



# TrendLabs 2016 Security Roundup: A Record Year for Enterprise Threats

#### 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

4

---

Ransomware Spiked 752% in New Families in 2016

8

---

BEC Scams Generate Hundreds of Thousands in Losses Across the World

10

---

Adobe Acrobat Reader DC and Advantech's WebAccess Have the Most Number of Vulnerabilities

13

---

Mirai Botnet's Massive DDoS Attack Elevates IoT Security Conversation

15

---

Biggest Data Breach in History Underscores Responsible Disclosure of Companies

18

---

Angler Leaves the Scene with Other Exploit Kits Rising

21


---

Bank Hacking Perseveres with Banking Trojans and ATM Malware Developments

24

---

Threat Landscape in Review

A person in a blue suit is holding a large white document, possibly a report or a set of plans, in a modern office setting. The background is a blurred office interior with a wooden floor and a potted plant. The text is overlaid on a dark, semi-transparent rectangular area.

2016 was an unprecedented year for cybersecurity, particularly for enterprises. Although there were considerable wins in terms of cybercriminal arrests—resulting in the drop in exploit kit numbers—an array of threats, which hit a record high, still caused billions of dollars in accumulated losses.

It was indeed the year of online extortion, with ransomware leading the charge. Over 200 new ransomware families triggered significant damages to a number of institutions worldwide. Business email compromise (BEC), likewise, raked in huge profits for cybercriminals while proving to everyone that social engineering is still very effective when targeting large organizations.

Vulnerabilities discovered in widely used platforms, including Supervisory Control and Data Acquisition (SCADA), also surpassed records in terms of volume. This left security researchers and malicious actors caught in a race to find weak points in a system first.

The biggest data breach in history was also reported in 2016. The event exposed issues in how some companies handle user data. Other organizations felt the effects of poor Internet of Things (IoT) security when the Mirai botnet surfaced and took down their servers. Banking threats also continued to develop, posing new challenges to the financial sector.

This roundup reviews the pertinent security stories of 2016 and aims to help enterprises determine what to expect in the months ahead and what security strategies they can adopt to stay protected.

## Ransomware Spiked 752% in New Families in 2016

In a span of 12 months, the number of discovered ransomware families jumped from 29 to 247. This marks a 752% increase compared to the volume of ransomware families detected in 2015.

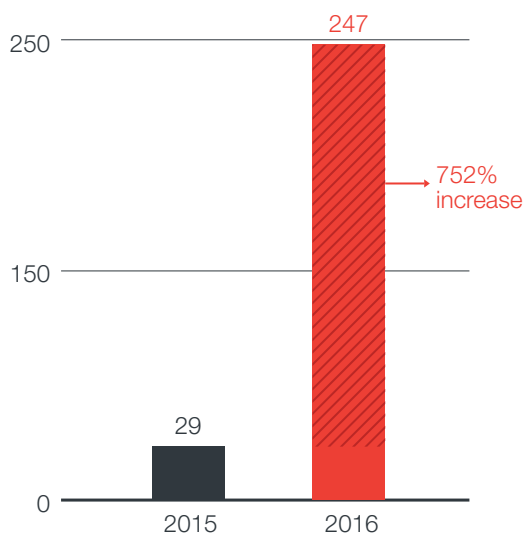


Figure 1. Number of newly added ransomware families, 2016

This record increase in new families can be a result of different factors, the first being how effective ransomware is as a moneymaking scheme. Using ransomware, cybercriminals reportedly managed to rake in about US\$1 billion in 2016.<sup>1</sup> The whopping amount is the result of several affected enterprises still choosing to pay their attackers to have their data and assets decrypted and restored.

Although many organizations are advised not to pay the ransom and focus on creating backups, this is easier said than done. Many of 2016's new ransomware families were designed to target specific file types critical to businesses. These include tax return files, server files, virtual desktop images and the like. Database files that are used to manage pertinent business information have also become targets.<sup>2</sup>

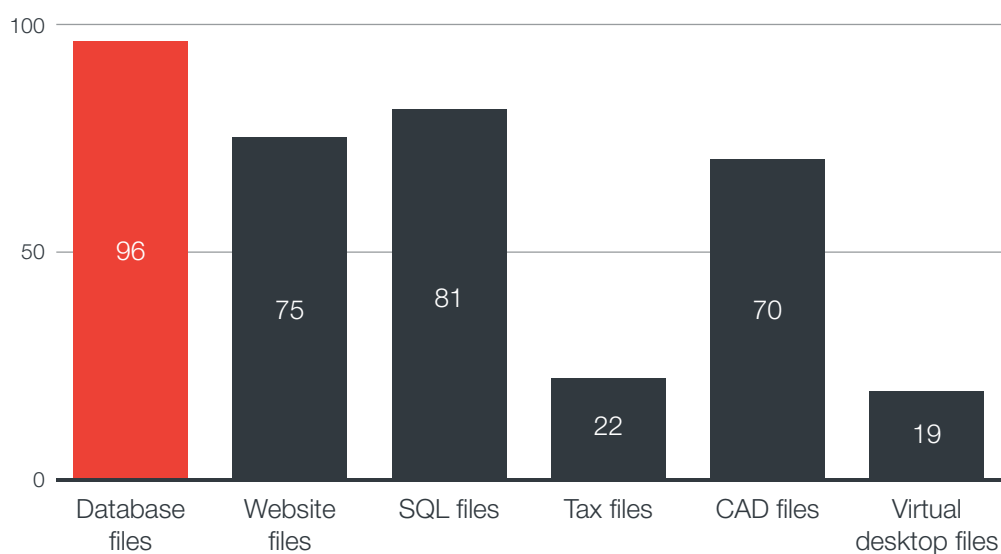


Figure 2. Number of known ransomware families encrypting business-related files, 2016

NOTE: For the full list of ransomware families, refer to table 7 in the appendix.

Affected enterprises also had to withstand significant system downtime and corporate data loss. Despite not having any guarantee of getting their data back, many organizations still opted to give in to cybercriminal demands. In November, the San Francisco Municipal Transportation Agency was asked to pay 100 bitcoins (approximately US\$70,000) after a ransomware attack locked their computers.<sup>3</sup> VESK, a provider of hosted virtual desktops, paid approximately US\$23,000 to get the decryption keys that will restore all of their services.<sup>4</sup> The New Jersey Spine Center paid an undisclosed amount after attackers encrypted electronic medical records, disabled their phone system, and even locked out staff members from accessing their backup files.<sup>5</sup>

Other factors driving the increase of ransomware families were the presence of open source ransomware and the introduction of ransomware-as-a-service (RaaS). Originally designed for educational purposes, open source ransomware like Hidden Tear and EDA2 were used by cybercriminals to target web servers and databases.<sup>6</sup> The source codes for those ransomware strains have already been taken down after the reported abuse. RaaS also made it easier for rookie cybercriminals to utilize ransomware. Since RaaS is available in the underground, the service provides fledgling cybercriminals the necessary tools to run their own extortion campaigns.<sup>7</sup>

Among the ransomware threats we detected and blocked in 2016, spam remained the top ransomware vector, accounting for 79%. Since email has become the most common entry point for ransomware—either via malicious attachments or URLs found in the email—organizations should be able to utilize web and email gateway solutions. Possible ransomware threats can be prevented through effective monitoring of email traffic and filtering potentially unsafe URLs, attachments, and other malicious payloads.

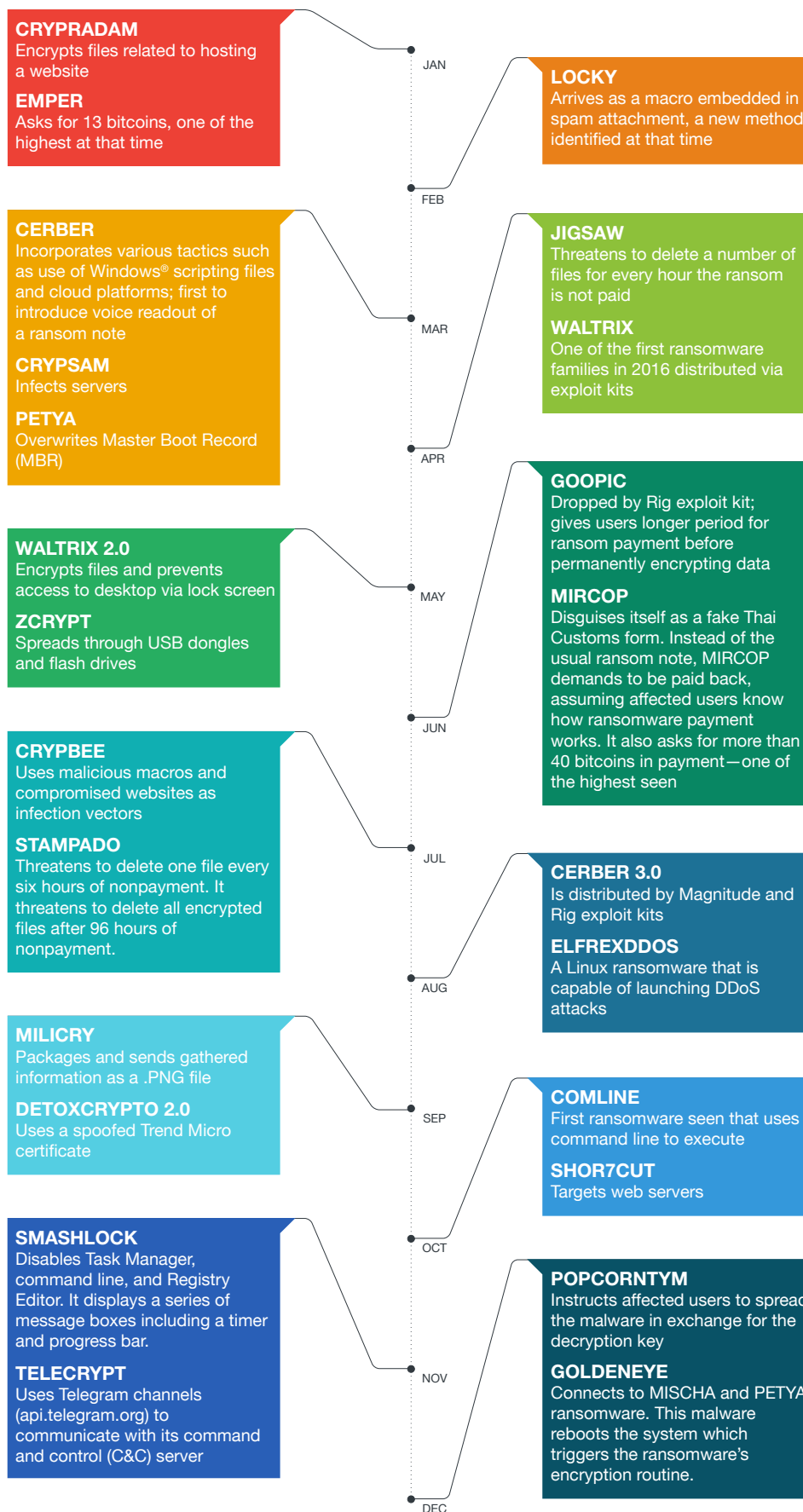


Figure 3. A timeline of noteworthy ransomware families, 2016

Reputation-based analysis should also be able to filter against web and file threats. Based on the number of ransomware-related detections, downloads from URLs that host ransomware or exploit kits distributing ransomware were at 20%, while detections from actual ransomware files were at 1%.

Security solutions that are able to blend this kind of reputation technology with other anti-ransomware capabilities like whitelisting and application control, behavioral analysis, network monitoring, vulnerability shielding, and high-fidelity machine learning can better protect organizations while minimizing the impact on their computing resources. Endpoint application control, for example, allows users within the organization to access known good files while the rest go through filtering. This provides uninterrupted access to safe content while limiting incidents of false positives. Machine learning, utilized during pre-execution and run time, can further provide more accurate detection.

As ransomware families continue to evolve and multiply, it is critical for enterprises to recognize this reality and help make their data security strategy stronger and more efficient.

## BEC Scams Generate Hundreds of Thousands in Losses Across the World

BEC attacks are responsible for causing an average of US\$140,000 in losses for companies worldwide.<sup>8</sup> Leoni AG, the fourth largest wire and cable manufacturer in the world, became a victim of a BEC attack when its Chief Financial Officer (CFO) was tricked into transferring about US\$44.6 million to a foreign account.<sup>9</sup> Scammers also swindled approximately US\$330,000 from the local council of Brisbane in Australia after they posed as one of the council’s suppliers.<sup>10</sup> SS&C Technology also lost US\$6 million to a BEC scam that forced the company to temporarily take its operations offline.<sup>11</sup>

BEC scams have spread in 92 countries. Those most affected countries include the United States, the United Kingdom, Hong Kong, Japan, and India. The map below shows all the affected regions in 2016.

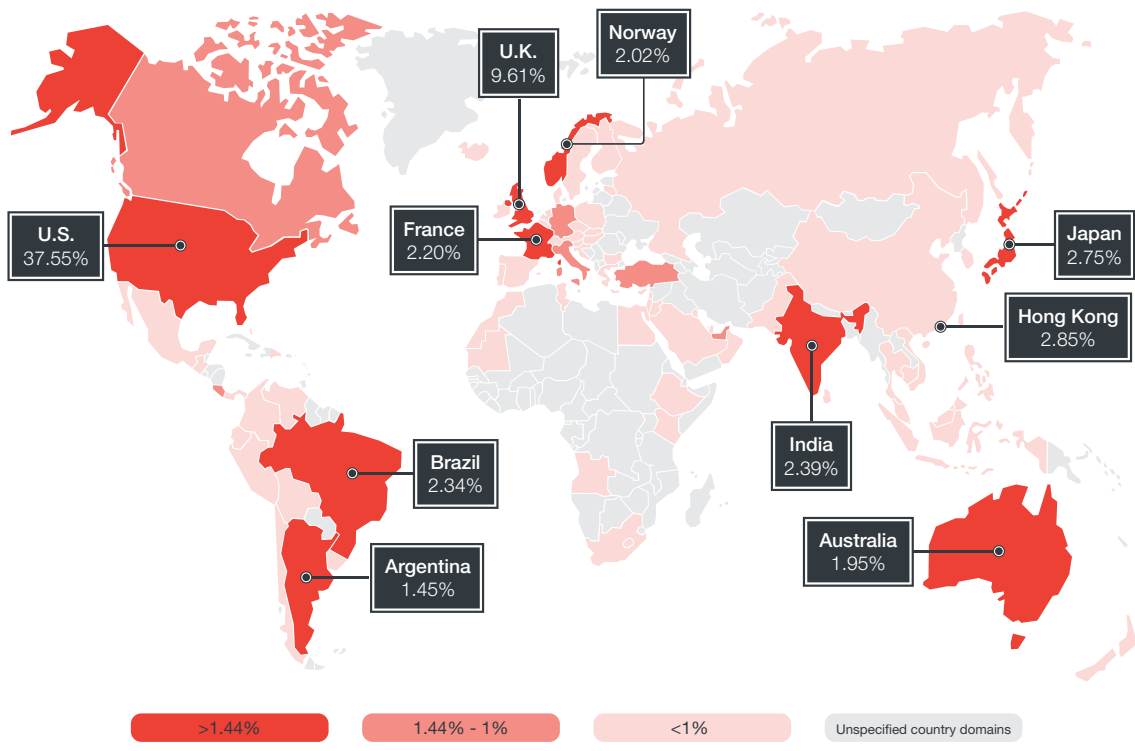


Figure 4. Countries with the most number of companies affected by BEC, 2016



In the latter part of the year, cybercriminals ramped up their campaigns with CEO fraud schemes, a type of BEC scam wherein cybercriminals impersonate a CEO or any executive who can authorize fund transfers. Cybercriminals used this technique when they targeted 17 healthcare institutions in the United States, 10 in the United Kingdom, and eight in Canada in just two weeks.<sup>12</sup> These institutions included general and teaching hospitals, specialty care and walk-in clinics, and even pharmaceutical companies.

Since BEC scams heavily rely on social engineering, there's great weight on the human factor. The more staff members—from a CEO to a rank-and-file employee—are aware of how BEC works and how to identify it, the more equipped an organization will be to defend against this threat. Fraudulent wire transfer requests usually require urgent action from the targeted employee. And so it is important for everyone to scrutinize and double-check transfer details first. Recognizing phishing emails, in particular, and being wary of clicking on any links can also reduce the chances of being at the mercy of cybercriminals.

When processing confidential emails, it is also recommended to manually enter the email addresses of the concerned parties instead of just relying on the provided default addresses. Manually typing addresses from a contact list will help ensure that correspondences and wire transfers are indeed legitimate. Having another efficient method of verifying a fund transfer, such as phone verification, will also help reduce the risk of processing a fraudulent request.

Since most types of BEC emails don't involve a malware payload, traditional email solutions that tend to only detect malicious behavior won't be able to stop these kinds of scams from landing inside an employee's inbox. Organizations are recommended to have web and email gateway solutions that don't only have anti-spam and anti-phishing capabilities but also context-aware social engineering attack protection features, which are capable of inspecting email headers and other social engineering tactics used in BEC attacks.

## Adobe Acrobat Reader DC and Advantech’s WebAccess Have the Most Number of Vulnerabilities

In 2016, Trend Micro and the Zero Day Initiative (ZDI) (with TippingPoint) discovered a record high of 765 vulnerabilities (including 60 zero days)—an increase from 714 in 2015. Of the 765 total, Trend Micro researchers independently discovered 103 vulnerabilities, while ZDI found 678. Sixteen vulnerabilities are common to both.

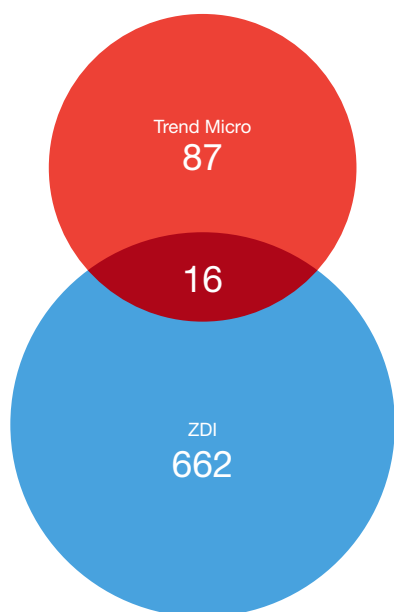


Figure 5. Number of vulnerabilities discovered by Trend Micro and ZDI, 2016

Product	Number of Vulnerabilities
Advantech WebAccess	109
Adobe® Acrobat® Reader DC	89
Apple® OS X®	52
Android	52
Foxit® Reader	49
Adobe Flash®	38
Microsoft® Internet Explorer®	33
Microsoft Windows® OS	26
SolarWinds®	25
Microsoft Edge	22

Table 1. Trend Micro and ZDI (with TippingPoint) Top 10 applications based on number of vulnerabilities discovered in 2016

Most of the vulnerabilities were found in Adobe Acrobat Reader DC and Advantech’s WebAccess (with 26 zero days). The former is an enterprise application that handles .PDF files, while the latter is used in SCADA systems.

Although Adobe Acrobat Reader DC saw no increase or decrease from its 2015 record, the application still had the most number of vulnerabilities compared to all other Adobe products. Adobe Flash noticeably had fewer vulnerabilities compared to last year’s 67 vulnerabilities, which marks a 43% decrease. That number may continue to drop as more browsers are disabling Flash by default and are now migrating to HTML5.<sup>13</sup> Despite that, the presence of Adobe Flash zero-day vulnerabilities<sup>14</sup> still leaves outdated systems vulnerable to attacks. For instance, an Adobe Flash zero day allowed attackers behind Pawn Storm to ramp up their spear-phishing campaigns against governments and embassies across the world.<sup>15</sup>

Meanwhile, Microsoft saw a 47% decrease in its vulnerabilities, with a total of 93 recorded vulnerabilities—down from the previous year’s 175. While Internet Explorer still has the highest number of vulnerabilities among all Microsoft products, the total volume of the vulnerabilities found on the platform got significantly lower. From 121 recorded vulnerabilities in 2015, it came down to only 33, indicating a 73% decrease. There are a few factors which may have affected this drop. Apart from Microsoft offering bounty programs for bugs and vulnerabilities, the vendor has also been proactive in rolling out security patches. Instead of making individual bulletins for each patch available, Microsoft is pooling all the updates into a single monthly deployment.<sup>16</sup> This streamlined approach is better at providing users with continued security.

Vendor	Product	2015 vs. 2016	
Microsoft		47%	▼
	Internet Explorer	73%	▼
	Office®	53%	▼
	Windows	26%	▼
	Edge	2,100%	▲
	MSXML	100%	▼
	Chakra	100%	▲
	.NET	100%	▲
	Reader	100%	▲
	Windows Media® Center	100%	▲
0Days		17%	▼
Android		206%	▲

Vendor	Product	2015 vs. 2016	
Adobe		8%	▼
	Flash	43%	▼
	Acrobat Reader DC	0%	—
	Acrobat Pro DC	133%	▲
	Digital Edition	200%	▲
	Creative Cloud®	100%	▲
Apple		145%	▲
	iOS®	275%	▲
	OS X	189%	▲
	QuickTime®	57%	▼
	Safari®	175%	▲
SCADA		421%	▲

Table 2. Trend Micro and ZDI (with TippingPoint) discovered vulnerabilities 2015 versus 2016

The number of vulnerabilities found in Apple products, on the other hand, saw a considerable rise in 2016. There were 81 vulnerabilities in its products in 2016—a 145% increase from the 33 discovered vulnerabilities in 2015. Its desktop computing (OS X) and smartphone (iOS) products, both of which are used in enterprises, saw a 189% and 275% increase, respectively, in 2016. In October, attackers abused the iOS platform to replace a legitimate app in the App Store® with a malformed and enterprise-signed app. Through the repackaged and adware-laden apps, hackers were able to manipulate iOS's code signing process, and granted them access to a user's personally identifiable information (PII) and banking credentials.

Advantech's WebAccess had the most number of discovered vulnerabilities for 2016. These and other SCADA vulnerabilities can be leveraged to compromise critical components in industrial automation networks. Many essential services and utilities, like water and electricity, rely on SCADA so failing to secure these systems could lead to real-world risks. An example of which was the power outage caused by a malware called BlackEnergy. The attack was directed against a power grid, which left about half of the homes in a Ukrainian region with no access to electricity for several hours.<sup>18</sup> For the list of other SCADA applications with discovered vulnerabilities, refer to Table 5 in the Threat Landscape in Review section.

As for mobile platforms, our data showed that Android vulnerabilities increased by 206% in 2016. A malware variant called DressCode allows attackers to gain access to internal networks every time devices with Trojanized apps are connected to them. At least 3,000 Trojanized apps were found in well-known Android markets and even Google Play.<sup>19</sup>

Knowing that there are a number of vulnerabilities on SCADA systems allows the private and public sectors to develop an efficient security framework before attackers can find ways to exploit them. Initiatives like ZDI (founded by TippingPoint) can help in this aspect. ZDI rewards security researchers for responsibly reporting vulnerabilities in various products and platforms. After these vulnerabilities are disclosed, vendors create and deliver the patches.

System administrators should make it a habit to apply security patches once they're made available. In the absence of official vendor fixes, they can use virtual patching is an interim solution that will help protect systems from possible zero days.

## Mirai Botnet's Massive DDoS Attack Elevates IoT Security Conversation

Previously, attacks on IoT devices have only been proofs of concept (PoCs). Smart watches<sup>20</sup> and smart light bulbs<sup>21</sup> were some of the connected devices that were repeatedly hacked by researchers to demonstrate how, with the right tools and methods, IoT devices can be exploited. All of these hacks have been isolated cases; none of which have been replicated on a massive scale.

During the last quarter of 2016, attackers—through the use of the Mirai botnet—targeted DNS provider Dyn with a distributed denial-of-service (DDoS) attack.<sup>22</sup> Attackers hijacked approximately 100,000 vulnerable IoT devices such as security cameras to be part of a botnet.<sup>23</sup> The large-scale attack against Dyn, which caused packet flow bursts of up to 50 times higher than its normal volume, forced various websites and services to go offline for several hours. Some of Dyn's clients include Twitter, Reddit, and Spotify.

Other reports of actual IoT device hacking also surfaced in recent months. FLOCKER ransomware on smart TVs, for example, pretends to be a law enforcement agency and accuses its victims of crimes they did not commit. After displaying the warning, FLOCKER locks the device and demands US\$200 worth of iTunes® gift cards.<sup>24</sup> Another incident left residents of two buildings in Finland out in the cold after a DDoS attack took the buildings' environmental control systems down.<sup>25</sup>

These recent attacks should serve as a wake-up call to enterprises. Attackers can now use IoT to attack an organization from within or from the outside. Vulnerable IoT devices and systems inside a network can either be used as entry points for further attacks or they can be manipulated to disrupt operations. And whether or not organizations currently use IoT technology, they are still susceptible to business-halting outside threats like Mirai.

End users should know that not all smart devices are built with security in mind. This makes users, therefore, responsible in securing their devices until all manufacturers implement robust security. Some of the first steps toward maintaining security are to change passwords frequently and to keep a device's firmware up-to-date. IoT devices are often sold with default passwords, and neglecting to change passwords is already a case for potential abuse. For enterprises, implementing stronger IoT security policies within organizations is a good start. They should also complement this by securing all the devices connected to their system.

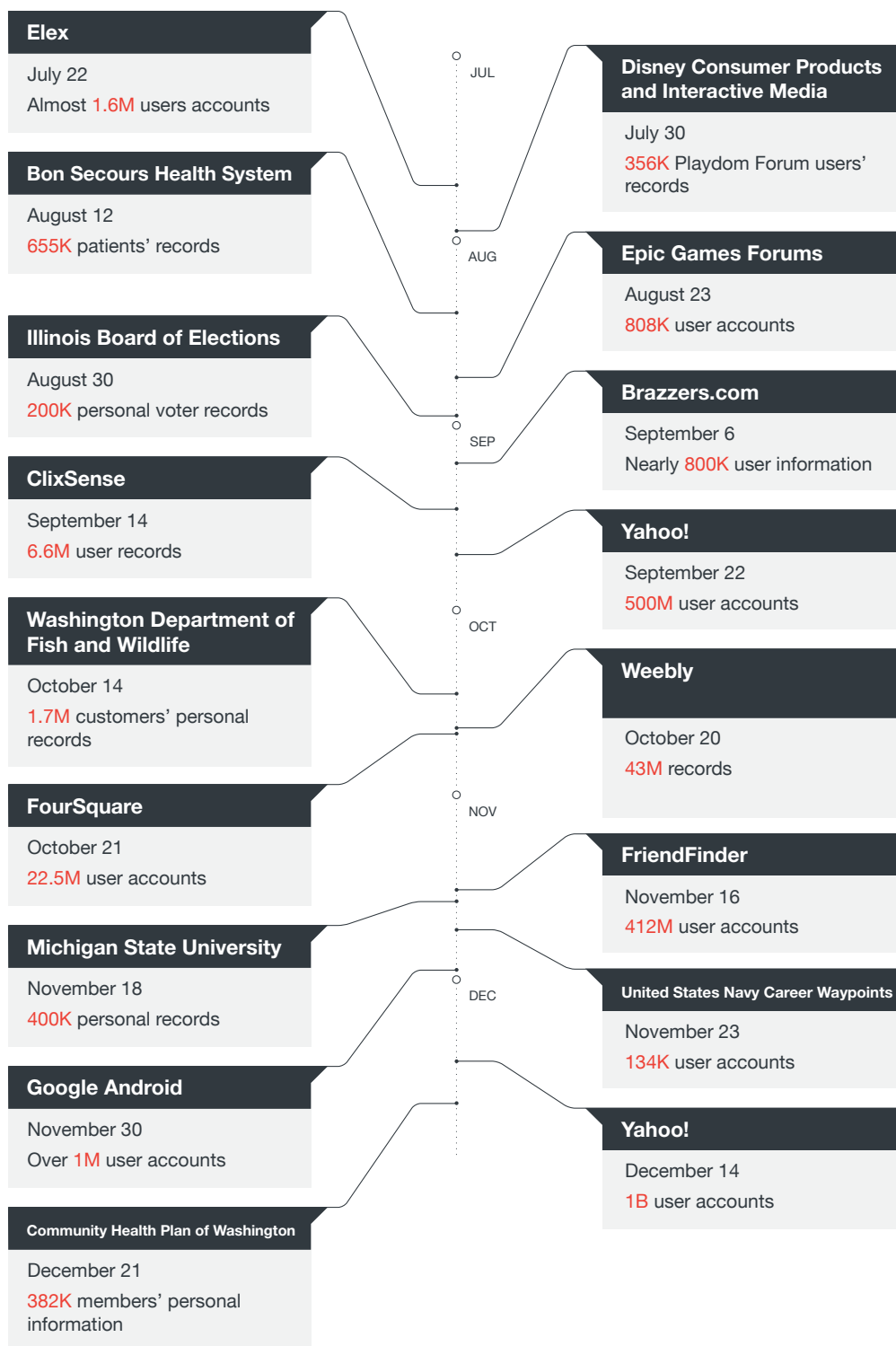
In the long run, the responsibility of providing IoT security lies heavily on the manufacturers. After all, not every user could be expected to be fully aware of the risks involved in an attack. Securing communication protocols and devices' software development kits (SDKs) can protect against potential exploits, privacy intrusions, and malware infections that can lead to DDoS attacks.

## Biggest Data Breach in History Underscores Responsible Disclosure of Companies

Reports of a company suffering from a data breach are no longer a surprise. Time and again, we have seen how organizations—from education systems<sup>26</sup> to healthcare institutions<sup>27</sup>—can become a victim of data breaches.

For instance, the recent Yahoo breach brought the issue of responsible disclosure to the fore. Yahoo has been under a lot of scrutiny for the late disclosure of an August 2013 data breach that exposed over 1 billion of their users' accounts—including names, dates of birth, email addresses, MD5-hashed passwords, and phone numbers.<sup>28</sup> This makes it the biggest data breach in history. The recent disclosure came three months after the company reported a separate breach in September, which involved 500 million accounts.

Yahoo was severely criticized for the way they handled user information and for the time it took them to disclose the breaches. The magnitude of this breach raised concerns and questions on users' data security. Such an event emphasized how a company's policies in securing customer data have an effect on their reputation. The crux of the matter is that companies are responsible for their customers' data and should make it a priority to be accountable to them. Responding to data breaches not only entails getting to the bottom of the intrusion, but it's also about informing customers as well. When Leoni AG was scammed out of millions of dollars, the company released a statement shortly after on their site. The statement includes details of the fraudulent activity, the extent of the impact, and how they responded to the attack. Doing so affirms an organization's commitment to protecting their customers' data and privacy.



Note: Of the data breaches with more than a hundred thousand records stolen, hacking was found to be the most common method. Additionally, reported data breaches in the U.S. reached an all-time record high in 2016, increasing by 40% over the 2015 figures.<sup>29</sup>

Figure 6. Timeline of data breaches, 2H 2016  
Data from [privacyrights.org](http://privacyrights.org)



Enterprises should have security solutions with breach detection systems that will allow them to monitor network traffic across all ports, spot any irregularities, and prevent attackers from infiltrating systems. Custom sandboxing can also provide enterprises the ability to analyze malware, detect any C&C activity, and identify other hacking techniques used in data breaches. Additionally, deploying machine learning techniques allows quick and accurate identification of whether network content—be it files or behaviors—are malicious or not.

## Angler Leaves the Scene with Other Exploit Kits Rising

By the third quarter of the year, the once dominant Angler exploit kit disappeared. Following the arrest of 50 cybercriminals on June 2016,<sup>30</sup> Angler detections dwindled and ceased to exist. Since then, attackers switched to other exploit kits to up the ante.

The Neutrino exploit kit picked up the pace by distributing CRYPMIC, WALTRIX, and CERBER 4.0 ransomware.<sup>31</sup> However, by September, there were lower access numbers of Neutrino as it dropped out of active circulation in the underground and moved to cater to select clientele.<sup>32</sup> The Rig exploit kit also took advantage of Angler’s absence when it distributed CERBER,<sup>33</sup> LOCKY,<sup>34</sup> and MILICRY ransomware in a malvertising campaign.<sup>35</sup> The campaign abuses legitimate services such as Google Maps, Imgur, and Pastee to infect systems and lock files with ransomware.

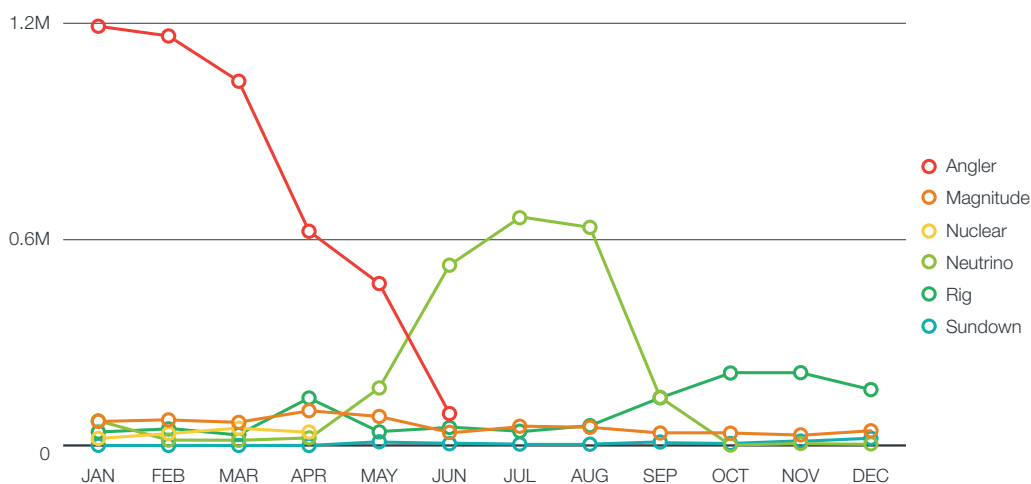


Figure 7. Number of access to exploit-kit-hosting URLs, 2016

Other exploit kits also had updates in their techniques. Bizarro Sundown was spotted in early October and was used to compromise sites and deliver two versions of LOCKY ransomware.<sup>36</sup> Sundown malware designers, on the other hand, incorporated steganography to hide their exploit code in seemingly harmless image files.<sup>37</sup>

More exploit kits distributed ransomware in 2016. The recent variant of the notorious CERBER ransomware family, for example, was incorporated in several infection campaigns.<sup>38</sup> CERBER 4.0 emerged in early October and became popular to cybercriminals who wanted to use the malware in malvertising campaigns and to compromise sites. Neutrino, Magnitude, and Rig are three of the prominent exploit kits that delivered CERBER 4.0 in 2016. Compared to the time when Angler was in active distribution in 2015, 2016 saw a significant decrease in vulnerabilities included in exploit kits.

Exploit Kit	Ransomware Delivered	
	2015	2016
Angler	CRYPWALL	CRYPWALL
	CRYPTESLA	CRYPTESLA
	CRILOCK	CRILOCK
		WALTRIX
		CRYPMIC
Neutrino	CRYPWALL	CRYPWALL
	CRYPTESLA	CRYPTESLA
		CERBER
		WALTRIX
		LOCKY
	CRYPMIC	
Magnitude	CRYPWALL	CRYPWALL
		CERBER
		LOCKY
		MILICRY
Rig	CRYPWALL	GOOPIC
	CRYPTESLA	CERBER
		CRYPMIC
		LOCKY
		CRYPHYDRA
		CRYPTOLUCK
		MILICRY
Nuclear	CRYPWALL	CRYPTESLA
	CRYPTESLA	LOCKY
	CRYPCTB	
	CRYPshed	
Sundown		CRYPTOSHOCKER
		LOCKY
		PETYA
		MILICRY
Hunter		LOCKY
Fiesta	CRYPTESLA	

Table 3. Ransomware families delivered by exploit kits



Figure 8. Exploits to specific vulnerabilities included in certain exploit kits, 2016

In 2015, there were a total of 17 recorded vulnerabilities that were included in exploit kits. By 2016, this number significantly dropped to five, marking a 71% overall decrease. Adobe Flash remained to be the product with the most number of vulnerabilities used by exploit kits. This number, however, decreased by 80% in 2016.

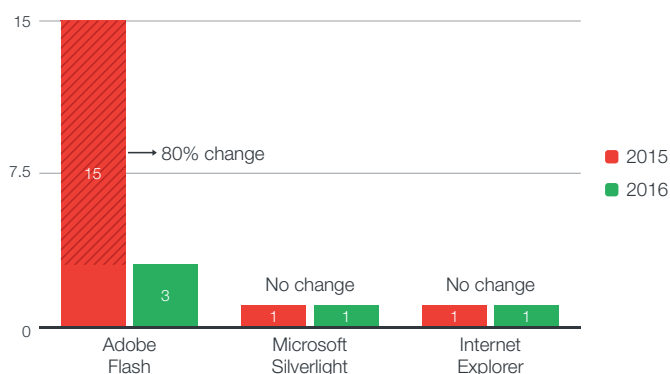


Figure 9. Number of specific vulnerabilities included in exploit kits 2015 versus 2016

Despite dwindling numbers in 2016, exploit kits still remained in the arsenal of many cybercriminals and attackers. Exploit kits still fit into malvertising, ransomware attacks, and other cybercriminal campaigns. The effectiveness of these kits against a platform or system is very much dependent on how secure or vulnerable it is. This is why the use of legacy systems puts enterprises at risk. It’s always critical for organizations to keep their software and operating systems (OS) up-to-date with the latest security patches to ensure all they are protected from potential abuse.

Virtual patching can eliminate risk exposure by shielding vulnerabilities while an official patch is unavailable. Enterprises can look into this option for ease of deployment and better scalability without using up a lot of resources. Security solutions with high-fidelity machine learning can also help detect and block exploits in real time.

# Bank Hacking Perseveres with Banking Trojans and ATM Malware Developments

With the use of malware and skimming cards, gaining quick profits from ATMs became easier for cybercriminals. ATM malware has been around for a while now, with the Skimer variant first observed in 2009. Since then, Skimer was recently updated to turn ATMs into skimming machines.<sup>39</sup>



Figure 10. ATM malware families and their geographical origins<sup>40</sup>

One of the primary reasons cybercriminals continue to use ATM malware is because many of the machines still run outdated operating systems like Windows® XP Embedded. This particular OS is vulnerable since Microsoft already ended support for it in 2016,<sup>41</sup> meaning all systems running Windows XP Embedded may be susceptible to attacks since the vendor will no longer release security patches.

To diversify their attacks, cybercriminals continued to use different variants of ATM malware. Recently we discovered a bare-bones ATM malware called ALICE that had been in the wild since October 2014.<sup>42</sup> What makes ALICE particularly noteworthy is that it makes no attempt to connect to other ATM-specific hardware, such as the machine’s numeric pad, in order to empty an ATM’s safe. It also has no elaborate install or uninstall mechanism. It works as soon the cybercriminal runs the executable in the target environment.

ALICE’s design suggests that a cybercriminal would need to physically open the ATM and infect the machine by using a CD-ROM or USB. The criminal would then need to connect a keyboard to the machine’s motherboard to execute the malware.

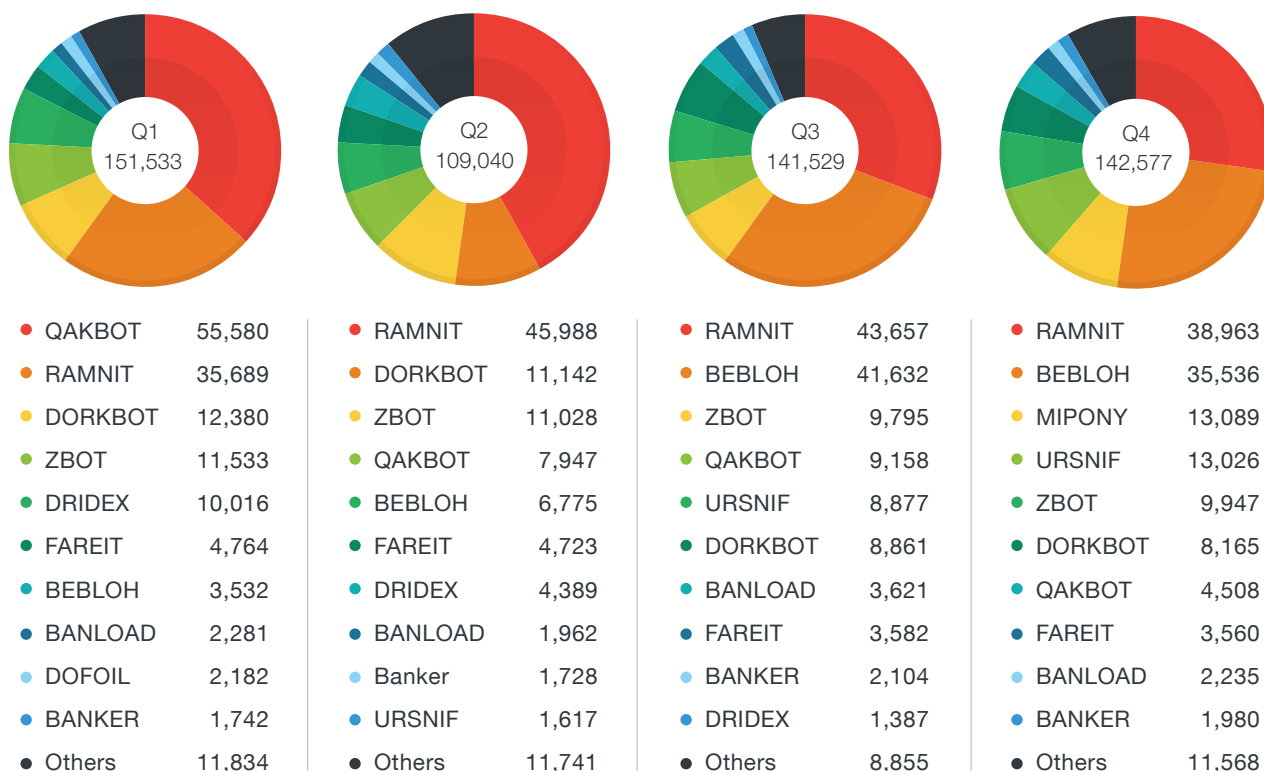


Figure 11. Top banking malware families, 2016

On the other hand, banking Trojans still shared the spotlight for banking-related threats. Earlier this year, QAKBOT detections reemerged after the malware authors of the DYRE/DYREZA banking malware were arrested.<sup>43</sup> By the second quarter of the year, however, the RAMNIT banking Trojan resurfaced with two new live attack servers and a new C&C server.<sup>44</sup> The banking Trojan’s long period of silence, since the attempted takedown of RAMNIT servers in 2015,<sup>45</sup> ended when RAMNIT targeted major banks in the United Kingdom.<sup>46</sup> The banking Trojan also managed to maintain its presence toward the end of the year.

As ATM malware and banking Trojans continue to spread, banking institutions are responsible for guaranteeing the security of their systems by ensuring the physical security of their ATMs, updating operating systems, and devoting the time to regularly inspect and address any software vulnerabilities with equipment manufacturers. We also recommend implementing solutions that provide application control and whitelisting. Deploying such features will block the installation or usage of applications that are not included in the whitelist.

When it comes to the responsibility of securing online transactions, consumers also have a role to play. After all, they are also exposed to these banking-related threats every time they perform on-site and online banking transactions. Through the use of banking malware, for example, cybercriminals may gain access to a user's PII and credentials. Knowing this, users should regularly change banking-related passwords and/or PINs and remain vigilant when doing online transactions. Enterprises should also adopt endpoint machine solutions with advanced anti-malware protection and employ two-factor authentication on their sites to secure online banking sessions. Additionally, it is also recommended for bank users to secure various entry points such as web, file, and email.

## Threat Landscape in Review

Over 81 billion threats were blocked by the Trend Micro™ Smart Protection Network™ in 2016, a 56% increase from the total number of blocked threats in 2015. This increase is largely drawn from the total number of email threats blocked throughout the year and is consistent with the growth of ransomware and BEC, which are both widely propagated through email or spam.

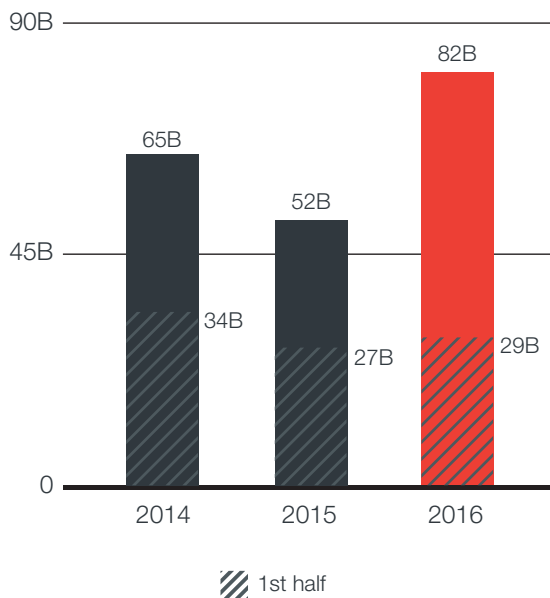


Figure 12. Overall threats blocked by the Trend Micro Smart Protection Network, 2016

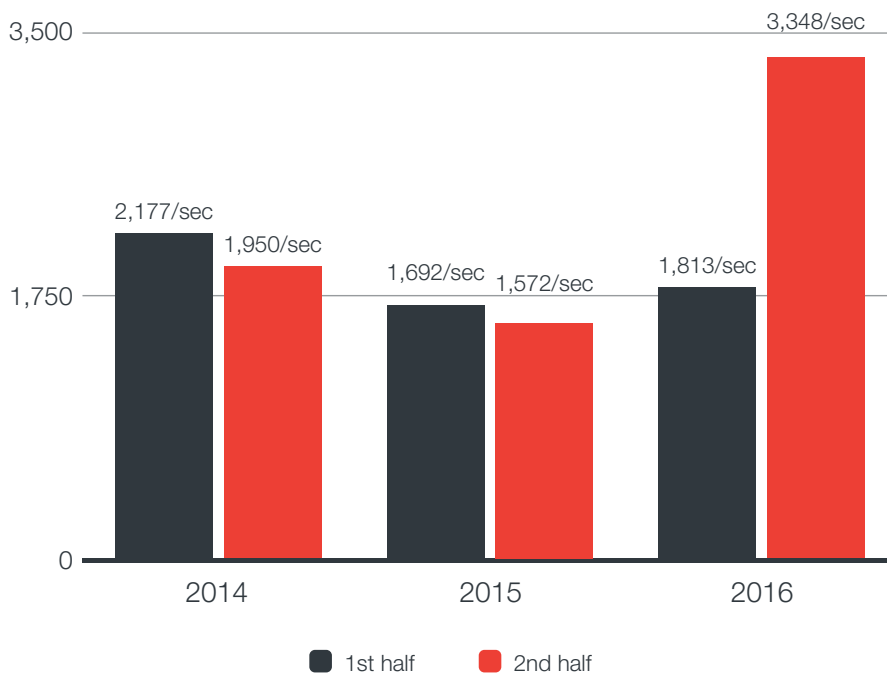


Figure 13. Number of threats blocked per second, 2016



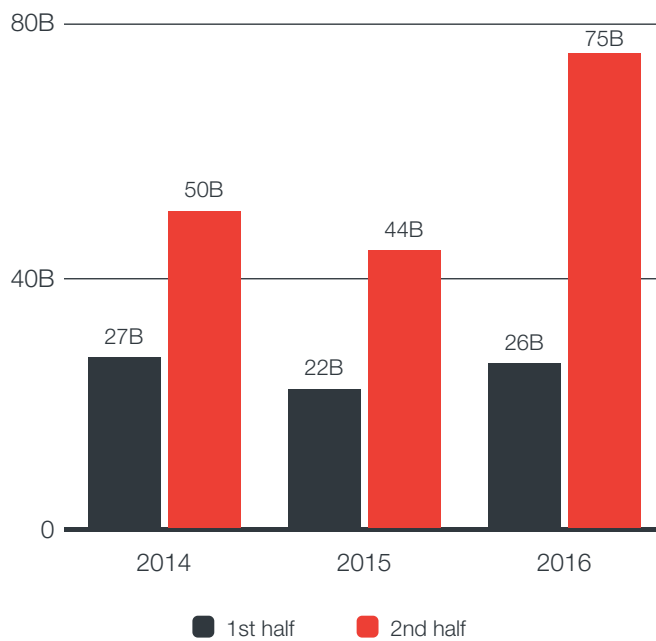


Figure 14. Number of email threats blocked, 2016

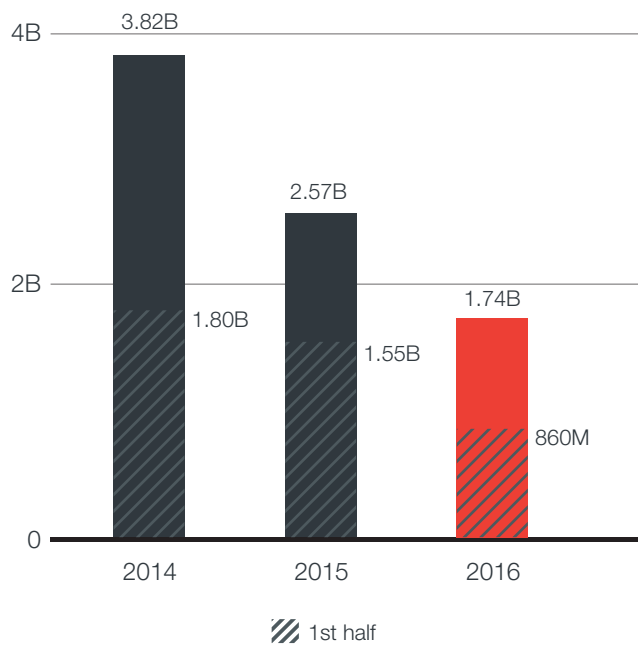


Figure 15. Number of malicious URLs blocked, 2016

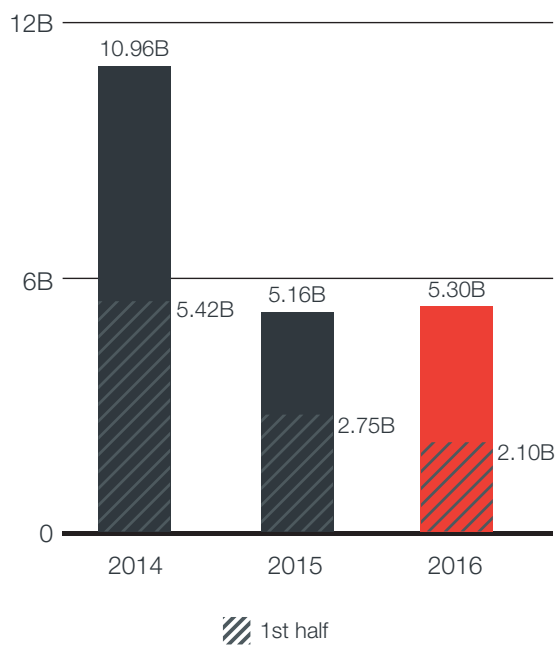
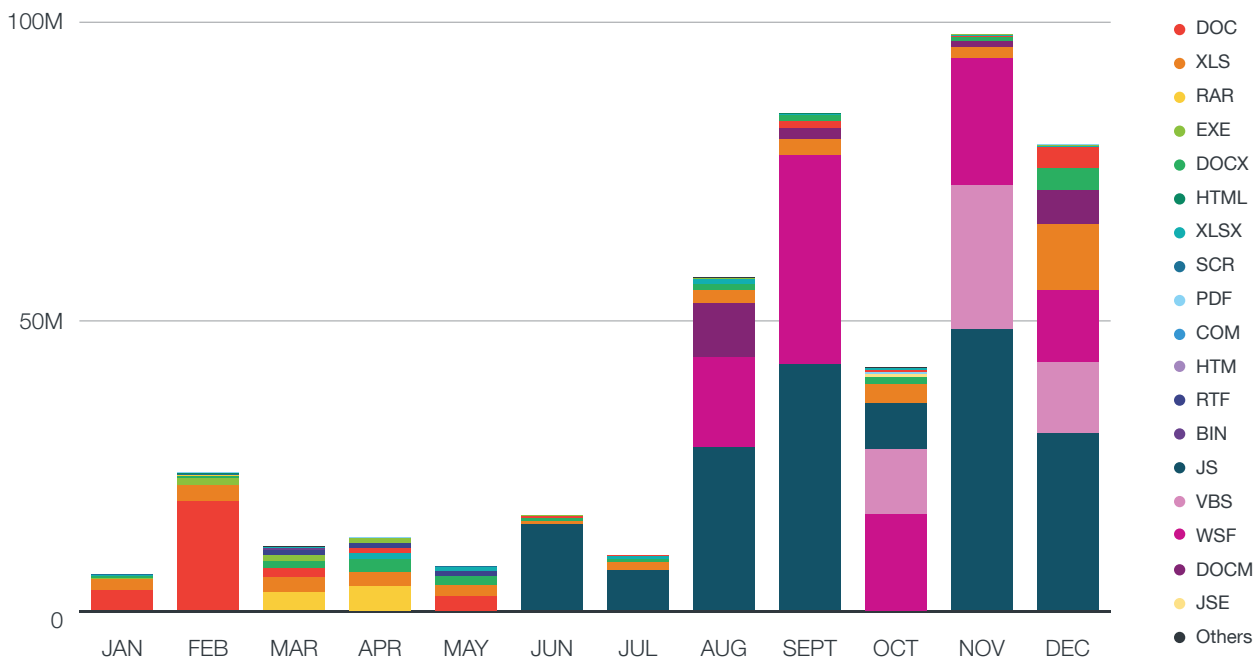


Figure 16. Number of malicious files blocked, 2016

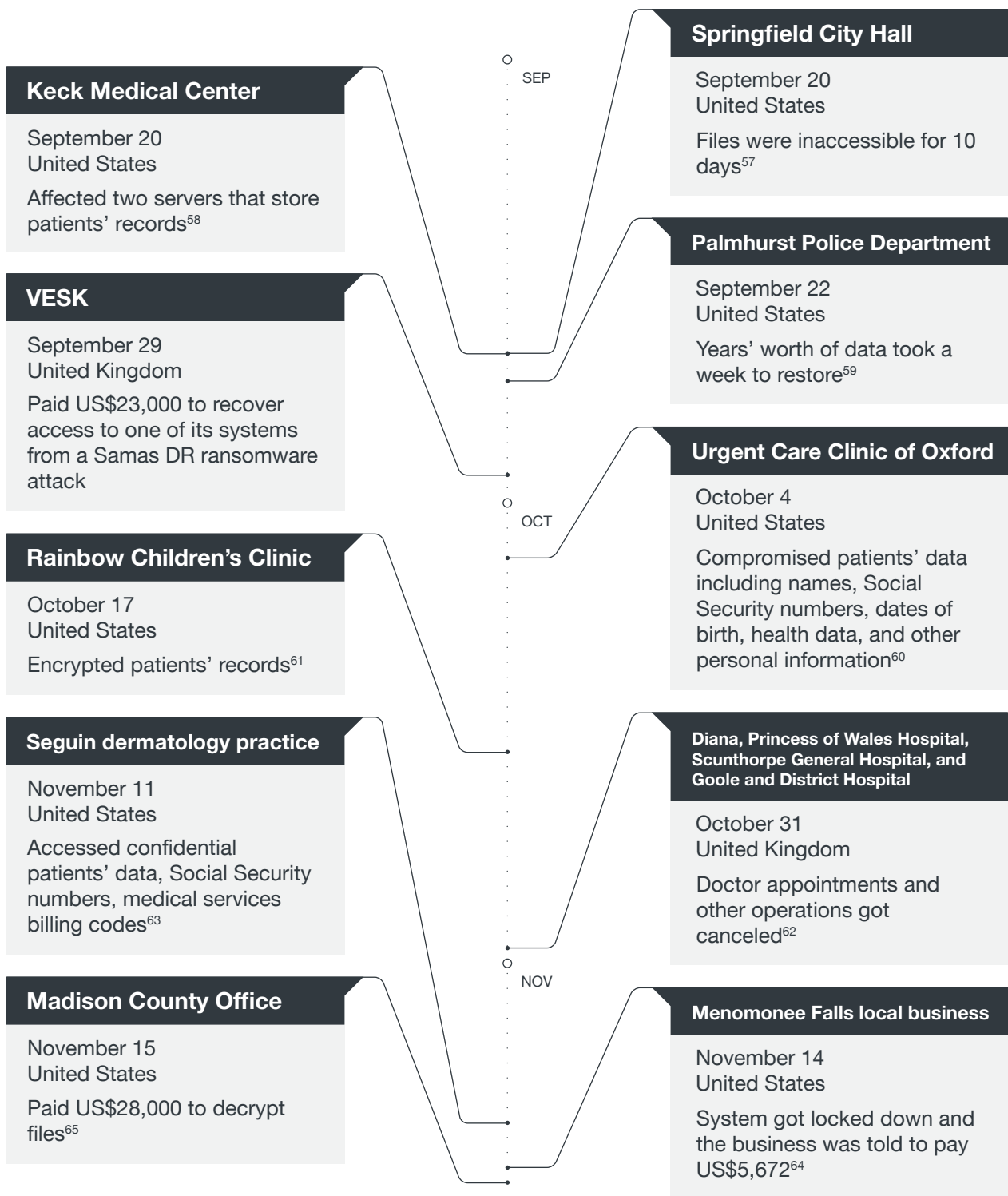


The upsurge of JavaScript attachments in spam from the month of June is primarily caused by ransomware-related spam.

Figure 17. Top file attachments seen in ransomware-related spam according to file type, 2016

Note: The significant surge in JavaScript attachments in November was caused by NEMUCOD, a known ransomware dropper. LOCKY ransomware distributed via email also contributed to this surge.





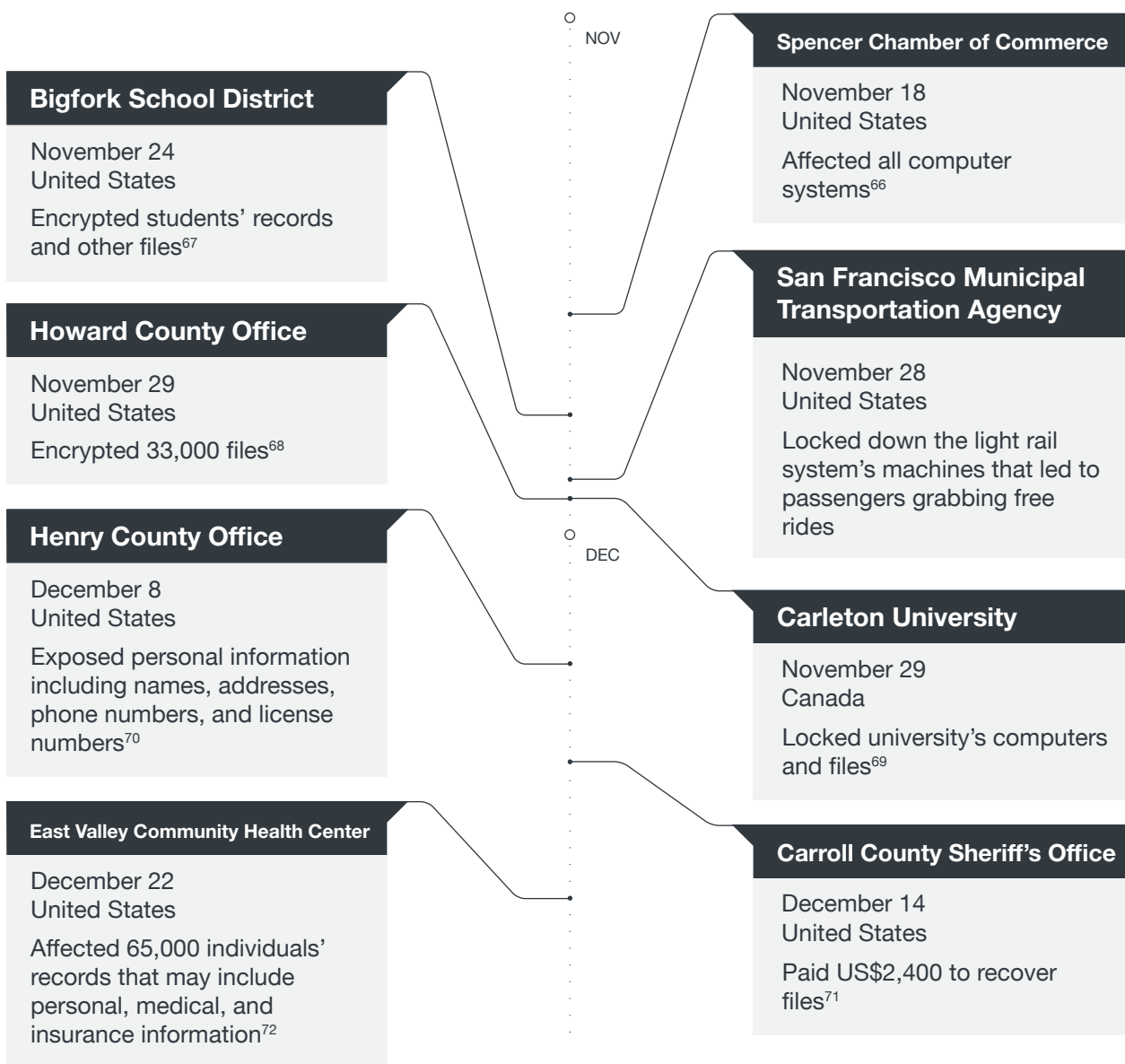


Figure 18. Ransomware incidents made public, 2H 2016

JAN	LECTOOL	EMPER	CRYPRADAM	MEMEKAP
	CRYPNISCA	CRYPJOKER	CRYPRITU	
FEB	CRYPGPCODE	CRYPHYDRA 1.0	CRYPDAP	CRYPZUQUIT
	MADLOCKER	LOCKY		
MAR	CERBER	CRYPAURA	KERANGER	TESLA
	MAKTUB	SURPRISE	PETYA	POWERWARE 1.0
	CRYPTOSO	COVERTON	CRYPTOHASU	KIMCIL
APR	CRYPTEAR 1.0	CRYPHAM		
	CRYPALAM	CRYPTOHOST 1.0	XORBAT	JIGSAW
	WALTRIX	ZIPPY	EMPER 2.0	CRYPVAULT
	CRYPCORE	CRYPPLIKI	CRYPALPHA	
MAY	ROKKU	BRLOCK	CRYPMAME	SHUJIN
	AUTOLOCKY	MISCHA	WALTRIX 2.0	ENIGMA
	SNSLOCK	BLOCCATO	TAKALOCKER	BADBLOCK
	ZCRYPT	ELFACRYPT	LOCKSCAM	DEMOCRY
	BUCBI	CRYPDAP	CRIPOTDC	
JUN	JIGSAW 2.0	WALTRIX 3.0	CRYPHERBST	CRYPEDA
	CRYPAGA	WALTRIX 4.0	GOOPIC	APOCALYPSE
	JSRAA	CRYPCUTE	CYPHERKEY	CRYPKEYIV
	CRYPSHOCKER	WHITELOCK	LOCKRVTN	JOKOZY
	MIRCOP	XORIST	BART	CRYPMIC 1.0
	SATANA	ZIRBAM		
JUL	CRYPMIC 2.0	FAKELock	ALFA	ZIPTB
	RUSHTEAR	WALTRIX 5.0	JUSINOMEL	SANCTEAR
	HOLYCRYPT	STAMPADO 1.0	POWERWARE 2.0	NOOBCRYPT
	TILDE	JAGER	UYARITEAR	CRYPBEE
	BANKTEAR	BAKSOCUTE	VENUSLOCK	TELANATEAR
	CERBER 2.0	SHINOLOCK	LERITH	REKTEDA
AUG	CRYPHYDRA 2.0	CRYPZXAS	POGOTEAR	CRYPTOHOST 2.0
	SHARKRAAS	CRYPTLOCK	KAOTEAR	FSOCEDA
	ATILOCKTEAR	DETOXCRYPTO 1.0	SCRNLOCKER	ALMALOCK
	PURGE	BART 2.0	WILDFIRE	DOMINO
	FANTOMCRYPT	CERBER 3.0	ELFREXDDOS	SERPICO
	CRYPMIC 3.0			
	CUCKTOX	RARVAULT	HDDCRYPTOR	CRYPTEAR 2.0
SEP	KAWAIILOCKER	STAMPADO 2.0	CRYPY	EDALOCK
	ATOM	HIDDENTEARDEVMARE	HIDDENTEARBLACKFEATHER	FENIX
	JOKEMARS	EREBUS	DETOXCRYPTO 2.0	HORCRUX
	CRYPTRX	PRINCESSLOCKER	STOPI	NULLBYTE
	MILICRY	CRYSIS		
	ENCRYPTILE	EDA2MASTERBUSTER	ESMERALDA	JACKPOT
OCT	COMLINE	EDA2BLA	TENSEC	LOCK93
	CRYPBTN	WILCRYPT	ANGRYDUCK	SHOR7CUT
	CLICKMEG	EDA2ANUBIS	EXOTIC	NUCLEAR
	VENIS	ENIGMA	HIDDENTEARSHADOW	SONIDO
	COMCIRCLE	KOSTYA	HIDDENTEARAPT	CRYPTGO
	HADESLOCK	ALCATRAZ	HIDDENTEARNOTORIOUS	EDA2NOTORIOUS
	CRYPTTOTROOPER	EDA2JANBLEED	KILLERLOCKER	LERITH 2.0
	CERBER 4.0			

NOV	MATRIX	CRYPHYDRA	PSHELL	CRYSIS 2.0
	CRYPshed	HIDDENTEARDECRYPTOR	SPICYCRYPT	VINDOWS
	LOMIX	EDA2RUNSOME	RUNELOCKER	CERBER 5.0.1
	CERBER 5.0.0	CERBER 4.1.6	CRYPTASN1	HIDDENTEARHOLLY
	RARLOCK	CRYPTOWIRE	CHIP	HOTDEM
	EXOSHELL	RANSOC	HAPPYLOCKER	PROTOBTC
	CRYPTON	CITOXE	CRYPTOLUCK	SURVEYLOCK
	KARMA	HIDDENTEARHAPPY	PCLOCK	TELECRYPT
	AIRACROP	ILOCKED	HIDDENTEARFSOCIETY	CRYPAYSAFE
	HIDDENTEARCERBER	PAYDOS	ISHTAR	GREMIT
	SMASHLOCK	ZEROCRYPT	HIDDENTEARHCRYPTO	DXXD
	RAZYCRYPT			
	DEC	HIDDENTEARGUSTER	ADAMLOCK	BADCRIP
BRAINCRYPT		DERIALOCK	SEOIRSE	FREROGA
MFESTUS		DONATO	AYTEP	CRYPBLOCK
CRYPTORIUM		CRYPEXTXX	SCRLOCKER	LEVILOCK
ANTIX		GOLDENEYE	POPCORNTYM	DESBLOQ
CERBER 5.0.x		MICROP	EDGELOCKER	

Note: Ransomware families discovered in the first half of 2016 have been updated.

Table 4. New ransomware families seen, 2016

Vendor	Product name	Vendor	Product name
ABB	DataManagerPro	Panasonic	FPWINPro
Advantech	SUSIAccess	Pro-face	GP-Pro EX
Advantech	WebAccess	Rockwell Automation	RSLogix Micro Starter Lite
Delta	Delta Industrial Automation	Schneider Electric	SoMachine HVAC
Eaton	ELCSoft	Siemens	SINEMA Server
Ecava	IntegraXor	Trihedral	VTScada
Fatek	Fatek Automation	Unitronics	VisiLogic
IBHsoftec	S7-SoftPLC	We-con	Levistudio

Table 5. SCADA applications with discovered vulnerabilities, 2016

2015 Total	714	2016 Total	765
High:	37.96%	High:	37.12%
Medium:	60.22%	Medium:	61.44%
Low:	1.54%	Low:	1.05%

*Note: While there is an increase in the number of vulnerabilities discovered and reported, most of the vulnerabilities are categorized as having Medium impact (according to the Common Vulnerability Scoring System (CVSS) rating). In addition, a very small percentage of the total vulnerabilities have no CVSS scores as of this writing.*

Table 6. Trend Micro and ZDI CVSS stats

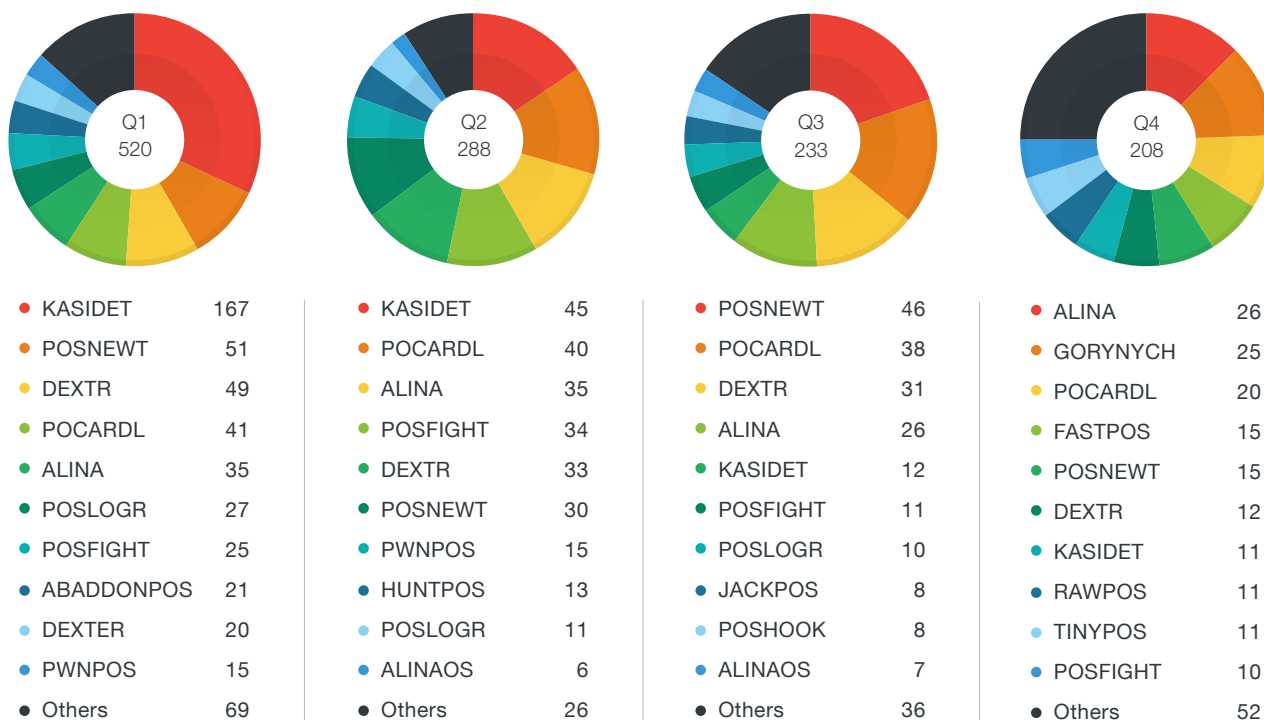


Figure 19. Top PoS malware families, 2016



	Database	Website	SQL	Tax	CAD	VD
SATANA	•			•	•	
BART	•	•	•			•
MIRCOP	•	•	•			
JOKOZY	•					
CRYPHOCKER	•		•	•	•	
CRYPKEYIV	•	•	•			
CRYPCUTE	•	•	•		•	
JSRAA	•				•	
JIGSAW 2.0	•	•	•		•	
WALTRIX 3.0	•	•	•		•	•
CRYPEDA		•				
WALTRIX 4.0	•	•	•		•	•
XORIST	•		•		•	
CRYPMIC 1.0	•	•	•		•	•
CRYPMAME	•	•	•	•		
ROKKU	•	•	•	•	•	
AUTOLOCKY	•	•			•	
MISCHA	•	•	•		•	
WALTRIX 2.0	•	•	•		•	•
ENIGMA	•	•	•		•	•
TAKALOCKER		•	•			
BADBLOCK	•	•	•		•	
ZCRYPT	•	•	•		•	
ELFACRYPT	•				•	
CRYPDAP	•	•	•		•	
CRIPTODC	•		•	•	•	
CRYPTOHOST 1.0	•	•			•	•
XORBAT	•	•	•		•	
JIGSAW	•	•	•		•	•
WALTRIX	•	•			•	•

	Database	Website	SQL	Tax	CAD	VD
ZIPPY	•		•			
EMPER 2.0			•		•	
CRYPVAULT		•				
CRYPCORE	•				•	
CRYPLIKI	•		•	•	•	
CRYPALPHA	•	•	•		•	•
CERBER	•		•		•	
CRYPAURA	•	•	•		•	
KERANGER	•		•	•	•	
TESLA	•		•	•	•	
MAKTUB	•	•	•	•	•	
PETYA	•	•	•	•	•	
CRYPTOSO	•	•	•		•	
KIMCIL	•	•	•			
CRYPTEAR 1.0	•	•			•	
CRYPHAM	•				•	
CRYPGPCODE	•	•	•	•	•	
CRYPDAP	•	•				
MADLOCKER	•	•	•			•
LOCKY	•		•			
LECTOOL	•		•			
EMPER	•		•		•	
CRYPRADAM	•	•	•	•	•	
CRYPNISCA	•	•	•			
CRYPJOKER	•	•	•		•	
CRYPRITU	•	•	•		•	
SANCTEAR		•	•			
CRYPBEE				•	•	•
VENUSLOCK		•				•
REKTEDA		•	•			
POGOTEAR		•	•			

	Database	Website	SQL	Tax	CAD	VD
BAKSOCUTE		•			•	
ATILOCKTEAR		•	•			
SHOR7CUT		•				
LOCK93	•	•			•	
ISHTAR	•			•		
HIDDENTEARCERBER	•	•	•		•	
HIDDENTEARFSOCIETY	•	•	•		•	
HIDDENTEARHAPPY	•	•	•		•	
CRYPTOLUCK	•	•	•		•	
CRYPTON	•					
HIDDENTEARHOLLY	•	•				
EDA2RUNSOME	•	•	•		•	
HIDDENTEARDECRYPTOR	•	•	•			
HIDDENTEARKOKO	•	•	•		•	
CRYPMIC 2.0	•		•		•	
ALFA	•		•		•	
RUSHTEAR		•	•			
WALTRIX 5.0	•		•			•
HOLYCRYPT	•	•	•			
STAMPADO 1.0	•	•			•	
POWERWARE 2.0				•	•	
UYARITEAR	•				•	
HDDCRYPTOR						
JOKEMARS	•	•	•	•	•	
EREBUS	•	•	•	•		•
DETOXCRYPTO 2.0	•		•		•	
PRINCESSLOCKER	•		•		•	
DXXD	•		•			•
EDA2JANBLEED	•		•			

	Database	Website	SQL	Tax	CAD	VD
HADESLOCK	•		•		•	•
HIDDENTEARAPT	•	•	•		•	
KOSTYA	•					
HIDDENTEARSHADOW	•	•	•			
ENIGMA	•		•		•	
CRYPTBTN	•					
EDA2BLA	•	•	•			
ZEROCRYPT		•				
CRYPHYDRA	•	•	•	•	•	
PSHELL						
CRYSIS 2.0	•			•	•	
CRYPSED		•			•	
SPICYCRYPT	•	•	•		•	
VINDOWS	•	•	•			
HOTDEM	•	•	•	•	•	
PROTOBTC	•			•	•	
CITOXE	•	•	•		•	
PCLOCK	•				•	
HIDDENTEARGUSTER	•	•	•			
SEOIRSE	•	•	•			
ANTIX	•	•	•		•	•
GOLDENEYE	•	•	•		•	
POPCORNTYM	•	•	•	•	•	•
MIRCOP	•	•	•			

Table 7. Business-related files encrypted by known ransomware families, 2016

## References

1. Maria Korolov. (5 January 2017). *CSO Online*. "Ransomware took in \$1 billion in 2016—improved defenses may not be enough to stem the tide." Last accessed on 17 January 2017, <http://www.csoonline.com/article/3154714/security/ransomware-took-in-1-billion-in-2016-improved-defenses-may-not-be-enough-to-stem-the-tide.html>
2. Mary Yambao and Francis Antazo. (22 November 2016). *TrendLabs Security Intelligence Blog*. "Businesses as Ransomware's Goldmine: How Cerber Encrypts Database Files." Last accessed on 17 January 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/how-cerber-encrypts-database-files/>
3. Thomas Fox-Brewster. (28 November 2016). *Forbes*. "Ransomware Crooks Demand \$70,000 After Hacking San Francisco Transport System – UPDATED." Last accessed on 17 January 2017, <http://www.forbes.com/sites/thomasbrewster/2016/11/28/san-francisco-muni-hacked-ransomware/#5f51e76f54dd>
4. Kat Hall. (29 September 2016). *The Register*. "VESK Coughs Up £18k in Ransomware Attack." Last accessed on 17 January 2017, [http://www.theregister.co.uk/2016/09/29/vesk\\_coughs\\_up\\_18k\\_in\\_ransomware\\_attack/](http://www.theregister.co.uk/2016/09/29/vesk_coughs_up_18k_in_ransomware_attack/)
5. Jessica Davis. (5 October 2016). *Healthcare IT News*. "Two Providers Forced to Pay Up in Ransomware Attacks." Last accessed on 17 January 2017, <http://www.healthcareitnews.com/news/two-more-ransomware-attacks-both-organizations-pay>
6. Francis Antazo, Byron Gelera, Jeanne Jocson, Ardin Maglalang, and Mary Yambao. (25 August 2016). *TrendLabs Security Intelligence Blog*. "New Open Source Ransomware Based on Hidden Tear and EDA2 May Target Businesses." Last accessed on 17 January 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/new-open-source-ransomwar-based-on-hidden-tear-and-eda2-may-target-businesses/>
7. Trend Micro. (7 September 2016). *Trend Micro Security News*. "Ransomware as a Service Offered in the Deep Web: What This Means for Enterprises." Last accessed on 17 January 2017, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-what-this-means-for-enterprises>
8. Trend Micro. (9 June 2016). *Trend Micro Security News*. "Billion-Dollar Scams: The Numbers Behind Business Email Compromise." Last accessed on 17 January 2017, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/billion-dollar-scams-the-numbers-behind-business-email-compromise>
9. Leoni AG. (16 August 2016). *Leoni*. "Leoni Targeted by Criminals." Last accessed on 17 January 2017, <https://www.leoni.com/en/press/releases/details/leoni-targeted-by-criminals/>
10. Trend Micro. (25 August 2016). *Trend Micro Security News*. "Brisbane Council Loses 450K AUD to BEC Scam." Last accessed on 17 January 2017, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/brisbane-council-loses-450k-aud-to-bec-scam>
11. Trend Micro. (21 September 2016). *Trend Micro Security News*. "\$6M Lost in Another BEC Scam: Who Is the Weakest Link?." Last accessed on 17 January 2017, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/6m-lost-in-another-bec-scam-who-is-the-weakest-link>
12. Ryan Flores. (23 November 2016). *TrendLabs Security Intelligence Blog*. "CEO Fraud Email Scams Target Healthcare Institutions." Last accessed on 17 January 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/ceo-fraud-email-scams-target-healthcare-institutions/>
13. DL Cade. (17 August 2017). *PetaPixel*. "All the Major Browsers Will Soon Block Flash, is Your Website Ready?." Last accessed 18 January 2017, <https://petapixel.com/2016/08/17/major-browsers-will-soon-block-flash-website-ready/>
14. Jonathan Leopando. (27 October 2016). *TrendLabs Security Intelligence Blog*. "Patch Your Flash: Another Zero-Day Vulnerability Hits Adobe Flash." Last accessed on 17 January 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/patch-flash-another-zero-day-vulnerability-hits-adobe-flash/>

15. Feike Hacquebord and Stephen Hilt. (9 November 2016). *TrendLabs Security Intelligence Blog*. "Pawn Storm Ramps Up Spear-phishing Before Zero-Days Get Patched." Last accessed on 17 January 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-ramps-up-spear-phishing-before-zero-days-get-patched/>
16. Brian Krebs. (11 October 2016). *Krebs on Security*. "Microsoft: No More Pick-and-Choose Patching." Last accessed 17 January 2017, <https://krebsonsecurity.com/2016/10/microsoft-no-more-pick-and-choose-patching/>
17. Trend Micro. (31 October 2016). *TrendLabs Security Intelligence Blog*. "Masque Attack Abuses iOS's Code Signing to Spoof Apps and Bypass Privacy Protection." Last accessed on 17 January 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/ios-masque-attack-spoof-apps-bypass-privacy-protection/>
18. Trend Micro. (6 October 2016). *Trend Micro Security News*. "First Malware-Driven Power Outage Reported in Ukraine." Last accessed on 1 February 2017, <http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/first-malware-driven-power-outage-reported-in-ukraine>
19. Echo Duan. (29 September 2016). *TrendLabs Security Intelligence Blog*. "DressCode and its Potential Impact for Enterprises." Last accessed on 17 January 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/dresscode-potential-impact-enterprises/>
20. Dan Goodin. (10 December 2014). *arsTechnica*. "PoC Hack on Data Sent Between Phones and Smartwatches (Updated)." Last accessed on 23 January 2017, <http://arstechnica.com/security/2014/12/connections-between-phones-and-smartwatches-wide-open-to-brute-force-hacks/>
21. Darren Pauli. (10 November 2016). *The Register*. "IoT Worm Can Hack Philips Hue Lightbulbs, Spread Across Cities." Last accessed on 23 January 2017, [http://www.theregister.co.uk/2016/11/10/iot\\_worm\\_can\\_hack\\_philips\\_hue\\_lightbulbs\\_spread\\_across\\_cities/](http://www.theregister.co.uk/2016/11/10/iot_worm_can_hack_philips_hue_lightbulbs_spread_across_cities/)
22. Kyle York. (22 October 2016). *Dyn*. "Dyn Statement on 10/21/2016 DDoS Attack." Last accessed on 23 January 2017, <http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/>
23. David Bisson. (27 October 2016). *Tripwire*. "100,000 Bots Infected with Mirai Malware Behind Dyn DDoS Attack." Last accessed on 18 January 2017, <https://www.tripwire.com/state-of-security/latest-security-news/100000-bots-infected-mirai-malware-caused-dyn-ddos-attack/>
24. Echo Duan. (13 June 2016). *TrendLabs Security Intelligence Blog*. "FLocker Mobile Ransomware Crosses to Smart TV." Last accessed on 23 January 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/flocker-ransomware-crosses-smart-tv/>
25. Janita. (7 November 2016). *Metropolitan.fi*. "DDoS Attack Halts Heating in Finland Amidst Winter." Last accessed on 23 January 2017, <http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter>
26. WXYZ. (18 November 2016). *WXYZ*. "Michigan State University Confirms Data Breach of Server Containing 400,000 Student, Staff Records." Last accessed on 18 January 2017, <http://www.wxyz.com/news/michigan-state-university-confirms-data-breach-of-server-containing-400000-student-staff-records>
27. Bob Young. (21 December 2016). *The Seattle Times*. "Data Breach Exposes Info for 400,000 Community Health Plan Members." Last accessed on 18 January 2017, <http://www.seattletimes.com/seattle-news/health/data-breach-exposes-info-for-400000-community-health-plan-members/>
28. Trend Micro. (15 December 2016). *Trend Micro Security News*. "Yahoo Discloses 2013 Breach that Exposed Over One Billion Accounts." Last accessed on 18 January 2017, <http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/yahoo-discloses-2013-breach-exposed-over-1billion-accounts>
29. Mathew Schwartz (20 January 2017). *Information Security Media Group, Corp.* "Report: US Data Breaches Reach Record Levels." Last accessed on 6 February 2017, <http://www.databreachtoday.com/blogs/report-us-data-breaches-reach-record-levels-p-2374>
30. Andrew Osborn. (1 June 2016). *Reuters*. "Russia Says Arrests Hacker Gang Who Defrauded Banks of Millions." Last accessed on 18 January 2017, <http://uk.reuters.com/article/uk-russia-cyber-arrests-idUKKCNOYN42R>

31. Kawabata Kohei. (20 July 2016). *TrendLabs Security Intelligence Blog*. "CrypMIC Ransomware Wants to Follow CryptXXX's Footsteps." Last accessed on 18 January 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/crypmic-ransomware-wants-to-follow-cryptxxx/>
32. Kafeine. (2 October 2016). *Malware Don't Need Coffee*. "RIG Evolves, Neutrino Waves Goodbye, Empire Pack Appears." Last accessed on 18 January 2017, <http://malware.dontneedcoffee.com/2016/10/rig-evolves-neutrino-waves-goodbye.html>
33. Trend Micro. (18 October 2016). *Trend Micro Security News*. "Ransomware Recap: Oct. 14, 2016." Last accessed on 18 January 2017, <http://www.trendmicro.com.ph/vinfo/ph/security/news/cybercrime-and-digital-threats/ransomware-recap-oct-14-2016>
34. Trend Micro. (4 October 2016). *Trend Micro Security News*. "Ransomware Recap: Sept. 30, 2016." Last accessed on January 18, 2017, <http://www.trendmicro.com.ph/vinfo/ph/security/news/cybercrime-and-digital-threats/ransomware-recap-sept-30-2016>
35. Kawabata Kohei, Joseph C. Chen, and Jeanne Jocson. (9 September 2016). *TrendLabs Security Intelligence Blog*. "Picture Perfect: CryLocker Ransomware Uploads User Information as PNG Files." Last accessed on 18 January 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/picture-perfect-crylocker-ransomware-sends-user-information-as-png-files/>
36. Brooks Li and Joseph C. Chen. (4 November 2016). *TrendLabs Security Intelligence Blog*. "New Bizarro Sundown Exploit Kit Spreads Locky." Last accessed on 18 January 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/new-bizarro-sundown-exploit-kit-spreads-locky/>
37. Brooks Li and Joseph C. Chen. (29 December 2016). *TrendLabs Security Intelligence Blog*. "Updated Sundown Exploit Kit Uses Steganography." Last accessed on 18 January 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/updated-sundown-exploit-kit-uses-steganography/>
38. Joseph C. Chen (12 October 2016). *TrendLabs Security Intelligence Blog*. "Several Exploit Kits Now Deliver Cerber 4.0." Last accessed on 18 January 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/several-exploit-kits-now-deliver-cerber-4-0/>
39. Trend Micro. (20 May 2016). *Trend Micro Security News*. "Skimer ATM Malware Gets Updated, Turns ATMs into Skimming Machines." Last accessed on 19 January 2017, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/skimer-atm-malware-updated-turns-atm-into-skimmer>
40. David Sancho and Numaan Huq. (12 April 2016). *TrendLabs Security Intelligence Blog*. "ATM Malware on the Rise." Last accessed on 19 January 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/atm-malware-on-the-rise/>
41. Dave Massy. (17 February 2014). Microsoft Developer Network. "What Does the End of Support of Windows XP Mean for Windows Embedded?" Last accessed on 23 February 2017 on, <https://blogs.msdn.microsoft.com/windows-embedded/2014/02/17/what-does-the-end-of-support-of-windows-xp-mean-for-windows-embedded/>
42. David Sancho and Numaan Huq. (20 December 2016). *TrendLabs Security Intelligence Blog*. "Alice: A Lightweight, Compact, No-Nonsense ATM Malware." Last accessed on 19 January 2017, <https://blog.trendmicro.com/trendlabs-security-intelligence/alice-lightweight-compact-no-nonsense-atm-malware/>
43. Cklaudioney Mesa and Christopher Ordonez. (18 February 2016). *TrendLabs Security Intelligence Blog*. "QAKBOT Resurges: Despite Takedowns, Online Banking Threats Persist." Last accessed on 19 January 2017, <http://blog.trendmicro.com/trendlabs-security-intelligence/despite-arrests-and-takedowns-online-banking-threats-persist/>
44. SecurityWeek. (27 August 2016). *SecurityWeek*. "Ramnit Banking Trojan Resumes Activity." Last accessed on 19 January 2017, <http://www.securityweek.com/ramnit-banking-trojan-resumes-activity>
45. Brian Prince. (25 January 2015). *SecurityWeek*. "Ramnit Botnet Brought Down in Joint Operation by Police, Security Researchers." Last accessed on 19 January 2017, <http://www.securityweek.com/ramnit-botnet-brought-down-joint-operation-police-security-researchers>
46. Limor Kessel. (26 August 2016). *SecurityIntelligence*. "Ramnit Rears Its Ugly Head Again, Targets Major UK Banks." Last accessed on 19 January 2017, <https://securityintelligence.com/ramnit-rears-its-ugly-head-again-targets-major-uk-banks/>
47. Kayla Thrailkill. (13 September 2016). *PC Pitstop TechTalk*. "University Gastroenterology Informs Patients of Data Security Incident." Last accessed on 20 February 2017, <http://techtalk.pcpitstop.com/2016/09/13/ugi-security-incident/>

48. Ian Richardson. (2 August 2016). *Sioux City Journal*. "Supervisors Approve investigation into Cyber Attack that Compromised 3,700 County Files." Last accessed on 17 January 2017, [http://siouxcityjournal.com/news/supervisors-approve-investigation-into-cyber-attack-that-compromised-county-files/article\\_6273cb18-7704-5803-bd66-c88a9931a4d0.html](http://siouxcityjournal.com/news/supervisors-approve-investigation-into-cyber-attack-that-compromised-county-files/article_6273cb18-7704-5803-bd66-c88a9931a4d0.html)
49. Kaitlyn Schwerts. (16 November, 2016). *Belleville News-Democrat*. "Unionized Grocery Workers May be Victimized by Computer Hack." Last accessed on February 20 2017, <http://www.bnd.com/news/local/article115148918.html>
50. Jessica Davis. (5 October, 2016). *Healthcare IT News*. "Two Providers Forced to Pay Up in Ransomware Attacks." Last accessed on 20 February 2017, <http://www.healthcareitnews.com/news/two-more-ransomware-attacks-both-organizations-pay>
51. Akanksha Jayanthi. (4 October, 2016). *Beckers' Hospital Review*. "New Jersey Spine Center Pays Ransom to Cyberattackers After 'Seeing No Other Option'." Last accessed on 20 February 2017, <http://www.beckershospitalreview.com/healthcare-information-technology/new-jersey-spine-center-pays-ransom-to-cyberattackers-after-seeing-no-other-option.html>
52. Bobeth Yates. (20 August 2016). *ABC 7 MySuncoast*. "City of Sarasota's System Hacked by Ransomware, Data Held Hostage." Last accessed on 17 January 2017, [http://www.mysuncoast.com/news/local/city-of-sarasota-s-system-hacked-by-ransomware-data-held/article\\_706019e2-6635-11e6-94cc-af3af2bb01f1.html](http://www.mysuncoast.com/news/local/city-of-sarasota-s-system-hacked-by-ransomware-data-held/article_706019e2-6635-11e6-94cc-af3af2bb01f1.html)
53. Daniel Tyson. (27 August 2016). *TheRegister-Herald.com*. "ARH Bomputers Breached." Last accessed on 17 January 2017, [http://www.register-herald.com/news/arh-computers-breached/article\\_5159665b-7786-523b-b233-c3524259b538.html](http://www.register-herald.com/news/arh-computers-breached/article_5159665b-7786-523b-b233-c3524259b538.html)
54. Kobe University. (7 September 2016). *Kobe University*. "On the Computer Virus Infection of Our Professional Computer." Last accessed on 17 January 2017, [http://www.kobe-u.ac.jp/NEWS/info/2016\\_09\\_07\\_01.html](http://www.kobe-u.ac.jp/NEWS/info/2016_09_07_01.html)
55. Amy Dalrymple. (12 September 2016). *Grand Forks Herald*. "ND Department Attacked by Ransomware." Last accessed on 17 January 2017, <http://www.grandforksherald.com/news/4113494-nd-department-attacked-ransomware>
56. Monica Vaughan. (12 September 2016). *Appeal Democrat*. "Ransomware Attack Hits Yuba City Clinic." Last accessed on 17 January 2017, [http://www.appeal-democrat.com/news/ransomware-attack-hits-yuba-city-clinic/article\\_23755354-7954-11e6-8506-5f7d1b5d1d53.html](http://www.appeal-democrat.com/news/ransomware-attack-hits-yuba-city-clinic/article_23755354-7954-11e6-8506-5f7d1b5d1d53.html)
57. Nicole Young. (20 September 2016). *The Tennessean*. "Springfield City Hall Recovers From Ransomware Attack." Last accessed on 17 January 2017, <http://www.tennessean.com/story/news/local/robertson/2016/09/20/springfield-city-hall-recovers-ransomware-attack/90746176/>
58. Rodney Hanners. (20 September 2016). *Keck Medicine*. "Notice of Data Breach." Last accessed on 17 January 2017, <http://www.keckmedicine.org/wp-content/uploads/2016/09/doc11167320160920094345.pdf>
59. KRGV. (22 September 2016). *KRGV.com*. "Palmhurst Police Department Avoids Data Loss." Last accessed on 17 January 2017, <http://www.krgv.com/story/33153212/palmhurst-police-department-avoids-data-loss>
60. Jessica Davis. (4 October 2016). *Healthcare IT News*. "Ransomware Attack on Urgent Care Clinic of Oxford, Purportedly Caused by Russian Hackers." Last accessed on 17 January 2017, <http://www.healthcareitnews.com/node/530046>
61. Dissent. (17 October 2016). *DataBreaches.net*. "Rainbow Children's Clinic Notifies 33,368 Patients of Ransomware Attack." Last accessed on 17 January 2017, <https://www.databreaches.net/rainbow-childrens-clinic-notifies-33368-patients-of-ransomware-attack/>
62. Abe Hawken. (31 October 2016). *Daily Mail*. "NHS Trust Cancels EVERY Operation at Three Hospitals After its Electronic System Was Hit by a Computer Virus Attack." Last accessed on 17 January 2017, <http://www.dailymail.co.uk/news/article-3890964/NHS-Trust-cancels-operation-three-hospitals-electronic-hit-computer-virus-attack.html>
63. Lynn Brezosky. (11 November 2016). *San Antonio Express-News*. "Ransomware Attack Targets Seguin Dermatology Practice." Last accessed on 17 January 2017, <http://www.expressnews.com/business/local/article/Ransomware-attack-targets-Seguin-dermatology-10609268.php>
64. Brittany Seemuth. (10 November 2016). *Northwest Now*. "Cyber Ransoming Hits Menomonee Falls Businesses." Last accessed on 17 January 2017, <http://www.mynorthwestnow.com/story/news/local/menomonee-falls/2016/11/10/cyber-ransoming-hits-menomonee-falls-businesses/93548816/>



65. Herald Bulletin. (15 November 2016). *Indiana Economic Digest*. "EDITORIAL: Madison County Hacker Attack Will Cost More Than Ransom Payment." Last accessed on 17 January 2017, <http://indianaeconomicdigest.com/main.asp?SectionID=31&subsectionID=201&articleID=85949>
66. Kayla Thrailkill. (18 November 2016). *PC Pitstop Tech Talk*. "Spencer Chamber of Commerce Infected With Ransomware." Last accessed on 17 January 2017, <http://techtalk.pcpitstop.com/2016/11/18/spencer-chamber-infected-ransomware/>
67. Associated Press. (24 November 2016). *Billings Gazette*. "Ransomware Attack on Bigfork Schools; Fix in Works." Last accessed on 17 January 2017, [http://billingsgazette.com/news/state-and-regional/montana/ransomware-attack-on-bigfork-schools-fix-in-works/article\\_7ff38855-e5a1-59d8-84de-18869e1c0df6.html](http://billingsgazette.com/news/state-and-regional/montana/ransomware-attack-on-bigfork-schools-fix-in-works/article_7ff38855-e5a1-59d8-84de-18869e1c0df6.html)
68. Devin Zimmerman. (29 November 2016). *kokomoperspective*. "Ransomware Targets Howard County Government." Last accessed on 17 January 2017, [http://kokomoperspective.com/kp/news/ransomware-targets-howard-county-government/article\\_9a6d8640-b5bb-11e6-854b-ff832671083f.html](http://kokomoperspective.com/kp/news/ransomware-targets-howard-county-government/article_9a6d8640-b5bb-11e6-854b-ff832671083f.html)
69. Matthew Braga. (29 November 2016). *CBC News*. "Carleton University Computers Infected with Ransomware." Last accessed on 17 January 2017, <http://www.cbc.ca/news/technology/ransomware-carleton-university-computers-bitcoin-infects-1.3872702>
70. Erin Allen. (8 December 2016). *PC Pitstop Tech Talk*. "Henry County Hit with Ransomware, Leaving 18,000 Voters as Victims." Last accessed on 17 January 2017, <http://techtalk.pcpitstop.com/2016/12/08/henry-county-hit-ransomware-leaving-18000-voters-victims/>
71. Erin Allen. (14 December 2016). *PC Pitstop Tech Talk*. "Ransomware Strikes Arkansas Sheriff's Office." Last accessed on 17 January 2017, <http://techtalk.pcpitstop.com/2016/12/14/ransomware-strikes-arkansas-sheriffs-office/>
72. Joseph Goedert. (22 December 2016). *Information Management*. "California Health Center Ransomware Attack Affects 65,000." Last accessed on 17 January 2017, <http://www.information-management.com/news/security/california-health-center-ransomware-attack-affects-65000-10030545-1.html>

Created by:

**TrendLabs**

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

#### TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit [www.trendmicro.com](http://www.trendmicro.com)



Securing Your Journey  
to the Cloud