The Reign of Ransomware

TrendLabs℠ 2016 1H Security Roundup

Contents

By the end of 2015, we predicted that 2016 would be the Year of Online Extortion.[1] This particular forecast was influenced by the proliferation of stolen data from data breach incidents used for online extortion, and an increasing number of similar online threats.

True enough, the first half of 2016 witnessed a surge of ransomware attacks launched against a variety of industries. During the first half of 2016 we blocked and detected almost 80 million ransomware threats. The rapid rise of ransomware cases could be a clear indication of ransomware's effectiveness in granting cybercriminals the satisfaction of easy monetary reward. With the rising number of ransomware cases and more enterprises continuously losing money and opting to pay ransom,[2] we believe that the Reign of Ransomware will stay prevalent.

Cybercriminals using exploit kits also took notice of ransomware. During the first half of 2016, we detected exploit kits distributing ransomware to their victims. Sundown[3] and Hunter began carrying ransomware this year while Rig changed the type of ransomware incorporated in their kit. Meanwhile, new vulnerabilities were also added to existing exploit kits even as the number of attacks using the Angler exploit kit had gone down.

Aside from ransomware, another form of online extortion, Business Email Compromise (BEC) attacks, remained persistent in inflicting notable damage to its victims. With a total of US$3 billion worth of losses to victims, the U.S. Federal Bureau of Investigation (FBI) had issued several warnings to different industries about the prevalence of BEC attacks. The success of BEC campaigns relies on its ability to compromise legitimate business email accounts and appeal to its victims' regard for authority through social engineering and other intrusion techniques.

The year is not over yet. But we have already seen the existence of damaging threats that are capable of crippling organizations. In this report, we round up all the significant security stories during the first half of 2016 to encourage businesses to check for vulnerabilities cybercriminals may abuse. Our report also aims to highlight the need for enterprises to be vigilant in finding solutions that would stop cybercriminals from winning and letting our prediction become their reality.

NOTE: All mentions of "detections" within the text refer to instances when threats were found on users' devices and subsequently blocked by any Trend Micro security solution. Unless otherwise stated, the figures featured in this report came from data gathered by the Trend Micro Smart Protection Network cloud security infrastructure, which uses a combination of in-the-cloud technologies and client-based techniques to support on-premise products and hosted services.

Ransomware Dominates the Threat Landscape

In the first half of 2016, ransomware went over and beyond our expectations. During the first six months of 2016, we discovered a total of 79 new ransomware families—a figure that eclipsed the number of ransomware families we detected for 2015. Our discovery also marks a 172% increase in ransomware families for the first half of 2016. For the complete list of ransomware families, refer to Table 3 in the Threat Landscape in Review section.

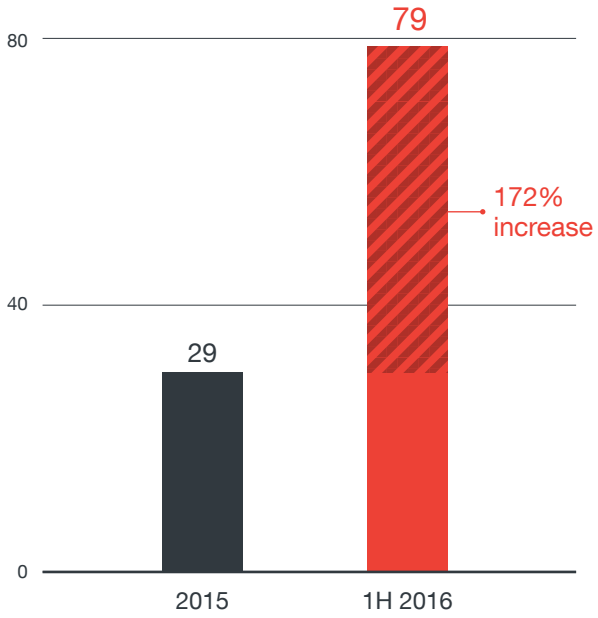

Figure 1. Number of newly added ransomware families, 1H 2016

Though the number of ransomware attacks is a cause for concern, the depth of damage ransomware inflicts on enterprises is also what makes the threat noteworthy. During the first three months of the year, the FBI revealed that ransomware caused enterprises a total of US$209 million in monetary losses. Although paying the ransom is strongly discouraged, this had become the quickest way to retrieve critical files for some companies like the Hollywood Presbyterian Medical Center (US$17,000),[4] the University of Calgary (US$16,000),[5] and the Horry Country School (US$10,000).[6] Aside from ransomware helping cybercriminals extort money from businesses, they had also caused businesses to shut down temporarily as productivity and daily operations were affected, such is the case with the Hollywood Presbyterian Medical Center when ransomware crippled the hospital's network.

Ransomware continued to grow with new variants showing up frequently. During the first half of 2016, we blocked and detected almost 80 million ransomware threats. Among the threats we blocked and detected, 58% of those were attachments in spammed email, 40% were downloads from URLs hosting ransomware or from exploit kits leading to ransomware, and 2% were actual ransomware files. Despite that, cybercriminals continued to add new routines and new tricks to convince users to pay the ransom. For example, JIGSAW ransomware threatened to delete a number of files for every hour the ransom isn't paid.[7] While SURPRISE,[8] another ransomware variant, would increase the ransom amount if the user fails to meet the deadline.

The first half of 2016 also saw the rise of several ransomware built with routines that were designed to attack enterprise machines and endpoints. For example, CRYPSAM was used to infect unpatched servers by exploiting a vulnerability found in Java-based applications. Once these servers were infected with CRYPSAM, every network connected to the server was infected with ransomware.[9] This left endpoint machines in the network to deal with ransomware on their own. The ZCRYPT ransomware is known to spread through USB dongles and flash drives, accessories which are widely used in any business.[10] Aside from CRYPSAM and ZCRYPT, there were also other ransomware families which exhibited routines that could harm enterprises. Some of these families include CRYPJOKER, the aforementioned SURPRISE, and POWERWARE[11] which targeted database-related files and even tax return files. Meanwhile CRYPRADAM and KIMCIL targeted files related to hosting a website.

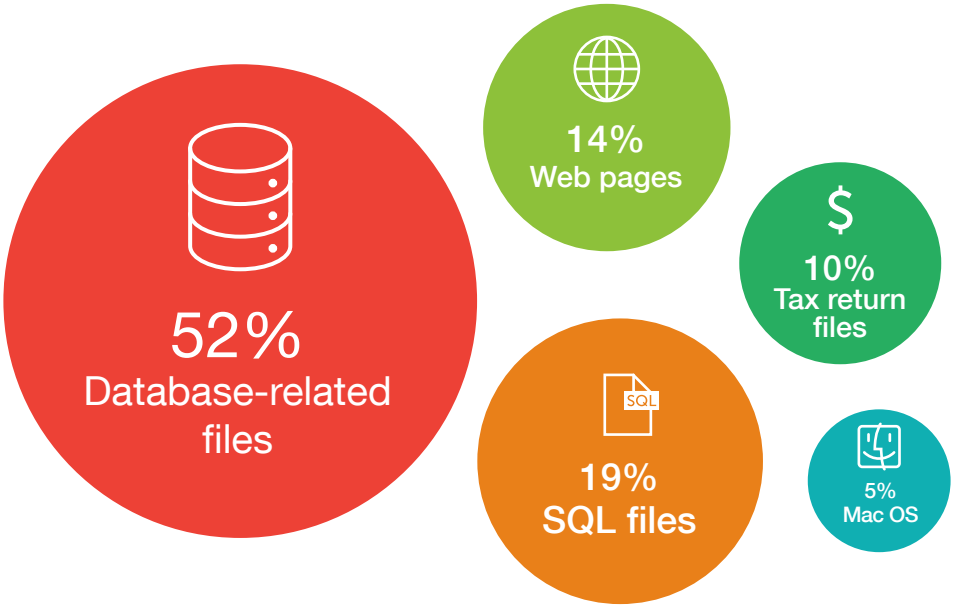

Figure 2. Breakdown of business-related files encrypted by known ransomware families, 1H 2016

When it comes to the mode of propagation, ransomware had begun to arrive through means other than email or spam. During the first half of 2016 we continued to see exploits delivering ransomware. However, we also saw ransomware being propagated through a remote desktop control application. As the means for distributing ransomware has changed, we believe that traditional security is no longer enough since attackers usually target areas organizations sometimes neglect to protect.

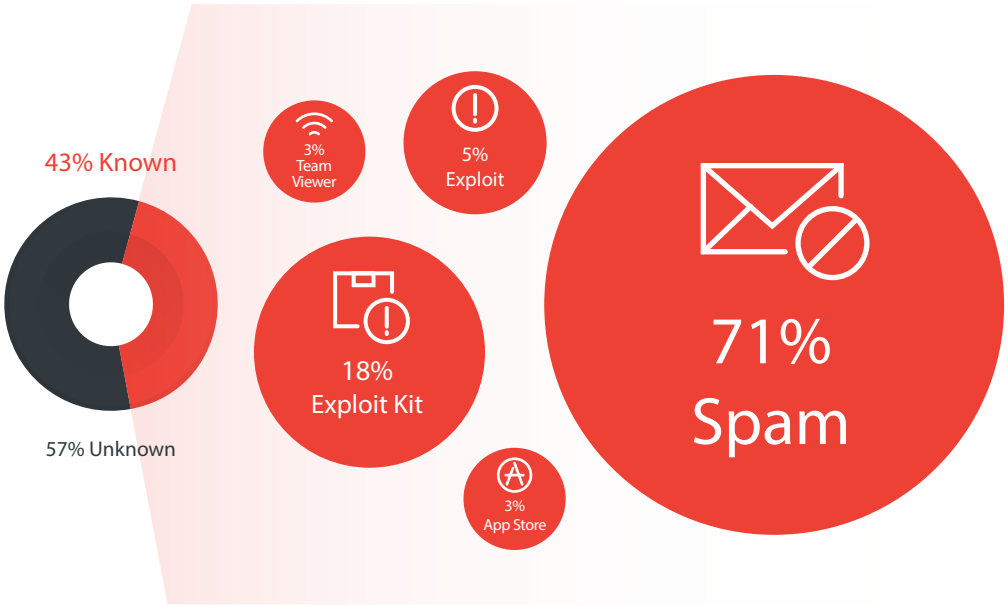

Figure 3. Breakdown of known infection vectors used to distribute ransomware, 1H 2016

Cybercriminals go after what enterprises value the most. Though an ominous threat, there are still several ways in which businesses can protect themselves against ransomware. While educating employees about the dangers of ransomware is important, adopting a multilayered security strategy could better prevent ransomware from infiltrating enterprise networks and endpoints and corrupting business-critical files and data.

As there had been ransomware attacks taking advantage of unpatched servers, regularly patching or updating software is a must. However, software patching is hugely dependent on how often vendors release official patches and how quickly network administrators can apply the said patches to all their endpoints. Therefore, enterprises should consider virtual patching solutions that will effectively defend critical systems in the interim.

For network defense, enterprises should apply solutions that are capable of monitoring network ports with reputation-based analysis and blocking, script emulation, and zero-day exploit detection. Businesses should also look for solutions that allow custom sandbox analysis, a safe environment which IT administrators can use to examine potential ransomware behavior.

Another strategy that businesses can use to protect end-users involves the use of behavior monitoring and application control. Behavior monitoring defends endpoint machines from ransomware as it is able to detect rapid encryption of multiple files in a system, stop encryption, and block ransomware from spreading more damage. Solutions equipped with application control help since they only allow the execution of good apps identified in its whitelist.

BEC Scams Spread Across the World

Business Email Compromise (BEC) schemes are scam tactics which compromise business accounts in order to facilitate an unauthorized fund transfer. Today, they are considered one of the most dangerous threats to organizations. In terms of damage, the FBI listed over 22,000 victims to BEC scams from January 2015 to June 2016, with over US$3 billion in total losses all over the world.[12] Given BEC attacks' reach, it is clear that any enterprise or business can be a potential victim. Our initial findings showed that BEC scams were most prevalent in the United States, the United Kingdom, Hong Kong, Japan, and Brazil. In addition, we also saw BEC campaigns carried out in several other countries such as the ones identified in the map below. All these data helped us conclude that BEC is indeed becoming a big threat.

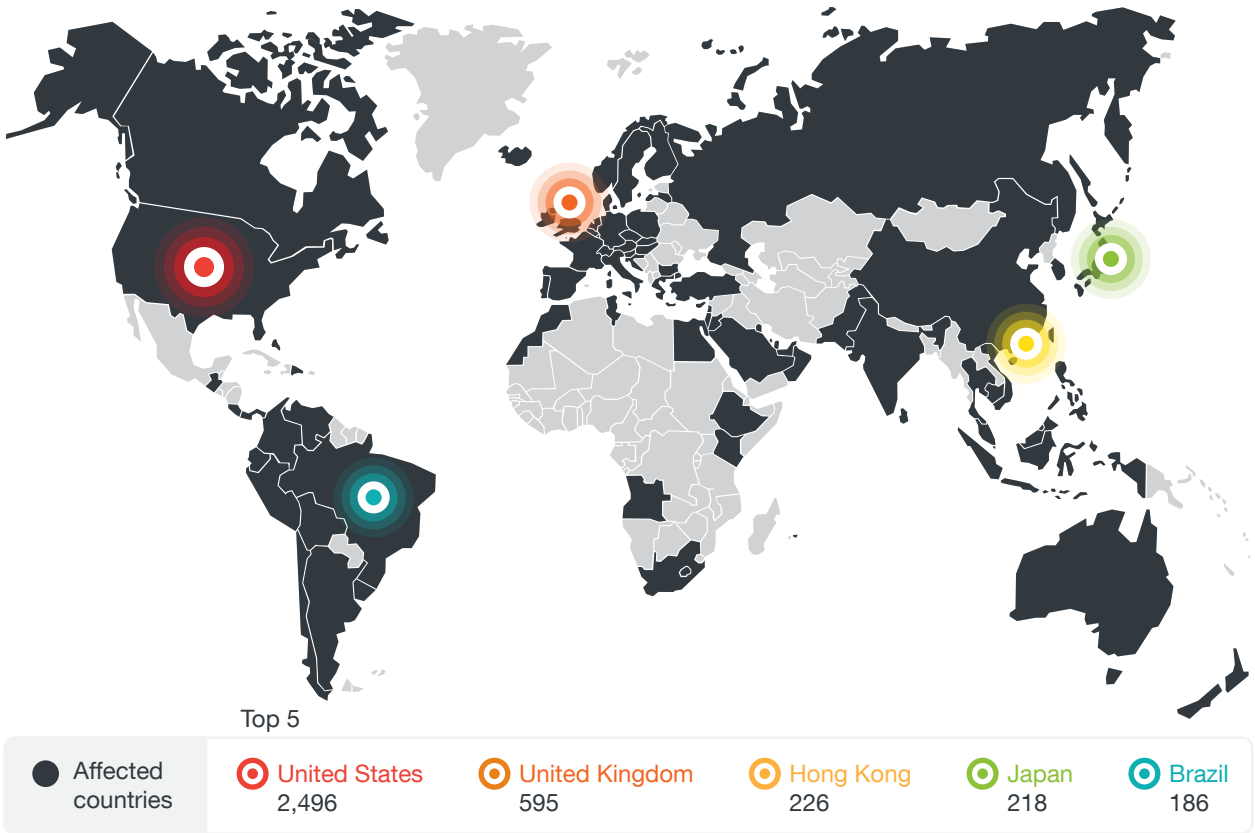

Figure 4. Countries with the most number of companies affected by BEC, 1H 2016

The effectiveness of BEC scams lies in the techniques employed against its preferred targets. Attackers are able to deceive victims by combining their knowledge of social engineering techniques and well-researched information about the target. Most of the time, attackers behind BEC scams impersonate people who have access to a company's finances—may it be a company's CEO, managing director, CFO, or even financial controller. Based on our monitoring from January 2016, we observed that BEC scams often targeted CFOs more than any other position in a company. Once attackers had picked someone of authority to spoof, their next move would involve tricking their victims to permit a fund transfer to serve as payment for an invoice or perhaps a legal settlement.[13]

Although BEC scams are usually devoid of malware, there are still a few instances when malware can be used to extort money. Some of these malware are in the form of simple, yet effective, information stealers such as keyloggers. In our 2014 reports on BEC scams we identified keyloggers like Predator Pain and Limitless being used in extensive BEC campaigns.[14] Some attackers include keyloggers in BEC campaigns to steal confidential information they can use for illegal transactions.

BEC scams are treacherous. Though their design is extremely simple, the tactics attackers use for a successful BEC campaign is quite complex and effective as it appeals to people's respect for authority. Therefore, an effective way to defend against BEC scams should be a mixture of proper employee education and security solutions that will help identify threats even before they reach a person's inbox.

Employees can be considered the last line of defense from BEC scams, so businesses must enact best practices for employees to follow when dealing with emails that urge them to make fund transfers. Some of these best practices may involve carefully scrutinizing emails requesting payment, raising employees' awareness of the existence of scams such as BEC, and reporting deceitful incidents to law enforcement agencies.

Since most BEC scams do not involve malware, traditional email solutions that only detect emails with malicious links or attachments are not enough to stop BEC. An email solution that is able to flag social engineering techniques is needed to effectively block malicious email messages that are used in BEC campaigns.

Exploit Kits Take On New Vulnerabilities and Ransomware Families

Despite ransomware taking center stage during the first half of 2016, exploit kits continued to make waves, though not as large and forceful as before. As 2016 began, we saw a changing trend in the numbers of attacks using the Angler exploit kit—the number of infections began dropping.

The shrinking number of Angler-related attacks can be connected to the recent arrest of 50 cybercriminals in the UK and Russia, which was reported on June 2016. The decrease in the use of Angler exploit kits could mean that cybercriminals already consider Angler a 'compromised' exploit kit which could lead law enforcement agencies right to their trail. Thus, cybercriminals decided to look elsewhere for profit. So with cases involving the Angler exploit kit going down, other exploit kits eased their way into the spotlight. We are seeing access counts to sites hosting the Neutrino exploit kit increase, following the drop in access counts for Angler-hosting sites.

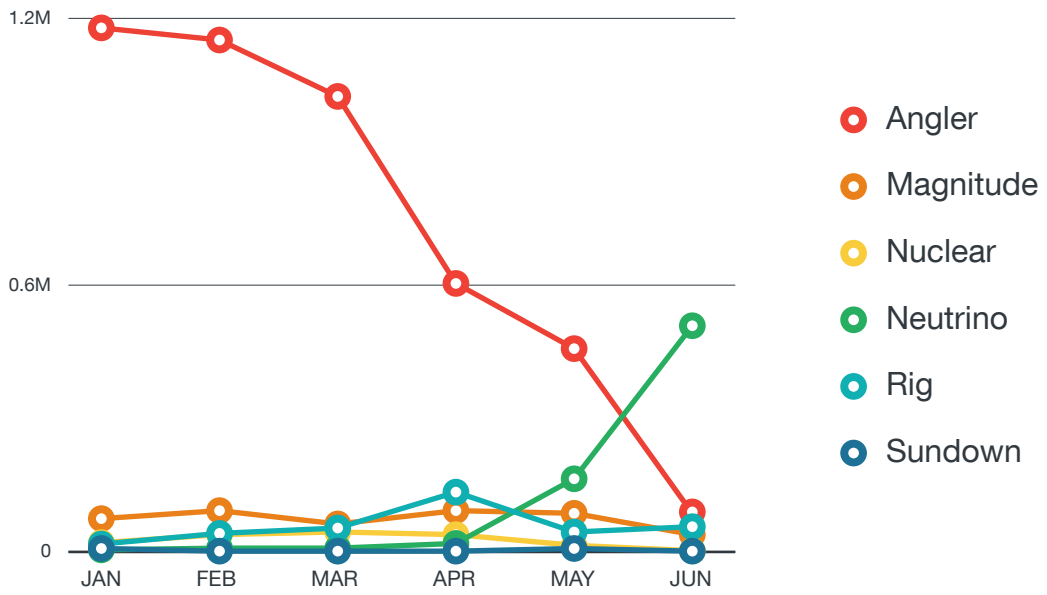

Figure 5. Number of access to exploit-kit-hosting URLs, 1H 2016

In June we released a report about how some exploit kits began distributing ransomware.[15] Some of the noteworthy exploit kits using this tactic are Rig, Hunter, and Sundown, which delivered ransomware variants such as GOOPIC and CRYPTOSHOCKER. Rig, though a relatively new exploit kit, had already infected victims from 40 different countries, with Japan users being its main target. Rig and Nuclear also caught our attention when they began distributing a different type of ransomware in their kits this year (moving from CRYPWALL, CRYPTESLA, and CRYPCTB to GOOPIC, CERBER, LOCKY, and CRYPTESLA). Meanwhile exploit kits Sundown and Hunter had only begun distributing ransomware this year.

Exploit Kits	Ransomware Delivered (2015)	(2016)
Angler	CRYPWALL	CRYPWALL
	CRYPTESLA	CRYPTESLA
	CRILOCK	CRILOCK
		WALTRIX
Neutrino	CRYPWALL	CRYPWALL
	CRYPTESLA	CRYPTESLA
		CERBER
		WALTRIX
		LOCKY
Magnitude	CRYPWALL	CRYPWALL
		CERBER
Rig	CRYPWALL	GOOPIC
	CRYPTESLA	CERBER
Nuclear	CRYPWALL	CRYPTESLA
	CRYPTESLA	LOCKY
	CRYPCTB	
	CRYPSHED	
Sundown		CRYPTOSHOCKER
Hunter		LOCKY
Fiesta	CRYPTESLA	

Table 1. Ransomware families delivered by exploit kits

The first half of 2016 also saw new vulnerabilities added to existing exploit kits; most of which were vulnerabilities for the Adobe® Flash® Player, followed by Microsoft Internet Explorer® and Microsoft Silverlight®.There are several exploit kits that adopted these new vulnerabilities. Angler exploit kit tops the list with the highest number of new vulnerabilities in its code, while Magnitude and Neutrino followed closely. Despite new vulnerabilities being added to exploit kits, the total number of added vulnerabilities for the first half of 2016 is still smaller than the ones added in 2015.

Even with the number of Angler-related attacks going down, it doesn't mean that businesses can be complacent. As our data showed, the threat of exploit kits is still very much alive—with new exploit kits picking up where Angler left off, exploit kits distributing ransomware, and even new vulnerabilities added to some kits. With that, businesses of any size and type must be more vigilant in protecting their systems from exploit kits. The figure below shows the increase of attempts made to exploit such vulnerabilities.

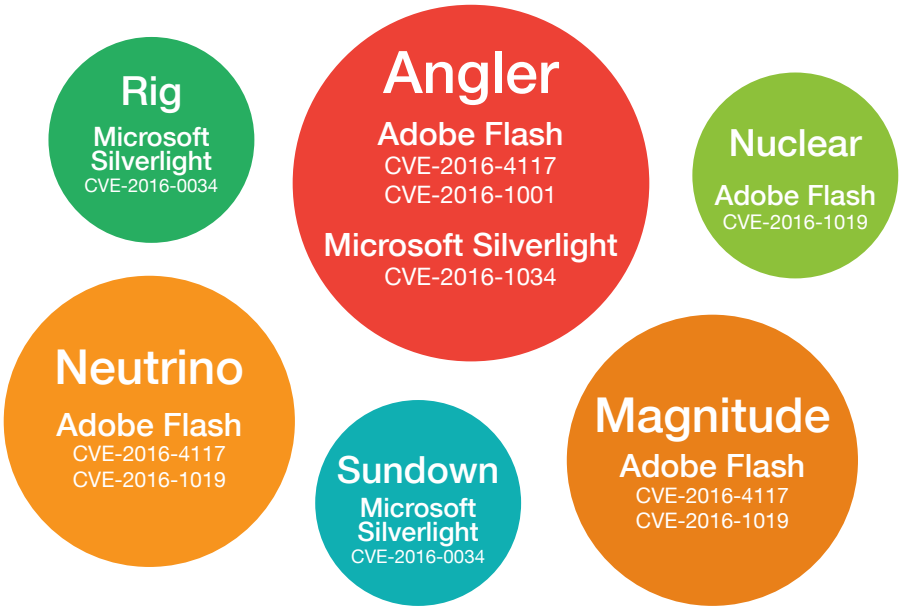

Figure 6. Exploits to specific vulnerabilities included in specific exploit kits, 1H 2016

One of the many ways exploit kits succeed in infecting networks is through vulnerabilities found in unpatched software. Most of the time, regularly applying a patch is challenging as it is time-consuming and costly. Another challenge to doing a manual patch is the presence of security gaps while businesses wait for an official patch. Enterprises also risk their safety when they continue to use legacy software. A good solution that can protect businesses from such vulnerabilities is virtual patching, as it shields vulnerable systems from exploit kits aiming at those weaknesses in a system.

Rising Number of Vulnerabilities Found in Adobe Flash Player and IoT Platforms

When it comes to spotting vulnerabilities, timing is everything. For security researchers, the best time to find a vulnerability is before it is used for an attack. For malicious actors, on the other hand, this is before the vulnerability is discovered by security researchers, or before the software vendor is able to issue a patch. Caught in this race to find vulnerabilities are enterprises that strive to be one step ahead in securing their networks from vulnerabilities that could expose them to damaging attacks.

For enterprises, keeping ahead means being constantly aware of the vulnerabilities being discovered and making sure that patches are applied to all applicable systems. For the first half of 2016 alone, Trend Micro (with TippingPoint) and the Zero Day Initiative (ZDI) had discovered a total of 473 vulnerabilities in a variety of products, with most of the vulnerabilities coming from Adobe Flash and Advantech's Web Access. Here is a list of the top 10 applications based on the number of vulnerabilities found:

Discovered by Trend Micro (In partnership with TippingPoint)		**Discovered through the Zero Day Initiative**	
Product	#CVE	Product	#CVE
Adobe Flash	28	Web Access	108
Android	11	Adobe Reader DC	26
OS X	11	Storage Resource Monitor Profiler Module	24
iOS	8	Foxit Reader	23
Microsoft Office	5	Internet Explorer	22
Internet Explorer	3	Adobe Acrobat Pro DC	19
Qualcomm	1	OS X	17
Apache Active MQ	1	Application Testing Suite	15
ffmpeg	1	LeviStudio	14
Edge	1	Edge	13

Table 2. Top 10 applications based on number of vulnerabilties found, 1H 2016

The number of vulnerabilities found in Adobe Flash Player can be attributed to the instances of attempted zero-day and ransomware attacks targeting the platform. Earlier this year we saw a few zero-day attacks from the Magnitude Exploit Kit that targeted the vulnerability (CVE-2016-1019) found in some versions of Adobe Flash Players. The exploit kit that incorporated the said vulnerability to its code had been able to leave systems affected with ransomware.[16]

The use of Adobe Flash Player vulnerabilities for zero-day attacks has been going on for a while now and is likely to continue in the future. Last year, there were several zero-day attacks abusing Adobe Flash Player vulnerabilities. One involved a zero-day attack using the Angler Exploit Kit for malvertisements,[17] then another allowed attackers to control the affected system,[18] while one more Adobe Flash zero-day exploit was used by attackers behind Pawn Storm—a ongoing campaign which targets several key figures around the world.[19]

Another application with quite a number of vulnerabilities found was Advantech's WebAccess, a web-based human machine interface (HMI) and Supervisory Control and Data Acquisition (SCADA) software that remotely automates industrial processes. Today SCADA software is used by a lot of companies in private and public sectors all over the world. Advantech, alone, operates in 23 countries—with most of their clients located in Greater China and the U.S.[20] Out of the 108 vulnerabilities discovered in Advantech's WebAccess, 28 were zero-day vulnerabilities.

The discovery of vulnerabilities through a process such as the ZDI can be considered a good thing—especially for certain software programs, like Advantech's WebAccess, that are used for the internet of things (IoT) and SCADA. A lot of these platforms had been primarily developed with the idea of functionality in mind and not security, and that opens up users to a lot of risk. With the continued adoption of IoT and the looming threat against SCADA infrastructures, it is important for SCADA and IoT support platforms to be secured.

Apart from those discovered through the partnertship of Trend Micro and TippingPoint, other notable vulnerabilities were found during the first half of the year. Aside from the zero-day exploits using Adobe Flash Player, there were 21 new vulnerabilities discovered during the 2016 Pwn2Own competition, a yearly vulnerability research competition attended by a lot of security researchers around the globe. There were also six browser vulnerabilities and six kernel vulnerabilities that were unveiled during the event.[21] Here are the products that were identified to have vulnerabilities:

- Microsoft Windows: 6
- Apple OS X: 5
- Adobe Flash: 4
- Apple Safari: 3
- Microsoft Edge: 2
- Google Chrome: 1

A month after the Pwn2Own event, TippingPoint's ZDI found two critical vulnerabilities affecting Apple®'s QuickTime® for Windows. The announcement of these two vulnerabilities came after Apple declared that they will no longer provide security updates for QuickTime on Windows.[22]

As the race to either secure or abuse vulnerabilities continues among security researchers and malicious actors, it is crucial for the security industry and enterprises in general to try to deal with vulnerabilities as systematically as possible. The ZDI, for example, rewards security researchers for the responsible disclosure of vulnerabilities and acts as a broker for security vulnerabilities found in their customers' products. This helps both vulnerability researchers and software vendors, as it provides a good channel to be able to communicate information. In the first half of 2016 alone, ZDI purchased more Adobe vulnerabilities than Microsoft vulnerabilities.

Although the partnership between Trend Micro and TippingPoint may not entirely stop cybercriminals from abusing vulnerabilities, the combined solutions will, however, help enterprises be one step ahead and have solid protection for their network—even against vulnerabilities that haven't been discovered yet. For the times that software vendors haven't released an official patch or perhaps decide to discontinue support for a particular program, enterprises must put to use virtual patching solutions that are capable of providing strong and efficient protection that will shield vulnerabilities from exploits. Using such security filters allows organizations to take control of their systems without fear of becoming a victim to damaging attacks. In addition, solutions that provide diligent and timely updates of critical vulnerabilities found in the wild will also provide another layer of defense to enterprises.

Data Breaches Plague Various Industries

Data breaches are a constant. No matter what the main threat of the year is, data breaches continue to be a prevalent and damaging threat, especially to businesses. One of the recent cases of data breach in 2016 involved the social media site Myspace, where 360 million usernames and passwords were hacked.[23] Though Myspace is no longer as popular as it used to be, attackers may still use the login credentials to hack other accounts the victim owns in other sites. In March, Verizon was hit by data breaches when a list containing the contact information of 1.5 million customers of Verizon Enterprise Solutions was publicly posted underground for sale.[24] It is important to note that 97% of the Fortune 500 companies are considered Verizon customers.

The first half of 2016 witnessed how data breaches affected organizations in the government, the healthcare industry, and even the entertainment industry. By the end of the first quarter, the 21st Century Oncology announced that personal information of 2.2 million of their patients had been stolen.[25] A month before that, hackers set their eyes on the U.S. Internal Revenue Service (IRS) and accessed 464,000 unique social security numbers which were used to file fraudulent tax returns.[26]

When a business or an organization falls victim to a data breach, perpetrators gain access to one of the most precious commodities today—information. Whether it's personally identifiable information (PII), health records, payment card data, or even log-in credentials, attackers may find a way to utilize that information to conduct financial fraud, identity theft, blackmail, espionage, and even extortion. Though the exposure of PII may not have equivalent monetary value businesses, however, risk losing a whole lot more when their credibility and reputation is questioned. When that happens, the future of any business becomes uncertain.

As data breaches continue to be a real risk for enterprises, IT administrators must prepare solutions that will effectively stop data breach incidents. When it comes to the cause for data breaches, device loss continues to claim the top spot. In our research, we found that device loss accounts for 41% of all data breaches.[27] In today's world, data have become more mobile. People are now storing and accessing data on laptops,

mobile devices, flash drives, and even the cloud. With that, it is important for enterprises to acquire solutions that are capable of tracking, securing, and encrypting confidential data on multiple points—even when a device is lost or stolen. To complement this, businesses should also enforce stricter policies when it comes to storing confidential information on mobile devices.

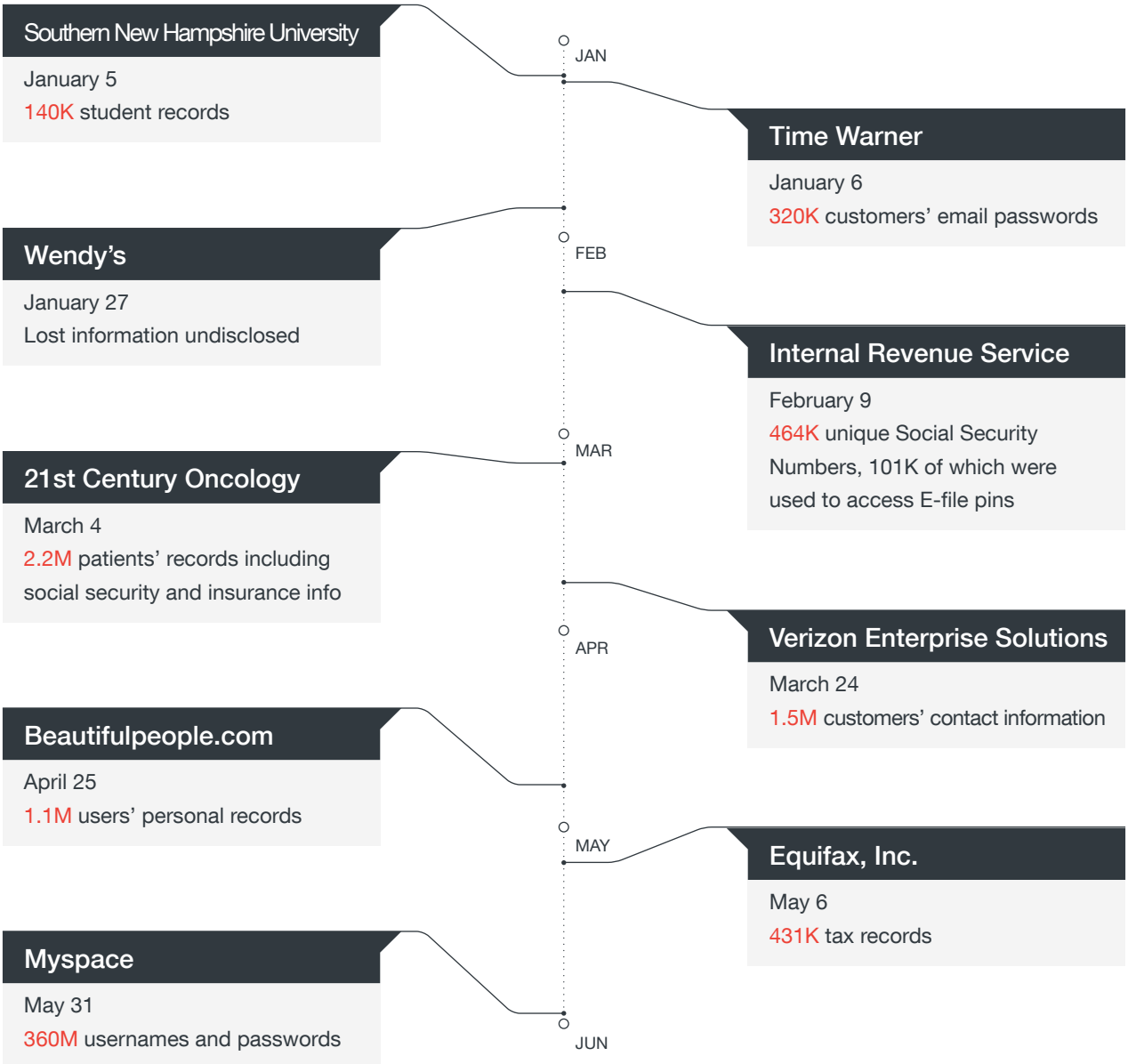

Figure 7. Timeline of data breaches, 1H 2016

Next to device loss, hacking—whether using brute force or social engineering—and malware are two of the most popular methods attackers use to conduct a data breach. To defend against these, enterprises must deploy solutions which can detect, analyze, and respond to advanced malware and other hacking techniques used for breaches.

Updates in PoS Malware Give Rise to New Attacks

In June, we detected a new Point-of-Sale (PoS) malware that was equipped with fast and efficient credit card theft capabilities. We named it FASTPoS because of the malware's capability to quickly send data from a swiped card to the attackers, instead of sending captured data periodically. Because of the speed in which FastPoS sends out information back to the attackers, we believed that this particular PoS malware was designed to target small and medium-sized businesses that move through a much smaller network environment. Despite that, we saw traces of the FastPoS malware affecting victims from Taiwan, Japan, Hong Kong, Brazil, France, Iran, and the United States.[28]

Aside from the FastPoS malware, the updated FighterPoS malware possesses 'worm-like' capabilities which allows it to propagate from one PoS terminal to another in the same network.[29] The addition of the malware's new routines seems to be a way for the attackers behind the FighterPoS to expand their campaign. Originally, FighterPoS was first seen affecting victims from Brazil but with the recent update, we noticed that the FighterPoS malware has already begun attacking victims in the U.S. Although PoS malware is no longer a new phenomenon, it continues to evolve—even in ways that are more damaging to businesses. Aside from the risk of businesses losing profit, they also have to face the consequences of exposed customer data.

To protect endpoints from PoS malware, businesses can opt for solutions that provide application control or whitelisting. Using such features allows IT administrators to block the installation and/or update of apps that are not included in the whitelist.

Exploits Revive Old Vulnerabilities in Their Attacks

In every attack, cybercriminals always look for an easy way in. One of the most accessible ways for attackers to enter a system is through vulnerabilities, both old and new. During the first half of 2016, we detected attacks attempting to exploit vulnerabilities found in Microsoft IIS (CVE-2015-1635) and two Shellshock Bash vulnerabilities (CVE-2014-6271/CVE-2014-6278).

For enterprises, the Shellshock or Bash Bug vulnerability matters a lot since it puts at risk half a billion servers and devices worldwide. Shellshock, which is mostly found in Unix, Linux, and Mac OSX systems, allows them to remotely execute commands and take over a system even without authentication. This vulnerability also allows them to access confidential data stored in the servers or perhaps set up the servers for future attacks with a backdoor.[30]

The first half of the year saw an increasing number of attacks exploiting Shellshock. Attacks using Shellshock or Bash Bug could mean that malicious actors are trying to make use of old vulnerabilities for new attacks. Below is a graph denoting the number of attacks that attempted to exploit the above-mentioned vulnerabilities.

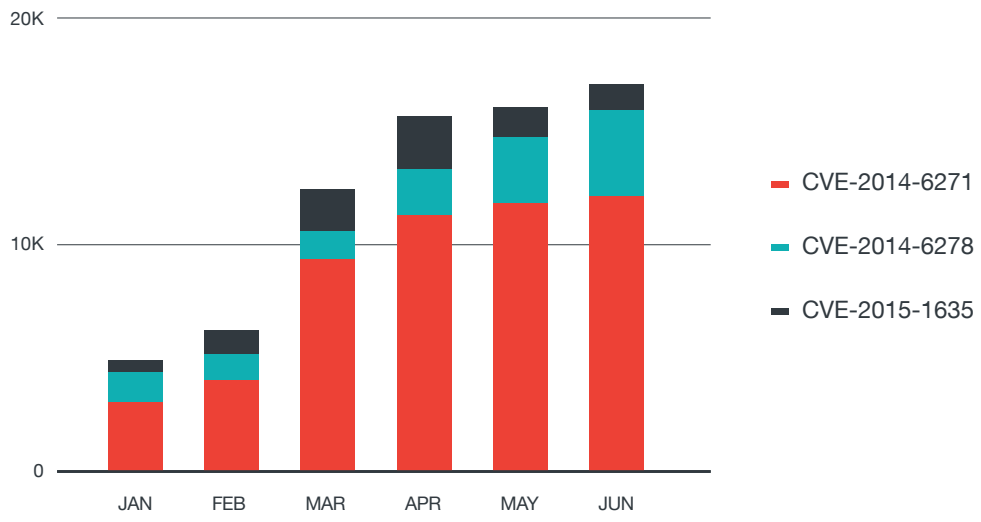

Figure 8. The number of attacks that attempted to exploit certain vulnerabilities, 1H 2016

To keep servers protected from exploits, businesses must regularly patch their servers. However, manually patching and updating software frequently is challenging since there are hundreds of software vulnerabilities exposed every month. The process of manually patching software is known to be inefficient; the time that businesses have to wait for an official patch creates a window of opportunity for attackers to use exploits for these vulnerabilities. To address this, businesses must avail of solutions that are capable of virtual patching, which can shield vulnerabilities while an official patch has not been applied. Virtual patching solutions also provide immediate protection from exploits that target legacy systems or software that are no longer supported.

Cybercriminals Defy the Odds with Banking Trojans

When criminals are arrested, the usual assumption is that the incidence of crime will go down. But in the case of banking Trojans, the opposite seemed to be the case. Before 2015 ended, the cybercriminal group behind the DYRE/DYREZA banking Trojan was arrested. Despite that, banking Trojans continued to resurface with the return of QAKBOT. We believe that this increase in the number of QAKBOT detections is attributed to other cybercriminals filling up the void the arrest of the DYRE/DYREZA authors created.[31]

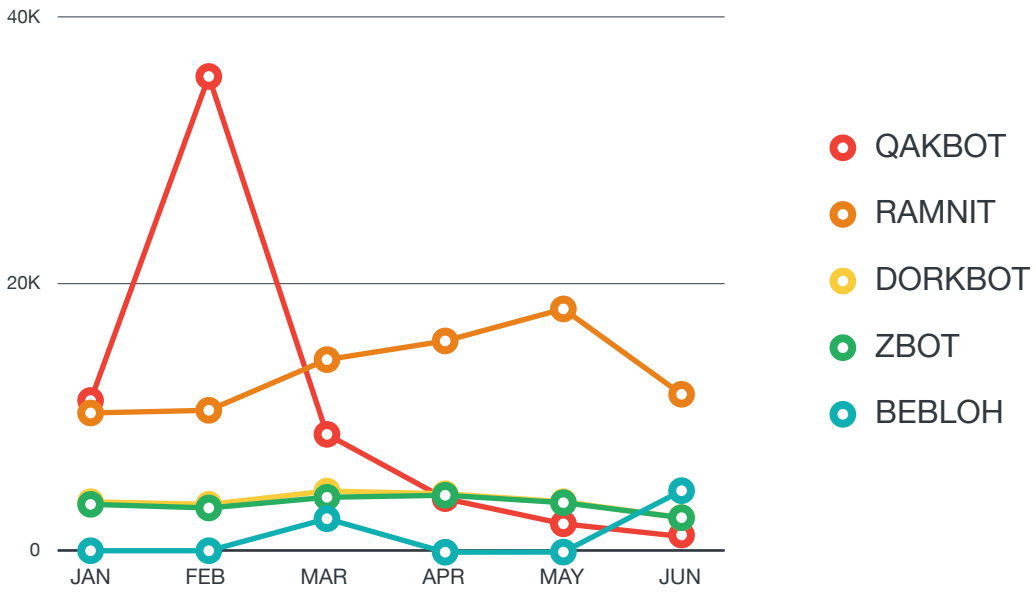

Figure 9. Top malware families, 1H 2016

QAKBOT is a multicomponent threat that can strongly affect enterprises. Since its conception in 2007, QAKBOT has been able to steal information and install malware on devices from the U.S., Canada, and Brazil. Some of the crucial information that QAKBOT targets are banking credentials, browsing habits, and user's sensitive data. The challenge in dealing with QAKBOT lies in its continued evolution (with new variants released earlier this year detected as *WORM_QAKBOT.SMUV* and *WORM_QAKBOT.SMUX*) and its stealth routines.

Banks and their customers share the burden of dealing with banking Trojans such as QAKBOT since there are a lot of employees who perform banking transactions, either on their desktop or mobile devices, within an enterprise's network. When users' banking information are stolen, the risk of losing money is highly unavoidable since cybercriminals would either use these banking credentials to conduct fraudulent transactions or perhaps sell it for profit. For companies in the banking industry, being affected by banking Trojans could also mean unexpected expenditure as companies would have to deal with compensating their customers for the money they lost and investing in repairing the damages incurred.

QAKBOT uses various infection vectors to enter a user's system, like when users visit a malicious site or when users download a malicious PDF from their email. With that, a solution that can protect a system's various entry points (web, file, and email) is ideal. These solutions must be able to offer a connected threat defense strategy, which will stop malicious activity based on collected information on threats from the web, files, and email.

Aside from protecting endpoint machines from this threat, banks should also adopt the use of two-factor authentication protocols on their sites. In addition, banking sites should encourage their customers to practice vigilance and safety when opening email messages, visiting websites, and downloading files.

Threat Landscape in Review

For the first half of 2016, we had blocked a total of 29 billion threats, which is already more than half of the total number of blocked threats in 2015. The increase in the number of threats could be attributed to the rising number of ransomware attacks.

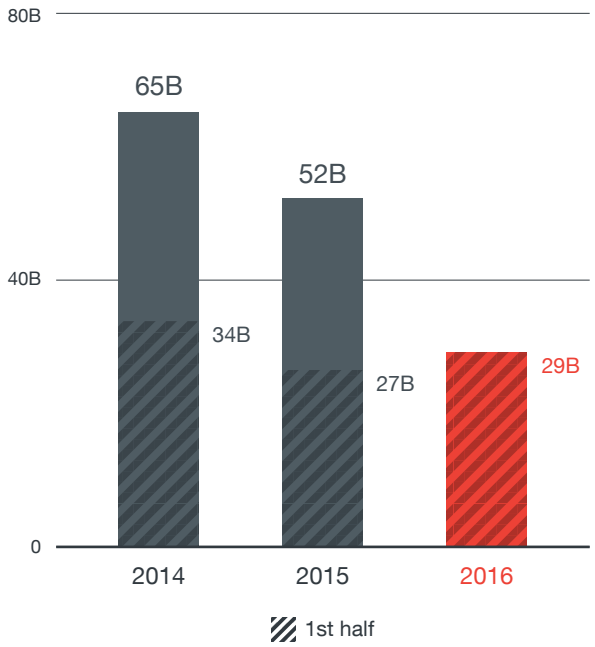

Figure 10. Overall threats blocked by the Trend Micro™ Smart Protection Network™, 1H 2016

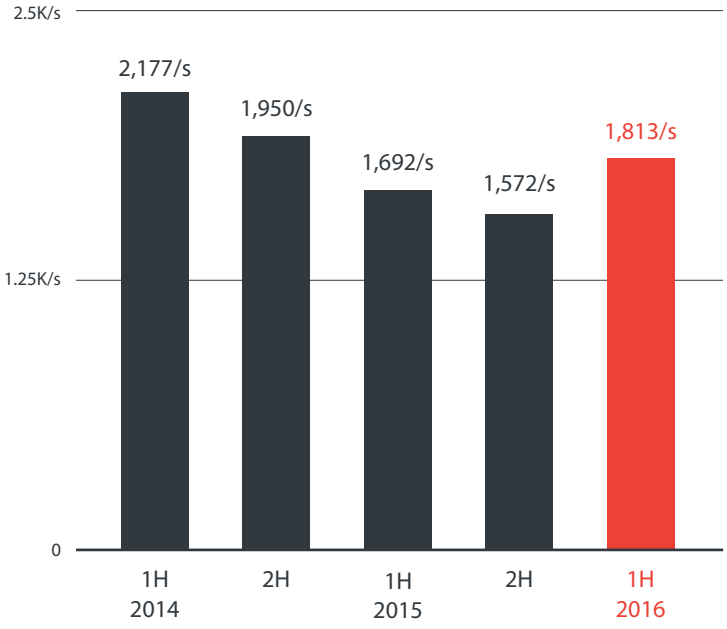

Figure 11. Number of of hits to threats blocked per second, 1H 2016

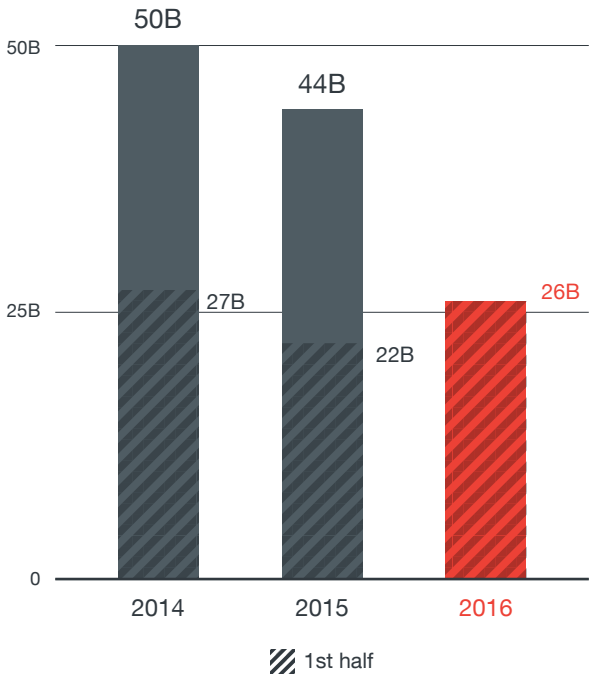

Figure 12. Number of email threats blocked, 1H 2016

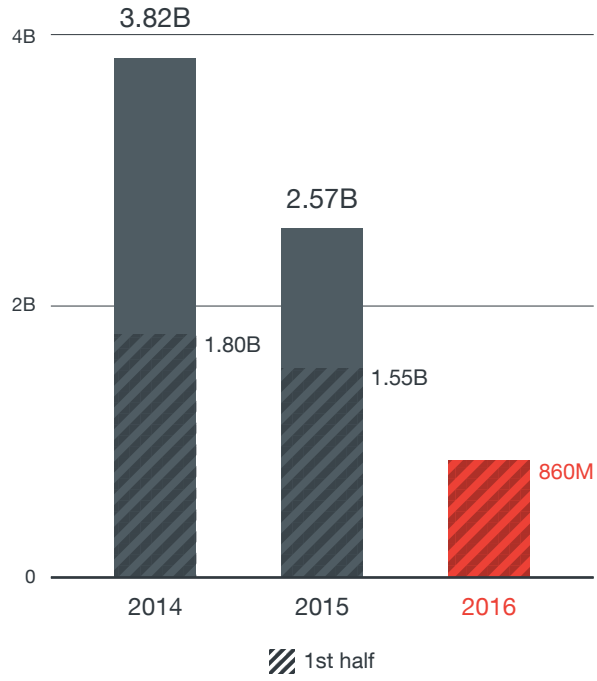

Figure 13. Number of malicious URLs blocked, 1H 2016

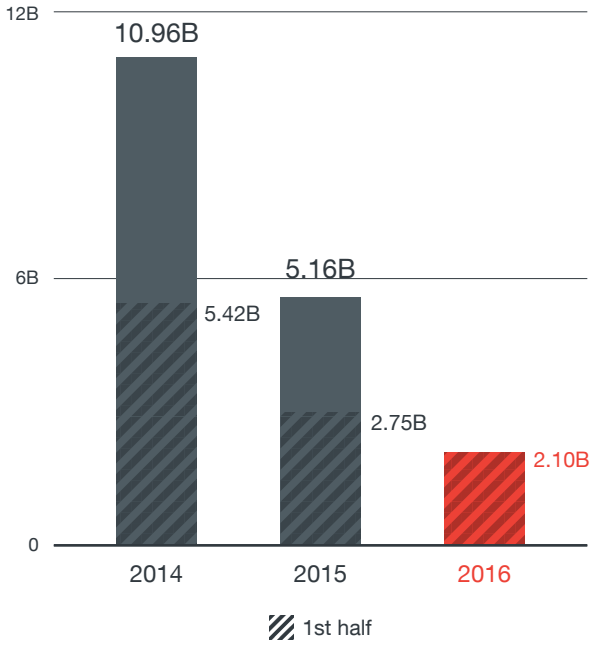

Figure 14. Number of malicious files blocked

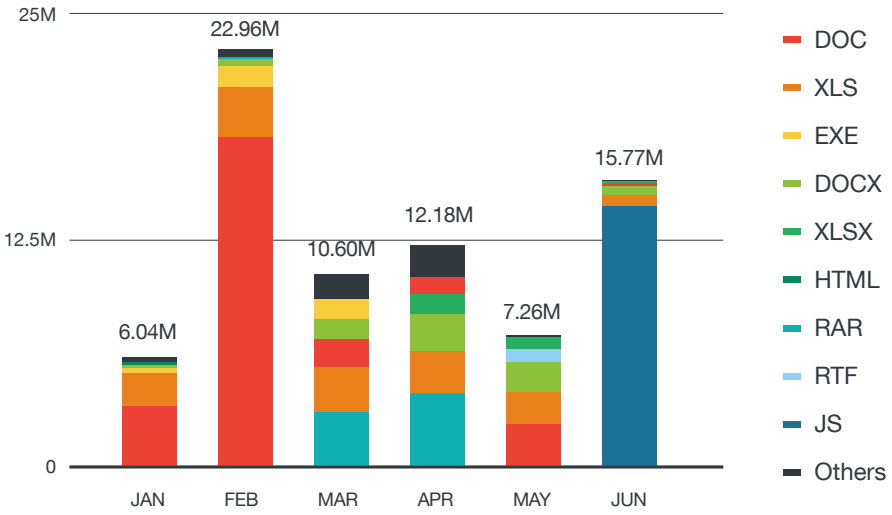

Figure 15. Top file attachments seen in ransomware-related spam email according to file type, 1H 2016

In June, there was a notable increase in JavaScript attachments in spam. This is primarily delivered by ransomware-related spam.

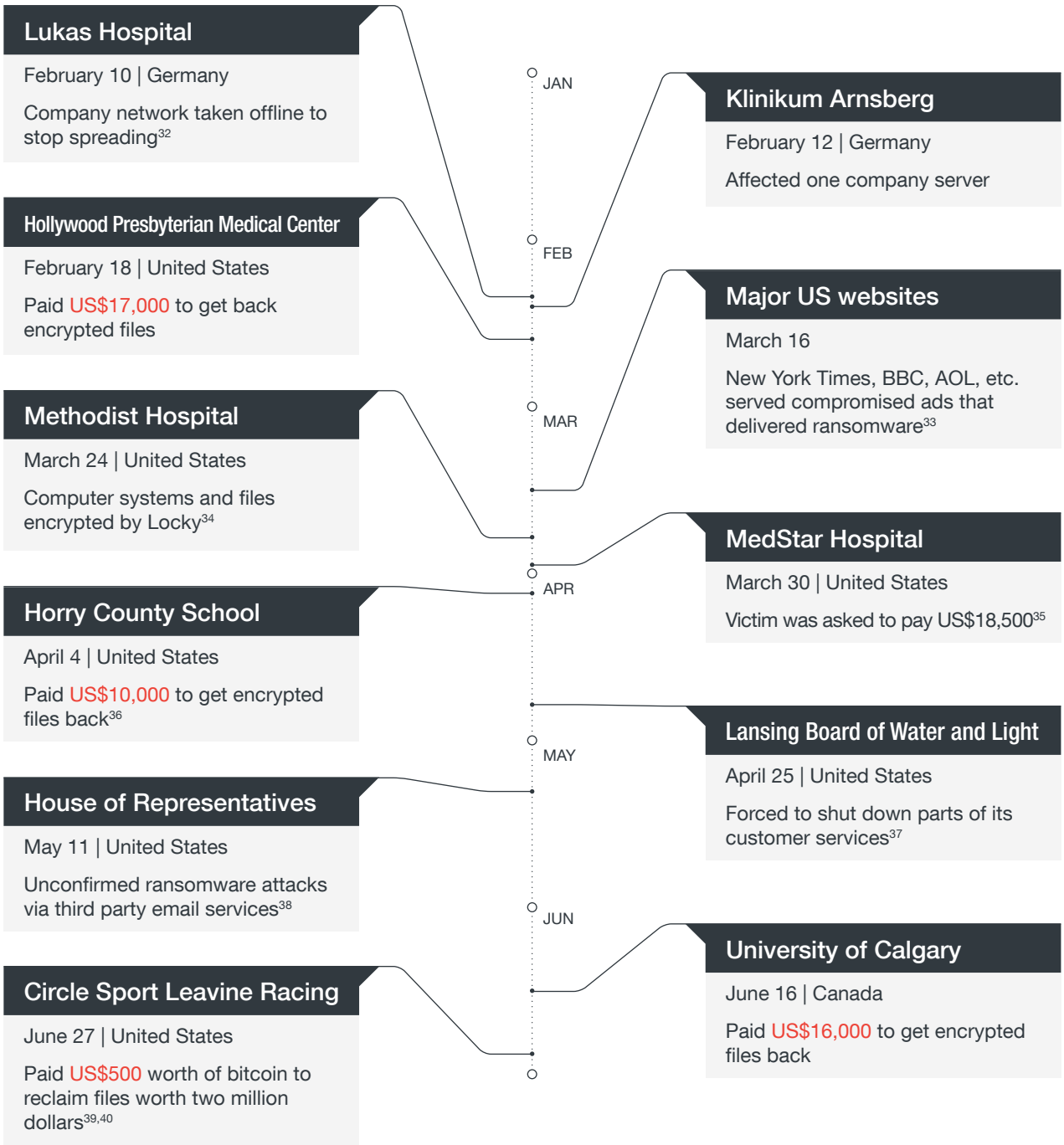

Figure 16. Ransomware incidents made public, 1H 2016

					TOTAL
JAN	LECTOOL	CRYPRADAM	CRYPNISCA	CRYPRITU	7
	EMPER	MEMEKAP	CRYPJOKER		
FEB	CRYPGPCODE	CRYPDAP	MADLOCKER		6
	CRYPHYDRA	CRYPZUQUIT	LOCKY		
MAR	CERBER	MAKTUB	CRYPTOSO	KIMCIL	14
	CRYPAURA	SURPRISE	COVERTON	CRYPTEAR	
	KERANGER	PETYA	CRYPSAM		
	CRYPTESLA	POWERWARE	CRYPTOHASU		
APR	CRYPSALAM	JIGSAW	EMPER 2.0	CRYPLIKI	11
	CRYPTOHOST	WALTRIX	CRYPVAULT	CRYPALPHA	
	XORBAT	ZIPPY	CRYPCORE		
MAY	ROKKU	MISCHA	TAKALOCKER	DEMOCRY	19
	BRLOCK	WALTRIX 2.0	BADBLOCK	BUCBI	
	CRYPMAME	ENIGMA	ZCRYPT	CRYPDAP	
	SHUJIN	SNSLOCK	ELFACRYPT	CRIPTODC	
	AUTOLOCKY	BLOCCATO	LOCKSCAM		
JUN	JIGSAW 2.0	GOOPIC	CRYPSHOCKER	BART	22
	WALTRIX 3.0	APOCALYPSE	WHITELOCK	CRYPMIC	
	CRYPHERBST	JSRAA	LOCKRVTN	SATANA	
	CRYPEDA	CRYPCUTE	JOKOZY	ZIRBAM	
	CRYPAGA	CYPHERKEY	MIRCOP		
	WALTRIX 4.0	CRYPKEYIV	XORIST		

Table 3. New ransomware families seen, 1H 2016

References

1. Trend Micro. (27 October 2015). *Trend Micro Security Intelligence.* "2016 Trend Micro Security Predictions: The Fine Line." Last accessed on 5 August 2016, http://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2016

2. Trend Micro. (15 February 2016). *Trend Micro Security News.* "Ransomware Attack Holds Hollywood Hospital Records Hostage." Last accessed on 5 August 2016, http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/ransomware-attack-holds-hollywood-hospital-records-hostage-for-3-6m

3. Joseph C. Chen. (22 June 2016). *TrendLabs Security Intelligence Blog.* "After Angler: Shift in Exploit Kit Landscape and New Crypto-Ransomware Activity." Last accessed on 5 August 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/angler-shift-ek-landscape-new-crytpo-ransomware-activity/

4. Allan Stefanek. (17 February 2016). *Hollywood Presbyterian.* "Hollywood Presbyterian Medical Center Memo from the CEO". Last accessed on 9 August 2016 on http://hollywoodpresbyterian.com/default/assets/File/20160217%20Memo%20from%20the%20CEO%20v2.pdf

5. University of Calgary. (8 June 2016). *UToday.* "University of Calgary makes significant progress to address system issues." Last accessed on 5 August 2016, http://www.ucalgary.ca/utoday/issue/2016-06-08/university-calgary-makes-significant-progress-address-systems-issues

6. Ryan Webb. (7 March 2016). *WBTW News13*. "Horry County pays nearly $10k to 'ransomware' hackers." Last accessed on 5 August 2016, http://wbtw.com/2016/03/07/horry-county-pays-nearly-10k-to-ransomware-hackers/

7. Jasen Sumalapao. (19 April 2016). *TrendLabs Security Intelligence Blog.* "New Crypto-Ransomware JIGSAW Plays Nasty Games." Last accessed on 5 August 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/jigsaw-ransomware-plays-games-victims/

8. Trend Micro. (5 August 2016). *Trend Micro Threat Encyclopedia.* "RANSOM_SURPRISE.A." Last accessed on 5 August 2016, http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/ransom_surprise.a

9. Trend Micro. (22 April 2016). *TrendLabs Security Intelligence Blog.* "A Lesson on Patching: The Rise of SAMSAM Crypto-Ransomware." Last accessed on 5 August 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/lesson-patching-rise-samsam-crypto-ransomware/

10. Jasen Sumalapao. (31 May 2016). *TrendLabs Security Intelligence Blog.* "ZCRYPT Crypto-ransomware Attacks Windows 7 and Later, Scraps Backward Compatibility." Last accessed on 5 August 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/crypto-ransomware-attacks-windows-7-later-scraps-backward-compatibility/

11. Trend Micro. (31 May 2016). *TrendLabs Security Intelligence Blog.* "Tax Day Extortion: PowerWare Crypto-ransomware Targets Tax Files." Last accessed on 5 August 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/tax-day-extortion-powerware-crypto-ransomware-targets-tax-files/

12. Federal Bureau of Investigation. (14 June 2016). *Internet Crime Complaint Center.* "Business E-mail Compromise: The 3.1 Billion Dollar Scam." Last accessed on 5 August 2016, https://www.ic3.gov/media/2016/160614.aspx

13. Trend Micro. (9 June 2016). *Trend Micro Security News.* "Billion-Dollar Scams: The Numbers Behind Business Email Compromise." Last accessed on 5 August 2016, http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/billion-dollar-scams-the-numbers-behind-business-email-compromise

14. Ryan Flores. (11 November 2014). *TrendLabs Security Intelligence Blog.* "Predator Pain and Limitless: Behind the Fraud." Last accessed on 5 August 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/predator-pain-and-limitless-behind-the-fraud/

15. Jon Oliver and Joseph C. Chen. (27 June 2016). *TrendLabs Security Intelligence Blog.* "Why Ransomware Works: Arrival Tactics" Lasr accessed on 11 August 2016 http://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-arrival-methods/

16. Peter Pi, Brooks Li, and Joseph Chen. (7 April 2016). *TrendLabs Security Intelligence Blog.* "Zero-Day Attack Discovered in Magnitude Exploit Kit Targeting CVE-2016-1019 in Older Versions of Adobe Flash Player." Last accessed on 5 August 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/cve-2016-1019-zero-day-integrated-in-exploit-kit/

17. Peter Pi. (2 February 2015). *TrendLabs Security Intelligence Blog.* "Trend Micro Discovers New Adobe Flash Zero-Day Exploit Used in Malvertisements." Last accessed on 5 August 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-discovers-new-adobe-flash-zero-day-exploit-used-in-malvertisements/

18. Peter Pi. (11 July 2016). *TrendLabs Security Intelligence Blog.* "New Zero-Day Vulnerability (CVE-2015-5123) in Adobe Flash Emerges from Hacking Team Leak." Last accessed on 5 August 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/new-zero-day-vulnerability-cve-2015-5123-in-adobe-flash-emerges-from-hacking-team-leak/

19. Trend Micro. (13 October 2015). *TrendLabs Security Intelligence Blog.* "New Adobe Flash-Zero-Day Used in Pawn Storm Campaign Targeting Foreign Affairs Ministries." Last accessed on 5 August 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-flash-zero-day-used-in-pawn-storm-campaign/

20. Advantech. (2016). *Advantech.* "Fast Facts." Last accessed on 5 August 2016, http://www.advantech.com/about/fastfacts

21. Steve Povolny. (21 March 2016). Trend Micro Simply Security. "Pwn2Own 2016 – Trend Micro TippingPoint DVLabs Exclusive Zero Day Coverage!" Last accessed on 5 August 2016, http://blog.trendmicro.com/pwn2own-2016-trend-micro-tippingpoint-dvlabs-exclusive-zero-day-coverage/

22. US-CERT. (14 April 2016). *United States Computer Emergency Readiness Team.* "Apple Ends Support for QuickTime for Windows; New Vulnerabilities Announced." Last accessed on 5 August 2016, https://www.us-cert.gov/ncas/alerts/TA16-105A

23. Elizabeth Weise. (31 May 2016). *USA Today.* "360 million Myspace accounts breached ." Last accessed on 5 August 2016, http://www.usatoday.com/story/tech/2016/05/31/360-million-myspace-accounts-breached/85183200/

24. Jon Brodkin. (25 March 2016). *arsTechnica.* "After Verizon breach, 1.5 million customer records put up for sale." Last accessed on 5 August 2016, http://arstechnica.com/security/2016/03/after-verizon-breach-1-5-million-customer-records-put-up-for-sale/

25. Frank Gluck (10 March 2016). *News-Press.* "Data Breach Affects 2.2M 21st Century Oncology Patients." Last accessed on 9 August 2016, http://www.news-press.com/story/news/2016/03/09/data-breach-affects-22m-21st-century-onoclogy-patients/81525656/

26. IRS. (9 February 2016). *Internal Revenue Service.* "IRS Statement on E-filing PIN." Last accesed on 5 August 2016, https://www.irs.gov/uac/Newsroom/IRS-Statement-on-Efiling-PIN

27. Trend Micro. (22 September 2015). *Trend Micro Security News.* "Follow the Data: Dissecting Data Breaches and Debunking the Myths." Last accessed on 5 August 2016, http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/follow-the-data

28. Trend Micro. (2 June 2016). *TrendLabs Security Intelligence Blog.* "FastPOS: Quick and Easy Credit Card Theft." Last accessed on 5 August 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/fastpos-quick-and-easy-credit-card-theft/

29. Erika Mendoza and Jay Yaneza. (25 February 2016). *TrendLabs Security Intelligence Blog.* "FighterPOS PoS Malware Gets Worm Routine." Last accessed on 5 August 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/fighterpos-gets-worm-routine/

30. Trend Micro. (29 September 2014). *TrendLabs Security Intelligence Blog.* "Summary of Shellshock-Related Stories and Materials." Last accessed on 5 August 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/summary-of-shellshock-related-stories-and-materials/

31. Cklaudioney Mesa. (18 February 2016). *TrendLabs Security Intelligence Blog.* "QAKBOT Resurges: Despite Takedowns, Online Banking Threats Persist." Last accessed on 5 August 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/despite-arrests-and-takedowns-online-banking-threats-persist/

32. Deutsche Welle. (10 February 2016). *DW.com.* "Hackers hold German hospital data hostage." Last accessed on 5 August 2016, http://www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030?maca=en-rss-en-all-1573-rdf

33. Alex Hern. (16 March 2016). *The Guardian.* "Major sites including New York Times and BBC hit by 'ransomware' malvertising." Last accessed on 5 August 2016, https://www.theguardian.com/technology/2016/mar/16/major-sites-new-york-times-bbc-ransomware-malvertising

34. Trend Micro. (24 March 2016). *Trend Micro Security News.* "Locky Ransomware Strain Led Kentucky Hospital to an "Internal State of Emergency"." Last accessed on 5 August 2016, http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/locky-ransomware-strain-led-kentucky-hospital-to-an-internal-state-of-emergency

35. Sean Gallagher. (1 April 2016). *Ars Technica.* "Maryland hospital group hit by ransomware launched from within." Last accessed on 5 August 2016, http://arstechnica.com/security/2016/03/maryland-hospital-group-hit-by-ransomware/

36. David Fitzpatrick and Drew Griffin. (4 April 2016). *CNN Money.* "'Ransomware' crime wave growing." Last accessed on 5 August 2016, http://money.cnn.com/2016/04/04/technology/ransomware-cybercrime/

37. Kevin Townsend. (3 May 2016). *SecurityWeek.* "Michigan Power and Water Utility Hit by Ransomware Attack." Last accessed on 5 August 2016, http://www.securityweek.com/michigan-power-and-water-utility-hit-ransomware-attack

38. Darlene Townsend. (11 May 2016). *Computerworld.* "Ransomware attacks on House of Representatives gets Yahoo Mail blocked." Last accessed on 5 August 2016, http://www.computerworld.com/article/3068623/security/ransomware-attacks-on-house-of-representatives-gets-yahoo-mail-blocked.html

39. Ericka Chickowski. (24 June 2016). *DarkReading.* "NASCAR Race Team Learns Ransomware Lesson The Hard Way." Last accessed on 5 August 2016, http://www.darkreading.com/attacks-breaches/nascar-race-team-learns-ransomware-lesson-the-hard-way/d/d-id/1326047

40. Phil Muncaster. (27 June 2016). *Infosecurity.* "Nascar Team Crippled by Ransomware Attack." Last accessed on 5 August 2016, http://www.infosecurity-magazine.com/news/nascar-team-crippled-by-ransomware/

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**

TREND MICRO™

Securing Your Journey to the Cloud