



# 2017 Annual Security Roundup: The Paradox of Cyberthreats

## 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.

# Contents

5

---

Ransomware brings about bigger global outbreaks despite fewer major players

10

---

Adaptable threats exploit known vulnerabilities in new ways

13

---

Amid growing awareness of the threat, BEC scams are still on the rise

16

---

Cryptocurrency's meteoric ascent inspires new mining malware and other threats

19

---

Cybercriminals abuse limited processing power of networked IoT devices

22

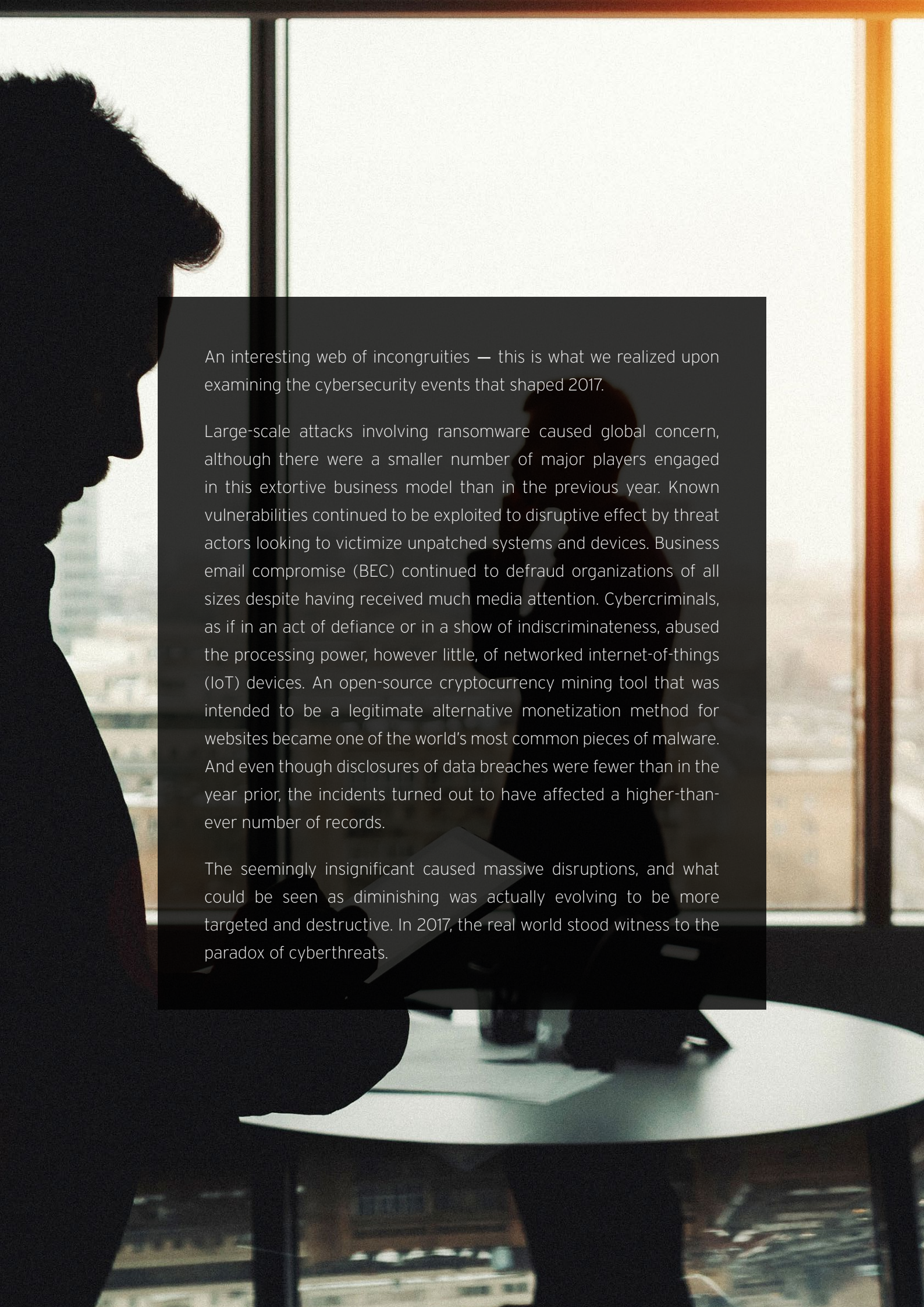
---

More enterprise records compromised in data breaches even as disclosures drop

25

---

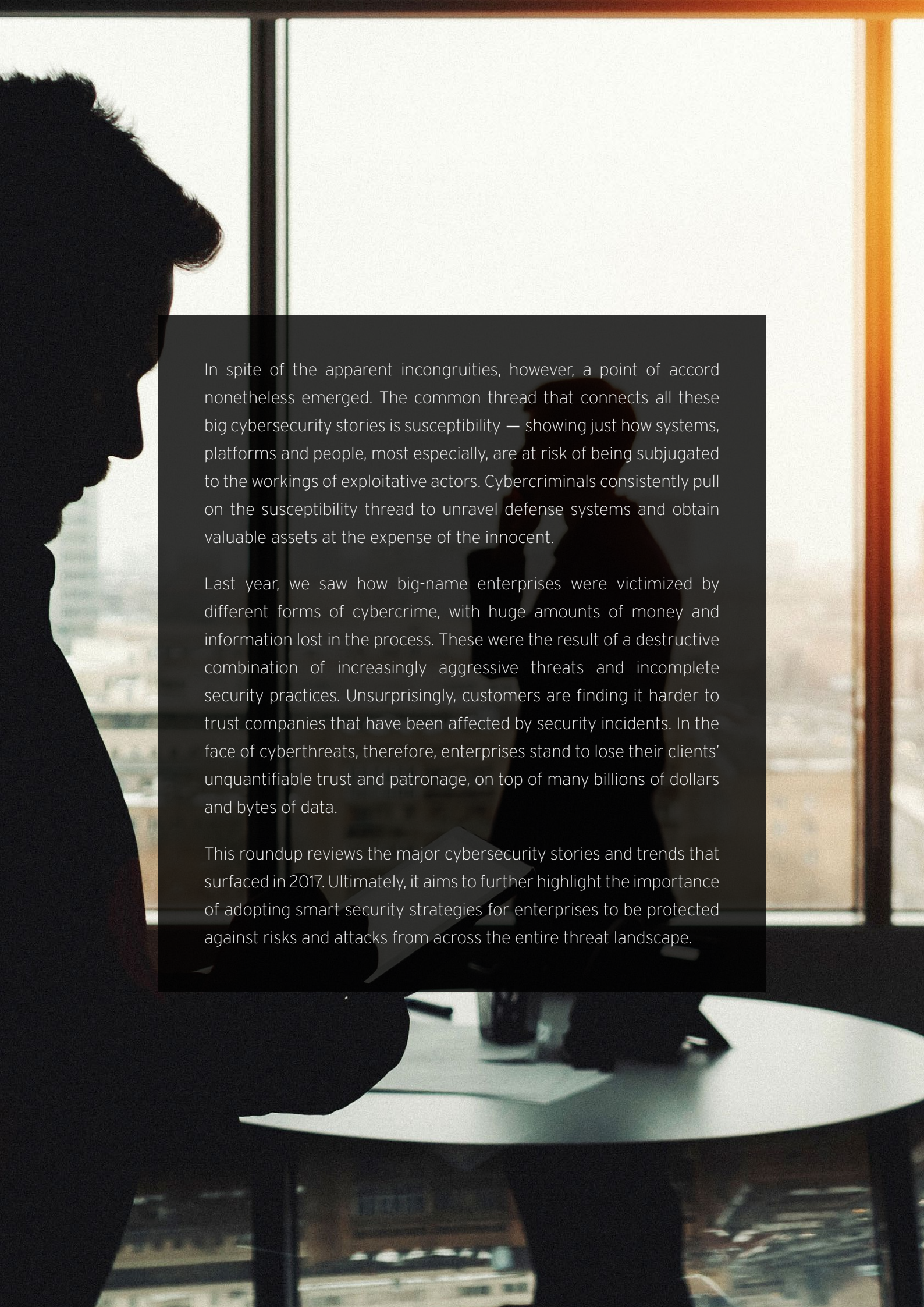
Threat Landscape in Review

A silhouette of a person's head and shoulders is visible on the left side of the image, looking out a large window. The window shows a blurred cityscape with buildings and a bright sky. The person is holding a tablet or laptop, which is partially visible in the foreground. The overall scene is dimly lit, with the primary light source being the window, creating a high-contrast silhouette effect.

An interesting web of incongruities — this is what we realized upon examining the cybersecurity events that shaped 2017.

Large-scale attacks involving ransomware caused global concern, although there were a smaller number of major players engaged in this extortive business model than in the previous year. Known vulnerabilities continued to be exploited to disruptive effect by threat actors looking to victimize unpatched systems and devices. Business email compromise (BEC) continued to defraud organizations of all sizes despite having received much media attention. Cybercriminals, as if in an act of defiance or in a show of indiscriminateness, abused the processing power, however little, of networked internet-of-things (IoT) devices. An open-source cryptocurrency mining tool that was intended to be a legitimate alternative monetization method for websites became one of the world's most common pieces of malware. And even though disclosures of data breaches were fewer than in the year prior, the incidents turned out to have affected a higher-than-ever number of records.

The seemingly insignificant caused massive disruptions, and what could be seen as diminishing was actually evolving to be more targeted and destructive. In 2017, the real world stood witness to the paradox of cyberthreats.

A silhouette of a man's head and shoulders is visible on the left side of the image, looking out a large window. The window shows a blurred cityscape with buildings and a bright sky. The overall lighting is warm and soft, suggesting an indoor setting during the day.

In spite of the apparent incongruities, however, a point of accord nonetheless emerged. The common thread that connects all these big cybersecurity stories is susceptibility — showing just how systems, platforms and people, most especially, are at risk of being subjugated to the workings of exploitative actors. Cybercriminals consistently pull on the susceptibility thread to unravel defense systems and obtain valuable assets at the expense of the innocent.

Last year, we saw how big-name enterprises were victimized by different forms of cybercrime, with huge amounts of money and information lost in the process. These were the result of a destructive combination of increasingly aggressive threats and incomplete security practices. Unsurprisingly, customers are finding it harder to trust companies that have been affected by security incidents. In the face of cyberthreats, therefore, enterprises stand to lose their clients' unquantifiable trust and patronage, on top of many billions of dollars and bytes of data.

This roundup reviews the major cybersecurity stories and trends that surfaced in 2017. Ultimately, it aims to further highlight the importance of adopting smart security strategies for enterprises to be protected against risks and attacks from across the entire threat landscape.

## Ransomware brings about bigger global outbreaks despite fewer major players

As the year drew to a close, it became more apparent just how ransomware changed the rules of the game.

As in the previous year, ransomware continued to be a substantial part of the cybersecurity narrative. Major outbreaks that caused global infections made headlines well into the year, proving that ransomware was still a burdensome threat for individuals and enterprises.

In the first half of 2017, we reported that ransomware growth had reached a plateau,<sup>1</sup> which matched our prediction for the year.<sup>2</sup> However, by year's end, there had been a 32-percent increase in the number of ransomware families from 2016 to 2017. But despite the increase, the number of major players for the year was considerably smaller compared to 2016. And this leaner number delivered a remarkable twist: A few of these major ransomware players were responsible for big, complex security threats, as evidenced by the highly disruptive WannaCry and Petya. Affecting victims on a global scale, these major ransomware families resulted in an estimated US\$5 billion in losses.<sup>3</sup>

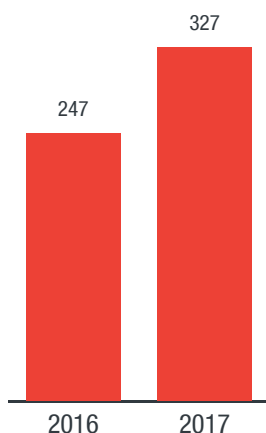


Figure 1. More ransomware families emerged in 2017: Comparison of total number of new ransomware families seen

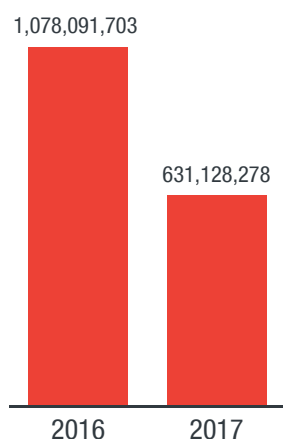


Figure 2. Fewer major players despite increase in new ransomware families: Comparison of total number of detected ransomware-related threats

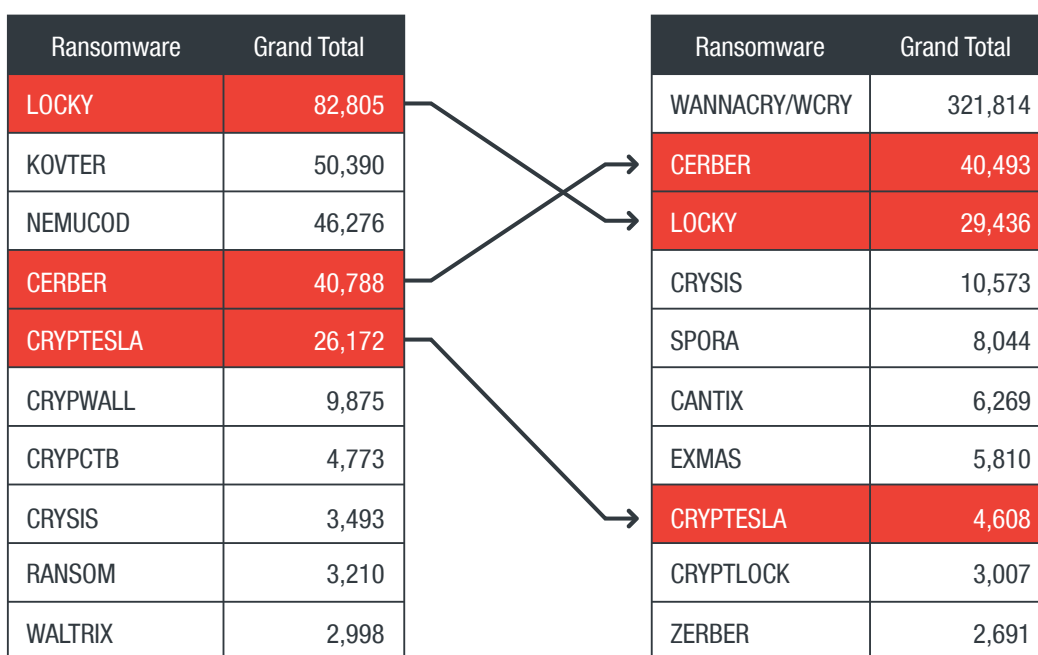


Figure 3. Prevailing ransomware families: Top ransomware families in 2017 remaining from 2016

A variant of WannaCry, detected by Trend Micro as RANSOM\_WANA.A and RANSOM\_WCRY.I, was one of the biggest ransomware threats that wreaked havoc to individuals and industries in 2017. Characterized by a self-propagating component, this new variant enabled the world’s first worm-based ransomware attack, which happened in mid-May.<sup>4</sup> Notably, it uses the EternalBlue exploit to take advantage of a vulnerability that was already patched by Microsoft in March.<sup>5</sup> WannaCry infected 300,000 computers in 150 countries within just a few days, encrypting files and demanding a ransom for their decryption.<sup>6</sup>

Overall, the total WannaCry detections towered over both Cerber and Locky, two of the biggest ransomware players in terms of longevity, and even the rest of the ransomware families combined. WannaCry dominated with 57 percent of ransomware detections in 2017, while the other ransomware families, Cerber and Locky trailed behind with 31 percent, 7 percent and 5 percent, respectively.

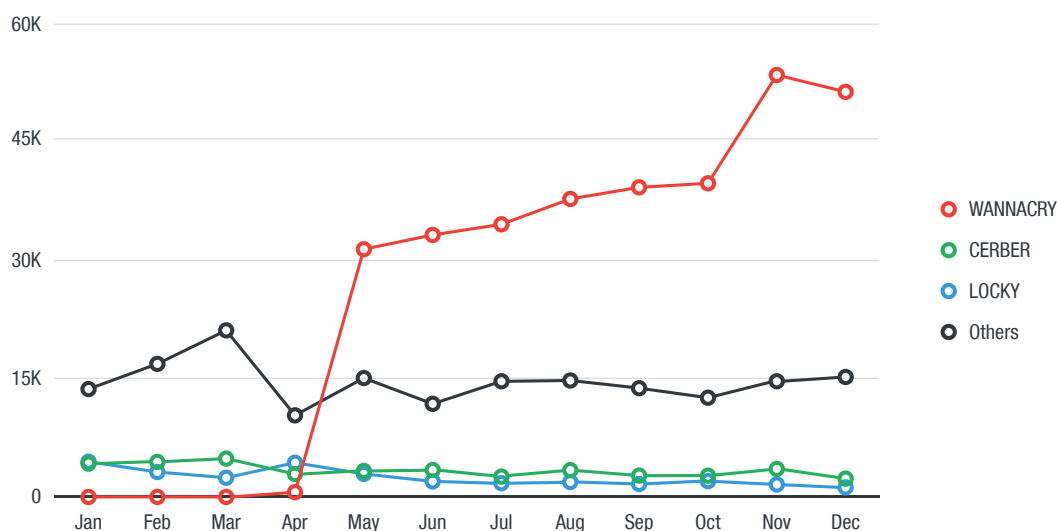


Figure 4. The upsurge of WannaCry in 2017: WannaCry detections based on data from the Trend Micro™ Smart Protection Network™ security infrastructure

Further aiding this self-propagating ransomware's proliferation were its finding a home in the underground market and its being sold for a surprisingly cheap amount, to boot. As uncovered by our researchers, upgradeable variants of WannaCry could already be bought for US\$50 in the Middle Eastern and North African (MENA) underground as early as two days after the ransomware's initial outbreak.<sup>7</sup> With cybercriminals having ready access to affordable ransomware, an increase in attacks is expected, especially since malware-as-a-service (MaaS) is considered the most widespread cyberattack commodity in the MENA underground.<sup>8</sup> It's important to note, however, that the affordability of ransomware in these circles is quite peculiar, and is due to a unique kinship shared by the threat actors.

Like WannaCry, Petya is no stranger to the threat scene. But a new variant of the ransomware, detected by Trend Micro as RANSOM\_PETYA.SMA, made big waves in 2017 due to its ability to modify or completely wipe system hard disks and its use of the dreaded blue screen of death as its display notification.<sup>9</sup>

The ransomware was first spotted in Ukraine, but soon spread to other countries, hitting a number of government departments, utility providers and businesses along the way.<sup>10</sup> By mid-2017, it was reported that Petya had infected more than 12,500 machines in 65 countries.<sup>11</sup>

In October, Eastern European companies awoke to a new ransomware attack. Bearing some resemblance to Petya, Bad Rabbit uses a propagation method involving fake Adobe Flash update installers from

compromised websites.<sup>12</sup> It spreads across the infected network by dropping and executing copies of itself using Windows Management Instrumentation (WMI) and Service Control Manager Remote Protocol.<sup>13</sup> It also propagates by means of Windows' Server Message Block (SMB) file sharing protocol; it tries to brute-force administrative shares and drops a copy of the malicious file there. Failing that, it uses EternalRomance to exploit an SMB vulnerability that was patched months before the attack.<sup>14</sup>

Earlier, in June, a new variant of Erebus hit the South Korean web hosting company Nayana, as attackers demanded a ransom of 550 bitcoins (US\$1.62 million at the time) in exchange for file decryption. Detected by Trend Micro as RANSOM\_ELFEREBUS.A, the ransomware infected 153 Linux servers and affected 3,400 business websites hosted by the company.<sup>15</sup>

The appearance of a new variant of Erebus that's aimed at Linux systems gave credence to our prediction that attack methods and targets would diversify in 2017.<sup>16</sup> Indeed, older kinds of ransomware resurfaced in the year armed with new techniques, having evolved into bigger, more disruptive threats in a short amount of time.

Cerber, detected by Trend Micro as RANSOM\_CERBER family, proved to be one of the fastest evolving threats of the year, having gone through a number of separate versions with variations in its routines.<sup>17</sup> In March, Cerber was discovered to have been upgraded with a new loader that was apparently designed to evade detection by pre-execution machine learning solutions.<sup>18</sup> Then, in August, a Cerber variant, detected by Trend Micro as RANSOM\_HPCERBER.SMALY5A, was found stealing wallet files from cryptocurrency wallet applications as well as saved passwords from web browsers such as Google Chrome, Internet Explorer and Mozilla Firefox.<sup>19</sup> All these evolutionary tactics contribute to Cerber's being regarded as the highest performing ransomware in the market for 2017.<sup>20</sup>

Locky, detected by Trend Micro as RANSOM\_LOCKY family, also managed to evolve with new campaigns. The variety of Locky's propagation methods extended to fake voicemail email notifications with malicious files or links,<sup>21</sup> bogus invoice emails bearing ransomware-ridden HTML attachments,<sup>22</sup> and stealthier tactics such as applying key technical changes in its attack method using encrypted dynamic link libraries (DLLs).<sup>23</sup> Another campaign involved the distribution of Locky alongside another ransomware called FakeGlobe and affected users in more than 70 countries.<sup>24</sup> In one of the ransomware's largest campaigns yet, a new Locky variant was distributed using 23 million weaponized emails in just 24 hours.<sup>25</sup>

Last year also showed how threats diversified to incorporate different attack routines, such as having fileless characteristics. Sorebrect, detected by Trend Micro as RANSOM\_SOUREBRECT.A and RANSOM\_SOUREBRECT.B, is a good case in point: a fileless ransomware that injects malicious code into a legitimate system process to encrypt files. This stealthy threat even goes as far as deleting event logs and other items that can lead to its being traced. It had affected different industries, including manufacturing, technology and telecommunications, in at least nine countries by the start of May.<sup>26</sup>



Year on year, ransomware-related threats also made a further move toward the email format. This is not surprising, given that spam has long been a preferred propagation mechanism among threat actors.

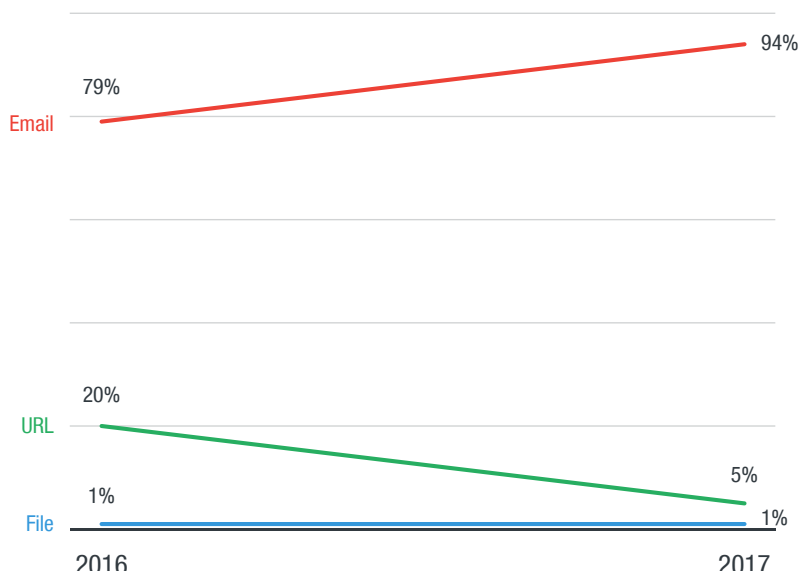


Figure 5. Email continued its ransomware reign: Comparison of ransomware-related threats between 2016 and 2017

Such shifts in the ransomware scene highlight how cybercriminals are quick to change gears, evolving threats with new tactics, techniques and procedures (TTPs) in hopes of taking in bigger hauls. As these threats continue to change courses and become harder to detect by traditional means, the importance of reliable security solutions is further underscored. Individuals and enterprises alike need a multilayered approach to threat protection, keeping data secure from the endpoint to the cloud in real time.

## Adaptable threats exploit known vulnerabilities in new ways

In April, the Shadow Brokers hacker group, which had carried out a data dump in 2016, further enabled the exploitation of major vulnerabilities in systems, networks and firewalls with another leak that included hacking tools from the National Security Agency (NSA). Some of the exploits from this leak, including EternalBlue and EternalRomance, were used in last year's major threat campaigns, most notably the WannaCry, Petya and Bad Rabbit ransomware attacks.

Later in the year, a known vulnerability was notably exploited to attack an ever expanding mobile user base. Dirty COW (CVE-2016-5195), a privilege-escalation vulnerability that provides attackers with root access to targeted systems, was first disclosed in October 2016<sup>27</sup> and found the following December on upstream Linux platforms like Redhat and on Android, which has a Linux-based kernel.<sup>28</sup> In 2017, our researchers discovered the first malware to exploit the vulnerability on Android: ZNIU, detected by Trend Micro as ANDROIDOS\_ZNIU. By the time it was discovered, the malware had affected at least 5,000 users in more than 40 countries, hidden as it was inside more than 1,200 malicious apps.<sup>29</sup>

This is not to say, though, that older vulnerabilities were out of the picture in 2017 — quite the contrary. For one thing, it was reported last year that around 200,000 unpatched systems were still susceptible to the Heartbleed vulnerability, which had been around since April 2014.<sup>30</sup>

We also reported that Downad, detected by Trend Micro as DOWNAD family and also known as Conficker, which first made news in 2008, was far from gone and was actually one of the top detections last year. As in 2016, the worm, a variant of which exploits the nine-year-old CVE-2008-4250 vulnerability, showed a strong monthly detection count of at least 20,000 in 2017.<sup>31</sup>

With the help of over 3,000 independent researchers who contribute to the Zero Day Initiative (ZDI) program, we discovered and disclosed 1,008 new vulnerabilities in 2017. Of these, we noted an increase in vulnerabilities for Adobe, Google and Foxit products, but a decrease in those for Apple and Microsoft products in 2017, compared to the previous year. Regardless of the direction the numbers took, however, the fact remains that vulnerabilities are being continuously discovered and thus are permanent security risks that enterprises in particular should always be heedful to. That the aforementioned products are in wide use

in offices and similar environments and on internet-of-things (IoT) devices and systems makes it all the more imperative for enterprises to implement security strategies that include measures against threats that take advantage of vulnerabilities.

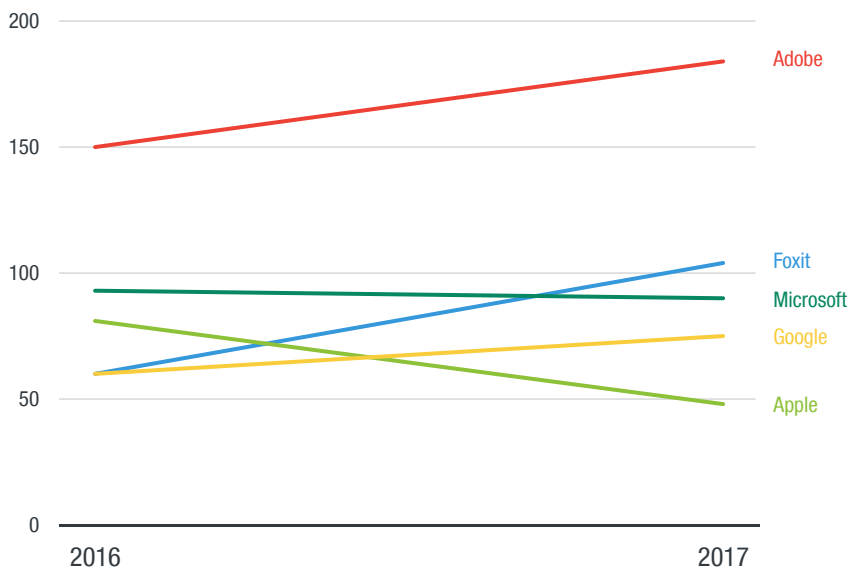


Figure 6. A variation in vulnerability count direction: Comparison of number of vulnerabilities found per vendor between 2016 and 2017

With ZDI’s contributing researchers, we also found that the vulnerability count for supervisory control and data acquisition (SCADA) systems dropped to 144 last year from 177 in 2016 — a 19-percent decrease. However, there was a steep rise in zero-day vulnerabilities between 2016 and 2017. Zero-day vulnerabilities increased 98 percent from 2016, and all but six of these were SCADA-related. Zero-day vulnerabilities related to SCADA surged from 46 in 2016 to 113, a 146-percent jump.

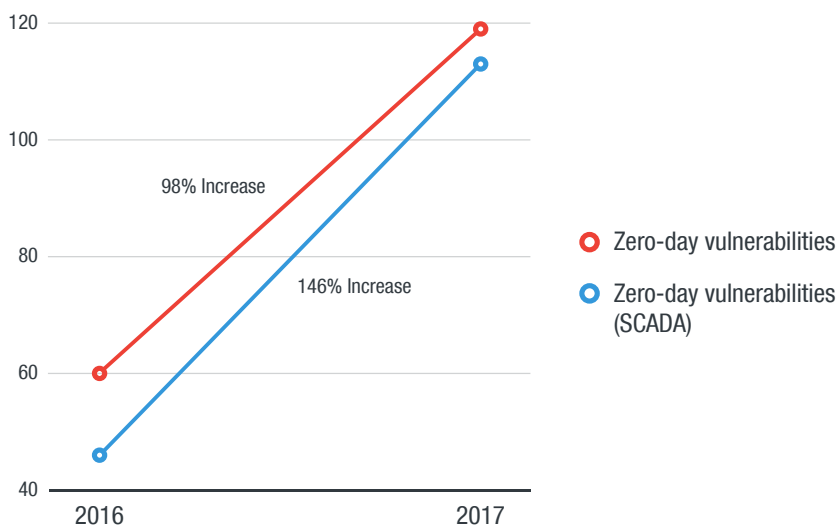


Figure 7. A marked increase in zero-day vulnerabilities: Comparison of number of zero-day vulnerabilities and SCADA-related zero-day vulnerabilities between 2016 and 2017

The past year demonstrated how threat actors are constantly on the prowl for weaknesses in systems and devices, as these serve as gateways to potentially lucrative exploits. Cybercriminals actively look for flaws to take advantage of in order to gain access and escalate privileges in systems, as well as to conduct denial-of-service attacks. These system and device vulnerabilities leave enterprises especially exposed to potential breaches and ripe for profiteering. In particular, organizations that continue to use outdated and unsupported operating systems and applications — ones that no longer receive vulnerability patches and other updates — are easier marks for threat actors.

As more and more vulnerabilities are uncovered and exploited, enterprises will benefit from strong anti-malware and threat security solutions. With proactive virtual patching, critical systems, especially legacy ones, will be kept protected. A blended approach is best to mitigate the effects of threats brought about by a growing number of vulnerability exploits across different platforms.

## Amid growing awareness of the threat, BEC scams are still on the rise

Business email compromise (BEC) had been far from obscure for quite some time. Even so, the scheme continued to siphon huge amounts of money off unsuspecting employees and executives.

2017 proved to be another busy year for fraudsters engaged in the con. In fact, our data shows that in 2017 alone, bids at BEC scams jumped a whopping 106 percent from the first half of the year to the second.

We were on the mark when we predicted that BEC, given its relative simplicity, would gain more traction with cybercriminals in 2017.<sup>32</sup> BEC incidents cost companies billions of dollars, a huge jump from the previous year's numbers. BEC scams had been so effective that it had been dubbed "the 5 billion dollar scam" by the Federal Bureau of Investigation (FBI), which reported in May that global BEC losses since 2013 had reached US\$5.3 billion<sup>33</sup> — US\$2.3 billion more than the cumulative losses reported by the FBI in June 2016.<sup>34</sup>

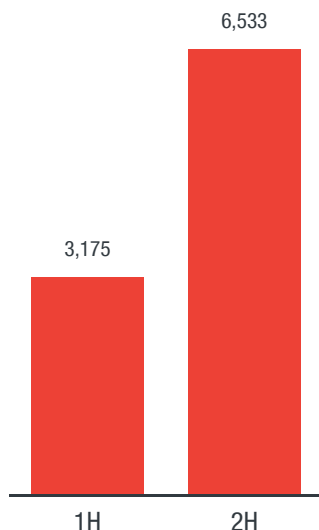


Figure 8. BEC attempts more than doubled in the second half of the year over the first half: Comparison of BEC attempts between 1H and 2H of 2017

The threat of BEC persisted even though it had gotten considerable attention in the press. In April, a supplier swindle story proved that even tech companies could fall prey to social engineering tactics, including the likes of Google and Facebook. It was reported then that the two tech giants had been defrauded of over US\$100 million by a man who allegedly used falsified invoices and convinced both companies that he was part of a partner manufacturing company. Fortunately, most of the losses for both companies were promptly recouped after the incident.<sup>35</sup>

In July, Germany’s national cybersecurity agency warned 5,000 possible targets and the general public about a BEC scam that had already victimized firms in the country using fraudulent memos and caused millions of euros in losses.<sup>36</sup> In October, it became apparent that even real estate could be fertile ground for BEC: Fraudsters were reported to have been impersonating people associated with title companies and bilking homebuyers of their down payments.<sup>37</sup>

A month later, reports surfaced of an email-based scam that had been tricking art galleries in the U.K. and the U.S. with tampered invoices and that had cost some dealers hundreds of thousands of pounds.<sup>38</sup> And in December, an Asian transportation company lost US\$3.4 million dollars in a BEC scam. The company failed to verify fake payment requests it received for vehicle leasing and other services, and proceeded to wire payments straight to fraudulent accounts.<sup>39</sup>

We reported that for the first half of the year, the most spoofed position was the chief executive officer (CEO), while the most targeted one was the chief financial officer (CFO). For the second half, the numbers reported the same story.

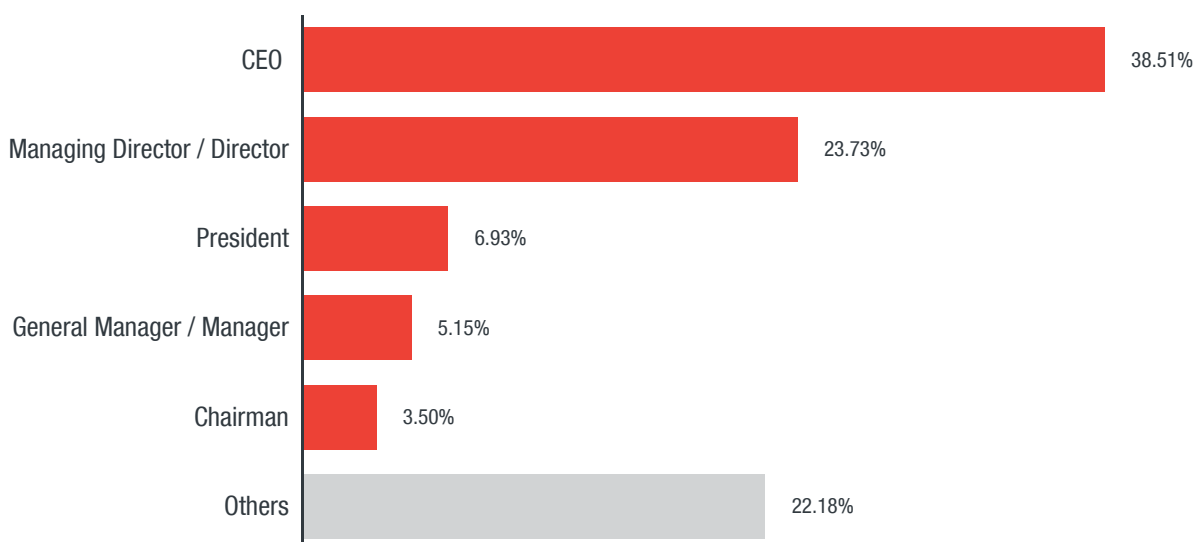


Figure 9. CEO emerged as most spoofed by cybercriminals: Percentage of BEC attack attempts that spoofed specific positions in 2017

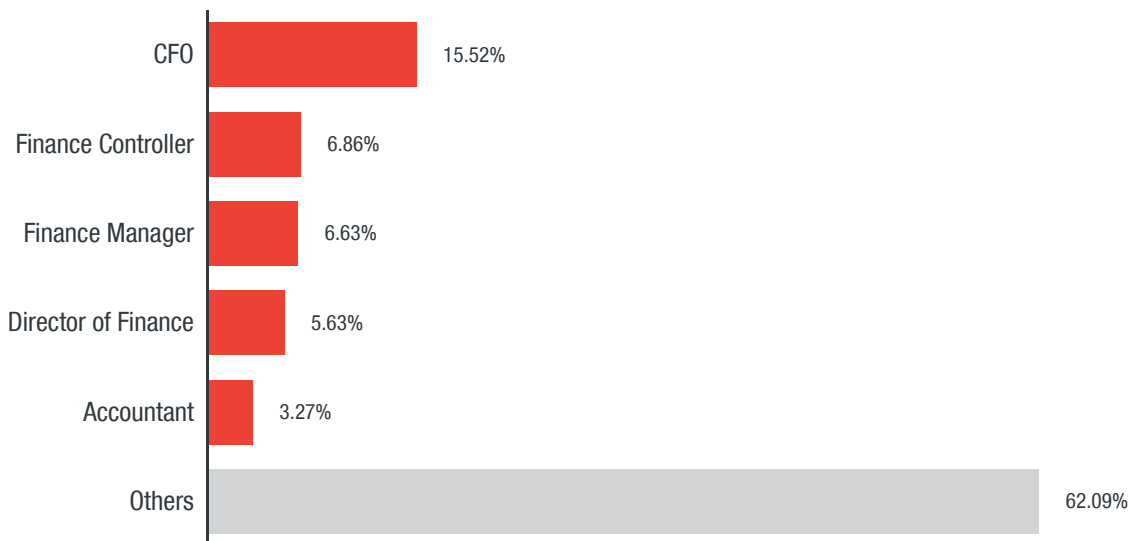


Figure 10. CFO remained the most targeted position: Percentage of BEC attack attempts that targeted specific positions in 2017

As threat actors continue to refine the social engineering tactics they use for financially motivated schemes, companies of all sizes need to beef up their cybersecurity practices. Educating executives and employees of all levels on how to effectively distinguish BEC scams and using security solutions that protect from spam and spear-phishing attempts are a company’s best defense against this growing, costly threat. It is also recommended to implement a multi-factor verification system for financial requests so as to spot scams before any money is paid out.

## Cryptocurrency's meteoric ascent inspires new mining malware and other threats

The popularity of cryptocurrency has sparked the interest of a global user base. And as the number of followers and adopters multiplies, so do the threats that aim to exploit it.

Cryptocurrency took the world by storm last year, as evidenced by the peaking of the value of bitcoin at US\$19,783.21 before the year came to a close.<sup>40</sup> More individuals, organizations<sup>41, 42, 43</sup> and even governments<sup>44, 45</sup> started adopting the use of certain cryptocurrencies as a legal payment method. And this quick rise to fame has prompted cybercriminals to jump in and make a profit through illicit means.

In some instances, they carry out heists on cryptocurrency exchanges, or online platforms where cryptocurrencies are bought and sold — as in the case of Youbit in South Korea, which was forced to shut down in December after being hacked twice in just eight months.<sup>46</sup> In others, they are given to mining cryptocurrency on the sly on victimized machines.



Figure 11. Various cryptocurrency attack methods: How attackers targeted cryptocurrency in 2017



Last year, attackers targeted mobile devices using Google Play apps with malicious cryptocurrency mining capabilities. To avoid detection, these cryptocurrency-mining apps, detected as ANDROIDOS\_JSMINER and ANDROIDOS\_CPUMINER, use JavaScript loading and native code injection.<sup>47</sup>

Cryptocurrency malware did not spare social media either. In December, we found a new cryptocurrency-mining bot, which we called Digmine, spreading through Facebook Messenger. Posing as a video file, the Monero-mining bot stays in a victim's machine for as long as possible to gain the highest possible amount of cryptocurrency.<sup>48</sup>

Variants of malware that had previously been used for other forms of cybercrime also sprang up to mine cryptocurrencies. Retadup, previously found in Israeli hospitals, was reported to have been using the available computing power of its infected machines for mining purposes.<sup>49</sup>

It should not be mistaken, however, that cryptocurrency mining per se is illegal. Coinhive, for example, is an open-source platform that allows companies to earn Monero cryptocurrency through their websites. But threat actors have been quick to abuse the programming of the platform for their own gain.

In November, an abused variant of the Coinhive miner ranked as the sixth most common malware in the world<sup>50</sup> — proof that this alternative to web advertising platforms is not exempt from corruption. Also last year, we discovered that the EITest campaign used tech support scams to deliver Coinhive's cryptocurrency miner.<sup>51</sup>

The rise of cryptocurrency mining is reflected in our own data, which shows a marked increase in mining detections in 2017 — especially in the last quarter, when it accounted for even more detections than the widely publicized WannaCry ransomware. This proves that mining tools, whether malicious or not, have indeed become prevalent.

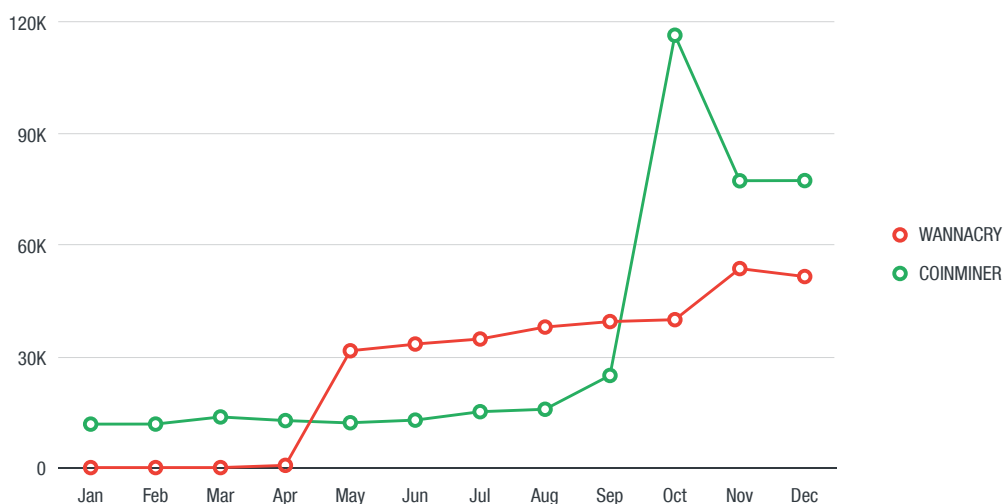


Figure 12. Rise in mining detections: Comparison between monthly detections of mining tools and WannaCry ransomware in 2017 based on data from the Trend Micro Smart Protection Network security infrastructure

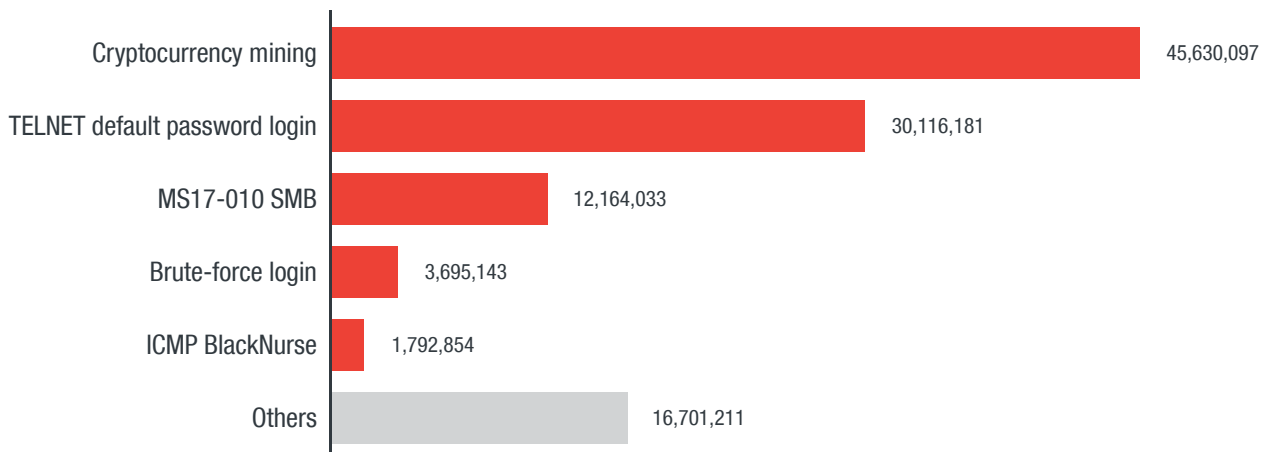
More countries and businesses are opening their doors to cryptocurrency as a virtual sort of legal tender. It is therefore important to be secure against the threats it can bring. Enterprises and government organizations must have security solutions that blend traditional protections with newer, more advanced approaches. An all-in-one solution that effectively incorporates machine learning technology, behavior monitoring, application control, web and mobile security, and email protection can mitigate the impact of cryptocurrency-related threats.

## Cybercriminals abuse limited processing power of networked IoT devices

With 20.3 billion connected devices in 2017 alone,<sup>52</sup> it's safe to say that the internet of things (IoT) is more than just a buzzword. The opportunities for operational efficiency and productivity it affords individuals, enterprises and even entire cities are seemingly endless. This is probably why threat actors are quick to find ways to exploit the interconnectedness of such devices for their nefarious ends.

The Mirai botnet attack is an example of how connected devices can be corrupted for ill purposes. In 2016, it managed to infect unsecure connected devices and use them to take down major websites such as Twitter and Netflix via massive distributed denial-of-service (DDoS) attacks.<sup>53</sup> Variants of Mirai soon surfaced later in the year, including one that attacked 900,000 home routers provided by Deutsche Telekom.<sup>54</sup> Within just a few hours on Nov. 29 last year, a new Mirai campaign detected in South American and North African countries was found to be responsible for 371,640 attack attempts coming from around 9,000 unique IP addresses.<sup>55</sup>

Interestingly, data for the network events in 2017 from the Trend Micro™ Smart Home Network solution shows that the trend for IoT has gone a different route. Rather than focusing on DDoS attacks, cybercriminals have started eyeing IoT devices for cryptocurrency mining.



*Note: The cryptocurrency mining activities and WannaCry-related events were seen mostly on desktops and laptops. The other events were attempts at harnessing IoT devices for botnets — cybercriminals tried to use default passwords to access devices or attempted brute force logins.*

Figure 13. Cryptocurrency mining and TELNET events outnumbered others: Network events in 2017 based on data from the Trend Micro™ Smart Home Network solution

The processing power of small IoT devices is limited, and so is the likelihood of individual devices being able to produce substantial amounts of cryptocurrency. However, to maximize their return on investment, cybercriminals zombify large numbers of these devices to mine cryptocurrency. This process involves computational tasks that are extremely demanding on a system’s resources, and hence too demanding for the finite processing power of IoT devices such as smartphones, IP cameras and smart TVs.

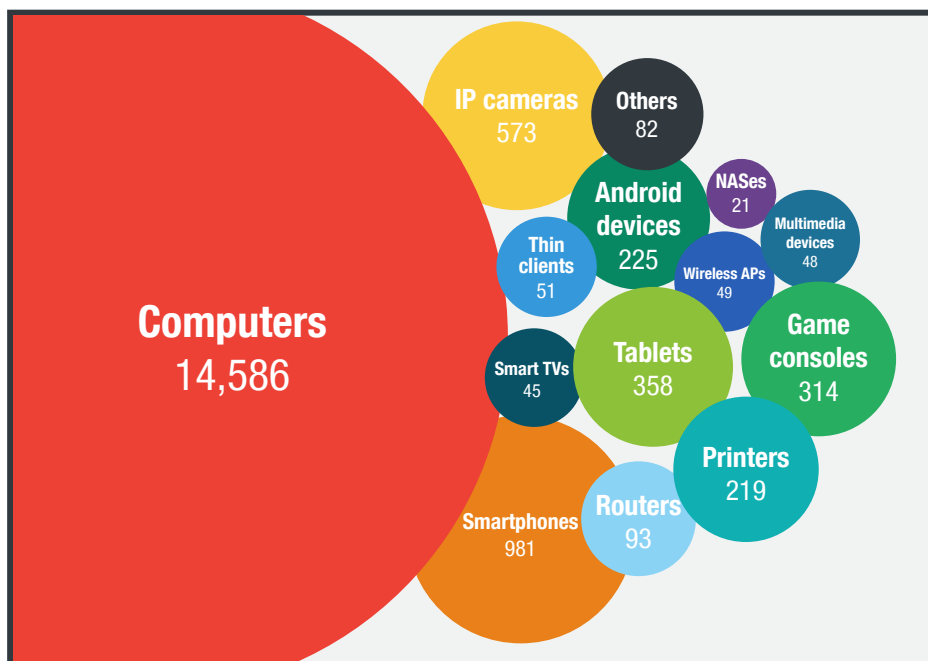


Figure 14. Computers eclipsed other cryptocurrency mining devices: Devices where cryptocurrency mining events were seen in 2017

However, it's important to note that TELNET login-related events far outnumbered the events related to the SMB vulnerability that the WannaCry ransomware exploited. Despite the WannaCry ransomware causing a worldwide stir, the IoT botnet-related events affected more devices — something enterprises should pay careful consideration to.

To further underscore the importance of security by design, we spearheaded IoT case studies on the security gaps in internet-connected speakers<sup>56</sup> and a covert, vendor-neutral car hack that is currently indefensible by modern car security technology.<sup>57</sup> These studies, which involve major companies, highlight just how vulnerable connected devices are to attacks and provide vital security insights for manufacturers of all types of IoT devices.

And as technologies continue to reach new frontiers, we foresee more attacks waged against the vulnerabilities of connected devices, such as those in intelligent transportation systems (ITS).

ITS continues to break new ground in providing convenience and in saving time, resources and money. This innovative use of internet-connected transport systems makes commuting and, ultimately, lives better. Transportation systems are swiftly becoming agile and conjoined. In the near future, connected vehicles will cruise alongside self-driving cars down so-called smart roads, and cybercriminals will go the extra mile to put the systems that depend on this progressive undertaking to a screeching halt.

Last year, we reported on the possible physical, wireless and over-the-network attacks that can affect ITS.<sup>58</sup> The methods for ITS attacks can spring from the seemingly trivial — such as traffic cameras, payment kiosks and even emission or air quality sensors<sup>59</sup> — and the attacks can cause not just economic damage to ITS providers and telecommunications companies, but also to the many businesses that rely upon the affected services. This risk sits just below the most damaging impact ITS threats pose: the endangerment of commuters' lives.

Given the IoT attacks that have occurred and that loom in the horizon, enterprises need to be protected against business disruptions to machines used in critical operations. Aside from adopting best practices, solutions that safeguard endpoints and provide accurate monitoring of internet traffic are ideal for discovering and alleviating the effects of advanced threats and targeted attacks.

## More enterprise records compromised in data breaches even as disclosures drop

Some of last year’s headlines bore the names of big companies in a less than favorable light: These companies, trusted by millions, were infiltrated and hit by massive data breaches.

Yahoo took the unenviable lead by admitting in October that all of its 3 billion users were affected in the August 2013 attack on its network — triple that of its previously disclosed number.<sup>60</sup> Equifax, a consumer credit reporting agency, also made news in September by divulging that the personally identifiable information (PII) of around 145.5 million U.S. users and 15.2 million U.K. users were compromised in a breach that could have started as early as May 2017.<sup>61</sup> The ride-sharing company Uber approached the end of an already troubled year by revealing that 57 million customer and driver records were exposed after a data breach in October 2016 (and a subsequent cover-up that proved unsuccessful).<sup>62</sup>

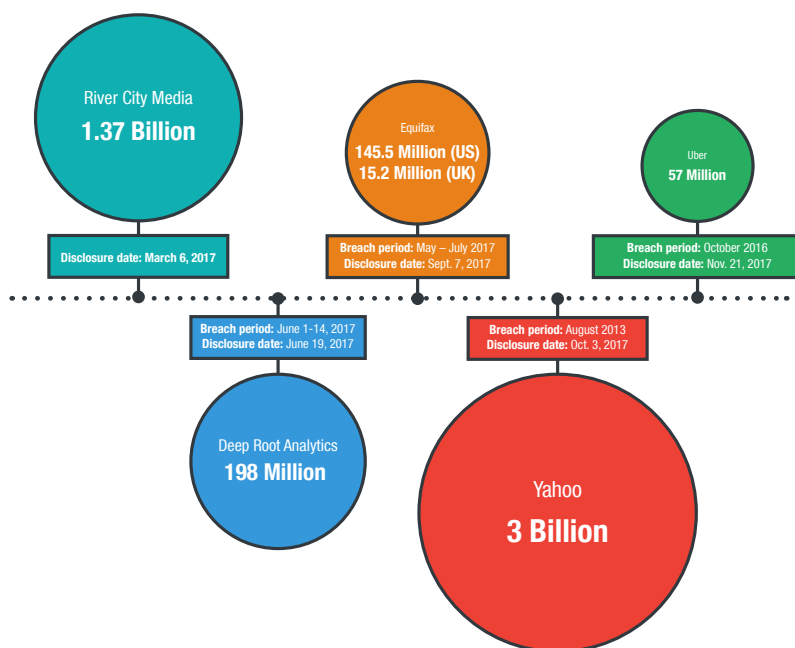


Figure 15. Yahoo leads with 3 billion affected records: Biggest data breaches disclosed in 2017

The surfacing of several heavyweight incidents isn't the only interesting development for data breaches last year. Though the number of affected records rose, the number of disclosures dropped by 32 percent from 2016 to 2017.

Year	Data breaches disclosed	Affected records
2016	813	3,310,435,941
2017	553	4,923,053,245

*Note: Yahoo's data breach disclosure reported in October 2017 is reflected in the number of affected records for 2017. The figures are computed based on data from Privacy Rights Clearinghouse.<sup>63</sup>*

Table 1. Fewer disclosures, greater number of affected records: Comparison of number of data breaches disclosed and number of affected records between 2016 and 2017

The dip in the number of publicized breaches seems to be a prelude to the implementation of the European Union's General Data Protection Regulation (GDPR) in May 2018.<sup>64</sup> GDPR will have rigid compliance standards pertaining to data breach notifications. Steep penalties also await enterprises in the event of their failure to act in accordance with the regulation. Elsewhere, similar moves to protect personal information with data privacy and management regulations have been initiated in countries including China,<sup>65</sup> Singapore,<sup>66</sup> and the U.S.<sup>67</sup>

Though the motives for breaking into enterprises' databases and systems vary, the methods continue to revolve around tried and tested practices. Notably, as in 2016,<sup>68</sup> hacking was found to be the most common method in 2017. Out of the 553 reported breaches, 320 — or 58 percent — resulted from hacking.<sup>69</sup> This was the method by which the Yahoo,<sup>70</sup> Equifax<sup>71</sup> and Uber<sup>72</sup> breaches were carried out.

Cybercriminals also used malware to steal vital data from enterprises. In the case of the drive-in fast food chain Sonic, malware was used to skim data from possibly 5 million of its customers, exposing their credit and debit card account information to threat actors.<sup>73</sup> InterContinental Hotels Group (IHG) was also victimized by a malware attack that accessed the credit card information of customers, affecting more than a thousand of its hotels in the U.S. and Puerto Rico.<sup>74</sup>

Not all data breaches are caused by sophisticated infiltration, though. Sometimes, they're the result of sheer carelessness or even neglect — a reality that bodes ill for enterprises big and small.

Take the case of the spam operator River City Media, in which an improperly configured backup system led to the exposure of 1.37 billion email addresses.<sup>75</sup> In addition, Deep Root Analytics had 1.1 terabytes of information on more than 198 million U.S. citizens leaked because the data was unintentionally uploaded to a publicly available server.<sup>76</sup> And there's the case of America's JobLink: An unpatched vulnerability in its

application code was exploited by a hacker, giving him access to the information of 4.8 million job seekers across 10 states in the U.S.<sup>77</sup>

What individuals and businesses of all sizes ought to realize from these incidents is that data breaches can be quite costly. Affected businesses bleed out billions of dollars in losses and legal fines, and worse, lose the support and earn the ire of millions of customers.

As data breaches can be an unforgiving event, extensive security hygiene must be practiced in all levels of the enterprise, including regular updating and system patching. Companies that use legacy systems and out-of-support software will benefit from solutions that regularly provide extensive patches that protect their systems from critical threats.



## Threat Landscape in Review

The Trend Micro [Smart Protection Network](#) security infrastructure<sup>78</sup> blocked over 66 billion threats in 2017.

66,436,980,714

By comparison, it blocked over 81 billion threats in 2016. We believe that the drop in the number of threats can be attributed to a shift from “spray and pray” methods to a more targeted approach to attacks.

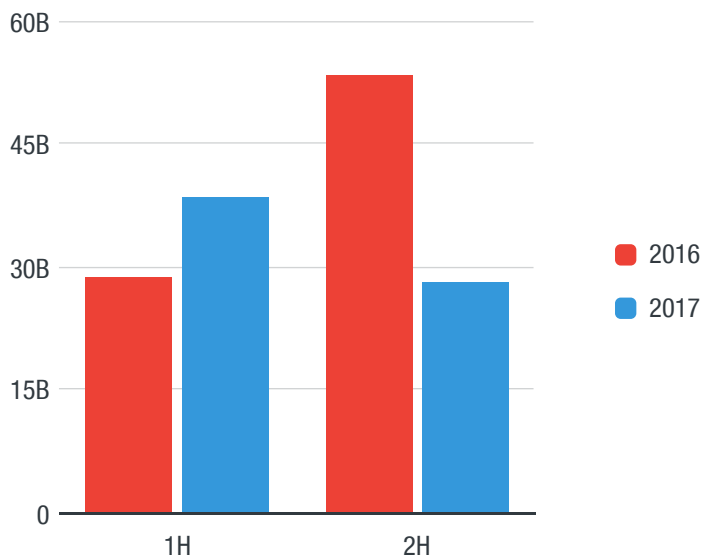


Figure 16. Fewer threats blocked in 2017 than in 2016: Overall threats blocked by the Trend Micro Smart Protection Network infrastructure, 2016 vs. 2017

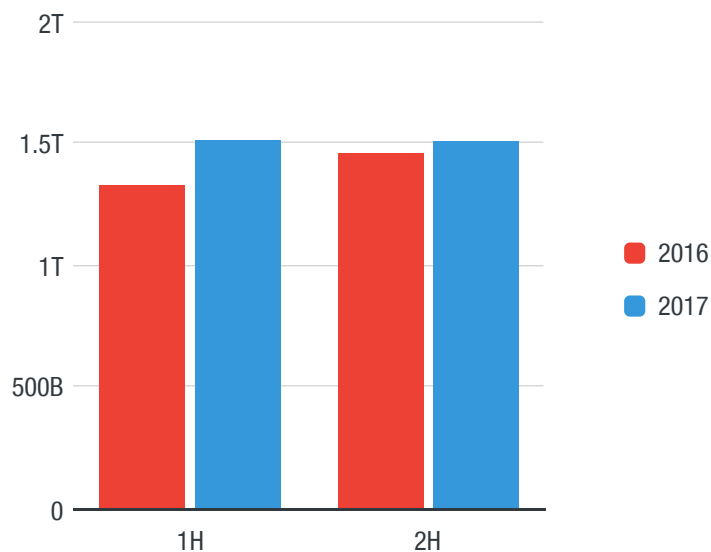


Figure 17. More client queries received in 2017: Volume of queries, based on feedback from the Trend Micro Smart Protection Network infrastructure, 2016 vs. 2017

In the first half of 2017, .PDF was the top file type for spam attachments. By year’s end, however, .XLS had become the most used file type across the 108,926,882 spam attachments in our dataset.

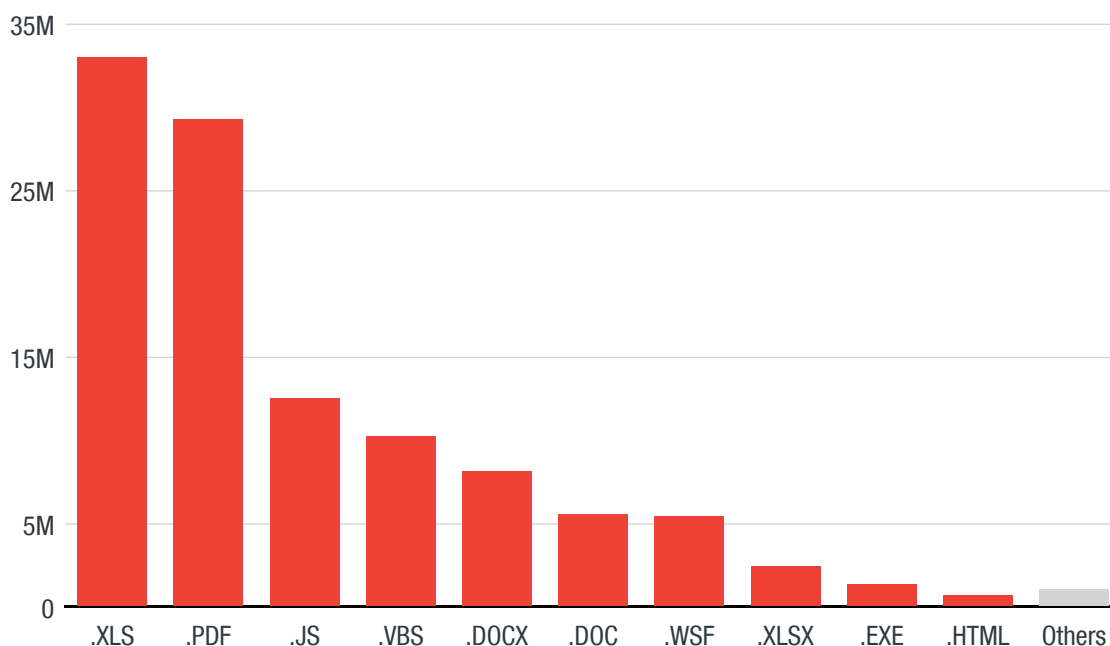


Figure 18. .XLS surfaced as the top spam attachment file type: Top 10 file types for spam attachments in 2017

Jan	CRYPFUN	REBOLOCK	VXLOCK	NETIX
	YUHAK	CRYPRAAS	HAVOC	MABORO
	SPORA	EVILWARE	CRYPTOPIC	BLEEDGREEN
	EXMAS			
Feb	CRYPPTYT	CRYPCYR	CZCRYPT	VANGUARD
	OSX_CRYPATCHER	TUSIKSLOCK	PYLEET	KASISKI
	CRYPNTK	HERMES	ONCRYPT	JOBCRYPTER
	FAKEGLOBE	WCRY	PABLUKLOCK	SERBRAN
	SOFADE	CRYPTCONSOLE	URCRYP	EREBUS
Mar	CUTSOME	JAVAWARE		
	NEDSOM	NARLAN	NXCRYP	CRYPDNC
	HAPPYDAYZZZ	BATHIDE	DARKLOCKER	METEORITAN
	LELELOCK	KRYPTA	CRYPDEVIL	CRPTX
	STUP	ROZALOCK	GGCRYP	KIRK
	WEOGO	VORTEX	KAENLUPUF	CRYPJACKY
Apr	CRYPDANGER	CRYPDAMG	YAFCOOKIE	
	DEADSEC	EXTRACTOR	TESTLOCKER	DONTSLIP
	ZIPIAC	BTCWARE	CRYPCTF	KAHAS
	PSHCRYPT	MEDLINZ	LOLI	GOSHIFR
	CONFICKER	SHWERER	CRADLE	RUSHQL
	SHIKEY	ALKA	TRESORAS	LAMBDALOCKER
	GXFORTY	FLUFFY	JANLOCKER	SALSA
May	MAYKOLIN	AMNESIA	CRYPEC	VCRYPT
	WANTMYFILES	CLOUDED	BITKANGROO	VIKI
	CRYPJAFF	ANIMESCREENLOCK	UIWIX	LOCKOUT
	FAKEWCYR	LOKTROM	DTOD	VISIONCRYPT
	MEMELOCKER	WIDIALOCKER	EGLUELOCKER	XORDEOS
	MOWARE	DEADDS	RIMALOCKER	THORNIA
	MANCROS	ROBLOCKER	LIGHTNING	WIRA
	QRLOCKER	MISORRY	FAKERA	TESLAWARE
	GOMME	ZIPRAMEN	BRICKR	XORGOT
	CUTWISH			

Jun	BLACKMAIL	BLUEHOWL	JOSKY	SNEKUD
	TUBELAW	DARKENCRYPTOR	DELS CARE	OGRE
	ZILLA	MALHUNT	DESUI	DYNACRYPT
	SAWORSED	MRLOCKER	BEETHOV	XXLECXX
	SPECTRE	GPAA	CASHOUT	PROTONOSX
	CRYPAYSAVE	XINTI	ADLITTLE	FREEZESCARE
	SCARAB	SKULLSCREEN	FAKECERBER	KTZWARE
	WINBAM	LIXLOCKER	QUAKEWAY	PSCRYPT
	DARKSCARE	REETNER	MARKOLOCK	KRYPTONITE
	GOJDUE	GRIFFINLOCK	RUBY	KARO
	VIACRYPT	EXECUTIONER	TRIPM	BUBBLE
	PIRATE	RANPHP	RANSIX	PYTHOCRYPT
	WIRUSLOCKER			
Jul	RANRANS	TAKEM	RADIATION	ZERO
	SHELOCKER	EIGHTZLOCK	CRYPTER	HOWLLOCK
	SUPALOCK	MAMOSHII	FAKEPETYA	STUPURGE
	MEGA	MALKI	SCARENOTE	BLACKOUT
	RANSED	STRIKED	REYPTSON	KCAUF
	OOPS	ASNONE	STUPALOISA	CRYPTOMIX
	CHIYUNLONG	BITSHIFT	BAM	SNAKELOCK
	DCRY	VINDOWSCARE	RDW	ABCLOCKER
	INVIS CARE	SPONGESCARE	STORM	GRYPHON
	FILER EKT	SIFRELI	DEMON	FCPSCARE
Aug	TPSCARE	DAYSCARE	PASTMONTH	WANNAPAY
	SHELLSKULL	NODEAD	CRYPSTAHL	GOLANG
	CONHOOD	JCODER	LOCKBOX	EBWALL
	ISRABYE	LOCKERPAY	PEYDAY	HELLSCRYPT
	CRYPZABLO	TOOLCryp	BITPAYMER	SHREKLOCK
	SHINIGAMI	INFINITETEAR	LOCKCRYPT	CRYPTWELVE
	SYNCRYPT	CLICOCryp	DYNAMITE	BRANGG
	WOODLOCK	CYRON	DZSPLITTER	FLATTENWARE
	ERROR	PASIEM	MINDSYS	STRAWHAT
	WOOLY	SURERAN	CYBER	AKIRA
HAZE				

Sep	CATLOCKER	HACKBIT	APOLLO	HAKKED
	DILMALOCKER	FAKELOCKY	HAPPYCRYPTER	LOCKED
	BLACKHAT	MYSTIC	MATROSKA	INFINITYLOCK
	ENTREPED	PENDOR	CRYPGG	DEKFOS
	CRYPMOD	CRYPROTO	BUD	SAPNUPUAS.A
	SOLDIERSCARE	CLONE	DEATHMSG	REDBOOT
	MBRLOCKER	ZONE	LOCKSCARE	CYPHERPY
	BLACKMIST	LASERLOCK		
Oct	POLSKY	ENDER	CRYPTROTCOD	AESBAT
	ALLCRY	BADRABBIT	LOSERS	WANNAHAPPY
	XIAOBA	XRANSOM	RYZERLO	
	KRISTINA	SAD	WAFFLE	HSDFSDCRYPT
Nov	FOXY	SIGMA	XMAS	CYBERPOLICE
	JCANDY	LOCKON	RASTAKHIZ	WANNASMILE
	WANADIE	KATAFRACK	SCRAM	NETCRYPT
	HCSIX	WPEACE		
Dec	MAURI	WMONEY	HANDSOMEWARE	BLIND
	HALLOWARE	PAYMENT	MRCYBER	XSCAREWARE
	PURGEN	ETERNITY	FILESPIDER	NOBLIS
	NOWAY	DYNACRYPT	CYCLONE	SITER
	PULPY	ROZLOK	MADBIT	

Table 2. Over 300 emerged: New ransomware families in 2017

Last year saw a drop in the entire exploit kit ecosystem, as cybercriminals continued to move away from using it due to poor infection rates and instead turned to other, more reliable tactics such as spam, phishing, and targeting specific, individual vulnerabilities.

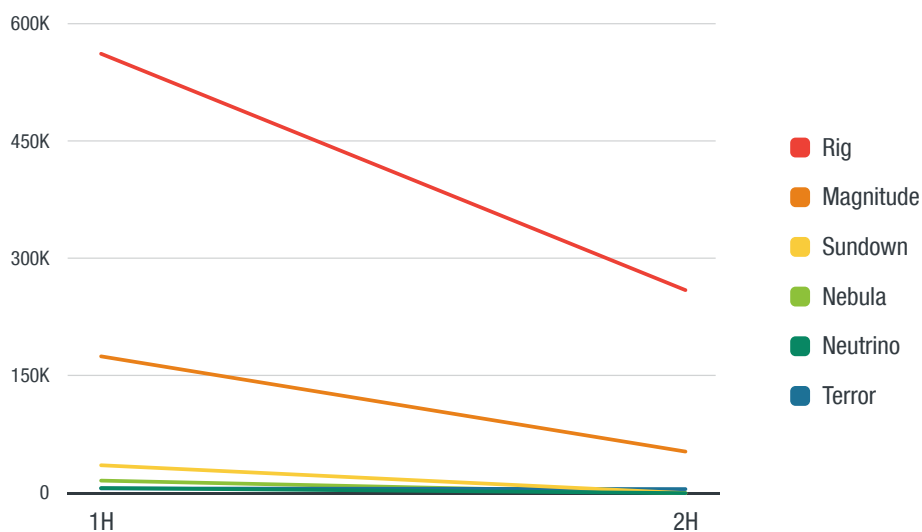


Figure 19. A drop in the exploit kit ecosystem: Declining number of exploit kit attacks from the first half to the second half of 2017

On the mobile front, our Mobile App Reputation Service (MARS) data shows that more unique ransomware families abused mobile devices in 2017 than in 2016. The SLocker mobile ransomware family led the pack with 499,634 sample counts, while the smallest ransomware family count was that of LeakerLocker, at only 16.

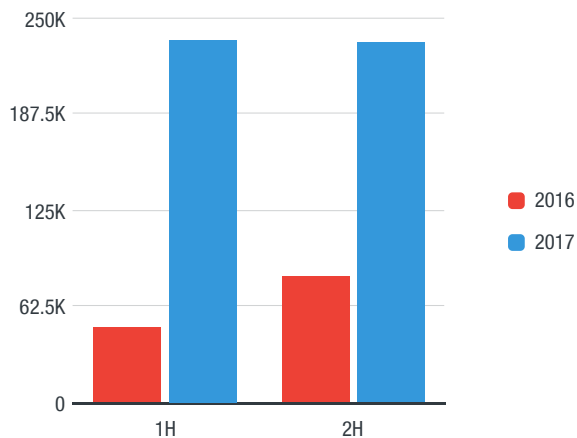


Figure 20. A huge increase in mobile ransomware for 2017: Comparison between unique mobile ransomware discovered by or added to MARS, 2016 vs. 2017

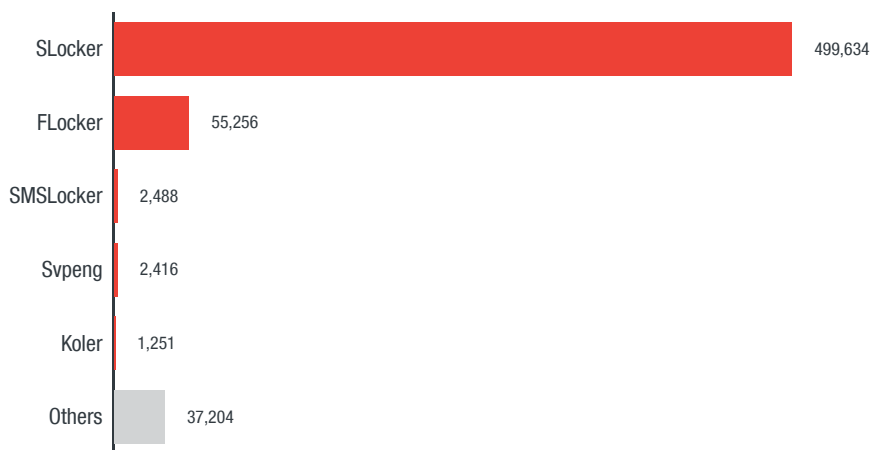


Figure 21. SLocker peaked as most popular mobile ransomware: Mobile ransomware families and sample counts from MARS data from January 2016 to December 2017

## References

1. Trend Micro. (11 September 2017). *Trend Micro*. “2017 Midyear Security Roundup: The Cost of Compromise.” Last accessed on 30 January 2018 at <https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup>.
2. Trend Micro. (6 December 2016). *Trend Micro*. “Security Predictions: The Next Tier.” Last accessed on 30 January 2018 at <https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2017>.
3. Steve Morgan. (17 May 2017). *Cybersecurity Ventures*. “Global ransomware damage costs predicted to exceed \$5 billion in 2017, up from \$325 million in 2015.” Last accessed on 15 January 2018 at <https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/>.
4. Ryan Delany. (18 May 2017). *Trend Micro Simply Security*. “Protecting Your Small Business From WannaCry.” Last accessed on 30 January 2018 <https://blog.trendmicro.com/protecting-small-business-wannacry/>.
5. Trend Micro. (21 May 2017). *Trend Micro Business Support*. “Preventing WannaCry (WCRY) ransomware attacks using Trend Micro products.” Last accessed on 30 January 2018 at <https://success.trendmicro.com/solution/1117391-updates-on-the-latestwcr-wannacry-ransomware-attack-and-trend-micro-protection>.
6. CBS News. (16 May 2017). *CBS News*. “North Korean hackers behind global cyberattack?” Last accessed on 30 January 2018 at <http://www.cbsnews.com/news/cyberattack-wannacry-ransomware-north-korea-hackers-lazarus-group/>.
7. Mayra Rosario Fuentes. (10 October 2017). *Trend Micro TrendLabs Security Intelligence Blog*. “WannaCry Ransomware Sold in the Middle Eastern and North African Underground.” Last accessed on 30 January 2018 at <https://blog.trendmicro.com/trendlabs-security-intelligence/wannacry-ransomware-middle-eastern-north-african-underground/>.
8. Mayra Rosario Fuentes. (10 October 2017). *Trend Micro*. “Digital Souks: A Glimpse into the Middle Eastern and North African Underground.” Last accessed on 7 February 2018 at [https://documents.trendmicro.com/assets/white\\_papers/wp-middle-eastern-north-african-underground.pdf](https://documents.trendmicro.com/assets/white_papers/wp-middle-eastern-north-african-underground.pdf).
9. Trend Micro. (29 August 2017). *Trend Micro Simply Security*. “Petya expands its scope: A global ransomware threat.” Last accessed on 30 January 2018 at <https://blog.trendmicro.com/petya-expands-its-scope-a-global-ransomware-threat/>.
10. Nicole Perlroth, Mark Scott, and Sheera Frenkel. (27 June 2017). *The New York Times*. “Cyberattack Hits Ukraine Then Spreads Internationally.” Last accessed on 30 January 2018 at <https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html>.
11. Trend Micro. (29 August 2017). *Trend Micro TrendLabs Security Intelligence Blog*. “Petya expands its scope: A global ransomware threat.” Last accessed on 30 January 2018 at <https://blog.trendmicro.com/petya-expands-its-scope-a-global-ransomware-threat/>.
12. Trend Micro. (25 October 2017). *Trend Micro*. “Protecting Yourself from Bad Rabbit Ransomware.” Last accessed on 30 January 2018 at <https://www.trendmicro.com/vinfo/ph/security/news/cyber-attacks/protecting-yourself-from-bad-rabbit-ransomware>.
13. Trend Micro. (3 November 2017). *Trend Micro*. “Ransomware Recap: The Short-Lived Spread of Bad Rabbit Ransomware.” Last accessed on 30 January 2018 at <https://www.trendmicro.com/vinfo/ph/security/news/cybercrime-and-digital-threats/ransomware-recap-the-short-lived-spread-of-bad-rabbit-ransomware>.
14. Trend Micro. (25 October 2017). *Trend Micro*. “Protecting Yourself from Bad Rabbit Ransomware.” Last accessed on 30 January 2018 at <https://www.trendmicro.com/vinfo/ph/security/news/cyber-attacks/protecting-yourself-from-bad-rabbit-ransomware>.
15. Trend Micro. (19 June 2017). *Trend Micro TrendLabs Security Intelligence Blog*. “Erebus Resurfaces as Linux Ransomware.” Last accessed on 30 January 2018 at <https://blog.trendmicro.com/trendlabs-security-intelligence/erebus-resurfaces-as-linux-ransomware/>.
16. Trend Micro. (6 December 2016). *Trend Micro*. “Security Predictions: The Next Tier.” Last accessed on 30 January 2018 at <https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2017>.



17. Gilbert Sison. (2 May 2017). *Trend Micro TrendLabs Security Intelligence Blog*. “Cerber Version 6 Shows How Far the Ransomware Has Come (and How Far it’ll Go).” Last accessed on 30 January 2018 at <https://blog.trendmicro.com/trendlabs-security-intelligence/cerber-ransomware-evolution/>.
18. Glibert Sison. (28 March 2017). *Trend Micro TrendLabs Security Intelligence Blog*. “Cerber Starts Evading Machine Learning.” Last accessed on 30 January 2018 at <https://blog.trendmicro.com/trendlabs-security-intelligence/cerber-starts-evading-machine-learning/>.
19. Gilbert Sison and Janus Agcaoili. (3 August 2017). *Trend Micro TrendLabs Security Intelligence Blog*. “Cerber Ransomware Evolves Again, Now Steals From Bitcoin Wallets.” Last accessed on 30 January 2018 at <https://blog.trendmicro.com/trendlabs-security-intelligence/cerber-ransomware-evolves-now-steals-bitcoin-wallets/>.
20. Max Metger. (13 April 2017). *SC Magazine UK*. “The King is dead, long live the King: Cerber wins in ransomware wars.” Last accessed on 18 January 2018 at <https://www.scmagazineuk.com/the-king-is-dead-long-live-the-king-cerber-wins-in-ransomware-wars/article/650255/>.
21. Trend Micro. (21 August 2017). *Trend Micro*. “Voice Message Malspam Arrives With Locky Ransomware.” Last accessed on 18 January 2018 at <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/spam/671/voice-message-malspam-arrives-with-locky-ransomware>.
22. Trend Micro. (9 September 2017). *Trend Micro*. “Fake invoice email with Html attachment spreads Locky ransomware.” Last accessed on 18 January 2018 at <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/spam/3621/fake-invoice-email-with-html-attachment-spreads-locky-ransomware>.
23. Brooks Li. (29 August 2017). *Trend Micro TrendLabs Security Intelligence Blog*. “Locky Ransomware Now Downloaded as Encrypted DLLs.” Last accessed on 17 January 2018 at <https://blog.trendmicro.com/trendlabs-security-intelligence/locky-ransomware-now-downloaded-encrypted-dlls/>.
24. Trend Micro. (18 September 2017). *Trend Micro*. “Locky Ransomware Pushed Alongside FakeGlobe in Upgraded Spam Campaigns.” Last accessed on 30 January 2018 at <https://blog.trendmicro.com/trendlabs-security-intelligence/locky-ransomware-pushed-alongside-fakeglobe-upgraded-spam-campaigns/>.
25. Trend Micro. (4 September 2017). *Trend Micro*. “New Locky Variant Lukitus Distributed in 23 Million Emails” Last accessed on 30 January 2018 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/new-locky-variant-lukitus-distributed-in-23-million-emails>.
26. Buddy Tancio. (15 June 2017). *Trend Micro TrendLabs Security Intelligence Blog*. “Analyzing the Fileless, Code-injecting SOREBRECT Ransomware.” Last accessed on 23 January 2018 at <https://blog.trendmicro.com/trendlabs-security-intelligence/analyzing-fileless-code-injecting-sorebrect-ransomware/>.
27. Veo Zhang. (6 December 2016). *Trend Micro TrendLabs Security Intelligence Blog*. “New Flavor of Dirty COW Attack Discovered, Patched.” Last accessed on 30 January 2018 at <https://blog.trendmicro.com/trendlabs-security-intelligence/new-flavor-dirty-cow-attack-discovered-patched/>.
28. Mobile Threat Response Team. (25 September 2017). *Trend Micro TrendLabs Security Intelligence Blog*. “ZNIU: First Android Malware to Exploit Dirty COW Vulnerability.” Last accessed on 30 January 2018 at <https://blog.trendmicro.com/trendlabs-security-intelligence/zniu-first-android-malware-exploit-dirty-cow-vulnerability/>.
29. Mobile Threat Response Team. (25 September 2017). *Trend Micro TrendLabs Security Intelligence Blog*. “ZNIU: First Android Malware to Exploit Dirty COW Vulnerability.” Last accessed on 30 January 2018 at <https://blog.trendmicro.com/trendlabs-security-intelligence/zniu-first-android-malware-exploit-dirty-cow-vulnerability/>.
30. Darre Pauli. (23 January 2017). *The Register*. “It’s 2017 and 200,000 services still have unpatched Heartbleeds.” Last accessed on 18 January 2018 at [https://www.theregister.co.uk/2017/01/23/heartbleed\\_2017/](https://www.theregister.co.uk/2017/01/23/heartbleed_2017/).
31. Trend Micro. (7 December 2017). *Trend Micro TrendLabs Security Intelligence Blog*. “CONFICKER/ DOWNAD 9 Years After: Examining its Impact on Legacy Systems.” Last accessed on 19 January 2018 at <https://blog.trendmicro.com/trendlabs-security-intelligence/conficker-downad-9-years-examining-impact-legacy-systems/>.

32. Trend Micro. (6 December 2016). *Trend Micro*. "Security Predictions: The Next Tier." Last accessed on 30 January 2018 at <https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2017>.
33. FBI IC3. (04 May 2017). *FBI IC3*. "Business E-mail Compromise, Email Account Compromise: The 5 Billion Dollar Scam." Last accessed on 18 January 2018 at <https://www.ic3.gov/media/2017/170504.aspx>.
34. Trend Micro. (16 June 2016). *Trend Micro*. "BEC Scams Amount to \$3 billion According to Latest FBI PSA." Last accessed on 30 January 2018 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/bec-scams-amount-to-3-billion-according-to-latest-fbi-psa>.
35. Samuel Gibb. (28 April 2017). *The Guardian*. "Facebook and Google were conned out of \$100m in phishing scheme." Last accessed on 30 January 2018 at <https://www.theguardian.com/technology/2017/apr/28/facebook-google-conned-100m-phishing-scheme>.
36. Reuters. (10 July 2017). *Reuters*. "German Firms Lost Millions of Euros in 'CEO Fraud' Scam: BSI." Last accessed on 18 January 2018 at <https://www.usnews.com/news/technology/articles/2017-07-10/german-firms-lost-millions-of-euros-in-ceo-fraud-scam-bsi>.
37. Kelli B. Grant. (19 October 2017). *CNBC*. "Scammers are conning homebuyers out of their down payment." Last accessed on 6 February 2018 at <https://www.cnn.com/2017/10/19/scammers-are-conning-home-buyers-out-of-their-down-payment.html>.
38. BBC News. (2 November 2017). *BBC News*. "Art galleries targeted by cyber-thieves." Last accessed on 18 January 2018 at <http://www.bbc.com/news/technology-41845965>.
39. Japan Times. (21 December 2017). *Japan Times*. "Japan Airlines Falls Victim to Email Fraud, Paying Out ¥384 Million to Hong Kong Accounts." Last accessed on 30 January 2018 at <https://www.japantimes.co.jp/news/2017/12/21/business/japan-airlines-bilked-%C2%A5384-million-getting-bogus-emails-seeking-lease-fees/#.WnA6N66WaM8>.
40. Stan Higgins. (29 December 2017). *CoinDesk*. "From \$900 to \$20,000: Bitcoin's Historic 2017 Price Run Revisited." Last accessed on 19 January 2017 at <https://www.coindesk.com/900-20000-bitcoins-historic-2017-price-run-revisited/>.
41. BBC News. (29 August 2017). *BBC News*. "Burger King launches WhopperCoin crypto-cash in Russia." Last accessed on 6 February 2018 at <http://www.bbc.com/news/technology-41082388>.
42. Gerrit De Vynck. (25 May 2017). *Bloomberg*. "Kik App Debuts Digital Currency Amid Bitcoin Boom." Last accessed on 6 February 2018 at <https://www.bloomberg.com/news/articles/2017-05-25/kik-messenger-app-debuts-own-digital-currency-amid-bitcoin-boom>.
43. Chris Cooper and Kiyotaka Matsuda. (22 May 2017). *Bloomberg*. "Peach Becomes Japan's First Airline to Accept Payment in Bitcoin." Last accessed on 6 February 2018 at <https://www.bloomberg.com/news/articles/2017-05-22/peach-becomes-japan-s-first-airline-to-accept-payment-in-bitcoin>.
44. Dom Galeon. (2 October 2017). *Business Insider*. "Dubai just got its first official cryptocurrency." Last accessed on 6 February 2018 at <http://www.businessinsider.com/dubai-official-cryptocurrency-blockchain-emcash-2017-10>.
45. Thomson Reuters. (25 October 2017). *Thomson Reuters*. "Cryptocurrencies by country." Last accessed on 6 February 2018 at <https://blogs.thomsonreuters.com/answeron/world-cryptocurrencies-country/>.
46. BBC News. (19 December 2017). *BBC News*. "Bitcoin exchange Yobit shuts after second hack attack." Last accessed on 2 February 2018 at <http://www.bbc.com/news/technology-42409815>.
47. Mobile Threat Response Team. (30 October 2017). *Trend Micro TrendLabs Security Intelligence Blog*. "Coin Miner Mobile Malware Returns, Hits Google Play." Last accessed on 19 January 2017 at <https://blog.trendmicro.com/trendlabs-security-intelligence/coin-miner-mobile-malware-returns-hits-google-play/>.
48. Trend Micro. (21 December 2017). *Trend Micro TrendLabs Security Intelligence Blog*. "Digmine Cryptocurrency Miner Spreading via Facebook Messenger." Last accessed on 30 January 2018 at <https://blog.trendmicro.com/trendlabs-security-intelligence/digmine-cryptocurrency-miner-spreading-via-facebook-messenger/>.

49. Trend Micro Cyber Safety Solutions Team. (20 September 2017). *Trend Micro TrendLabs Security Intelligence Blog*. “New RETADUP Variants Hit South America, Turn To Cryptocurrency Mining.” Last accessed on 30 January 2018 at <https://blog.trendmicro.com/trendlabs-security-intelligence/new-retadup-variants-hit-south-america-turn-cryptocurrency-mining/>.
50. Trend Micro. (15 November 2017). *Trend Micro*. “Coinhive Miner Emerges as the 6th Most Common Malware.” Last accessed on 30 January 2018 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coinhive-miner-the-6th-most-common-malware>.
51. Joseph Chen. (22 September 2017). *Trend Micro TrendLabs Security Intelligence Blog*. “EITest Campaign Uses Tech Support Scams to Deliver Coinhive’s Monero Miner.” Last accessed on 30 January 2018 at <https://blog.trendmicro.com/trendlabs-security-intelligence/eitest-campaign-uses-tech-support-scams-deliver-coinhives-monero-miner/>.
52. Statista. (November 2016). *Statista*. “Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions).” Last accessed on 23 January 2017 at <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>.
53. Trend Micro. (31 January 2017). *Trend Micro*. “Securing Your Routers Against Mirai and Other Home Network Attacks.” Last accessed on 30 January 2018 at <http://www.trendmicro.com.my/vinfo/my/security/news/internet-of-things/securing-routers-against-mirai-home-network-attacks>.
54. Trend Micro. (14 December 2016). *TrendLabs Security Intelligence Blog*. “Home Routers: Mitigating Attacks that can Turn them to Zombies.” Last accessed on 30 January 2018 at <https://blog.trendmicro.com/trendlabs-security-intelligence/home-routers-mitigating-attacks-that-turn-them-to-zombies/>.
55. Trend Micro. (1 December 2017). *Trend Micro TrendLabs Security Intelligence Blog*. “New Mirai Attack Attempts Detected in South America and North African Countries.” Last accessed on 30 January 2018 at <https://blog.trendmicro.com/trendlabs-security-intelligence/new-mirai-attack-attempts-detected-south-america-north-african-countries/>.
56. Stephen Hilt. (27 December 2017). *Trend Micro TrendLabs Security Intelligence Blog*. “The Need for Better Built-in Security in IoT Devices.” Last accessed on 26 January 2018 at <https://blog.trendmicro.com/trendlabs-security-intelligence/iot-devices-need-better-builtin-security/>.
57. Federico Maggi. (16 August 2017). *Trend Micro TrendLabs Security Intelligence Blog*. “The Crisis of Connected Cars: When Vulnerabilities Affect the CAN Standard.” Last accessed on 26 January 2018 at <https://blog.trendmicro.com/trendlabs-security-intelligence/connected-car-hack/>.
58. William Malik. (24 October 2017). *Trend Micro Simply Security*. “Accelerating Security for Intelligent Transportation Systems: A New Trend Micro Report.” Last accessed on 31 January 2018 at <https://blog.trendmicro.com/accelerating-security-intelligent-transportation-systems-new-trend-micro-report/>.
59. Trend Micro. (24 October 2017). *Trend Micro*. “High-Tech Highways.” Last accessed on 31 January 2018 at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/high-tech-highways-securing-the-future-of-transportation>.
60. Trend Micro. (4 October 2017). *Trend Micro*. “Yahoo!: All Three Billion User Accounts Affected in 2013 Data Breach.” Last accessed on 30 January 2018 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/yahoo-all-three-billion-user-accounts-affected-in-2013-data-breach>.
61. Trend Micro. (18 September 2017). *Trend Micro*. “The Equifax Breach: What to Do Now and What to Watch Out For.” Last accessed on 17 January 2018 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/equifax-breach-what-to-do-and-what-to-watch-out-for>.
62. Mark Nunnikhoven. (22 November 2017). *Trend Micro Simply Security*. “Uber: How Not To Handle A Breach.” Last accessed on 30 January 2018 at <https://blog.trendmicro.com/uber-how-not-to-handle-a-breach/>.
63. Privacy Rights Clearinghouse. (2017). *Privacy Rights Clearinghouse*. “Data Breaches.” Last accessed on 2 February 2018 at <https://www.privacyrights.org/data-breaches>.
64. Trend Micro. *Trend Micro*. “EU General Data Protection Regulation (GDPR).” Last accessed on 30 January 2018 at <https://www.trendmicro.com/vinfo/ph/security/definition/eu-general-data-protection-regulation-gdpr>.

65. Sophia Yan. (31 May 2017). *CNBC*. "China's New Cybersecurity Law Takes Effect Today, And Many are Confused." Last accessed on 30 January 2018 at <https://www.cnn.com/2017/05/31/chinas-new-cybersecurity-law-takes-effect-today.html>.
66. Kevin Kwang. (13 November 2017). *Channel News Asia*. "Singapore's Draft Cybersecurity Bill Tweaked to Include Public Feedback." Last accessed on 30 January 2018 at <https://www.channelnewsasia.com/news/singapore/singapore-s-draft-cybersecurity-bill-tweaked-to-include-public-9399378>.
67. James E. Lee. (9 May 2017). *Infosecurity Magazine*. "Will New Cybersecurity Legislation Offer Better Protection for Consumers?" Last accessed on 30 January 2018 at <https://www.infosecurity-magazine.com/opinions/will-new-cybersecurity-legislation/>.
68. Trend Micro. (28 February 2017). *Trend Micro*. "A Record Year for Enterprise Threats." Last accessed on 30 January 2018 at <https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/2016-roundup-record-year-enterprise-threats>.
69. Privacy Rights Clearinghouse. *Privacy Rights Clearinghouse*. "Data Breaches by Breach Type." Last accessed on 30 January 2018 at [https://www.privacyrights.org/data-breaches/breach-type?taxonomy\\_vocabulary\\_11\\_tid=2434](https://www.privacyrights.org/data-breaches/breach-type?taxonomy_vocabulary_11_tid=2434).
70. Privacy Rights Clearinghouse. (2017). *Privacy Rights Clearinghouse*. "Data Breaches." Last accessed on 2 February 2018 at <https://www.privacyrights.org/data-breaches?title=yahoo>.
71. Privacy Rights Clearinghouse. (2017). *Privacy Rights Clearinghouse*. "Data Breaches." Last accessed on 2 February 2018 at <https://www.privacyrights.org/data-breaches?title=equifax>.
72. Privacy Rights Clearinghouse. (2017). *Privacy Rights Clearinghouse*. "Data Breaches." Last accessed on 2 February 2018 at <https://www.privacyrights.org/data-breaches?title=uber>.
73. Brian Krebs. (26 September 2017). *Krebs on Security*. "Breach at Sonic Drive-In May Have Impacted Millions of Credit, Debit Cards." Last accessed on 18 January 2018 at <https://krebsonsecurity.com/2017/09/breach-at-sonic-drive-in-may-have-impacted-millions-of-credit-debit-cards/>.
74. Mariella Moon. (20 April 2017). *Engadget*. "Over 1,000 Intercontinental hotels hit by a data breach." Last accessed on 30 January 2018 at <https://www.engadget.com/2017/04/20/intercontinental-data-breach/>.
75. Mark Wycislik-Wilson. (6 March 2017). *BetaNews*. "Huge database leak reveals 1.37 billion email addresses and exposes illegal spam operation." Last accessed on 2 February 2018 at <https://betanews.com/2017/03/06/river-city-media-spam-database-leak/>.
76. Trend Micro. (15 December 2017). *Trend Micro*. "Year in Review: Notable Data Breaches for 2017." Last accessed on 30 January 2018 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/year-in-review-notable-data-breaches-for-2017>.
77. Trend Micro. (15 December 2017). *Trend Micro*. "Year in Review: Notable Data Breaches for 2017." Last accessed on 30 January 2018 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/year-in-review-notable-data-breaches-for-2017>.
78. Trend Micro. *Trend Micro*. "Smart Protection Network – Global Threat Intelligence." Trend Micro. Last accessed on 30 January 2018 at [https://www.trendmicro.com/en\\_us/business/technologies/smart-protection-network.html](https://www.trendmicro.com/en_us/business/technologies/smart-protection-network.html).



Created by:

**TrendLabs**

The Global Technical Support & R&D Center of **TREND MICRO**

**TREND MICRO™**

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and investigation, enabling better, faster protection. With almost 6,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro enables organizations to secure their connected world. For more information, visit [www.trendmicro.com](http://www.trendmicro.com).



Securing Your Journey  
to the Cloud