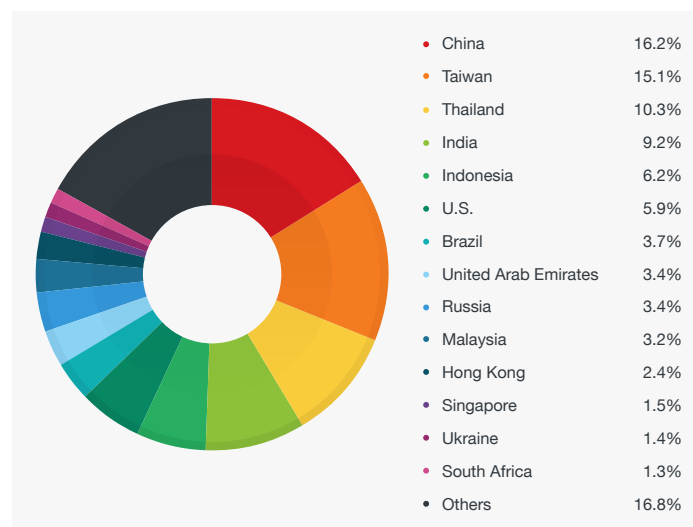


Figure 23. Most of the outbound events in the feedback came from countries in Asia:  
Country distribution of router-related outbound event feedback in 2018

As more home owners also become “smart home network administrators,” they must recognize and take on new responsibilities to ensure that their home routers do not become entry points for attackers. It is easy to overlook routers as just part of overall internet connectivity. But the role it plays, being the main hub for managing connections to and from the different devices that need the internet, is too critical not to secure.

# Mega breaches continue to pile up as privacy concerns and responses intensify

## Data privacy regulations kick into high gear

The General Data Protection Regulation (GDPR) came into effect in May, causing a deluge in reports and clarifications forwarded to the European Union (EU) as the different country regulators started handing out admonishments to violators.<sup>90</sup> In fact, on the same day the regulation took effect, large technology companies in the U.S. were called out by privacy groups that issued complaints.<sup>91</sup> However, it was not until toward the end of the year that data regulators started imposing fines: 5,280 euros for CCTV-related violations in Austria,<sup>92</sup> 20,000 euros for a social networking site in Germany that stored passwords in plain text,<sup>93</sup> and 400,000 euros for graver violations related to medical data committed by a hospital in Portugal.<sup>94</sup>

Other states and countries also implemented or launched their own privacy legislations in 2018. Australia's Notifiable Data Breaches scheme, for instance, had already been in effect since February,<sup>95</sup> with Canada following suit by publishing more enforceable regulations regarding breach notifications in April.<sup>96</sup> The Data Protection Bill in the U.K., which both ensures GDPR compliance once the country exits the EU and replaces its older Data Protection Act of 1998, underwent a public committee review in March.<sup>97</sup> In the U.S., the California Consumer Privacy Act of 2018 was unanimously passed in June;<sup>98</sup> it covers businesses — unlike the GDPR, which more broadly covers any entity that controls data — and focuses on data collected from customers — unlike the GDPR, which refers to all data on citizens. The declaration of equivalent adequacy of the GDPR with Japan's Act on the Protection of Personal Information was also finalized in July, meaning both countries consider the laws comparable to each other and allowing cross-border data transfers between the two.<sup>99</sup>

However, some of the aforementioned countries — Australia, Canada, the U.K., and the U.S. — are members, along with New Zealand, of the intelligence alliance known as Five Eyes, which maintains that information and communications companies have a responsibility to assist law enforcement. The member countries assert that any impediments encountered in accessing information that will help them protect their citizens will be met with “technological enforcement, legislative, or other measures to achieve lawful access solutions.”<sup>100</sup> Breakable encryption is unsecure encryption, so companies have the unenviable task of figuring out how to comply with the pronouncements should the need arise.

## Data breaches reach new peaks

Data breach disclosures in 2018 struck new peaks in the number of records exposed as at least 22 breaches reported in the U.S. affected more than 1 million records. More broadly, according to data from Privacy Rights Clearinghouse, there were 807 reported breaches in the U.S. in total — a 46-percent increase from the previous year.<sup>101</sup> While this could be partly attributed to increased reporting of breaches in response to stronger regulations, it is nonetheless an indicator that there is much left to be desired in regard to data privacy and security.

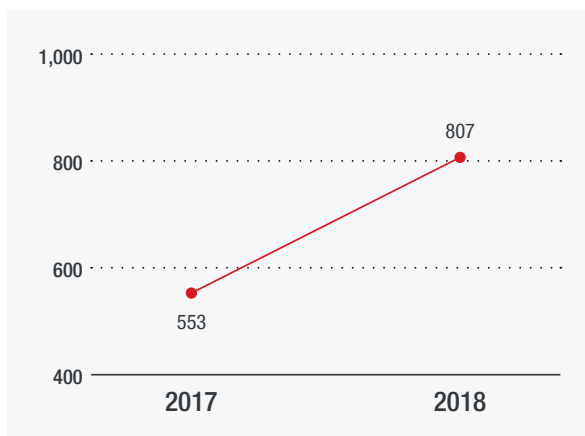


Figure 24. Data breaches in the U.S. increased:  
Year-on-year comparison of U.S. data breach reports

Outside the U.S., in addition to those mentioned in our midyear report, notable breaches involved a hotel chain<sup>102</sup> and an airline,<sup>103</sup> where 130 million and 9.4 million users were affected, respectively.

Exposed data is immediate fodder for threat actors looking to launch attacks. Data dumps are either sold raw or cleaned up for a higher price in deep web forums and purchased by other threat actors. These threat actors in turn use the data for their own campaigns, from phishing to targeted attacks. This arrangement fuels a vicious cycle where breached data can lead to more data breaches. In fact, in the latter half of 2018, our deep web research led us to a post that seemed to be related to the mentioned hotel data breach,<sup>104</sup> allowing us to see the supply chain of illegally obtained personally identifiable information (PII).

# Further developments made in machine learning solutions, multisectoral research and law enforcement cooperation

## Machine learning applications strengthen solutions

Trend Micro Research emphasized the role and importance of machine learning in cybersecurity<sup>105</sup> by demonstrating how our solutions use different machine learning techniques to identify malicious activity. Our solutions have been using machine learning techniques for quite a while, but there seems to be a heightened public interest in the concept suggesting it is a newfangled technology. In reality, though, it is not. Machine learning has been around for a long time. But because of the nature of how it works, it becomes more powerful and accurate depending on the volume and quality of data that is fed into the system.

By that token, its applications are vast when it comes to protecting networks. In 2018 alone, we documented how we used machine learning to reduce the rate of unknown software downloads,<sup>106</sup> identify certificate abuse,<sup>107</sup> cluster malicious network flows to help spot connected malware campaigns,<sup>108</sup> and identify web defacement campaigns.<sup>109</sup>

Beyond malware and network flows, we also came up with a solution specific to BEC emails via a form of artificial intelligence (AI) called Expert System, which mimics how security personnel determine whether a specific email is suspicious or not.<sup>110</sup> Additionally, we used AI to power the Writing Style DNA technology, which prevents email impersonation by comparing previous emails to suspected forgeries. The Writing Style DNA technology pays attention to different combinations of telltale clues about a user's writing style. These include tokens like sentence length, repeated words, punctuation marks, and thousands of other writing characteristics.

Furthermore, we have foreseen that cybercriminals will deliberately try to evade machine learning in security solutions. To counter this, we have developed means to make machine learning systems more robust by generating adversarial samples.<sup>111</sup>

These developments prove that machine learning applications are endless and can be used in various aspects of securing networks and devices, and that machine learning should not be seen merely as a tacked-on component of security.

## Exposed cyber assets found in hospitals and ICSs

Making the digital world a safe place for information exchange requires several approaches. Not least of these is a deep understanding of the current landscape, especially around public service sector equipment and systems, to which connectedness introduces notable risks even as it provides expansive efficiency.

Trend Micro Research provided comprehensive risk assessments for the healthcare industry,<sup>112</sup> focusing on exposed medical devices and supply chain attacks. We concluded that the industry remained highly vulnerable to attacks due to both the nature of the data they keep and the state of network and supply chain security, particularly in connected hospitals.

Our researchers also uncovered exposed HMIs in oil, gas, biogas, power, and water companies, where there was little or no authentication required to view or interact with consoles.<sup>113</sup> This finding is especially concerning because of the nature of the services these companies supply; for instance, an attack on the water supply of a certain region can have disruptive results and may lead to several knockoff effects.

We delved even deeper into the internet of things (IoT) in general and the industrial internet of things (IIoT) in particular. We drew up several attack scenarios related to the exposure of the communication protocols Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP).<sup>114</sup> In doing so, we raised awareness about the risks of leaving default configuration settings to run as is and the need for enforced encryption and authentication methods.

# Takedowns made possible through public-private partnerships

The fight against cybercriminals and other threat actors is a never-ending struggle for the computing public, security teams, and law enforcement. But every now and then, important battles are won when cybercriminal services are taken down and cybercriminals themselves are apprehended. One major case in point is that of the counter anti-virus service Scan4You: It went offline in 2017<sup>115</sup> and one of its longtime operators was convicted and sentenced to 14 years in prison<sup>116</sup> following collaborative efforts between Trend Micro and the FBI.

Trend Micro has had a long history of working with different law enforcement agencies all over the world in public-private partnerships.<sup>117</sup> The importance of this arrangement lies in how the two parties empower each other. Security vendors, of course, do not have the manpower to bring a cybercriminal to justice, while law enforcement agencies sometimes have limited or no threat intelligence capabilities, especially for crimes that cross boundaries. Such a cooperative agenda notably leads to the crippling of organized crime in the digital underground.

While our threat research is primarily aimed at keeping our customers safe, the same information is vital in making a case against cybercriminals. Trend Micro will continue to tap into partnerships with law enforcement since these have been proved to lead to the elimination of criminal elements, which in turn makes the computing landscape a little safer.

# Full-ranged multilayered solutions best suited to today's threat landscape

Enterprises should view the specific protection challenges raised by the different security issues we saw in 2018 as evidence for the importance of a reexamined approach to security. Conducting business in the current landscape of rich, integrative, functional, convenient, and cost-efficient technologies has opened opportunities for expansion and progress. But it also broadens the attack surface and exposes networks to new risks. Security should thus always be an important consideration whenever a new initiative, such as cloud adoption or ICS modernization efforts, is undertaken, or whenever old ones are reviewed.

Multilayered solutions should be able to address most of the issues raised in this report. These comprise solutions that can help detect threats in gateways, networks, servers, and endpoints via a combination of detection technologies such as behavior monitoring, sandboxing, and intrusion prevention. Fileless threats, in particular, can be mitigated despite the lack of a discrete binary. For instance, network administrators should be alerted to even the most subtle irregularities in network traffic or even system registry that suggest the existence of an ongoing attack.

Social engineering is a topic that should be taken seriously as part of any company's culture, considering how crucial it is in the context of attacks by cybercriminals and other threat actors. Security awareness programs should be regularly implemented. Also, new habits should be inculcated through security drills, where employees are routinely tested regarding their level of caution in their everyday online activities.

Home users should take advantage of security technologies that can protect computers, tablets, smartphones, and other connected devices, and the data inside them. On top of that, they should change their passwords regularly, have unique passwords for different accounts, take advantage of multifactor authentication features whenever possible, and use a password management tool to help securely store credentials. Smart home administrators should also use security solutions that can block threats at the router level so that even devices connected to routers are protected.

## Threat Landscape in Review

In 2018, the Trend Micro™ Smart Protection Network™ infrastructure was able to protect users from over 48 billion threats — a multitude of email, file, and URL threat components.

**48,387,151,118**

Overall threats blocked in 2018

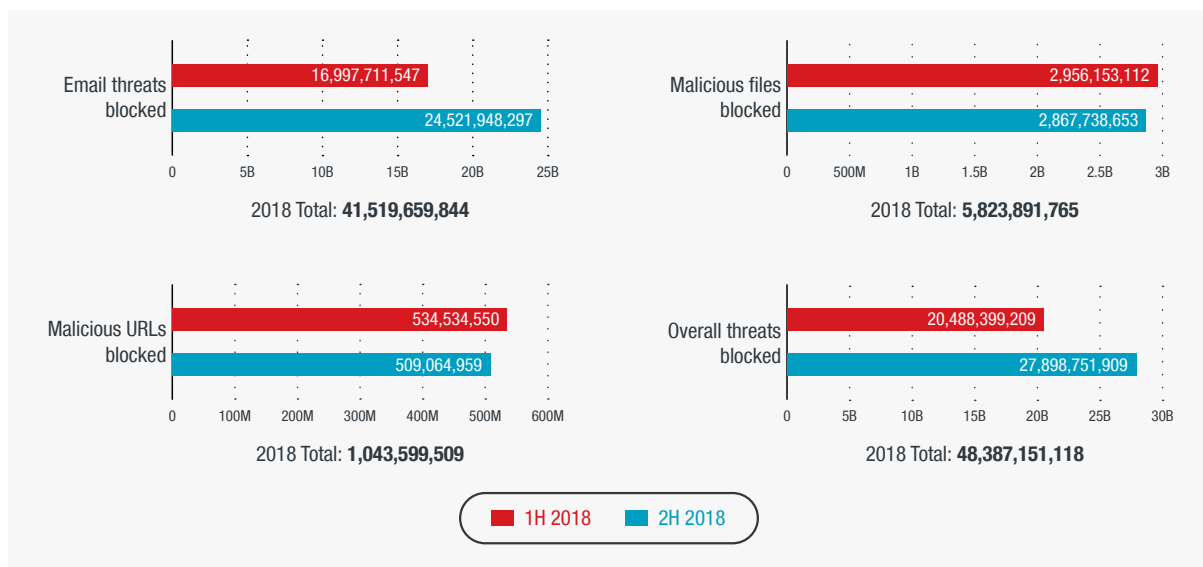


Figure 25. Email threats blocked increased: Half-year comparison of email, file, and URL threats blocked by the Trend Micro™ Smart Protection Network™ infrastructure

Ransomware threats might have declined overall, but new families were still being discovered. Many of these exhibited new behaviors or fine-tuned functionalities and improved on their predecessors.

ACKNYS	DEATHNOTE BATCH	GOODRABBIT	MINOTAUR	STINGER
ADAMLOCKER	DEDWARE	GRUJARSORIUM	MONEROPAY	STOP
ANIMUS	DEFENDER	GUILLOTINE	MRDEC	STUPJ
ANNABELLE	DELPHIMORIX	GUSLOCKER	NECNE	SURESOME
ARGUS	DESKLOCKER	HAKNATA	NEGOZI	SURI
ARMAGE	DESKTOP	HARROS	NIKSEAD	SYMMYWARE
AURORA	DEUSCRYPT	HAXLOCKER	NMCRYPT	SYSTEM
AUSIV	DGER	HEARTBLEED	NOTOPEN	TALINSLOCKER
AUTISMLOCKER	DIRCRYPT	HERMES	NOWORI	TBLOCKER

AUTOCRYPT	DISKDOC	HIDDENBEER	NOZELESN	TEARDROP
AVCRYPT	DISTRICT	HIGUNIEL	OUTSIDER	TEERAC
BANACRYPT	DONUT	HOLA	PABGEE	TERMITE
BHOOD	DOTZERO	HONOR	PACTELUNG	THANATOS
BIRBWARE	DWORRY	HORSUKE	PAIN	TK
BLACKEYE	DYAR	ICRYPT	PEDCOT	TQV
BLACKHEART	EBOLA	INSANECRYPT	PESQJ	TROLDESH
BLACKRUBY	ELGOSCAR	INSTALADOR	PEWDIEPIE	TRON
BLACKWORM	EMBRACE	ITBOOK	POSITIONFANG	USELESS
BLANK	ENCODER	JEFF	POTTIEQ	VAPOR
BLOODJAWS	ENYBENY	KASITOO	PYLOCKY	VBRSCARE
BORSCH	EOEO	KATYUSHA	RANCIDLOCKER	VENDETTA
BOSLOKI	EPAR	KCTF	RANDOMLOCKER	VERTUN
BYTELOCKER	EVERBE	KILLMBR	RAPID	VIBOROT
CARDSOME	EXOCRYPT	KILLRABBIT	RARA	WADHRAMA
CCP	FAKEKILLBOT	KINGBOROS	REDEYE	WANNAPEACE
CDLLM	FBLOCKER	KRAKATOWIS	RONT	WARRIOR
CESLOCKER	FILECODER	KRAKEN	RSAUTIL	WHITEROSE
CREAMPI	FILECRYPTOR	KYMER	RUSSENGER	WHOOPIE
CRISIS	FILEF	LADON	RYUK	WINLOCK
CRYAR	FILESLOCKER	LAZAGNECRYPT	SAR	WISE
CRYBRZ	FLKR	LEBANA	SATURN	WYVERN
CRYPT	FLYTERPER	LIGMA	SATWANCRYPT	XBASH
CRYPTG	FOREIGN	LILFINGER	SATYR	XEROWARE
CRYPTOLITE	FORMA	LIME	SEPSIS	XLOCKR
CRYPTOLOOT	FURY	MAFYA	SEUR	XUY
CRYPTOPAL	GAMEOVER	MAGICIAN	SHRUG	YAMI
CRYPTOR	GANDCRAB	MARYAH	SIGMA	ZENIS
CRYPWALKER	GANDCRYPT	MCRANSOM	SIGRUN	ZGAMES
CSGO	GARRANTYDECRYPT	MCRYPT	SKIDDY	ZLOCKER
CYPEN	GEGLOCKER	MEDUZA	SKULL	ZOLDON
CYRLOCKER	GERBER	MEGACRYPTOR	SKYFILE	ZYKA
CYSEARCHER	GHOST	MEINE	SNEAKYJ	ZZZ
DABLIO	GLOBIM	MIMICRY	SNOWPICNIC	
DATAKEEPER	GODCRYPT	MINDCRYPT	SOBACHKA	
DEADCRYPT	GOLDEN	MINDLOST	STACUS	

Table 3. 222 new ransomware families were seen:  
New ransomware families in 2018

Exploit kit activity was on the decline compared to 2017. Several exploit kits died out and only a few sprang up to replace them.

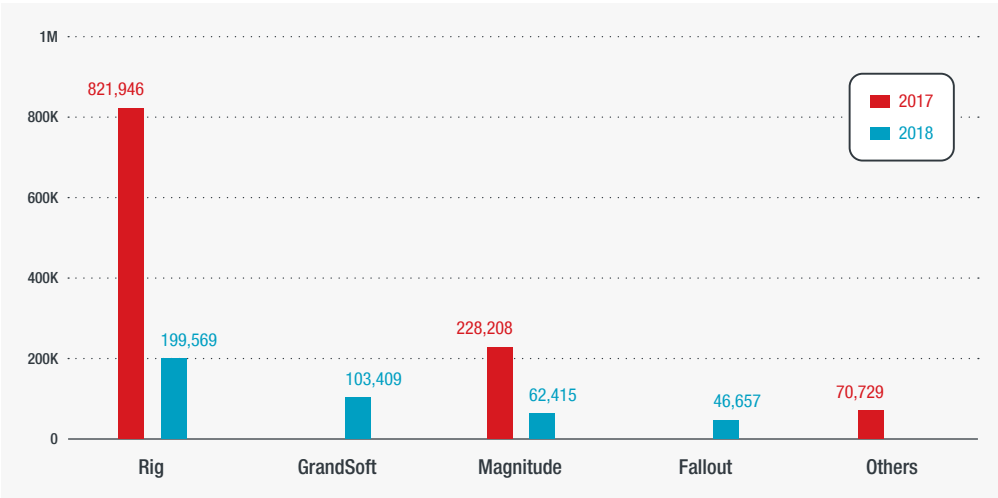


Figure 26. Rig and Magnitude remained active, as new exploit kits took over from inactive ones:  
Year-on-year comparison of exploit kit activity by exploit kit

XLS was still the most used file type for spam attachments in our dataset, with EXE (executable) files not far behind.

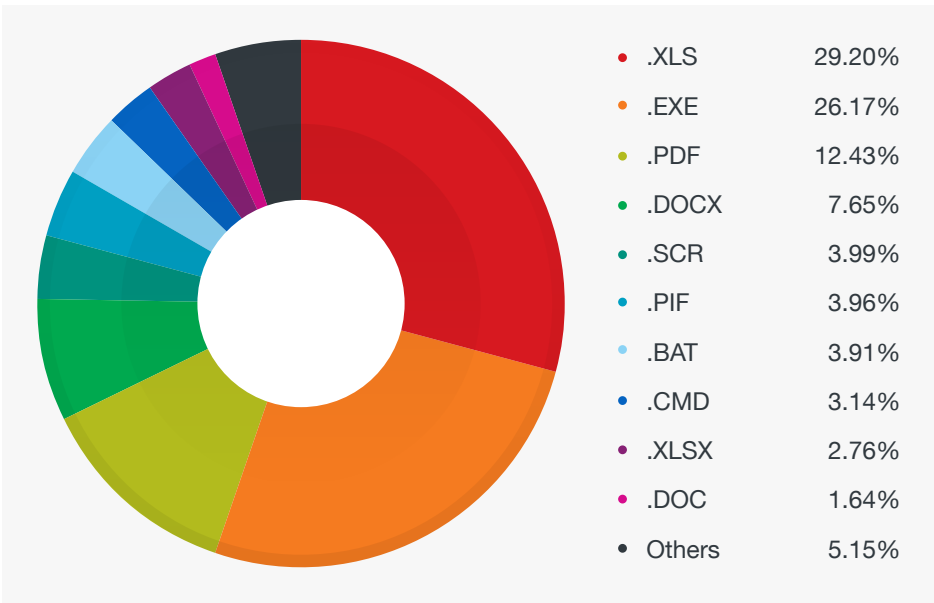


Figure 27. XLS and EXE were the most common file types in spam attachments:  
Distribution of file types used as attachments in spam in 2018

# References

1. Black Hat USA 2018. (June 2018). *Black Hat*. "The 2018 Black Hat USA Attendee Survey: Where Cybersecurity Stands." Last accessed on 28 January 2019 at <https://www.blackhat.com/docs/us-18/black-hat-intel-where-cybersecurity-stands.pdf>.
2. Black Hat Europe 2018. (November 2018). *Black Hat*. "The 2018 Black Hat Europe Attendee Survey: Europe's Cybersecurity Challenges." Last accessed on 28 January 2019 at [http://images.blackhat.com/Web/UBMAmericasTech/%7Bc0e36393-4267-48d4-b493-0c963173c732%7D\\_BH\\_EU18\\_Report.pdf](http://images.blackhat.com/Web/UBMAmericasTech/%7Bc0e36393-4267-48d4-b493-0c963173c732%7D_BH_EU18_Report.pdf).
3. Black Hat Asia 2018. (March 2018). *Black Hat*. "The 2018 Black Hat Asia Attendee Survey: Cybersecurity Risk in Asia." Last accessed on 28 January 2019 at [https://www.blackhat.com/docs/us-18/Cybersecurity\\_Risk\\_In\\_Asia.pdf](https://www.blackhat.com/docs/us-18/Cybersecurity_Risk_In_Asia.pdf).
4. Trend Micro. (11 December 2018). *Trend Micro*. "Mapping the Future: Dealing With Pervasive and Persistent Threats." Last accessed on 22 February 2019 at <https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2019>.
5. StatCounter. *Statcounter Global Stats*. "Operating System Market Share Worldwide, Jan-Dec 2013." Last accessed on 28 January 2019 at <http://gs.statcounter.com/os-market-share#monthly-201301-201312>.
6. Cathy Jett. (8 May 2018). *Fredericksburg.com*. "Hackers break into Fredericksburg school system's emails, file system." Last accessed on 28 January 2019 at [https://www.fredericksburg.com/news/local/fredericksburg/hackers-break-into-fredericksburg-school-system-s-emails-file-system/article\\_d2b4e537-83ae-5160-8d6c-bbccf705e75a.html](https://www.fredericksburg.com/news/local/fredericksburg/hackers-break-into-fredericksburg-school-system-s-emails-file-system/article_d2b4e537-83ae-5160-8d6c-bbccf705e75a.html).
7. Andy Mannix. (9 August 2018). *Star Tribune*. "Cyberattackers infiltrate Hennepin County workers' e-mails." Last accessed on 28 January 2019 at <http://www.startribune.com/cyber-attackers-infiltrate-hennepin-county-workers-e-mails/490508031>.
8. Unity Point Health. (2018). *Unity Point Health*. "Security Notice Frequently Asked Questions." Last accessed on 28 January 2019 at <https://www.unitypoint.org/security-faq.aspx>.
9. Jindrich Karasek. (10 May 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "New Phishing Scam Uses AES Encryption and Goes After Apple IDs." Last accessed on 28 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/new-phishing-scam-uses-aes-encryption-and-goes-after-apple-ids>.
10. Trend Micro. (5 June 2018). *Trend Micro Security News*. "SMiShing Attacks Leverage Punycode Technique." Last accessed on 28 January 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/smishing-attacks-leverage-punycode-technique>.
11. Erika Mendoza, Anjali Patil, and Jay Yaneza. (9 October 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Phishing Campaign Uses Hijacked Emails to Deliver URSNIF By Replying to Ongoing Threads." Last accessed on 28 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/phishing-campaign-uses-hijacked-emails-to-deliver-ursnif-by-replying-to-ongoing-threads/>.
12. Jill McCabe. (11 December 2018). *FBI*. "FBI Tech Tuesday: Business Email Compromise (BEC)-Gift Card Fraud." Last accessed on 28 January 2019 at <https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-tech-tuesday-business-email-compromise-bec-gift-card-fraud>.
13. Trend Micro. (13 May 2017). *Trend Micro Security News*. "WannaCry/WCRY Ransomware: How to Defend against It." Last accessed on 28 January 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/wannacry-wcry-ransomware-how-to-defend-against-it>.
14. Trend Micro. (6 December 2017). *Trend Micro Business Support*. "Preventing WannaCry (WCRY) ransomware attacks using Trend Micro products." Last accessed on 28 January 2019 at <https://success.trendmicro.com/solution/1117391-preventing-wannacry-wcry-ransomware-attacks-using-trend-micro-products>.

15. Andy Patrizio. (23 May 2017). *Network World*. "WannaCry was a Windows 7 Phenomenon." Last accessed on 28 January 2019 at <https://www.networkworld.com/article/3197762/microsoft-subnet/wannacry-was-a-windows-7-phenomenon.html>.
16. Russell Brandom. (15 May 2017). *The Verge*. "Is Microsoft to blame for the largest ransomware attacks in internet history?" Last accessed on 28 January 2019 at <https://www.theverge.com/2017/5/15/15641198/microsoft-ransomware-wannacry-security-patch-upgrade-wannacrypt>.
17. Trend Micro. (30 April 2018). *Trend Micro Security News*. "New GandCrab Variants, Varied Payloads Delivered via Spam Campaign." Last accessed on 28 January 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/new-gandcrab-variants-varied-payloads-delivered-via-spam-campaign>.
18. Trend Micro. (13 September 2018). *Trend Micro Security News*. "New Exploit Kit Fallout Delivering Gandcrab Ransomware." Last accessed on 28 January 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/new-exploit-kit-fallout-delivering-gandcrab-ransomware>.
19. Donald Castillo. (20 August 2018). *Trend Micro Security News*. ".EGG Files in Spam Delivers GandCrab v4.3 Ransomware to South Korean Users." Last accessed on 28 January 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/-egg-files-in-spam-delivers-gandcrab-v4-3-ransomware-to-south-korean-users>.
20. Charlie Osborne. (12 October 2018). *ZDNet*. "GandCrab ransomware operators team up with crypter service." Last accessed on 28 January 2019 at <https://www.zdnet.com/article/gandcrab-ransomware-teams-up-with-crypter-service/>.
21. Joseph C. Chen. (22 March 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Pop-up Ads and Over a Hundred Sites are Helping Distribute Botnets, Cryptocurrency Miners and Ransomware." Last accessed on 28 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/pop-up-ads-and-over-a-hundred-sites-are-helping-distribute-botnets-cryptocurrency-miners-and-ransomware/>.
22. Raphael Centeno. (1 May 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Legitimate Application AnyDesk Bundled with New Ransomware Variant." Last accessed on 28 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/legitimate-application-anydesk-bundled-with-new-ransomware-variant/>.
23. Raphael Centeno and Noel Llimos. (21 September 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Viro Botnet Ransomware Breaks Through." Last accessed on 28 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/virobot-ransomware-with-botnet-capability-breaks-through/>.
24. Ian Kenefick. (10 September 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "A Closer Look at the Locky Poser PyLocky Ransomware." Last accessed on 28 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/a-closer-look-at-the-locky-poser-pylocky-ransomware/>.
25. Joseph Chen. (9 August 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Ransomware as a Service Princess Evolution Looking for Affiliates." Last accessed on 28 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-as-a-service-princess-evolution-looking-for-affiliates/>.
26. Joseph Chen. (26 January 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Malvertising Campaign Abuses Google's DoubleClick to Deliver Cryptocurrency Miners." Last accessed on 28 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/malvertising-campaign-abuses-googles-doubleclick-to-deliver-cryptocurrency-miners/>.
27. Joseph Chen and Chaoying Liu. (4 April 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Cryptocurrency Web Miner Script Injected into AOL Advertising Platform." Last accessed on 28 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-web-miner-script-injected-into-aol-advertising-platform/>.
28. Joseph C Chen. (22 March 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Pop-up Ads and Over a Hundred Sites

are Helping Distribute Botnets, Cryptocurrency Miners and Ransomware.” Last accessed on 28 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/pop-up-ads-and-over-a-hundred-sites-are-helping-distribute-botnets-cryptocurrency-miners-and-ransomware/>.

29. Hubert Lin. (11 May 2018). *Trend Micro TrendLabs Security Intelligence Blog*. “Malicious Traffic in Port 7001 Surges as Cryptominers Target Patched 2017 Oracle WebLogic Vulnerability.” Last accessed on 28 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/malicious-traffic-in-port-7001-surges-as-cryptominers-target-patched-2017-oracle-weblogic-vulnerability/>.
30. Hubert Lin. (19 January 2018). *Trend Micro TrendLabs Security Intelligence Blog*. “Struts and DotNetNuke Server Exploits Used For Cryptocurrency Mining.” Last accessed on 28 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/struts-dotnetnuke-server-exploits-used-cryptocurrency-mining/>.
31. Joseph Chen. (30 April 2018). *Trend Micro TrendLabs Security Intelligence Blog*. “FaceXWorm Targets Cryptocurrency Trading Platforms, Abuses Facebook Messenger for Propagation.” Last accessed on 28 January 2018 at <https://blog.trendmicro.com/trendlabs-security-intelligence/facexworm-targets-cryptocurrency-trading-platforms-abuses-facebook-messenger-for-propagation/>.
32. Lorin Wu. (28 March 2018). *Trend Micro TrendLabs Security Intelligence Blog*. “Monero-Mining HiddenMiner Android Malware Can Potentially Cause Device Failure.” Last accessed on 28 January 2018 at <https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-hiddenminer-android-malware-can-potentially-cause-device-failure/>.
33. Trend Micro Cyber Safety Solutions Team. (21 March 2018). *Trend Micro TrendLabs Security Intelligence Blog*. “Cryptocurrency Miner Distributed via PHP Weathermap Vulnerability, Targets Linux Servers.” Last accessed on 28 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-miner-distributed-via-php-weathermap-vulnerability-targets-linux-servers/>.
34. Trend Micro. (19 November 2018). *Trend Micro TrendLabs Security Intelligence Blog*. “Outlaw Group Distributes Botnet for Cryptocurrency-Mining, Scanning, and Brute-Force.” Last accessed on 28 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/outlaw-group-distributes-botnet-for-cryptocurrency-mining-scanning-and-brute-force/>.
35. Jindrich Karasek and Loseway Lu. (26 June 2018). *Trend Micro TrendLabs Security Intelligence Blog*. “Cryptocurrency-Mining Bot Targets Devices With Running SSH Service via Potential Scam Site.” Last accessed on 28 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-mining-bot-targets-devices-with-running-ssh-service-via-potential-scam-site/>.
36. Janus Agcaoili and Gilbert Sison. (8 November 2018). *Trend Micro TrendLabs Security Intelligence Blog*. “Cryptocurrency-Mining Malware uses Various Evasion Techniques, Including Windows Installer, as Part of its Routine.” Last accessed on 28 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-mining-malware-uses-various-evasion-techniques-including-windows-installer-as-part-of-its-routine/>.
37. Trend Micro Cyber Safety Solutions Team. (26 July 2018). *Trend Micro TrendLabs Security Intelligence Blog*. “New Underminer Exploit Kit Delivers Bootkit and Cryptocurrency-mining Malware with Encrypted TCP Tunnel.” Last accessed on 28 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/new-underminer-exploit-kit-delivers-bootkit-and-cryptocurrency-mining-malware-with-encrypted-tcp-tunnel/>.
38. Don Ladores and Angelo Deveraturda. (17 April 2018). *Trend Micro TrendLabs Security Intelligence Blog*. “Ransomware XIAOBA Repurposed as File Infector and Cryptocurrency Miner.” Last accessed on 28 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-xiaoba-repurposed-as-file-infector-and-cryptocurrency-miner/>.
39. Gertrude Chavez-Dreyfuss. (29 January 2019). *Yahoo! Finance*. “Cryptocurrency thefts, scams hit \$1.7 billion in 2018: report.” Last accessed on 29 January 2019 at <https://finance.yahoo.com/news/cryptocurrency-thefts-scams-hit-1-7-billion-2018-143345592.html>.

40. Fernando Mercés. (May 2018). *Trend Micro Research*. "Cryptocurrency-Mining Malware in the Underground." Last accessed on 28 January 2019 at [https://documents.trendmicro.com/assets/research\\_brief\\_Cryptocurrency-Mining\\_Malware\\_in\\_the\\_Underground.pdf](https://documents.trendmicro.com/assets/research_brief_Cryptocurrency-Mining_Malware_in_the_Underground.pdf).
41. Marvin Cruz. (1 June 2017). *Trend Micro Security News*. "Security 101: The Rise of Fileless Threats that Abuse PowerShell." Last accessed on 28 January 2019 at <https://www.trendmicro.com/vinfo/us/security/news/security-technology/security-101-the-rise-of-fileless-threats-that-abuse-powershell>.
42. Trend Micro. (30 July 2018). *Trend Micro Security News*. "Fileless Malware PowerGhost Targets Corporate Systems." Last accessed on 28 January 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fileless-malware-powerghost-targets-corporate-systems>.
43. Buddy Tancio. (15 June 2017). *Trend Micro TrendLabs Security Intelligence Blog*. "Analyzing the Fileless, Code-injecting SOREBRECT Ransomware." Last accessed on 28 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/analyzing-fileless-code-injecting-sorebrect-ransomware/>.
44. Michael Villanueva. (2 August 2017). *Trend Micro TrendLabs Security Intelligence Blog*. "A Look at JS\_POWMET, a Completely Fileless Malware." Last accessed on 28 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/look-js-powmet-completely-fileless-malware/>.
45. Jai Vijayan. (10 May 2018). *Dark Reading*. "Author of TreasureHunter PoS Malware Releases Its Source Code." Last accessed on 28 January 2019 at <https://www.darkreading.com/vulnerabilities---threats/author-of-treasurehunter-pos-malware-releases-its-source-code-/d/d-id/1331778>.
46. Trend Micro. (3 January 2018). *Trend Micro Security News*. "Source Code of IoT Botnet Satori Publicly Released on Pastebin." Last accessed on 28 January 2019 at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/source-code-of-iot-botnet-satori-publicly-released-on-pastebin>.
47. Francis Antazo, Byron Gelera, Jeanne Jocson, Ardin Maglalang, and Mary Yambao. (25 August 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "New Open Source Ransomware Based on Hidden Tear and EDA2 May Target Businesses." Last accessed on 28 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/new-open-source-ransomware-based-on-hidden-tear-and-eda2-may-target-businesses/>.
48. Hubert Lin, Fyodor Yarochkin, and Alfredo Oliveira. (25 October 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Misconfigured Container Abused to Deliver Cryptocurrency-mining Malware." Last accessed on 28 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/misconfigured-container-abused-to-deliver-cryptocurrency-mining-malware/>.
49. Docker. *Docker Documentation*. "Secure Engine." Last accessed on 13 February 2019 at <https://docs.docker.com/engine/security/>.
50. Woody Leonhard. (9 January 2018). *Computer World*. "Microsoft yanks buggy Windows Meltdown/Spectre patches for AMD computers." Last accessed on 28 January 2019 at <https://www.computerworld.com/article/3246188/microsoft-windows/microsoft-yanks-buggy-windows-meltdown-spectre-patches-for-amd-computers.html>.
51. Claudio Canella, Jo Van Bulck, Michael Schwarz, Moritz Lipp, Benjamin von Berg, Philipp Ortner, Frank Piessens, Dmitry Evtushkin and Daniel Gruss. (13 November 2018). *ArXiv*. "A Systematic Evaluation of Transient Execution Attacks and Defenses." Last accessed on 28 January 2019 at <https://arxiv.org/pdf/1811.05441.pdf>.
52. Lily Hay Newman. (3 January 2019). *Wired*. "The Elite Intel Team Still Fighting Meltdown and Spectre." Last accessed on 29

January 2019 at <https://www.wired.com/story/intel-meltdown-spectre-storm/>.

53. Steven J. Vaughan-Nichols. (3 December 2018). *ZDNet*. "Kubernetes' first major security hole discovered." Last accessed on 29 January 2019 at <https://www.zdnet.com/article/kubernetes-first-major-security-hole-discovered/>.
54. Jordan Liggitt. (26 November 2018). *Github*. "CVE-2018-1002105: proxy request handling in kube-apiserver can leave vulnerable TCP connections." Last accessed on 28 January 2019 at <https://github.com/kubernetes/kubernetes/issues/71411>.
55. Trend Micro. (2 February 2018). *Trend Micro Security News*. "North Korean Hackers Allegedly Exploit Adobe Flash Player Vulnerability (CVE-2018-4878) Against South Korean Targets." Last accessed on 28 January 2019 at <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/north-korean-hackers-allegedly-exploit-adobe-flash-player-vulnerability-cve-2018-4878-against-south-korean-targets>.
56. Chris Williams. (9 May 2018). *The Register*. "It's 2018, and a webpage can still pwn your Windows PC – and apps can escape Hyper-V." Last accessed on 29 January 2019 at [https://www.theregister.co.uk/2018/05/09/microsoft\\_windows\\_hyperv\\_patch\\_tuesday/](https://www.theregister.co.uk/2018/05/09/microsoft_windows_hyperv_patch_tuesday/).
57. Trend Micro. (31 May 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Rig Exploit Kit Now Using CVE-2018-8174 to Deliver Monero Miner." Last accessed on 29 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/rig-exploit-kit-now-using-cve-2018-8174-to-deliver-monero-miner/>.
58. Charlie Osborne. (15 August 2018). *ZDNet*. "Microsoft Patch Tuesday: 60 vulnerabilities resolved including two active exploits." Last accessed on 29 January 2019 at <https://www.zdnet.com/article/microsoft-patch-tuesday-60-vulnerabilities-resolved-including-two-active-exploits/>.
59. Catalin Cimpanu. (12 November 2018). *ZDNet*. "Internet Explorer scripting engine becomes North Korean APT's favorite target in 2018." Last accessed on 29 January 2019 at <https://www.zdnet.com/article/internet-explorer-scripting-engine-becomes-north-korean-apt-favorite-target-in-2018/>.
60. Dustin Childs. (14 August 2018). *Zero Day Initiative*. "The August 2018 Security Update Review." Last accessed on 29 January 2019 at <https://www.zerodayinitiative.com/blog/2018/8/14/the-august-2018-security-update-review>.
61. Catalin Cimpanu. (9 October 2018). *ZDNet*. "Microsoft October 2018 Patch Tuesday fixes zero-day exploited by FruityArmor APT." Last accessed on 29 January 2019 at <https://www.zdnet.com/article/microsoft-october-2018-patch-tuesday-fixes-zero-day-exploited-by-fruityarmor-apt/>.
62. Trend Micro. (14 November 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "November Patch Tuesday Fixes Another Zero-Day Win32k Bug, Other Public Vulnerabilities." Last accessed on 29 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/november-patch-tuesday-fixes-another-zero-day-win32k-bug-other-public-vulnerabilities/>.
63. Trend Micro Smart Home Network and IoT Reputation Service Teams. (21 June 2018). *TrendLabs Security Intelligence Blog*. "Drupal Vulnerability (CVE-2018-7602) Exploited to Deliver Monero-Mining Malware." Last accessed on 29 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/drupal-vulnerability-cve-2018-7602-exploited-to-deliver-monero-mining-malware/>.
64. Catalin Cimpanu. (25 April 2018). *Bleeping Computer*. "Hackers Don't Give Site Owners Time to Patch, Start Exploiting New Drupal Flaw Within Hours." Last accessed on 29 January 2019 at <https://www.bleepingcomputer.com/news/security/hackers-dont-give-site-owners-time-to-patch-start-exploiting-new-drupal-flaw-within-hours/>.
65. Hubert Lin. (15 February 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Vulnerabilities in Apache CouchDB Open the Door to Monero Miners." Last accessed on 29 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/>

[vulnerabilities-apache-couchdb-open-door-monero-miners/](#).

66. Jan Lehnardt. (14 November 2017). *Apache Mail Archives*. "Viewing email #6c405bf3f8358e6314076be9f48c89a2e0ddf005... (and replies)." Last accessed on 29 January 2019 at <https://lists.apache.org/thread.html/6c405bf3f8358e6314076be9f48c89a2e0ddf00539906291ebdf0c67@%3Cdev.couchdb.apache.org%3E>.
67. Hubert Lin. (15 February 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Vulnerabilities in Apache CouchDB Open the Door to Monero Miners." Last accessed on 29 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/vulnerabilities-apache-couchdb-open-door-monero-miners/>.
68. Oracle Technology Network. (October 2017). *Oracle*. "Oracle Critical Patch Update Advisory - October 2017." Last accessed on 29 January 2019 at <https://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html>.
69. Johnlery Triunfante and Mark Vicente. (26 February 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Oracle Server Vulnerability Exploited to Deliver Double Monero Miner Payloads." Last accessed on 29 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/oracle-server-vulnerability-exploited-deliver-double-monero-miner-payloads/>.
70. Hubert Lin. (11 May 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Malicious Traffic in Port 7001 Surges as Cryptominers Target Patched 2017 Oracle WebLogic Vulnerability." Last accessed on 29 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/malicious-traffic-in-port-7001-surges-as-cryptominers-target-patched-2017-oracle-weblogic-vulnerability/>.
71. Veo Zhang. (29 March 2016). *Trend Micro TrendLabs Security Intelligence Blog*. "Critical 'CVE-2015-1805' Vulnerability Allows Permanent Rooting of Most Android Phones." Last accessed on 29 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/critical-cve-2015-1805-vulnerability-allows-permanent-rooting-android-phones/>.
72. Mobile Threat Response Team. (13 February 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "New AndroRAT Exploits Dated Privilege Escalation Vulnerability, Allows Permanent Rooting." Last accessed on 29 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/new-androrat-exploits-dated-permanent-rooting-vulnerability-allows-privilege-escalation/>.
73. Android. (18 March 2016). *Android*. "Android Security Advisory—2016-03-18." Last accessed on 29 January 2019 at <https://source.android.com/security/advisory/2016-03-18.html>.
74. Mobile Threat Response Team. (13 February 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "New AndroRAT Exploits Dated Privilege Escalation Vulnerability, Allows Permanent Rooting." Last accessed on 29 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/new-androrat-exploits-dated-permanent-rooting-vulnerability-allows-privilege-escalation/>.
75. CVE Details. (2018). *CVE Details*. "Browse Vulnerabilities by Date." Last accessed on 29 January 2019 at <https://www.cvedetails.com/browse-by-date.php>.
76. Dan Goodin. (21 October 2016). *Ars Technica*. "Most serious" Linux privilege-escalation bug ever is under active exploit (updated)." Last accessed on 29 January 2019 at <http://arstechnica.com/security/2016/10/most-serious-linux-privilege-escalation-bug-ever-is-under-active-exploit/>.
77. Robert Abel. (19 November 2018). *SC Magazine*. "DirtyCOW is back in backdoor attack targeting Drupal Web Servers." Last accessed on 29 January 2019 at <https://www.scmagazine.com/home/security-news/dirtycow-is-back-in-backdoor-attack-targeting-drupal-web-servers/>.
78. Zach Whittaker. (14 April 2017). *ZDNet*. "NSA's arsenal of Windows hacking tools has leaked." Last accessed on 29 January 2019 at <https://www.zdnet.com/article/shadow-brokers-latest-file-drop-shows-nsa-targeted-windows-pcs-banks/>.

79. Charlie Osborne. (17 September 2018). *ZDNet*. "Why the 'fixed' Windows EternalBlue exploit won't die." Last accessed on 29 January 2019 at <https://www.zdnet.com/article/why-the-fixed-windows-eternalblue-exploit-wont-die/>.
80. Zero Day Initiative. (2018). *Zero Day Initiative*. "Published Advisories." Last accessed on 29 January 2019 at <https://www.zerodayinitiative.com/advisories/published/2018/>.
81. Zero Day Initiative. (17 January 2019). *Zero Day Initiative*. "The ZDI 2018 Retrospective." Last accessed on 29 January 2019 at <https://www.thezdi.com/blog/2019/1/17/the-zdi-2018-retrospective>.
82. Garrett Graff. (18 September 2018). *Wired*. "The Mirai Botnet Architects are Now Fighting Crime with the FBI." Last accessed on 29 January 2019 at <https://www.wired.com/story/mirai-botnet-creators-fbi-sentencing/>.
83. Catalin Cimpanu. (28 October 2018). *ZDNet*. "Satori botnet author in jail again after breaking pretrial release conditions." Last accessed on 29 January 2019 at <https://www.zdnet.com/article/satori-botnet-author-in-jail-again-after-breaking-pretrial-release-conditions/>.
84. Trend Micro IoT Reputation Service Team. (11 April 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Mirai-like Scanning Activity Detected From China, With Targets in Brazil." Last accessed on 29 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/mirai-like-scanning-activity-detected-from-china-targets-in-brazil/>.
85. Trend Micro. (24 May 2018). *Trend Micro Security News*. "Reboot Your Routers: VPNFilter Infected Over 500,000 Routers Worldwide." Last accessed on 29 January 2019 at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/reboot-your-routers-vpnfilter-infected-over-500-000-routers-worldwide>.
86. Trend Micro. (28 August 2018). *Trend Micro Security News*. "Unseen Threats, Imminent Losses." Last accessed on 29 January 2019 at <https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/unseen-threats-imminent-losses>.
87. Joseph Chen. (11 December 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "New Exploit Kit 'Novidade' Found Targeting Home and SOHO Routers." Last accessed on 29 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/new-exploit-kit-novidade-found-targeting-home-and-soho-routers/>.
88. Trend Micro. (3 August 2018). *Trend Micro Security News*. "Over 200,000 MikroTik Routers Compromised in Cryptojacking Campaign." Last accessed on 29 January 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/over-200-000-mikrotik-routers-compromised-in-cryptojacking-campaign>.
89. Joseph Chen. (11 December 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "New Exploit Kit 'Novidade' Found Targeting Home and SOHO Routers." Last accessed on 29 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/new-exploit-kit-novidade-found-targeting-home-and-soho-routers/>.
90. Foo Yun Chee. (10 October 2018). *Reuters*. "Exclusive: EU privacy chief expects first round of fines under new law by year-end." Last accessed on 29 January 2019 at <https://www.reuters.com/article/us-eu-gdpr-exclusive/exclusive-eu-privacy-chief-expects-first-round-of-fines-under-new-law-by-year-end-idUSKCN1MJ2AY>.
91. Chris Foxx. (25 May 2018). *BBC News*. "Google and Facebook accused of breaking GDPR laws." Last accessed on 29 January 2019 at <https://www.bbc.com/news/technology-44252327>.
92. European Data Protection Board. (12 September 2018). *European Data Protection Board*. "First Austrian Fine: CCTV Coverage – Summary." Last accessed 29 January 2019 at [https://edpb.europa.eu/news/national-news/2018/first-austrian-fine-cctv-coverage-summary\\_en](https://edpb.europa.eu/news/national-news/2018/first-austrian-fine-cctv-coverage-summary_en).
93. Ionut Ilascu. (23 November 2018). *Bleeping Computer*. "First GDPR Sanction in Germany Fines Flirty Chat Platform EUR

- 20,000.” Last accessed on 29 January 2019 at <https://www.bleepingcomputer.com/news/security/first-gdpr-sanction-in-germany-fines-flirty-chat-platform-eur-20-000/>.
94. HIPAA Journal. (7 December 2018). *HIPAA*. “First Hospital GDPR Violation Penalty Issued: Portuguese Hospital to Pay €400,000 GDPR Fine.” Last accessed on 29 January 2019 at <https://www.hipaajournal.com/first-hospital-gdpr-violation-penalty-issued-portuguese-hospital-to-pay-e400000-gdpr-fine/>.
95. Trend Micro. (4 May 2018). *Trend Micro Security News*. “Australia’s Notifiable Data Breaches Scheme: Prelude to GDPR’s Data Breach Notification.” Last accessed on 29 January 2019 at <https://www.trendmicro.com/vinfo/us/security/news/online-privacy/australia-s-notifiable-data-breaches-scheme-prelude-to-gdpr-s-data-breach-notification>.
96. Trend Micro. (9 May 2018). *Trend Micro Security News*. “Canada to Impose Own Data Breach Notification Regulations.” Last accessed on 29 January 2019 at <https://www.trendmicro.com/vinfo/us/security/news/online-privacy/canada-to-impose-own-data-notification-regulations>.
97. Trend Micro. (2 April 2018). *Trend Micro Security News*. “UK’s Data Protection Bill: Beyond GDPR Compliance.” Last accessed on 29 January 2019 at <https://www.trendmicro.com/vinfo/us/security/news/online-privacy/uk-s-data-protection-bill-beyond-gdpr-compliance>.
98. Issie Lapowsky. (28 June 2018). *Wired*. “California Unanimously Passes Historic Privacy Bill.” Last accessed on 13 February 2019 at <https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill/>.
99. Trend Micro. (24 July 2018). *Trend Micro Security News*. “EU-JEPA Inked, Reciprocal Adequacy of Japan Data Protection Law and the GDPR Finalized.” Last accessed on 29 January 2019 at <https://www.trendmicro.com/vinfo/us/security/news/online-privacy/eu-jepa-inked-reciprocal-adequacy-of-japan-data-protection-law-and-the-gdpr-finalized>.
100. Stilgherrian. (2 September 2018). *ZDNet*. “Five Eyes governments get even tougher on encryption.” Last accessed on 29 January 2019 at <https://www.zdnet.com/article/five-eyes-governments-get-even-tougher-on-encryption/>.
101. Privacy Rights Clearinghouse. (2018). Privacy Rights Clearinghouse. “Data Breaches.” Last accessed on 15 January 2019 at <https://www.privacyrights.org/data-breaches>.
102. Daniel Ren. (29 August 2018). *South China Morning Post*. “Shanghai police investigate data leak of 130 million hotel clients available on dark web for 8 bitcoin.” Last accessed on 29 January 2019 at <https://www.scmp.com/business/companies/article/2161800/shanghai-police-investigate-data-leak-130-million-hotel-clients>.
103. Raymond Zhong. (25 October 2018). *The New York Times*. “Cathay Pacific Data Breach Exposes 9.4 Million Passengers.” Last accessed on 29 January 2019 at <https://www.nytimes.com/2018/10/25/business/cathay-pacific-hack.html>.
104. Trend Micro Forward-Looking Threat Research Team. (7 September 2018). *Trend Micro TrendLabs Security Intelligence Blog*. “Stolen Data from Chinese Hotel Chain and Other Illicit Products Sold in Deep Web Forum.” Last accessed on 29 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/we-uncovered-personally-identifiable-information-pii-stolen-from-a-china-based-hotel-chain-being-sold-on-a-deep-web-forum-we-were-monitoring/>.
105. Trend Micro. (2017). *Trend Micro Security News*. “Machine Learning.” Last accessed on 29 January 2019 at <https://www.trendmicro.com/vinfo/us/security/definition/machine-learning>.
106. Marco Balduzzi. (12 April 2018). *Trend Micro TrendLabs Security Intelligence Blog*. “Uncovering Unknown Threats With Human-Readable Machine Learning.” Last accessed on 29 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/uncovering-unknown-threats-with-human-readable-machine-learning/>.
107. Jon Oliver. (11 June 2018). *Trend Micro TrendLabs Security Intelligence Blog*. “How Machine Learning Techniques Helped Us

Find Massive Certificate Abuse by BrowseFox.” Last accessed on 29 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/how-machine-learning-techniques-helped-us-find-massive-certificate-abuse-by-browsefox/>.

108. Joy Nathalie Avelino, Jessica Patricia Balaquit, and Carmi Anne Loren Mora. (13 November 2018). *Trend Micro TrendLabs Security Intelligence Blog*. “Using Machine Learning to Cluster Malicious Network Flows From Gh0st RAT Variants.” Last accessed on 29 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/using-machine-learning-to-cluster-malicious-network-flows-from-gh0st-rat-variants/>.
109. Trend Micro. (9 August 2018). *Trend Micro TrendLabs Security Intelligence Blog*. “How Machine Learning Can Help Identify Web Defacement Campaigns.” Last accessed on 29 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/how-machine-learning-can-help-identify-web-defacement-campaigns/>.
110. Trend Micro. (16 April 2018). *Trend Micro Security News*. “Curbing the BEC Problem Using AI and Machine Learning.” Last accessed on 29 January 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/curbing-the-bec-problem-using-ai-and-machine-learning>.
111. Weimin Wu. (2 August 2018). *Trend Micro TrendLabs Security Intelligence Blog*. “Adversarial Sample Generation: Making Machine Learning Systems Robust for Security.” Last accessed on 29 January 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/adversarial-sample-generation-making-machine-learning-systems-robust-for-security/>.
112. Trend Micro. (5 April 2018). *Trend Micro Security News*. “Exposed Devices and Supply Chain Attacks: Overlooked Risks in Healthcare Networks.” Last accessed on 29 January 2019 at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/exposed-medical-devices-and-supply-chain-attacks-in-connected-hospitals>.
113. Trend Micro. (20 October 2018). *Trend Micro Security News*. “Critical Infrastructures Exposed and at Risk: Energy and Water Industries.” Last accessed on 29 January 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/exposed-and-vulnerable-critical-infrastructure-the-water-energy-industries>.
114. Trend Micro. (4 December 2018). *Trend Micro Security News*. “MQTT and CoAP: Security and Privacy Issues in IoT and IIoT Communication Protocols.” Last accessed on 29 January 2019 at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/mqtt-and-coap-security-and-privacy-issues-in-iiot-and-iiot-communication-protocols>.
115. Trend Micro. (16 May 2018). *Trend Micro Security News*. “The Rise and Fall of Scan4You.” Last accessed on 29 January 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-rise-and-fall-of-scan4you>.
116. Mathew J. Schwartz. (25 September 2018). *Information Security Group*. “Scan4You Operator Gets 14-Year Prison Sentence.” Last accessed on 29 January 2019 at <https://www.bankinfosecurity.com/scan4you-operator-gets-14-year-prison-sentence-a-11554>.
117. Trend Micro. (29 October 2018). *Trend Micro Security News*. “Evolution of Cybercrime.” Last accessed on 29 January 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/evolution-of-cybercrime>.



## **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)

