Unseen Threats, Imminent Losses

2018 Midyear Security Roundup

Cover image: SFIO CRACHO/Shutterstock.com

For Raimund Genes (1963-2017)

Contents

The year in security started out with the discovery of serious vulnerabilities in the hardware level, a revelation that eroded the implicit trust the industry had on the bedrock of modern computing: microprocessors. In other parts of the security landscape, this might as well have been a signal of what was to come.

The traditional assumptions or indicators about what, where, and how security risks can enter the network have never been as unreliable as seen in recent concurrent developments: the shift from attention-getting ransomware to the more subtle but incrementally damaging cryptocurrency miners; the continued emergence of "fileless" threats; the escalation of financial losses suffered from deceptively simple business email compromise (BEC) scams; and even the realization that router attack payloads have progressed beyond distributed denial-of-service (DDoS) attacks. While the usual entry points of these threats — email, vulnerabilities, malicious websites — have been mostly taken for granted, the direct and subsequent repercussions from their successful exploitation are very real.

In this midyear report, we track the tendency of security risks to emerge from aspects of computing that are often overlooked and show how costly they can be especially for enterprises.

Given their increasingly complex and fast-paced tasks in addition to the range of responsibilities that they carry today, IT administrators in particular must find some way to navigate the additional burden that these developments entail. For instance, cryptocurrency mining does not announce its presence in the network: IT admins must learn to look for telltale signs lest their enterprises suffer the weight on system resources, the wear and tear on company assets, and a larger power bill. Attacks involving BEC, a heavily socially engineered threat that can lead to significant losses, adds a human component to the security equation that IT admins must also be empowered to deal with. Likewise, IT admins likely have not had to apply patches to a wide swath of computer firmware for a long time, but waiting will only expand the window of exposure now that proof-of-concept exploits have become publicly available. And with the number and variety of emerging threats, IT admins must find a way to see the bigger picture — Is there an ongoing targeted attack against the company? — in order to provide an adequate security response.

As enterprises face the rest of the year and beyond, it is worth reviewing the first half of 2018 to see what has changed in the landscape, to ascertain which emerging threats to watch out for, and at least in some cases, to realize that the traditional way of securing networks no longer applies.

Serious vulnerabilities discovered in hardware make patching even more challenging

Pervasive CPU firmware flaws introduce more patching challenges

In January, Google announced the discovery of severe, microprocessor-level vulnerabilities that give attackers a means to access sensitive information previously thought of as fundamentally isolated.[1] The vulnerabilities used by Meltdown (CVE-2017-5754) and Spectre (CVE-2017-5753, CVE-2017-5715) are flaws related to the speculative execution of CPU instructions in certain brands of microprocessors.[2] Meltdown affects computing devices, including desktops and laptops that use any Intel processor released since 1995 (other than Intel® Itanium® and Intel Atom® processors before 2013).[3] For variants of Spectre, devices running x86 (Intel and AMD) and ARM-based processors are affected.[4]

Unlike regular software vulnerabilities, which are limited to certain operating systems or specific versions of specific software and which can be addressed by single vendors, Meltdown and Spectre pose unique challenges to the computing industry at large and to individual corporate networks in particular.

The discovery of the flaws means that the entire computing ecosystem has been vulnerable for a long time. Additionally, the design flaws are so basic and integral to the function of modern computers that it is likely that similar types of vulnerabilities exist alongside them. In fact, less than five months after the announcement, a Speculative Store Bypass flaw, a vulnerability similar to Spectre, was disclosed.[5] The computing industry can thus expect to live with the repercussions of these discoveries in the foreseeable future.

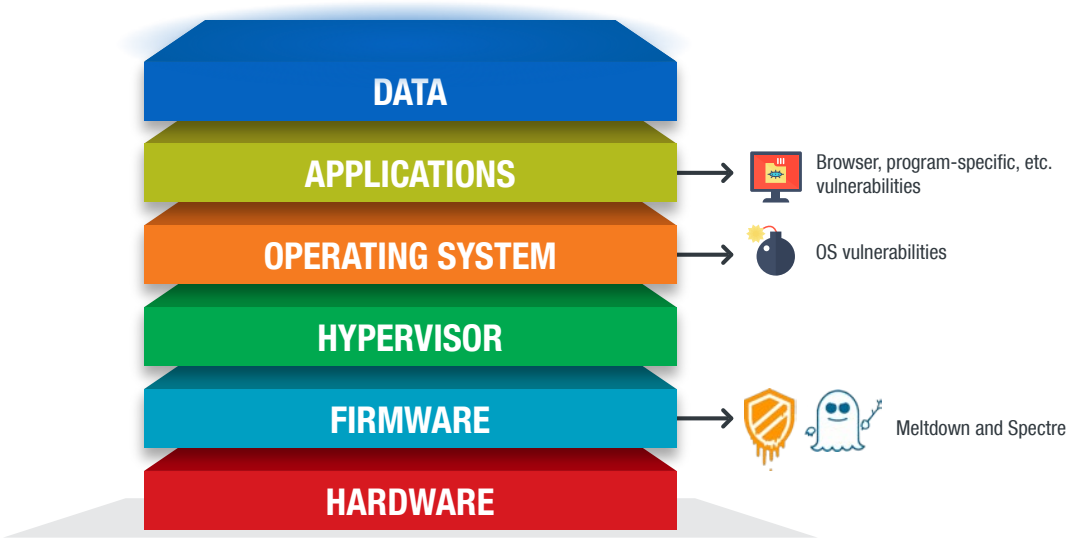

Figure 1. Meltdown and Spectre are weaknesses that lie deeper in the computing stack than regular software vulnerabilities: Diagram of a sample computing stack and where vulnerabilities are located

More concerning, however, is that while vendors have repeatedly assured that no exploit has been found in the wild, attackers now know to look at this aspect of the computing stack more closely than ever before. A possible indicator of this interest is the appearance of a number of Meltdown- or Spectre-related samples in an antivirus-testing firm's malware database,[6] although the number might point to little more than researcher interest or slightly modified versions of the disclosed proofs of concept. Actual working exploits for these would be highly valuable information considering the large market share of the affected vendors.

For IT admins, patching each and every computing device in the network is nonnegotiable, but it's not as easy as it sounds. For one thing, the involvement of multiple microprocessor vendors, operating system developers, and even browser makers that can provide either complete solutions or partial mitigations to the flaws can prove difficult to manage because of the differing rollout strategies and timelines.

On top of that, IT admins need to make calculated decisions about whether they value security or system performance more before they install patches. In certain instances, as in Microsoft's system performance study after patching for Meltdown and Spectre, computers running older operating systems have been found to suffer a noticeable decrease in system performance.[7] In other cases, even modern systems can be rendered unbootable.[8]

Legacy and older systems definitely remain at risk as well. Industries that tend to retain them for ease of use or practicality, including healthcare organizations where system upgrades would require downtime, should therefore examine their internal security strategies.

Volume of vulnerability advisories topped by Adobe, Foxit, Microsoft

Vulnerability research is critical in the overall health of the security landscape. In an environment of responsible disclosure, vulnerability researchers have a platform that will recognize their efforts and lead to immediate mitigations and responses from affected software vendors. In the first half of 2018, with the help of over 3,000 independent researchers who contribute to the Zero Day Initiative (ZDI) program, we published 602 advisories (up from 578 in the previous half year), only 23 of which exceeded their vendor coordination timelines and thus were released without vendor patches or mitigations.

The largest share of advisories pertained to the supervisory control and data acquisition (SCADA) human-machine interface (HMI) software vendor Advantech. But among home and office software vendors, Adobe was issued the most number of advisories. Of the different Adobe products, Adobe Acrobat Pro DC was issued the most number of advisories, a number of which were for ImageConversion processes. Interestingly, Foxit, which is largely considered an alternative PDF reader, had vulnerability issues of its own. As for Microsoft, roughly a third of its vulnerabilities had to do with its Internet Explorer and Edge browsers, while the rest were mostly in Windows.

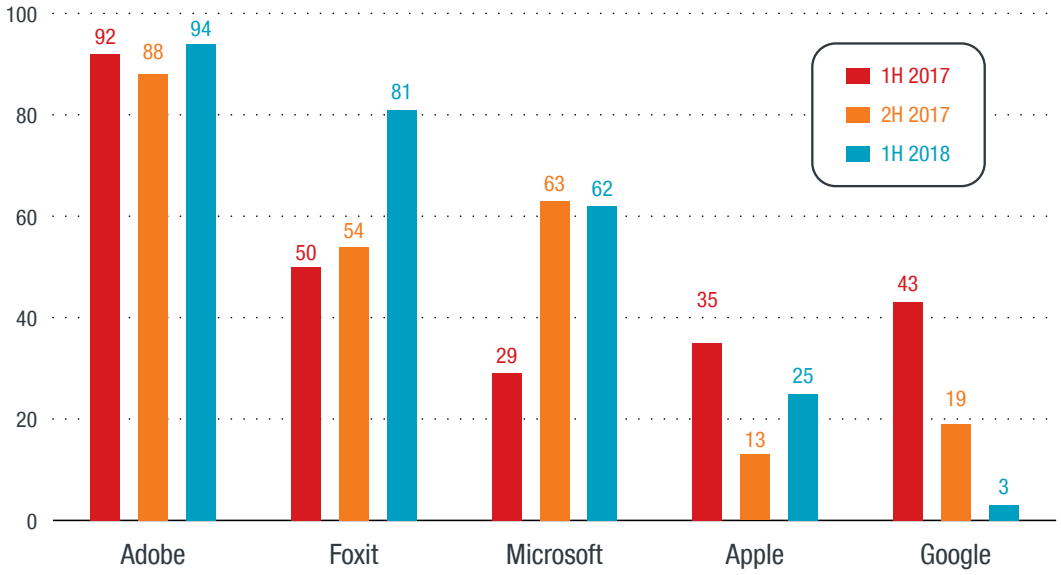

Figure 2. Adobe had the most number of advisories among home and office software vendors: Half-year comparison by vendor (non-SCADA) of number of vulnerabilities found

Vulnerabilities will continue to be in the background for enterprises, but these organizations must never be lulled into a sense of complacency, given how closely cybercriminals pay attention to these kinds of developments. In May, the Rig exploit kit started using CVE-2018-8174,[9] a remote code execution bug in the Windows VBScript Engine affecting Microsoft Office and Internet Explorer,[10] 35 days after the vulnerability was first disclosed[11] and 17 days after the vulnerability was patched by Microsoft. Rig also used CVE-2018-4878, a use-after-free bug in Adobe Flash.[12] Eventually, other exploit kits like Magnitude and Grandsoft started using CVE-2018-8174 as well.[13]

The continuous onslaught of newly discovered vulnerabilities only makes it that much harder for enterprises to catch up. Oftentimes, due to the volume of vulnerabilities and the competing priority of keeping the network available, they need to make practical tradeoffs by assigning importance to certain vulnerabilities and leaving open patches to other vulnerabilities to a later time. Consequently, enterprises have their own individual windows of exposure that rely heavily on when an exploit is made known or discovered and whether they have deemed the vulnerability important enough to fix the day a patch is released. Since cybercriminals are always on the lookout for easy-to-exploit and widespread vulnerabilities, enterprises need to make sure they are making the right tradeoffs.

SCADA advisories increase by 30%

Vulnerability researchers have found a considerable number of SCADA-related vulnerabilities in 2018 so far, 30 percent more than those found in the previous half year. Fortunately, the number of advisories released where vendor coordination exceeded timelines decreased significantly, meaning vendors were able to release a patch or some form of mitigation for the corresponding issue alongside our advisory.

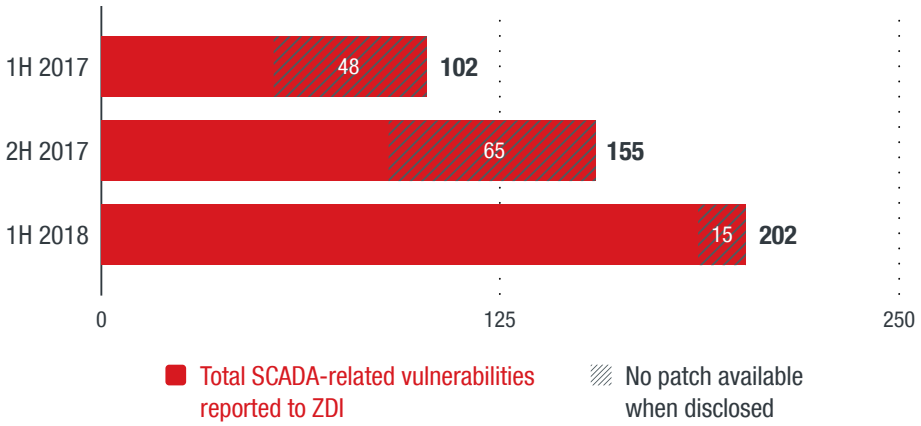

Figure 3. More SCADA vulnerabilities were disclosed in 1H 2018: Half-year comparison of disclosed SCADA vulnerabilities

Notably, 65 percent of the SCADA-related vulnerabilities were found in the web-based HMI software Advantech WebAccess. A SCADA HMI is the main digital hub that manages critical infrastructure and oversees the status of different control systems, which in turn have direct control over plant operations. It typically has limited access to the individual processes, but is able to send production goals or value targets and harvest diagnostic data about specific operations. In this sense, data shown in the HMI has reconnaissance value for attackers. On the other extreme, if an attacker is able to make damaging set point changes to containers of sensitive substances, then damage to equipment and property is possible, although less likely.

The SCADA market is highly active with vendors[14] large and small all over the world, and the focus of these vendors is often on the more profitable side of the business, which is the actual industrial equipment. Because of this, the resolution of a discovered SCADA-related vulnerability can take around 150 days on average, according to a study conducted by our researchers.[15] This picture varies widely from one vendor to another, which can be a problem for organizations hoping to patch the HMI software as soon as possible.

Addressing security vulnerabilities in the SCADA space will become especially important for IT admins of critical infrastructures in the European Union (EU) because of the newly enacted directive on security of network and information systems (NIS Directive).[16] The directive applies to organizations in EU member states running essential services, and requires them, among others, to secure their operations by establishing an incident response team and cooperation groups and by imbibing a culture of security. Noncompliance with the directive could carry the same hefty penalties as the EU General Data Protection Regulation (GDPR):[17] up to €20million or 4 percent of the company's global annual turnover, whichever is higher.[18]

Cryptocurrency mining detections more than doubles while ransomware remains an enterprise threat

Cryptocurrency mining detections peak

If the price hike on high-end graphics cards in 2017[19] is any indication, enthusiasts are keen on acquiring cryptocurrency such as bitcoin, Ether, or Monero by setting up expensive mining rigs or participating in mining pools. Mining virtual coins, which are seen as an alternative and theoretically more secure medium of exchange, sounds deceptively simple. But the real technical challenge is how miners can generate enough computing resources in a sustainable manner while still turning a profit, i.e., how to keep electricity costs below the price of coins mined, while keeping US$1,000-plus graphic cards from overheating or getting damaged over the course of round-the-clock mining.

It should come as no surprise that this interest would bleed into the cybercriminal realm. Cybercriminals would have predictably realized that they could outsource mining activities to unsuspecting users' computers. We have seen this trend late last year when we started detecting pieces of software that are performing or contributing to mining activities without explicitly asking for the user or device owner's consent to do so. In some cases, even legitimate mining tools are abused, but when these are installed in an unauthorized manner — for instance, inside an enterprise network unrelated to cryptocurrencies — they would be considered unwanted software. For the purpose of our discussion, we have grouped these kinds of software under "cryptocurrency mining detections."

In 2017, cryptocurrency mining detections climbed from around 75,000 detections in the first half of the year to about 326,000 in the second half.[20] Compared to the previous half year, the first half of 2018 saw a 141-percent increase in cryptocurrency mining detections.

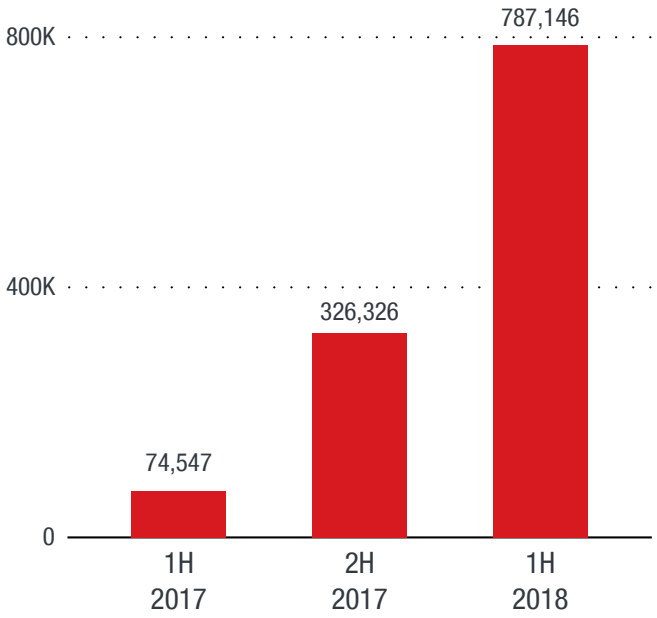

Figure 4. Cryptocurrency mining continues to rise:
Half-year comparison of cryptocurrency mining detections

In 2018, we also started detecting only cryptocurrency miner families that have outright malicious behaviors. Despite this distinction, we still saw 47 new cryptocurrency miner malware families. This indicates that different groups, rather than just an invested few, are mobilizing to take advantage of stealthy means to mine cryptocurrency.

Throughout the first half of 2018, hackers used a variety of vectors, including server exploits, a PHP vulnerability, malvertisements, other forms of malware, and even a potential financial scam site, with the end goal of installing miners. This pattern continues the trend seen in 2017, where cybercriminals seemed to be exploring all possible avenues, knocking down multiple paths to see which would bring them the most gains.

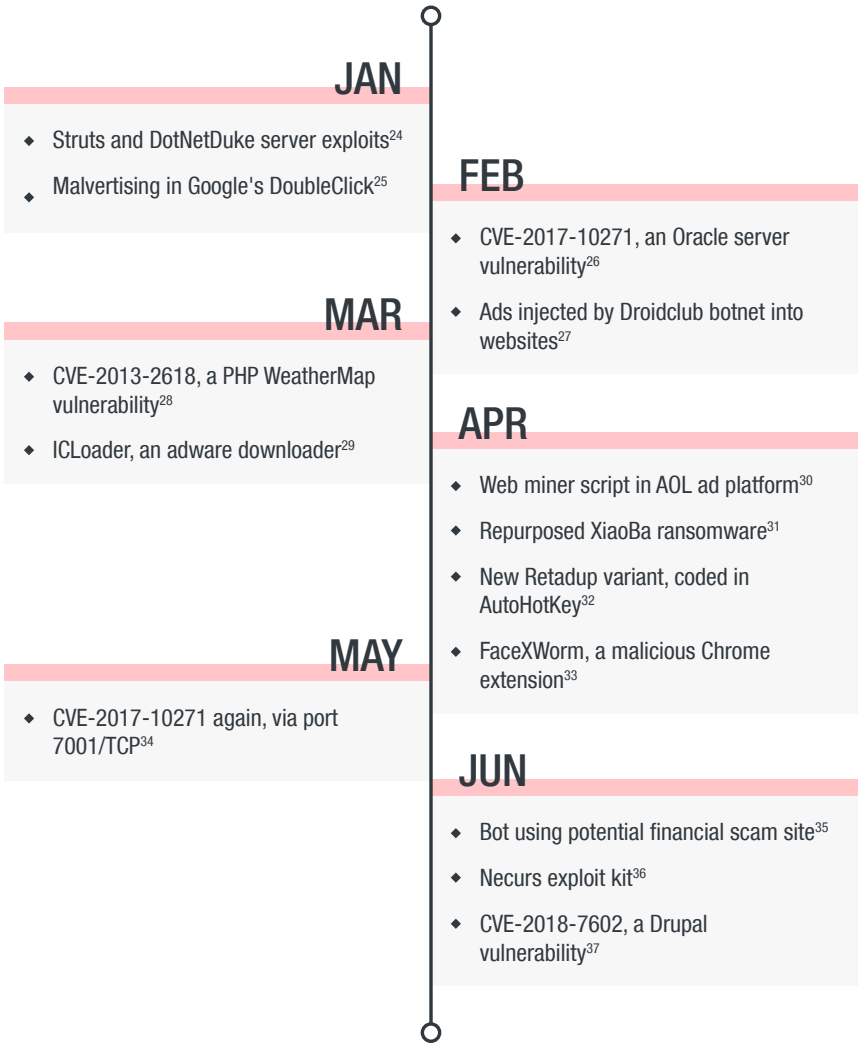

Figure 5. Cybercriminals used different tactics to distribute cryptocurrency miners: Timeline of tactics used in 1H 2018

The interest in cryptocurrency is so high that some hackers have gone the direct route to the virtual currency by hacking into large cryptocurrency exchanges. Hackers took off with US$500 million worth of NEM coins by breaking into one such cryptocurrency exchange in January,[21] while hackers in India stole US$3.3 million worth of bitcoins from another in April.[22] Interestingly, these trends persisted even as the value of cryptocurrency itself declined throughout the first half of the year.[23]

From an enterprise point of view, the presence of unauthorized cryptocurrency miners in the network is a red flag not only for the affected individual user device but also for overall network security. The damage from cryptocurrency miners, particularly the intentionally malicious ones, is not as straightforward as the more visceral effects of ransomware, but this does not mean that enterprises do not pay a price. Cryptocurrency miners hijack computer resources, which can be maxed out in the process of mining. This can affect network performance and result in hardware wear and tear, which in turn can lead to diminished asset life span and increased energy consumption. The new challenge for enterprises lies in the fact that cryptocurrency miners are less visible, more silent threats, the non-detection of which is likely to induce a false sense of security.

Ransomware slowing down in volume, but continuously evolving

In the first half of 2018, ransomware detections grew just 3 percent from the previous half year, a noticeable slowing down compared to previous periods. But while cryptocurrency mining detections may have replaced ransomware as the top detection, attackers have not completely lost sight of the ransomware profit model.

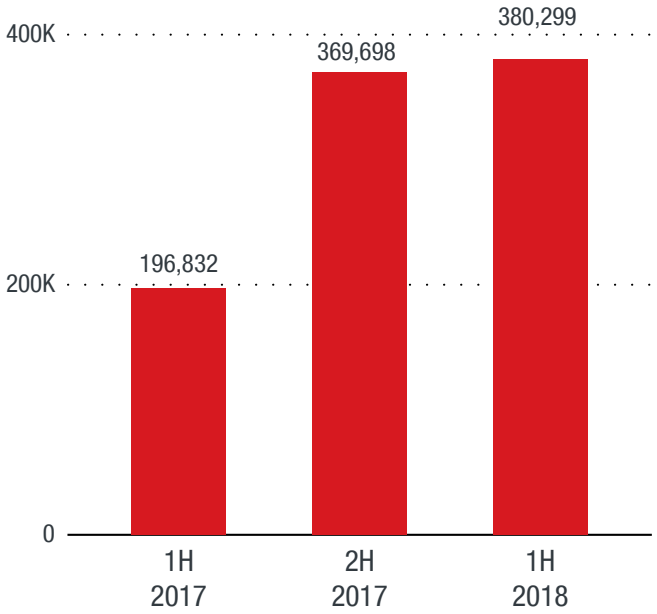

Figure 6. Ransomware detections grew just 3 percent: Half-year comparison of ransomware detections

The slowdown is more likely an expected result not only of the increased public attention on ransomware attacks but also of the corresponding mitigation and improved backup practices conducted on the network level resulting from their coverage.

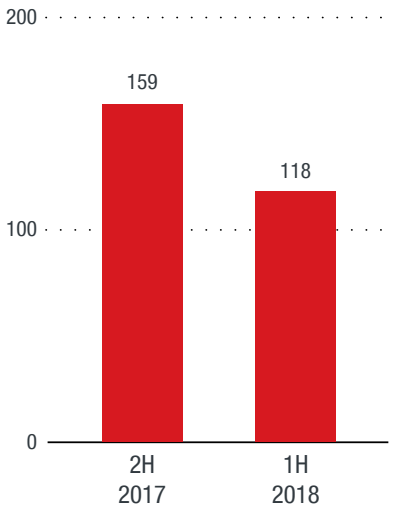

Figure 7. Fewer ransomware families emerged: Half-year comparison of new detected ransomware families

Cybercriminals appeared to respond by continuing to evolve their approach to maintaining and deploying ransomware, as can be observed in the notable new ransomware families seen in the first half of 2018: GandCrab, BlackHeart, SynAck, and Black Ruby. GandCrab emerged in the first quarter of 2018 and was noted for improving not only its encryption and decryption routines but also its persistence in the system,[38] indicating developers who could adjust quickly to the ransomware's success or failure in the wild. BlackHeart packages a malicious payload alongside a legitimate but outdated version of AnyDesk, which seems to be a front to hide what the ransomware is doing in the background.[39] SynAck was the first to use process doppelgänging, a technique, introduced only in 2017, that can make detection and analysis by researchers difficult.[40] As for Black Ruby,[41] it not only functions as ransomware but also installs a Monero miner — further evidence that both ransomware and cryptocurrency mining are considered profitable by cybercriminals.

Ransomware uses a variety of entry points and techniques, so there is no singular mode of protection that can ensure that it can be detected, let alone blocked, in all cases. Enterprises must therefore employ not only a multilayered approach to protection, but also a security solution that blends different threat defense techniques intelligently to apply the appropriate technology at the right time.

Mega breaches rise even as GDPR penalties loom

In April 2016, the adoption of the EU General Data Protection Regulation (GDPR), a landmark regulation that imposes heavy fines even on non-EU organizations as long as they are found to have handled EU citizen data inadequately, made waves in the security landscape.[42] Affected companies had two years to prepare for compliance: The regulation had a May 25, 2018, enforcement date.[43]

A reduction of reported breaches in the months leading up to the enforcement of the GDPR is perhaps the biggest indicator that companies have ramped up their data protection strategies. Unfortunately, the number of breaches did not decline. According to the relevant data set from Privacy Rights Clearinghouse, which monitors data breaches reported in the U.S. through either government agencies or verifiable media sources, 259 cases of data breaches were reported in the first six months of 2018 — only marginally higher than in the previous half year.

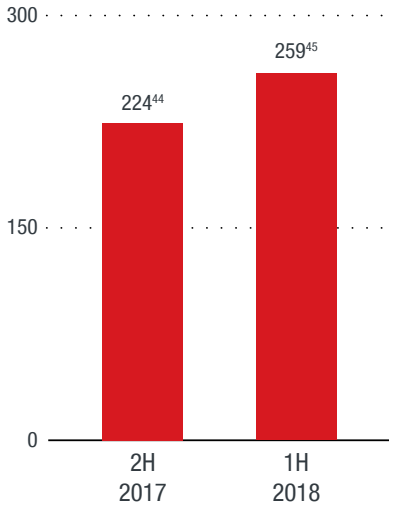

Figure 8. More data breaches were disclosed:
Half-year comparison ofdata breaches reported in the U.S.

Using the same data set, we determined that 15 data breaches in the first half of 2018 involved more than a million exposed data records in each case. The majority of these so-called "mega breaches" affected retailers or online merchants. While the number of these breaches rose by only six compared to the previous half year, that seemingly negligible increase meant that at least six million more records — certainly a not negligible number — were affected.

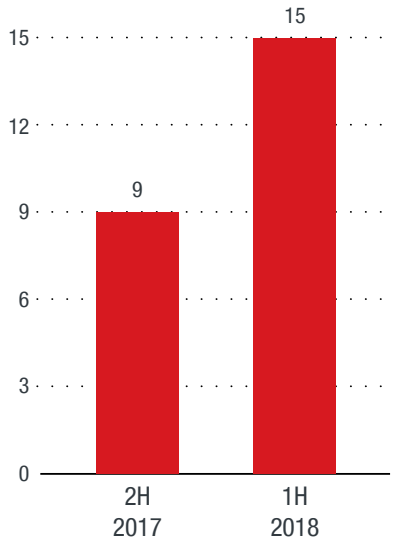

Figure 9. More mega breaches were disclosed: Half-year comparison of data breaches reported in the U.S. each with more than one million affected records

Data breaches have been a regular feature of the threat landscape for quite some time now. And the recent rise in data breaches can be an indication of both an increase in actual incidents and an increase in the reporting of these attacks for compliance with data-related regulations.

What's more interesting is that, from the same data set, it appears that 42 percent of the incidents occurred via unintended disclosure, while 41 percent resulted from hacking. Additionally, based on information available about the reported breaches, more records were exposed inadvertently than were affected by hacker activity. This means that even if enterprises are aware of the risks of data breaches, they may still be unable to enforce proper data protection mechanisms in a comprehensive manner.

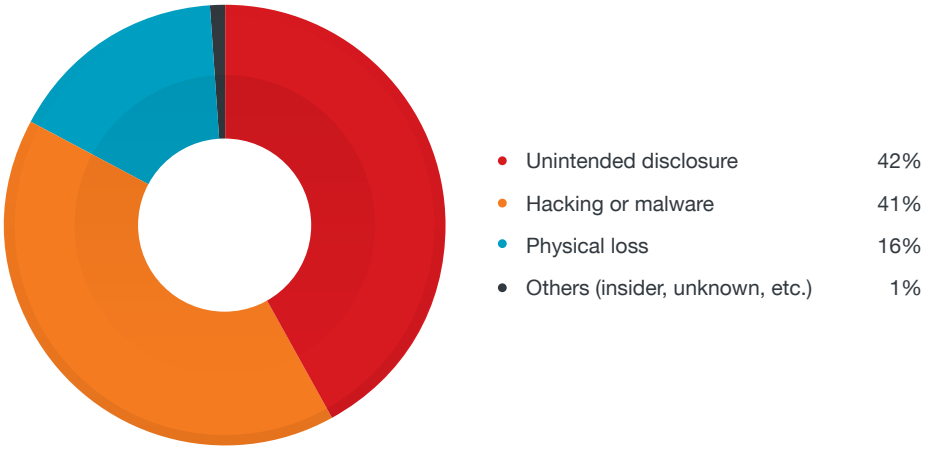

Figure 10. The top data breach method was unintended disclosure: Distribution of data breach methods in 1H 2018

A number of the larger breaches were related to unattended cloud assets. A nearly 2-terabyte database of up to 340 million records maintained by a marketing firm was discovered by a security researcher to have been exposed on a publicly accessible server.[46] A bug in a mobile network operator's website allowed anyone, using just a cellphone number, to access the personal details of any customer, although the bug was in a customer care portal and not on the main site.[47] A data technology company left a cloud storage bucket in a public cloud location — without a password — where the file it contained unpacked to over a terabyte of 48 million records representing individual profiles scraped from different social networks.[48] And a bakery-café chain company leaked millions of names, email addresses, and other customer records after simply leaving customer registration information in plain text on its website.[49] This series of incidents made it seem as though the previous years' data breaches, including several high-profile ones, had done little to change at least the basic aspects of enterprises' security hygiene, such as where and how customer data is kept.

Another interesting data point relates to how healthcare is the most breached industry in terms of number of incidents. In our research on exposed medical systems,[50] we highlighted several possible reasons that healthcare facilities seem to be having some difficulty in improving network security. These reasons include patient care's being the highest priority and hence where the bulk of resources are spent, the number of internal users who are in heavy rotation and have access to several systems, and the lack of dedicated cybersecurity response teams.

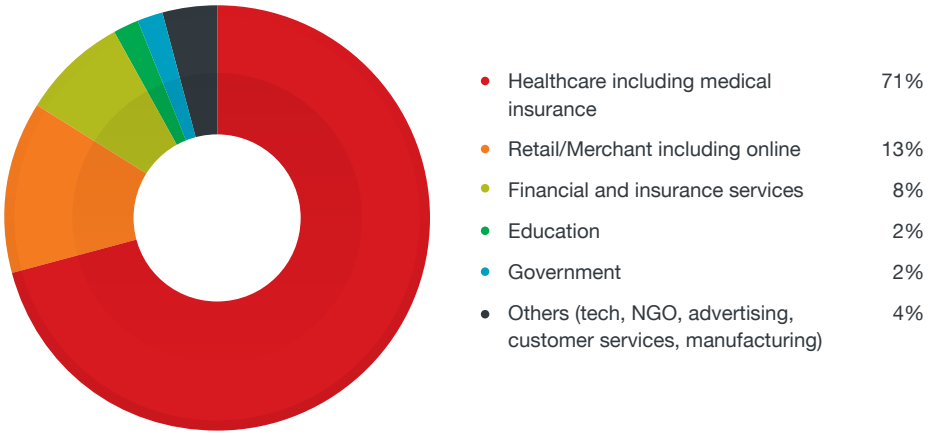

Figure 11. Healthcare was the most breached industry: Industry distribution of breaches in 1H 2018

We also looked at data breach advisories and disclosures from all over the world to get a broader view of the problem. (A summary of these publicly available data breach disclosures outside the U.S. is available in the Threat Landscape in Review section of this report.) We found no fewer than 18 data breaches that exposed at least 100,000 records, and at least nine that could be considered mega breaches.

The mega breaches outside the U.S. included one involving a Chinese video-sharing and streaming site, where close to 10 million records such as user IDs, nicknames, and passwords were leaked.[51] In Norway, a hacking attack on a healthcare provider exposed almost three million patient records.[52] In Israel, an app that connects preschool teachers with parents was found to have a vulnerability that allowed information shared in the app to be leaked online, including some six million photographs that might have contained children's faces or personal details.[53] And in Dubai, the storage system of a ride-hailing service was found to have been accessed by hackers, exposing the personal data of 14 million customers.[54]

It's easy to discount the impact of a data breach these days, considering that companies have bounced back even after experiencing major breaches.[55] But the impact of a data breach to an enterprise's bottom line is all too real. According to a global study that factors in several aspects of data breaches, the cost of mega breaches, specifically, can range from US$40 million to US$350 million.[56] Until enterprises learn their lesson, they will continue to run the risk of suffering the consequences of data breaches, including lost business and customers, reputation nosedives, and re-appropriation of resources for remediation.

Enterprises should shore up their defenses against data privacy issues, especially in light of the enforcement of the GDPR.[57] The regulation mandates the implementation of data privacy policies among companies that harvest, keep, process, or otherwise handle data of EU citizens. Notably, it requires affected companies to notify their customers, supervisory authorities, and at-risk parties of a data breach within 72 hours of becoming aware of it. Compliance with the GDPR can surely promote the proper

security posture for protecting data, whether or not it belongs to EU citizens, and it could have prevented a number of the incidents mentioned here.

Beyond mere compliance, however, enterprises should work toward fulfilling a comprehensive data protection strategy that implements security measures and multilayered technologies and also sets forth contingencies in the event of a security incident. And since unintended disclosures with regard to the use of cloud-based services were also a large part of recent data breaches, enterprises must also extend their security practices to the cloud and even to third-party partners that store their data.

Router security still weak despite Mirai alert

We have long been monitoring the threat landscape for the emergence of significant threats to the internet of things (IoT). However, as smart devices continue to increase in number, the standardization of the associated software still leaves much to be desired. Consequently, attackers are unlikely to find a homogeneous enough deployment of a specific device type or software to successfully exploit, and we have yet to see a massive attack that targets only smart devices. Meanwhile, an oft-overlooked component of internet communications is opening home and office networks, which can host all kinds of devices like regular computers and smart coffee machines, to cybercriminal attacks: the inconspicuous router.

In late March, we picked up scanning activity reminiscent of Mirai from infected routers in China, with Brazil-based devices as apparent targets.[58] First seen in 2016, Mirai was responsible for DDoS attacks coming from infected vulnerable devices.[59] Its source code has since been publicly released,[60] meaning cybercriminals can use and modify it to launch their own campaigns. As in previous cases, the use of default credentials was exploited by hackers to hijack internet-connected devices, a large portion of which were home routers and IP cameras.[61]

At around the same week, we were also able to obtain code indicating that a similar campaign was running in Brazil.[62] And in May, we detected another Mirai-like scanning activity in Mexico, but with the difference being the use of vulnerabilities specific to Gigabit Passive Optical Network (GPON),[63] a technology used in providing fiber connectivity to home or office networks.

However, the biggest networking device-based attack in the first half of 2018 was the multistage VPNFilter attack. Earlier similar pieces of malware like Mirai and Reaper, which affected more than one million organizations in 2017,[64] have relatively simple structures and payloads. VPNFilter, though, is quite different: It comprises a persistence component, a data harvester, and a sniffer plugin, and includes a virtual kill switch that can render a router unusable. While its activities have been seen since as early as 2016, at its peak, it was able to infect half a million networking or networked devices in at least 54 countries.[65]

Mirai (first variant in 2016)	Reaper (October 2017)	VPNFilter
• Scans a wide range of IP addresses. • Brute-forces devices with weak credentials via a predefined list of default credentials. • Used in DDoS attacks that involved hundreds of thousands of commandeered CCTV cameras, DVRs, and routers. • Caused several high-profile websites to be inaccessible. **Its source code has since been released, meaning other cybercriminals can build their own versions of the malware.*[69]	• Uses exploits in IoT devices. • Affects routers, IP cameras, and NAS devices. • Affected more than one million organizations. • Integrates an execution environment that allows operators to deliver codes for DDoS, traffic proxying, and other activities.	• Composed of three components built for redundancy and ensuring persistence. • Has a reconnaissance component that can also harvest data. • Contains a self-destruct function that can leave routers unrecoverable. • Affected 500,000 routers in at least 54 countries. • Has several plugins for increased functionality.

Table 1. VPNFilter had considerably more components than previous large router-based attacks: Comparison of Mirai, Reaper, and VPNFilter

Despite the awareness raised regarding this attack, which even included a public service announcement by the Federal Bureau of Investigation (FBI) warning users to power-cycle their routers,[70] small business and home office networks remained vulnerable not only to the VPNFilter attack but also to several other vulnerabilities. In our scan data on potentially VPNFilter-affected routers, we were able to identify 19 bugs in total to which said devices are vulnerable. The vulnerabilities were a mix of years-old vulnerabilities, like CVE-2011-4723, and relatively newer ones, including several password- and authentication-related issues.[71]

VPNFilter's coverage, along with the combined impact of the earlier attacks, paints a vivid picture of what exactly is at risk when users continue to fail to heed common-sense router security best practices, such as changing default username and password combinations (since these are often searchable and thus easy to crack remotely), changing default settings, and regularly checking for and installing firmware updates.

Fileless, macro and small-sized malware challenges purely file-based security technologies

Traditional antimalware solutions have a straightforward relationship with new malware variants: Vendors can create a range of pattern types that can detect the specific malware or variants thereof. While no groundbreaking evasion technique has been seen in 2018 so far, we have observed how cybercriminals persist in fine-tuning individual malware campaigns in order to increase their chances of circumventing file-based detection technologies. We have seen cybercriminals do this in the first half of 2018 notably through their use of fileless threats, macros, and malware with small file sizes.

Fileless threats are so named because they are typically executed in a system's memory or they reside in the system registry, rather than making use of binaries or executables that are written to a machine's local storage. In a way, their use is akin to getting rid of the paper trail and performing the malicious activities on the fly. The malicious code can be injected into the memory of a running application or by running scripts via otherwise legitimate tools like PowerShell. We are able to detect fileless threat activities by tracking non-file-based indicators such as specific execution events or behaviors.

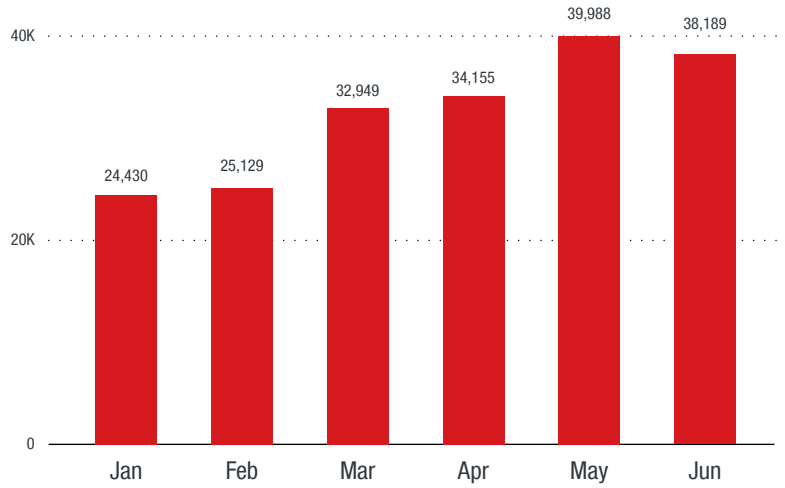

Figure 12. Fileless malware continued to be seen: Fileless events blocked by month in 1H 2018

Macros also continued to be part of the threat landscape, but an uptick in May was seen in part due to Powload, specifically its distribution via malicious spam.[72] The spam typically leads to malware like Ursnif and Bebloh, but first relies on the attached or linked macro to execute the download of the final payload. Outside of spam, however, we saw malicious macros used even in targeted-attack campaigns. Similar to the MuddyWater campaign tactic used in 2017, a targeted attack component we found in May involved a malicious Word document embedded with a malicious macro. Once macros are enabled, the code will execute the crafted PowerShell scripts to ultimately download a backdoor, which presumably is the main reconnaissance component.[73]

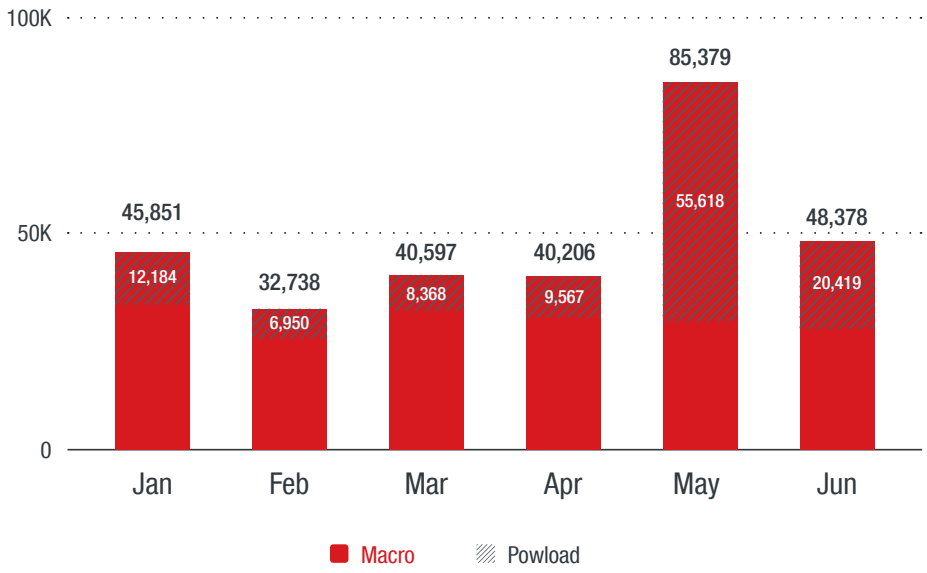

Figure 13. The uptick in macro malware detections was due to Powload: Macro malware and Powload detections by month

Macros continue to be attractive to cybercriminals as a delivery mechanism because they provide another way of concealing malicious intent while retaining powerful functionality. Macro malware is more difficult to detect than malware executables because they run the intended code only after a user enables macros in a file, thereby keeping traditional file scanning from revealing any malicious code at the onset.

Another important uptick we observed in the first half of 2018 concerned the proliferation of TinyPOS, a years-old family of point-of-sale (POS) malware that has an extremely small size. It was so prevalent during this period that it accounted for about three quarters of the total POS malware detected.

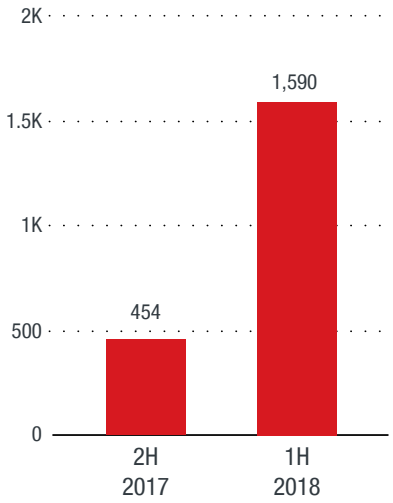

Figure 14. POS malware detections increased:
Half-year comparison of POS malware detections

We believe the increase might be in part due to the release in May of the source code of TreasureHunter, a POS malware family that has been seen since as early as 2014.[74] It's not unusual for similar or related malware infections to see a spike in the event of a malware source code leak. The source code release widens the reach of POS malware to other cybercriminals wanting to venture into the lucrative retailer space and building their own versions for their own campaigns. Additionally, a new family of POS malware called PinkKite emerged,[75] which Trend Micro also detects as TinyPOS.

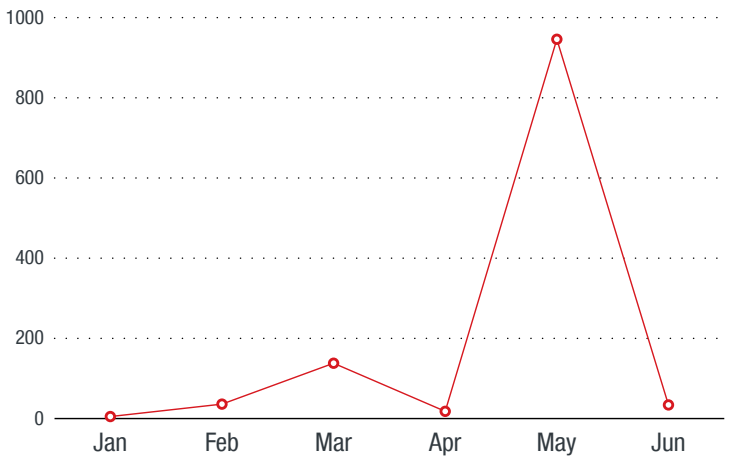

Figure 15. TinyPOS detection spike happened in May:
TinyPOS monthly detections for 1H 2018

These pieces of POS malware have small file sizes, which typically leave cybercriminals a few options in terms of commands — for instance, there is only space to include a URL or an IP address for call-home purposes. This structure, however, can be easily mistaken for normal or benign files, so detecting it, though not impossible, becomes a bit more challenging.

For IT admins in charge of large retailers that use POS terminals heavily, it is important to establish a multilayered means of protection. Endpoint application control can protect retailer networks from POS malware by restricting execution of software only to whitelisted applications, while network-based solutions can flag outbound communications on top of examining inbound ones.

The prevalent trend of fileless threats and the like signals an awareness by cybercriminals of the inherent weaknesses of relying solely on antimalware technologies. Fortunately, most threats are multi-component by nature: They use emails or links as delivery mechanisms, deliver other components or the final payloads via servers, or leave behavioral clues in network or system logs. Enterprises can manage the risk of fileless and macro threats by taking a cross-generational approach and employing additional, integrated layers of protection across the network.

BEC losses exceed projection as BEC attempts exhibit steady growth

Incidents of business email compromise (BEC) continue to be a problem for enterprises. In BEC attacks, the classic social engineering tactic is at work: By impersonating certain people (like C-level executives, a regular supplier or employee asking for payment, an attorney) via email, scammers can intercept funds in what should have been routine money transfers to other people inside the company or third parties such as vendors and service providers. In some cases scammers would steal personally identifiable information of employees and executives towards the same goal.

While the actual attack details may differ per incident, BEC requires attackers to conduct enough reconnaissance about the target company to identify clues or weaknesses that they can exploit. They can then either convincingly impersonate a figure of authority, usually a C-level executive, who can authorize wire transfers or request sensitive information (like a company's W-2 records[76]), or hijack that person's email account. BEC is low-tech — it relies heavily on open-source intelligence and social engineering — but it is incredibly high-yield. This is why we predicted the continued increase of BEC losses well into 2018.[77]

The FBI, which has been monitoring BEC scams since October 2013, has recently updated its running total of losses incurred in reported BEC and email account compromise (EAC) incidents to US$12.5 billion,[78] which represents a 136-percent increase from the agency's last tally in May 2017. This number is also 39-percent higher than our minimum projection of cumulative losses from BEC attacks, indicating a worsening ability by targets to identify scams from normal email communications despite regular advisories from law enforcement and considerable media coverage of the activities.

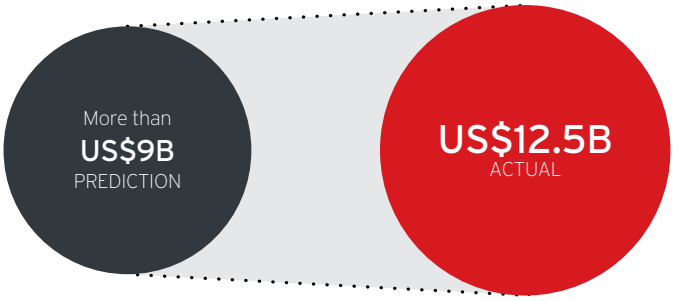

Figure 16. Actual cumulative losses from BEC and EAC exceeded Trend Micro's minimum projection: Cumulative losses from BEC and EAC incidents according to the FBI

Meanwhile, we observed a 5-percent increase in BEC attempts in the first half of 2018, compared to the second half of 2017.

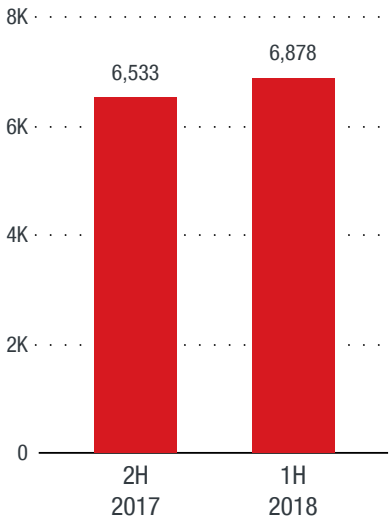

Figure 17. Number of BEC attempts increased: Half-year comparison of recorded BEC attempts

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

The BEC problem has become such an international issue that federal authorities in the U.S., including the FBI and the Department of Justice, have launched Operation WireWire. The coordinated effort has led to 74 arrests in the U.S. and other countries (including Nigeria, Canada, Mauritius, and Poland) and the recouping of around US$14 million in fraudulent money transfers.[79] This development will definitely affect the volume of BEC scams, but new individuals or groups could step up given the ease of implementation of these attacks.

On the network level, enterprises need to start looking at better strategies to deal with email-based threats. Because of their use of social engineering, file-based detection will not work, but email reputation technologies can, to a certain extent, assist in protection. In addition, BEC-specific solutions, such as artificial intelligence-powered solutions that use expert rules and machine learning techniques[80] like analyzing email senders' writing styles to scrutinize as to whether certain emails are spoofing persons in the company, are worth looking into.

Threat Landscape in Review

In the first half of 2018, the Trend Micro™ Smart Protection Network™ infrastructure was able to protect users from over 20 billion threats — a multitude of different email, file, and URL components used in different cybercriminal operations.

20,488,399,209

Overall threats blocked in the first half of 2018

This volume of threats is just a few billion threats lesser than in the previous half year.

Figure 18. Volume of email and URL threats blocked increased slightly: Quarterly comparison of blocked email, file, and URL threats

We observed a spike in the number of new detected cryptocurrency miner families as well, owing to cybercriminals' increasing interest in mining virtual currency using as many user devices as they can infect.

BATMINE	DLDRETN	MALKARBO	MINERBOT	POWXMR	TOOLXMR
BLOUIROET	HELAMINE	MALLTC	MMBTC	RETADUP	TOOLZEC
BTCTOOL	LINDMINE	MALREP	MMETH	SHAOSMINE	WEBJSE
COFFEE	MALBTC	MALXCN	MMXMR	SILVERSPACEETN	XENOM
CRYPTOLOOT	MALDCR	MALXMR	MNRGRIMEX	TOOLBTC	XMRMINE
CRYPTONIGHT	MALELI	MALXMRIG	OPMINE	TOOLDBL	XMRTOOL
DASH	MALETH	MALXR	OTOTI	TOOLETN	ZCAMINE
DLDRETH	MALETN	MALZEC	POOLVAULT	TOOLRVN	

Table 2. 47 new cryptocurrency miner malware families were detected:
New cryptocurrency miner malware families detected in 1H 2018

Meanwhile, this development does not mean that ransomware has disappeared from the landscape. The business model of extortion via ransomware will likely remain as a viable means of gaining profit for cybercriminals. However, the total number of new ransomware families decreased overall.

ACKNYS	CRYPTOR	EXOCRYPT	INSTALADOR	PAIN	STINGER
ADAMLOCKER	CRYPWALKER	FAKEKILLBOT	KASITOO	PEDCOT	SURESOME
ANIMUS	CSGO	FBLOCKER	KINGBOROS	PESOJ	TALINSLOCKER
AURORA	CYPEN	FILECODER	KRAKATOWIS	RANCIDLOCKER	TBLOCKER
AUSIV	CYSEARCHER	FILECRYPTOR	LADON	RANDOMLOCKER	TEARDROP
AUTISMLOCKER	DATAKEEPER	FOREIGN	LAZAGNECRYPT	RAPID	TEERAC
AVCRYPT	DEATHNOTEBATCH	FURY	LEBANA	REDEYE	THANATOS
BANACRYPT	DEDWARE	GANDCRAB	LILFINGER	RONT	TK
BLACKHEART	DEFENDER	GEGLOCKER	LIME	RSAUTIL	TRON
BLACKRUBY	DEUSCRYPT	GLOBIM	MAGICIAN	RUSSENGER	USELESS
BLANK	DGER	GOODRABBIT	MEINE	SATURN	VBRSCARE
BOSLOKI	DIRCRYPT	HAKNATA	MINDCRYPT	SATWANCRYPT	VERTUN
BYTELOCKER	DISKDOC	HARROS	MINDLOST	SATYR	WADHRAMA
CARDSOME	DONUT	HAXLOCKER	MONEROPAY	SEPSIS	WANNAPEACE
CCP	DOTZERO	HEARTBLEED	NECNE	SEQUR	WHITEROSE
CESLOCKER	DWORRY	HERMES	NIKSEAD	SIGMA	WYVERN
CRUSIS	DYAR	HOLA	NMCRYPT	SIGRUN	ZENIS
CRYBRZ	ELGOSCARE	HONOR	NOWORI	SKIDDY	ZLOCKER
CRYPT	EMBRACE	HORSUKE	PABGEE	SKYFILE	
CRYPTOLOOT	EVERBE	INSANECRYPT	PACTELUNG	STACUS	

Table 3. 118 new ransomware families were seen: New ransomware families in 1H 2018

Exploit kits, likewise, continued its somewhat subdued presence in the landscape. The total number of attacks decreased, even if operators continued to update the kits with newer exploits, as discussed earlier.

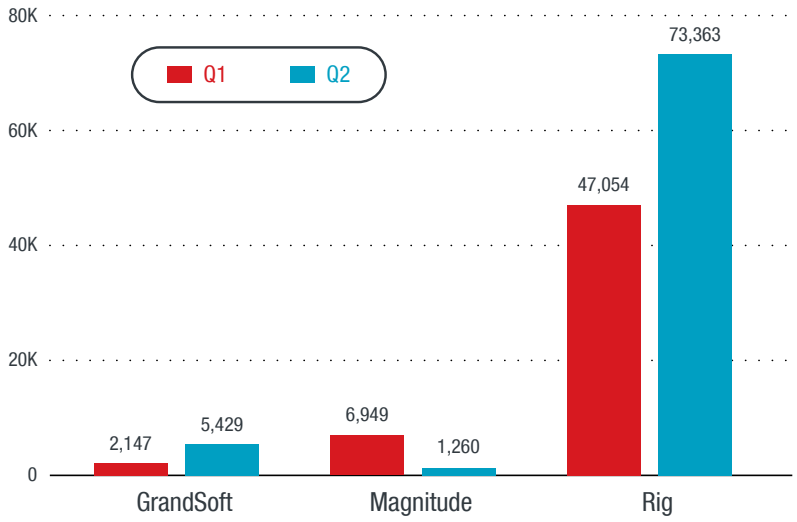

Figure 19. Exploit kit activity increased in Q2, Rig being the most active: Quarterly exploit kit activity by exploit kit

The decline in ransomware is also reflected in the volume of mobile apps that have ransomware capabilities. However, they have not completely dropped out of the threat landscape and are thus still an important threat that smartphone users need to be aware of.

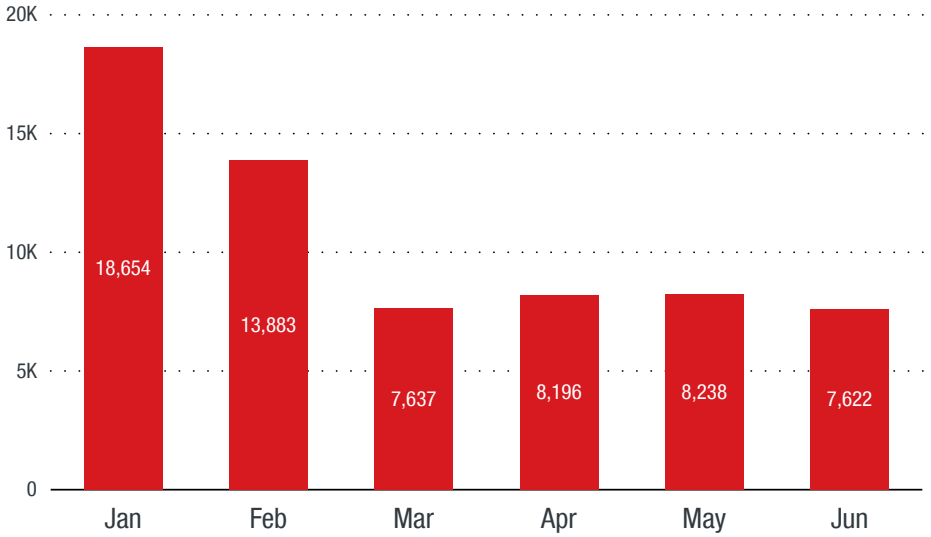

Figure 20. Unique mobile ransomware sourced by Mobile App Reputation Service (MARS) decreased: Monthly unique mobile ransomware detections in 1H 2018

Data breaches have been part and parcel of the increasing reliance of more and more organizations on online resources and cloud services for several years now. However, media attention has often been on breaches that occur in the U.S., where a lot of technology services are based. This does not mean, though, that data breaches are not an issue outside that country.

Company description	Date made public	Country/ Territory	Total records
Ride-hailing service	Apr 23	U.A.E.	14,000,000[81]
Bank	May 2	Australia	12,000,000[82]
State-franchised lottery group	Mar 16	U.K.	10,500,000[83]
Online school exam analysis system	Jun 10	Malaysia	10,300,000[84]
Video streaming and sharing site	Jun 13	China	10,000,000[85]
Consumer electronic retailer	Jun 13	U.K.	10,000,000[86]
Child-centric communication app	Mar 11	Israel	8,500,000[87]
Government ministry	Mar 24	India	5,000,000[88]
Healthcare facility	Jan 18	Norway	3,000,000[89]
Telecommunications provider	Feb 7	Switzerland	800,000[90]
News magazine organization	Mar 1	France	693,000[91]
IT-oriented online portal	Feb 20	Singapore	685,000[92]
Payroll system	Feb 17	India	550,000[93]
Parcel delivery company	Feb 7	Ukraine	500,000[94]
Broadband provider	Apr 18	Hong Kong	380,000[95]
Wireless telecommunications provider	Feb 12	Canada	350,000[96]
Hotel	Jun 26	Japan	124,963[97]
Telecommunications provider	Jan 24	Canada	100,000[98]

Table 4. As many as 18 non-U.S. data breaches exposed at least 100,000 records each: Non-U.S. data breaches in 1H 2018

References

1. Jann Horn. (3 January 2018). *Google Project Zero*. "Reading Privileged Memory with a Side-Channel." Last accessed on 31 July 2018 at https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html.

2. Vit Sembera. (5 January 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "When Speculation Is Risky: Understanding Meltdown and Spectre." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/speculation-risky-understanding-meltdown-spectre/.

3. Graz University of Technology. (2018). *Graz University of Technology*. "Meltdown and Spectre." Last accessed on 31 July 2018 at https://meltdownattack.com/.

4. Vit Sembera. (5 January 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "When Speculation Is Risky: Understanding Meltdown and Spectre." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/speculation-risky-understanding-meltdown-spectre/.

5. Tom Warren. (21 May 2018). *The Verge*. "Google and Microsoft disclose new CPU flaw, and the fix can slow machines down." Last accessed on 1 August 2018 at https://www.theverge.com/2018/5/21/17377994/google-microsoft-cpu-vulnerability-speculative-store-bypass-variant-4.

6. Liam Tung. (1 February 2018). *ZDNet*. "Meltdown-Spectre: Malware is already being tested by attackers." Last accessed on 1 August 2018 at https://www.zdnet.com/article/meltdown-spectre-malware-is-already-being-tested-by-attackers/.

7. Tom Warren. (9 January 2018). *The Verge*. "Microsoft reveals how Spectre updates can slow your PC down." Last accessed on 1 August 2018 at https://www.theverge.com/2018/1/9/16868290/microsoft-meltdown-spectre-firmware-updates-pc-slowdown.

8. Microsoft. (3 January 2018). *Microsoft*. "January 3, 2018—KB4056892 (OS Build 16299.192)." Last accessed on 31 July 2018 at https://support.microsoft.com/en-us/help/4056892/windows-10-update-kb4056892?ranMID=24542&ranEAID=nOD%2FrLJHOac&ranSiteID=nOD_rLJHOac-D9iMSKjIaU4uYO.RnHdkpA&tduid=(ec86be2bfc16e6f8ec4721531d601e74)(256380)(2459594)(nOD_rLJHOac-D9iMSKjIaU4uYO.RnHdkpA)().

9. Kafeine. (25 May 2018). *MDNC | Malware don't need coffee*. "CVE-2018-8174 (VBScript Engine) and Exploit Kits." Last accessed on 14 August 2018 at https://malware.dontneedcoffee.com/2018/05/CVE-2018-8174.html.

10. Security Tech Center. (8 May 2018). *Microsoft*. "CVE-2018-8174 | Windows VBScript Engine Remote Code Execution Vulnerability." Last accessed on 31 July 2018 at https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8174.

11. Weibo. (20 April 2018). *Weibo*. "新型Office攻击使用浏览器"双杀"漏洞." Last accessed on 31 July 2018 at https://www.weibo.com/ttarticle/p/show?id=2309404230886689265523.

12. Miguel Ang, Martin Co, and Michael Villanueva. (31 May 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Rig Exploit Kit Now Using CVE-2018-8174 to Deliver Monero Miner." Last accessed on 31 July 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/rig-exploit-kit-now-using-cve-2018-8174-to-deliver-monero-miner/.

13. Martin Co and Joseph C. Chen. (2 July 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Down but Not Out: A Look into Recent Exploit Kit Activities." Last accessed on 31 July 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/a-look-into-recent-exploit-kit-activities/.

14. Trend Micro Zero Day Initiative Team. (23 May 2017). *Trend Micro Security News*. "Hacker Machine Interface." Last accessed on 31 July 2018 at https://documents.trendmicro.com/assets/wp/wp-hacker-machine-interface.pdf.

15. Ibid.

16. European Commission. (5 July 2016). *European Commission*. "The Directive on Security of Network and Information Systems (NIS Directive)." Last accessed on 1 August 2018 at https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

17. UK Government. (8 August 2017). *UK Government*. "New Fines for Essential Service Operators with Poor Cyber Security." Last accessed on 31 July 2018 at https://www.gov.uk/government/news/new-fines-for-essential-service-operators-with-poor-cyber-security.

18. EUGDPR.org. *EU GDPR Portal*. "GDPR Key Changes." Last accessed on 31 July 2018 at https://www.eugdpr.org/key-changes.html.

19. Justin Wetherill. (21 March 2018). *Forbes*. "Cryptocurrency Gold Rush And The Unforeseen Effect On PC Gamers." Last accessed on 1 August 2018 at https://www.forbes.com/sites/forbestechcouncil/2018/03/21/cryptocurrency-gold-rush-and-the-unforeseen-effect-on-pc-gamers/#5f4ca1f36286.

20. Menard Oseña. (28 February 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Cryptocurrency-Mining Malware: 2018's New Menace?" Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-mining-malware-2018-new-menace/.

21. Bloomberg. (31 January 2018). *Fortune.com*. "How to Steal $500 Million in Cryptocurrency." Last accessed on 1 August 2018 at http://fortune.com/2018/01/31/coincheck-hack-how/.

22. Charlie Osborne. (13 April 2018). *ZDNet*. "Coinsecure, not so Secure: Millions in Cryptocurrency Stolen, CSO Blamed." Last accessed on 1 August 2018 at https://www.zdnet.com/article/coinsecure-not-so-secure-millions-in-cryptocurrency-stolen-cso-branded-as-thief/.

23. Bitcoin Price News. (22 June 2018). *CCN*. "Cryptocurrency Market Suffers Ongoing Decline, Analysts Weigh Causes." Last accessed on 1 August 2018 at https://www.ccn.com/cryptocurrency-market-suffers-ongoing-decline-analysts-weigh-causes/.

24. Hubert Lin. (19 January 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Struts and DotNetNuke Server Exploits Used For Cryptocurrency Mining." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/struts-dotnetnuke-server-exploits-used-cryptocurrency-mining/.

25. Chaoying Liu and Joseph C. Chen. (26 January 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Malvertising Campaign Abuses Google's DoubleClick to Deliver Cyrptocurrency Miners." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/malvertising-campaign-abuses-googles-doubleclick-to-deliver-cryptocurrency-miners/.

26. 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 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/oracle-server-vulnerability-exploited-deliver-double-monero-miner-payloads/.

27. Joseph C. Chen. (1 February 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Malicious Chrome Extensions Found in Chrome Web Store, Form Droidclub Botnet." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/malicious-chrome-extensions-found-chrome-web-store-form-droidclub-botnet/.

28. 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 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-miner-distributed-via-php-weathermap-vulnerability-targets-linux-servers/.

29. 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 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/pop-up-ads-and-over-a-hundred-sites-are-helping-distribute-botnets-cryptocurrency-miners-and-ransomware/.

30. Chaoying Liu and Joseph C. Chen. (4 April 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Cryptocurrency Web Miner Script Injected into AOL Advertising Platform." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-web-miner-script-injected-into-aol-advertising-platform/.

31. 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 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-xiaoba-repurposed-as-file-infector-and-cryptocurrency-miner/.

32. Lenart Bermejo and Ronnie Giagone. (21 April 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Monero-Mining RETADUP Worm Goes Polymorphic, Gets an AutoHotKey Variant." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-retadup-worm-goes-polymorphic-gets-an-autohotkey-variant/.

33. Joseph C. Chen. (30 April 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "FacexWorm Targets Cryptocurrency Trading Platforms, Abuses Facebook Messenger for Propagation." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/facexworm-targets-cryptocurrency-trading-platforms-abuses-facebook-messenger-for-propagation/.

34. 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 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/malicious-traffic-in-port-7001-surges-as-cryptominers-target-patched-2017-oracle-weblogic-vulnerability/.

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 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-mining-bot-targets-devices-with-running-ssh-service-via-potential-scam-site/.

36. Anita Hsieh, Rubio Wu, and Kawabata Kohei. (28 June 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "The New Face of Necurs: Noteworthy Changes to Necurs' Behaviors." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/the-new-face-of-necurs-noteworthy-changes-to-necurs-behaviors/.

37. Trend Micro Smart Home Network and IoT Reputation Service Teams. (21 June 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Drupal Vulnerability (CVE-2018-7602) Exploited to Deliver Monero-Mining Malware." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/drupal-vulnerability-cve-2018-7602-exploited-to-deliver-monero-mining-malware/.

38. Curtis Franklin, Jr. (21 March 2018). *Dark Reading*. "GandCrab Ransomware Goes 'Agile'." Last accessed on 1 August 2018 at https://www.darkreading.com/attacks-breaches/gandcrab-ransomware-goes-agile/d/d-id/1331336?ngAction=register&ngAsset=389473.

39. Raphael Centeno. (1 May 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Legitimate Application AnyDesk Bundled with New Ransomware Variant." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/legitimate-application-anydesk-bundled-with-new-ransomware-variant/.

40. Trend Micro. (11 May 2018). *Trend Micro Security News*. "SynAck Ransomware Leverages Process Doppelgänging for Evasion and Infection." Last accessed on 1 August 2018 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/synack-ransomware-leverages-process-doppelg-nging-for-evasion-and-infection.

41. Trend Micro. (20 February 2018). *Trend Micro Security News*. "Black Ruby Ransomware Targets Non-Iranian Users, Adds Coinminer." Last accessed on 1 August 2018 at https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/black-ruby-ransomware-targets-non-iranian-users-adds-coinminer.

42. Trend Micro. (2016). *TrendLabs Primer*. "Securing Data Through Network Segmentation in Modern Enterprises." Last accessed on 1 August 2018 at https://documents.trendmicro.com/assets/primers/securing-data-through-network-segmentation.pdf.

43. Ibid.

44. Privacy Rights Clearinghouse. (2017). *Privacy Rights Clearinghouse*. "Data Breaches." Last accessed on 2 February 2018 at https://www.privacyrights.org/data-breaches?title=&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&orsg_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&org_type%5B%5D=2437&taxonomy_vocabulary_11_tid%5B%5D=2434.

45. Privacy Rights Clearinghouse. (2018). *Privacy Rights Clearinghouse*. "Data Breaches." Last accessed on 11 July 2018 at https://www.privacyrights.org/data-breaches?title=&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&org_type%5B%5D=2437&taxonomy_vocabulary_11_tid%5B%5D=2436.

46. Andy Greenberg. (27 June 2018). *Wired*. "Marketing Firm Exactis Leaked a Personal Info Database with 340 Million Records." Last accessed on 1 August 2018 at https://www.wired.com/story/exactis-database-leak-340-million-records/.

47. Zack Whittaker. (24 May 2018). *ZDNet*. "T-Mobile Bug Let Anyone See Any Customer's Account Details." Last accessed on 31 July 2018 at https://www.zdnet.com/article/tmobile-bug-let-anyone-see-any-customers-account-details/.

48. Robert Abel. (19 April 2018). *SC Magazine*. "Social Media Aggregator LocalBlox Leaves 48M Records Exposed." Last accessed on 1 August 2018 at https://www.scmagazine.com/in-the-wake-of-the-facebook-cambridge-analytica-scandal-social-media-data-aggregation-firm-localblox-left-an-aws-bucket-misconfigured/article/759886/.

49. Brian Krebs. (2 April 2018). *Krebs on Security*. "Panerabread.com Leaks Millions of Customer Records." Last accessed on 31 July 2018 at https://krebsonsecurity.com/2018/04/panerabread-com-leaks-millions-of-customer-records/.

50. Mayra Rosario Fuentes and Numaan Huq. (5 April 2018). *Trend Micro*. "Securing Connected Hospitals." Last accessed on 1 August 2018 at https://documents.trendmicro.com/assets/rpt/rpt-securing-connected-hospitals.pdf.

51. ACFun. (13 June 2018). *ACFun*. "【公告】关于AcFun受黑客攻击致用户数据外泄的公." Last accessed on 1 August 2018 at http://www.acfun.cn/a/ac4405547.

52. Sooraj Shah. (18 January 2018). *The Inquirer*. "'Professional' hack on Norwegian health authority compromises data of three million patients." Last accessed on 1 August 2018 at https://www.theinquirer.net/inquirer/news/3024692/norway-health-south-east-rhf-hacked.

53. Amitai Ziv. (11 March 2018). *Haaretz*. "Data Breach Left Millions of Israeli Kids' Pictures Vulnerable to Hacking." Last accessed on 1 August 2018 at https://www.haaretz.com/israel-news/data-breach-left-millions-of-israeli-kids-pics-vulnerable-to-hacking-1.5889251.

54. Khaleej Times. (24 April 2018). *Khaleej Times*. "Dubai's Careem Admits to Data Breach of 14 Million Users." Last accessed on 1 August 2018 at https://www.khaleejtimes.com/nation/dubai//dubais-careem-admits-to-data-breach-of-14-million-users.

55. Natalie Gagliordi. (27 November 2015). *ZDNet*. "The Target Breach, Two Years Later." Last accessed on 1 August 2018 at https://www.zdnet.com/article/the-target-breach-two-years-later/.

56. Dean Takahashi. (10 July 2018). *VentureBeat*. "IBM Security Study: Mega Data Breaches Cost $40 Million to $350 Million." Last accessed on 1 August 2018 at https://venturebeat.com/2018/07/10/ibm-security-study-mega-data-breaches-cost-40-million-to-350-million/.

57. Trend Micro. *Trend Micro*. "EU General Data Protection Regulation (GDPR)." Last accessed on 1 August 2018 at https://www.trendmicro.com/vinfo/us/security/definition/eu-general-data-protection-regulation-gdpr.

58. 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 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/mirai-like-scanning-activity-detected-from-china-targets-in-brazil/.

59. Trend Micro. (26 October 2016). *Trend Micro TrendLabs Security Intelligence Blog*. "The Internet of Things Ecosystem is Broken. How Do We Fix It?" Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/internet-things-ecosystem-broken-fix/.

60. Brian Krebs. (1 Ocotber 2016). *Krebs on Security*. "Source Code for IoT Botnet 'Mirai' Released." Last accessed on 1 August 2018 at https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/.

61. 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 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/mirai-like-scanning-activity-detected-from-china-targets-in-brazil/.

62. Fernando Mercês. (17 April 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Not Only Botnets: Hacking Group in Brazil Targets IoT Devices With Malware." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/not-only-botnets-hacking-group-in-brazil-targets-iot-devices-with-malware/.

63. Trend Micro IoT Reputation Service Team and Trend Micro Smart Home Network Team. (21 May 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "GPON Vulnerabilities Exploited for Mexico-based Mirai-like Scanning Activities." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/gpon-vulnerabilities-exploited-for-mexico-based-mirai-like-scanning-activities/.

64. Trend Micro. (24 October 2017). *Trend Micro Security News*. "Millions of Networks Compromised by New Reaper Botnet." Last accessed on 1 August 2018 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/millions-of-networks-compromised-by-new-reaper-botnet.

65. Trend Micro. (24 May 2018). *Trend Micro Security News*. "Reboot Your Routers: VPNFilter Infected Over 500,000 Routers Worldwide." Last accessed on 1 August 2018 at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/reboot-your-routers-vpnfilter-infected-over-500-000-routers-worldwide.

66. Kevin Y. Huang, Fernando Mercês, and Lion Gu. (14 December 2016). *Trend Micro TrendLabs Security Intelligence Blog*. "Home Routers: Mitigating Attacks That Can Turn Them to Zombies." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/home-routers-mitigating-attacks-that-turn-them-to-zombies/.

67. Trend Micro. (24 October 2017). *Trend Micro Security News*. "Millions of Networks Compromised by New Reaper Botnet." Last accessed on 1 August 2018 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/millions-of-networks-compromised-by-new-reaper-botnet.

68. Trend Micro. (24 May 2018). *Trend Micro Security News*. "Reboot Your Routers: VPNFilter Infected Over 500,000 Routers Worldwide." Last accessed on 1 August 2018 at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/reboot-your-routers-vpnfilter-infected-over-500-000-routers-worldwide.

69. Brian Krebs. (1 October 2016). *Krebs on Security*. "Source Code for IoT Botnet 'Mirai' Released." Last accessed on 1 August 2018 at https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/.

70. Federal Bureau of Investigation Internet Crime Commission. (25 May 2018). *FBI IC3*. "Foreign Cyber Actors Target Home and Office Routers and Networked Devices Worldwide." Last accessed on 1 August 2018 at https://www.ic3.gov/media/2018/180525.aspx.

71. Tony Yang and Peter Lee. (13 July 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "VPNFilter-affected Devices Still Riddled with 19 Vulnerabilities." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/vpnfilter-affected-devices-still-riddled-with-19-vulnerabilities/.

72. Trend Micro. (10 May 2018). *Trend Micro Virus Encyclopedia*. "X2KM_POWLOAD.AOEDT Virus Definition." Last accessed on 1 August 2018 at https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/x2km_powload.aoedt.

73. Michael Villanueva and Martin Co. (14 June 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Another Potential MuddyWater Campaign uses Powershell-based PRB-Backdoor." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/another-potential-muddywater-campaign-uses-powershell-based-prb-backdoor/.

74. Jai Vijayan. (10 May 2018). *Dark Reading*. "Author of TreasureHunter PoS Malware Releases Its Source Code." Last accessed on 1 August 2018 at https://www.darkreading.com/vulnerabilities---threats/author-of-treasurehunter-pos-malware-releases-its-source-code-/d/d-id/1331778.

75. Ionut Arghire. (16 March 2018). *Security Week*. "PinkKite POS Malware Is Small But Powerful." Last accessed on 31 July 2018 at https://www.securityweek.com/pinkkite-pos-malware-small-powerful.

76. John Wilson. (29 March 2018). *Forbes*. "Tax Time is W-2 Scam Time." Last accessed on 1 August 2018 at https://www.forbes.com/sites/forbestechcouncil/2018/03/29/tax-time-is-w-2-scam-time/#41578ee652fa.

77. Trend Micro. (5 December 2017). *Trend Micro*. "Paradigm Shifts." Last accessed on 1 August 2018 at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2018.

78. Federal Bureau of Investigation. (12 July 2018). *FBI IC3*. "Business Email Compromise: The 12 Billion Scam." Last accessed on 1 August 2018 at https://www.ic3.gov/media/2018/180712.aspx.

79. Federal Bureau of Investigation. (11 June 2018). *FBI*. "International Business E-Mail Compromise Takedown." Last accessed on 1 August 2018 at https://www.fbi.gov/news/stories/international-bec-takedown-061118.

80. Trend Micro. (16 April 2018). *Trend Micro Security News*. "Curbing the BEC Problem Using AI and Machine Learning." Last accessed on 1 August 2018 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/curbing-the-bec-problem-using-ai-and-machine-learning.

81. Careem. (23 April 2018). *Careem*. “Important Security Information.” Last accessed on 1 August 2018 at https://blog.careem.com/en/security/.

82. Paul Farrelll. (2 May 2018). *Buzzfeed News*. “Australia’s Largest Bank Lost The Personal Financial Histories Of 12 Million Customers.” Last accessed on 1 August 2018 at https://www.buzzfeed.com/paulfarrell/australias-largest-bank-lost-the-personal-financial?utm_term=.so2yyQbV8K#.qqGaakAm2X.

83. DataBreaches.net. (16 March 2018). *DataBreaches.net*. “National Lottery Hacked: 10.5M Players are Warned to Change Their Passwords.” Last accessed on 1 August 2018 at https://www.databreaches.net/national-lottery-hacked-10-5m-players-are-warned-to-change-their-passwords/.

84. Zurairi Ar. (9 June 2018). *MSN*. “Putrajaya’s Exam Portal Shut Down, After Data Breach Affecting Millions.” Last accessed on 1 August 2018 at https://www.msn.com/en-us/news/national/putrajaya%E2%80%99s-exam-portal-shut-down-after-data-breach-affecting-millions/ar-AAyrb5c?li=AAaD1A0.

85. Global Times. (13 June 2018). *Global Times*. “Hackers Attack Popular Video-Sharing Site, Breach Millions of Private Info.” Last accessed on 1 August 2018 at http://www.globaltimes.cn/content/1106860.shtml.

86. Rory Cellan-Jones. (31 July 2018). *BBC News*. “Dixons Carphone Says Data Breach affected 10 Million.” Last accessed on 1 August 2018 at https://www.bbc.com/news/business-45016906.

87. Amitai Ziv. (11 March 2018). *Haaretz*. “Data Breach Left Millions of Israeli Kids’ Pictures Vulnerable to Hacking.” Last accessed on 1 August 2018 at https://www.haaretz.com/israel-news/data-breach-left-millions-of-israeli-kids-pics-vulnerable-to-hacking-1.5889251.

88. JKR Staff. (24 March 2018). *Janta Ka Reporter*. “Revealed! Personal Data of 50 Lakh Ex-servicemen May Have Been Breached, Armed Forces Veteran Calls It Chilling.” Last accessed on 1 August 2018 at http://www.jantakareporter.com/india/personal-data-50-lakh-ex-servicemen-may-breached/177927/.

89. Sooraj Shah. (18 January 2018). *The Inquirer*. “‘Professional’ hack on Norwegian health authority compromises data of three million patients.” Last accessed on 1 August 2018 at https://www.theinquirer.net/inquirer/news/3024692/norway-health-south-east-rhf-hacked.

90. Jason Murdock. (7 February 2018). *International Busines Times*. “Swisscom data breach: Personal details of one in ten Swiss citizens stolen.” Last accessed on 1 August 2018 at https://www.ibtimes.co.uk/swisscom-data-breach-personal-details-one-ten-swiss-citizens-stolen-1659593.

91. Zack Whittaker. (1 March 2018). *ZDNet*. “French News Site L’Express Exposed Reader Data Online, Weeks Before GDPR Deadline.” Last accessed on 1 August 2018 at https://www.zdnet.com/article/french-magazine-lexpress-exposed-reader-data/.

92. Channel News Asia. (20 February 2018). *Channel News Asia*. “HardwareZone Forum Hit by Security Breach; 685,000 User Profiles Affected.” Last accessed on 1 August 2018 at https://www.channelnewsasia.com/news/singapore/hardwarezone-hwz-security-breach-685000-user-profiles-affected-9975156.

93. Joji Simon. (17 February 2018). *On Manorama*. “Data breach again: Salary bill of Supplyco staff leaked on WhatsApp.” Last accessed on 1 August 2018 at https://english.manoramaonline.com/news/kerala/2018/02/16/data-breach-salary-bill-of-supplyco-staff-leaked-on-whatsapp.html.

94. Kostiantyn Tsentsura. (7 February 2018). *Kyiv Post*. “Personal data of 500,000 Nova Poshta Clients Allegedly Leaked to Dark Web.” Last accessed on 1 August 2018 at https://www.kyivpost.com/technology/personal-data-500000-nova-poshta-clients-allegedly-leaked-dark-web.html.

95. Danny Mok. (18 April 2018). *South China Morning Post*. "Personal Data of Some 380,000 Hong Kong Broadband Customers Hacked, Service Provider Says." Last accessed on 1 August 2018 at https://www.scmp.com/news/hong-kong/law-crime/article/2142317/personal-data-some-380000-hong-kong-broadband-customers.

96. Rose Behar. (12 February 2018). *Mobile Syrup*. "Hacker Uncovers Freedom Mobile Customer Login Vulnerability." Last accessed on 1 August 2018 at https://mobilesyrup.com/2018/02/12/freedom-mobile-security-breach/.

97. Chisato Tanaka. (26 June 2018). *The Japan Times*. "Prince Hotels Hack Results in Loss of 124,000 Customers' Credit Card Numbers, Other Data." Last accessed on 1 August 2018 at https://www.japantimes.co.jp/news/2018/06/26/business/corporate-business/prince-hotels-hack-results-loss-124000-customers-credit-card-numbers-data/#.WzNPNadKhPY.

98. Christine Dobby. (23 January 2018). *The Globe and Mail*. "Police Probing Bell Canada Data Breach; Up to 100,000 Customers Affected." Last accessed on 1 August 2018 at https://www.theglobeandmail.com/report-on-business/police-probing-bell-canada-data-breach-up-to-100000-customers-affected/article37701579/.

Created by:

TrendLabs

The Global Technical Support and 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 over 6,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro secures your connected world. For more information, visit www.trendmicro.com.

TREND MICRO™

Securing Your Connected World