



2017 Midyear Security Roundup: The Cost of Compromise

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.

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.

Contents

4

Ransomware Reaches Peak With WannaCry and Petya

7

Enterprises Still Trip Over Old Vulnerabilities

9

Connected Devices Put Smart Factories at Risk

11

Business Email Compromise Losses Reach \$5 Billion Mark

14

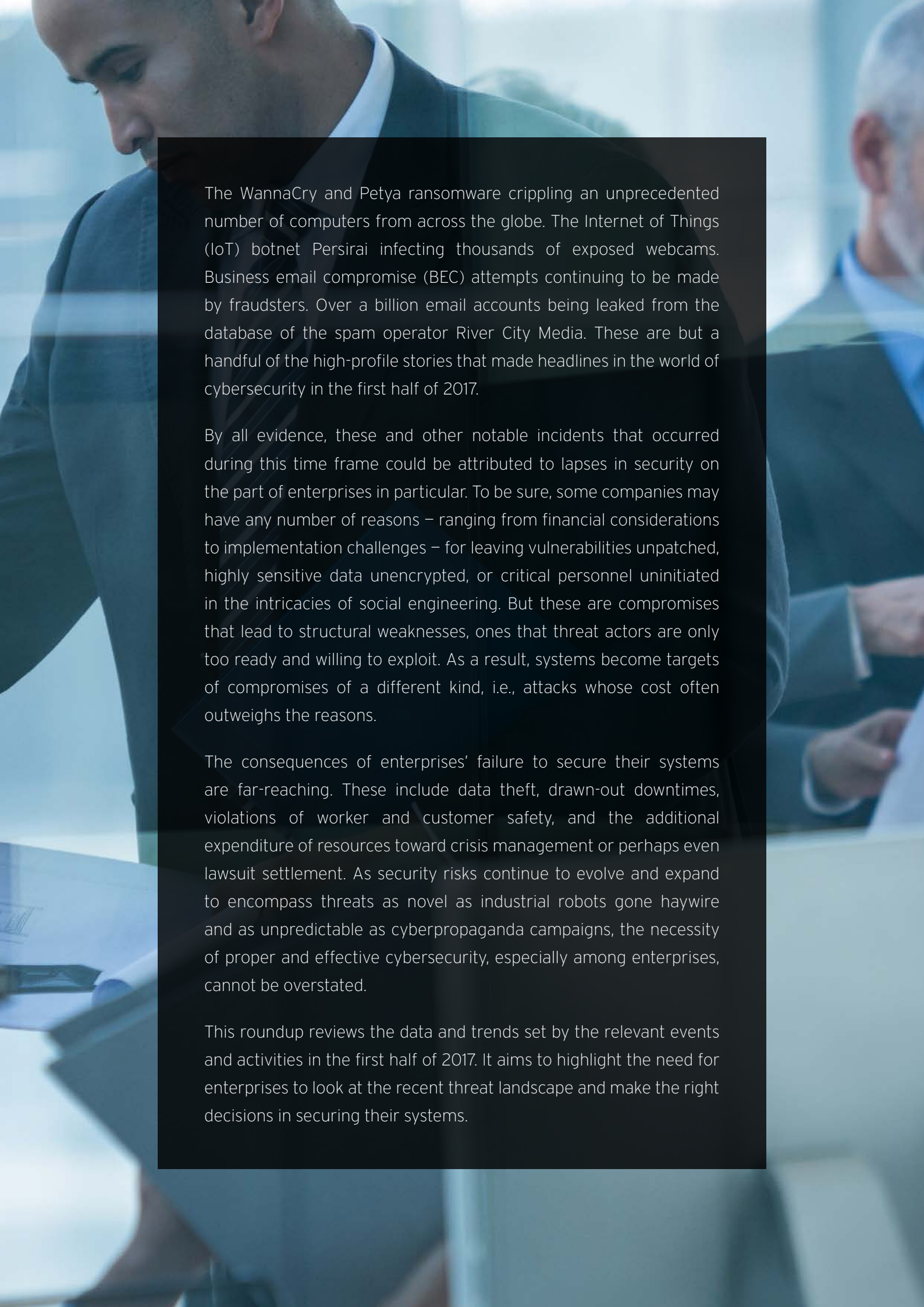
Cyberpropaganda Threatens Targeted Enterprises

16

Hacking Now Leading Cause of Data Breach

17

Threat Landscape in Review



The WannaCry and Petya ransomware crippling an unprecedented number of computers from across the globe. The Internet of Things (IoT) botnet Persirai infecting thousands of exposed webcams. Business email compromise (BEC) attempts continuing to be made by fraudsters. Over a billion email accounts being leaked from the database of the spam operator River City Media. These are but a handful of the high-profile stories that made headlines in the world of cybersecurity in the first half of 2017.

By all evidence, these and other notable incidents that occurred during this time frame could be attributed to lapses in security on the part of enterprises in particular. To be sure, some companies may have any number of reasons – ranging from financial considerations to implementation challenges – for leaving vulnerabilities unpatched, highly sensitive data unencrypted, or critical personnel uninitiated in the intricacies of social engineering. But these are compromises that lead to structural weaknesses, ones that threat actors are only too ready and willing to exploit. As a result, systems become targets of compromises of a different kind, i.e., attacks whose cost often outweighs the reasons.

The consequences of enterprises' failure to secure their systems are far-reaching. These include data theft, drawn-out downtimes, violations of worker and customer safety, and the additional expenditure of resources toward crisis management or perhaps even lawsuit settlement. As security risks continue to evolve and expand to encompass threats as novel as industrial robots gone haywire and as unpredictable as cyberpropaganda campaigns, the necessity of proper and effective cybersecurity, especially among enterprises, cannot be overstated.

This roundup reviews the data and trends set by the relevant events and activities in the first half of 2017. It aims to highlight the need for enterprises to look at the recent threat landscape and make the right decisions in securing their systems.

Ransomware Reaches Peak With WannaCry and Petya

“The year of online extortion” was how 2016 came to be known at Trend Micro.¹ Last year, not only was there a remarkable increase in the number of ransomware attacks, but there was also a staggering spike in the multiplicity of ransomware families. If nothing else, this should have been a clarion call to all concerned to put up fortifications against the evolving threat of ransomware. However, based on incidents in the first half of 2017 alone, it would seem that some individuals, enterprises, and even industries still failed to secure their systems to combat the threat and protect their data from being held hostage by cybercriminals. And nowhere was this shortcoming more apparent than in the successive successes of WannaCry and Petya.

Within just days since the initial outbreak in mid-May, WannaCry infected an unprecedented 300,000 computers in 150 countries.² In much of Europe, it forced car manufacturing plants to stop production and healthcare facilities to cancel thousands of medical appointments and procedures.³ In China, it affected around 30,000 institutions, including universities, petroleum stations, hospitals, and government agencies.⁴ It reportedly hit Russia the hardest, crippling government offices, railways, banks, and even one of the largest mobile phone operators in the country.⁵ The global losses from the attack, including the resultant reduction in productivity and cost of damage control, could amount to as much as US\$4 billion.⁶



Figure 1. WannaCry ransom note

The attack was carried out using a variant of the WannaCry ransomware that we first detected in April as RANSOM_WCRY.C.⁷ The new variant, which we detected as RANSOM_WANA.A and RANSOM_WCRY.I, propagates by using EternalBlue to exploit a vulnerability in Windows' Server Message Block (SMB) protocol.⁸ It affects older Windows®-based systems, specifically those with operating systems that Microsoft no longer supports. Unpatched systems are vulnerable to it as well. What makes it particularly insidious, though, is its worm component, which infects machines with an open port 445 and enables it to spread without user interaction across local area networks and even the internet.⁹

Just over a month after the WannaCry incident came another large-scale ransomware attack in the form of a variant of the Petya ransomware, which first emerged in 2016.¹⁰ Its outbreak, in late June, affected a number of government departments, utility providers, and businesses particularly in Ukraine and other parts of Europe.¹¹ It also led to major infections in Australia, Russia, and the United States.¹² The virulence of this variant, which we detected as RANSOM_PETYA.SMA, can be attributed to its use not only of the EternalBlue exploit used by WannaCry but also of the PsExec tool and Windows Management Instrumentation Command-line as infection vectors.¹³ Moreover, should EternalBlue fail, it attempts to propagate using another exploit, called EternalRomance.¹⁴

Improving on the original version's capability of encrypting the Master Boot Record, this Petya variant also encrypts the Master File Table and deletes the key.¹⁵ This makes the ransomware a wiper as well: It can overwrite and ultimately wipe the affected system's hard disk.¹⁶ Because of this update, it might be possible for attackers to infiltrate a target, exfiltrate massive amounts of data, encrypt the original data, and hold the stolen data for a bigger ransom.

Outside the widely publicized WannaCry and Petya attacks, there were other noteworthy pieces of ransomware that appeared in the first half of 2017. The Cerber ransomware, which we detected as RANSOM_CERBER family, evolved to evade detection by machine learning solutions¹⁷ and to sport defense mechanisms that include anti-sandbox and anti-antivirus techniques.¹⁸ The discovery of the MacOS® ransomware Patcher, which we detected as OSX_CRYPPATCHER.A, threw into sharp relief the rise of ransomware targeting non-Windows systems.¹⁹ There was also a new variant of the mobile ransomware SLocker, which we detected as ANDROIDOS_SLOCKER.OPST, that featured file encryption capability (rather than being a mere screen locker like most Android™ ransomware) and copied the graphical user interface (GUI) of WannaCry.²⁰

For all the wide-ranging publicity about these incidents involving ransomware, however, it is interesting to note that growth in the number of new ransomware families has plateaued in the first half of 2017, with 83 million total ransomware threats detected, and an average of 28 new families detected. This is consistent with our 2017 security forecast.²¹ Nevertheless, this period of relative stabilization sees cybercriminals focusing on diversifying in terms of potential victims, platforms, and bigger targets, which we also predicted. New ransomware tactics, techniques, and procedures (TTPs) have emerged, such as Erebus ransomware (detected by Trend Micro as RANSOM_ELFEREBUS.A), which targets Linux systems²²; UIWIX ransomware

(detected by Trend Micro as RANSOM_UIWIX.A), which uses the same SMB vulnerabilities as WannaCry but appears to be fileless²³; and KIRK ransomware (detected by Trend Micro as RANSOM_KIRK.A), which is possibly the first to demand payment in the cryptocurrency Monero (XMR)²⁴.

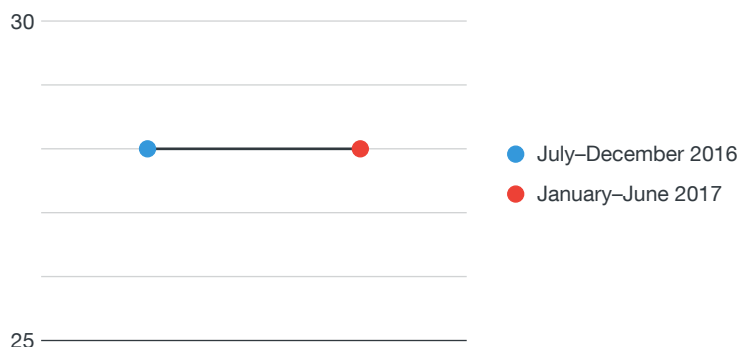


Figure 2. Comparison of average number of new ransomware families detected from July to December 2016 and from January to June 2017

Even though ransomware growth has leveled off, enterprises in particular should not be complacent when it comes to safeguarding their systems. To prevent and mitigate the effects of ransomware, systems must be protected by a multilayered defense strategy that preferably includes such capabilities as virtual patching and high-fidelity machine learning.

Poor security can lead to ransomware infections that can easily spread through a network. By not securing all infection vectors, enterprises risk losing data, experiencing downtime, and spending thousands of dollars paying for ransom that might not result in data recovery after all.

Enterprises Still Trip Over Old Vulnerabilities

With the help of over 3,000 independent researchers who contribute to the Zero Day Initiative (ZDI) program, we discovered and disclosed 382 new vulnerabilities in the first half of 2017.²⁵ Notably, there were drops in the vulnerability counts for the products of three of the largest software vendors in the world: Apple, Google, and Microsoft. However, the number of zero-day vulnerabilities increased from eight in the second half of 2016 to 49 in the first half of 2017. The supervisory control and data acquisition (SCADA) software vulnerability count also went up from 34 in the second half of 2016 to 54 in the second half of 2017.

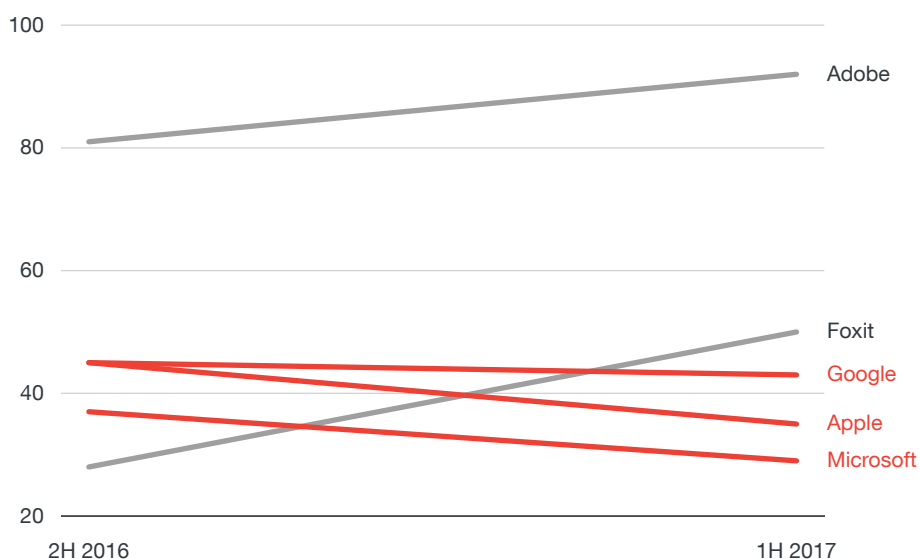


Figure 3. Comparison of vulnerabilities found in the second half of 2016 and the first half of 2017

We were also made aware of a number of vulnerabilities in some of our products through ZDI, and we have since worked to address them. This patching is in line with our commitment to the continuous improvement of our products and resolution of issues in a timely manner.

Perhaps no vulnerability gained more notoriety in the first half of 2017 than CVE-2017-0144. The two biggest cybersecurity stories of the period could be traced to this Microsoft vulnerability, which had been taken advantage of by the EternalBlue exploit. In May, a cyberattack that used EternalBlue — the WannaCry ransomware — caused significant disruptions around the world. This was followed in June by another

massive ransomware infection that used the same exploit — Petya. What is perhaps most lamentable about this double whammy is that, even though the EternalBlue exploit was introduced in April,²⁶ Microsoft had already patched the critical vulnerability with a security update released in March.²⁷

To be fair, it can be difficult especially for enterprises to defend their systems from exploited vulnerabilities since patch management is no easy task. There is a great deal of logistics to be considered, not least of which is the manpower necessary to update thousands of units. Patching also often disrupts operations. Furthermore, some cannot do away with legacy systems that are still in use even as they no longer receive patches.

Nevertheless, securing systems from vulnerabilities is necessary. Solutions that provide vulnerability protection in the form of virtual patching can prevent the abuse of unpatched vulnerabilities and secure legacy systems. This effectively keeps networks protected until patches are deployed or even after support for systems has ended.

Cybercriminals take advantage of unpatched and otherwise vulnerable systems to drop their payloads. Leaving systems unprotected can result in network intrusions, opening the door to further attacks like data breaches and ransomware infections.

Connected Devices Put Smart Factories at Risk

In our security forecast for 2017,²⁸ we mentioned that cybercriminals would perform distributed denial-of-service (DDoS) attacks using malware similar to that used in the infamous Mirai botnet that caused some of the most notable incidents of 2016.²⁹ By April, we had discovered a piece of malware that matched our prediction: an IoT botnet that had been targeting more than 1,000 Internet Protocol (IP) camera models based on various original equipment manufacturer products. This was Persirai, which we detected as ELF_PERSIRAI.A.³⁰ According to the Shodan data that we gathered in late April, as many as 120,000 IP cameras had been vulnerable to the malware.

But exposed cameras are only a fraction of the problem of connected devices bringing about security risks. When exposed, other machines of larger sizes and broader applications could also be exploited and could be cause for serious concern for enterprises.

In our research paper “Rogue Robots: Testing the Limits of an Industrial Robot’s Security,”³¹ produced in collaboration with Politecnico di Milano (POLIMI), we have proven that it is possible for industrial robots to be compromised. During our research, we saw over 83,000 exposed industrial routers and 28 exposed industrial robots through search engines such as Shodan, ZoomEye, and Censys. These routers allow users to connect to the robots remotely as if they were on a local network.

With our partners from POLIMI, we were able to demonstrate attack scenarios involving industrial robots in smart factories.³² Several of the attack types entail changes to the operation of the robot that cause it to move unexpectedly or inaccurately, or otherwise introduce defects in its workpiece. These attacks can lead to unusable or unsafe products, which in turn can result in the factories having to recall their products and pay for damages. Another attack type manipulates the status information of the robot, while another tampers with the true robot status of the affected machine. Both of these attacks can lead to serious injuries to the robot operator.

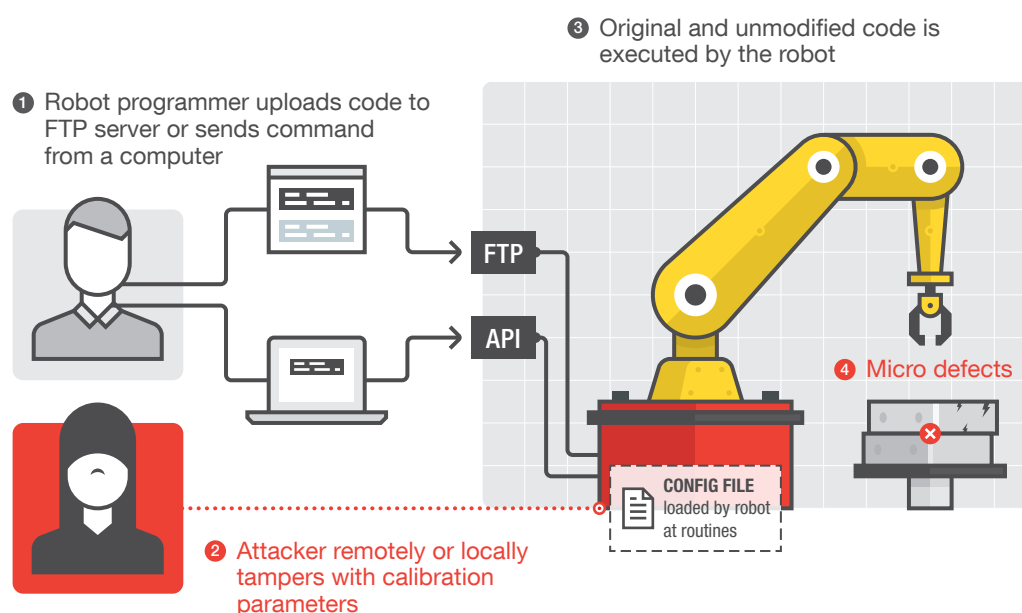


Figure 4. Attacker tampers with the calibration parameters to alter the execution of a program or command issued by the programmer

According to a forecast made by the International Federation of Robotics, there will be approximately 1.3 million industrial robots employed in factories all over the world by 2018.³³ With billions of dollars on the production line, smart factories should prioritize securing all connected devices so as to protect their current and future industrial robots from attacks. Since industrial robots are expected to perform with a high level of precision, enterprises cannot afford to give attackers the chance to take over.

Hacked industrial robots have diverse effects, from productivity loss and defective products to unsafe workplaces and the replacement of multimillion-dollar machines. In order to keep industrial robots secure, operators, robot vendors, software developers, network defenders, and cybersecurity standards makers should make attacks on industrial robots expensive to the point of being impractical. Physical safety protocols and solutions to mitigate vulnerabilities must also be in place. For their part, program designers must enforce stringent software engineering practices to improve code robustness, harden underlying platforms, and implement strong authentication measures.

Connected devices such as IP cameras and industrial routers can be major risks if they can be exploited. Depending on the exposed machine and the attacker's expertise, damages may vary between thousands of devices used for botnet attacks and hacked industrial robots that can jeopardize accuracy, integrity, and safety.

Business Email Compromise Losses Reach \$5 Billion Mark

The first half of 2017 showed that business email compromise (BEC) is still one of the top threats that enterprises should look out for. According to a document published by the Federal Bureau of Investigation in May, global losses attributed to BEC scams since 2013 have reached US\$5.3 billion.³⁴

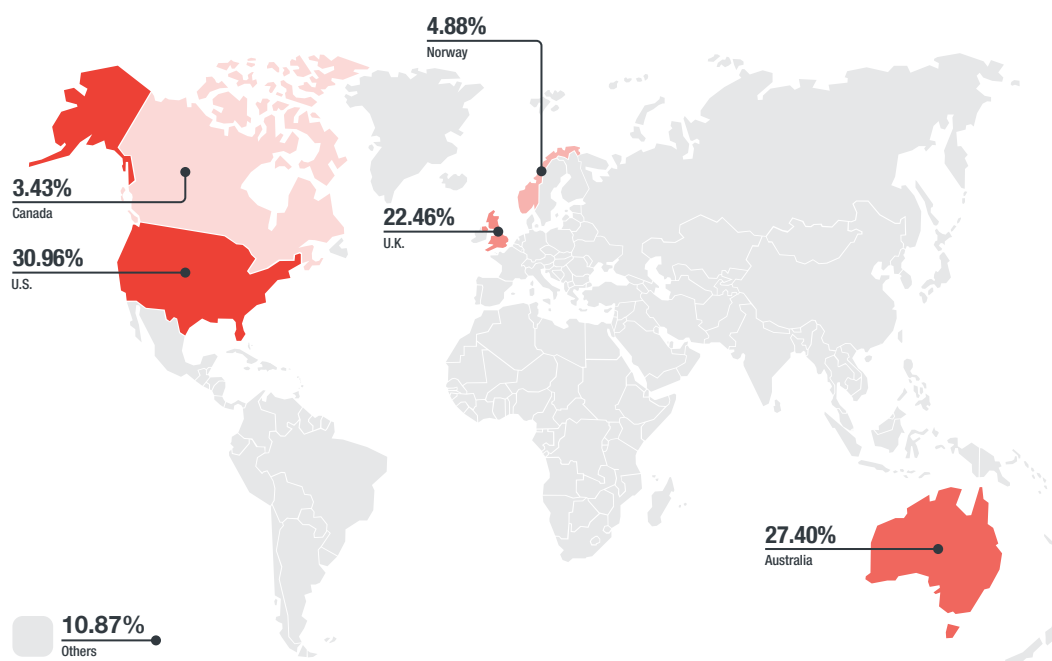


Figure 5. Countries with the most BEC attempts, 1H 2017³⁵

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

Based on random sampling of BEC email attacks, we have observed that the most spoofed position in BEC is the CEO, followed by the managing director, and the most targeted positions are the CFO and the finance director.

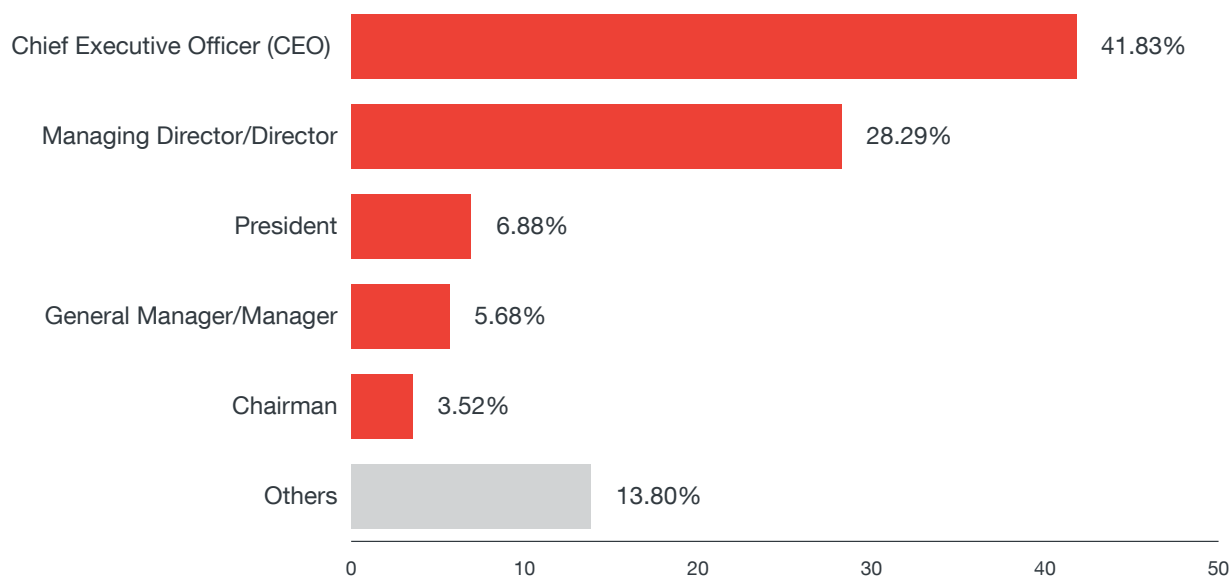


Figure 6. Percentage of BEC attack attempts that spoof specific positions, 1H 2017

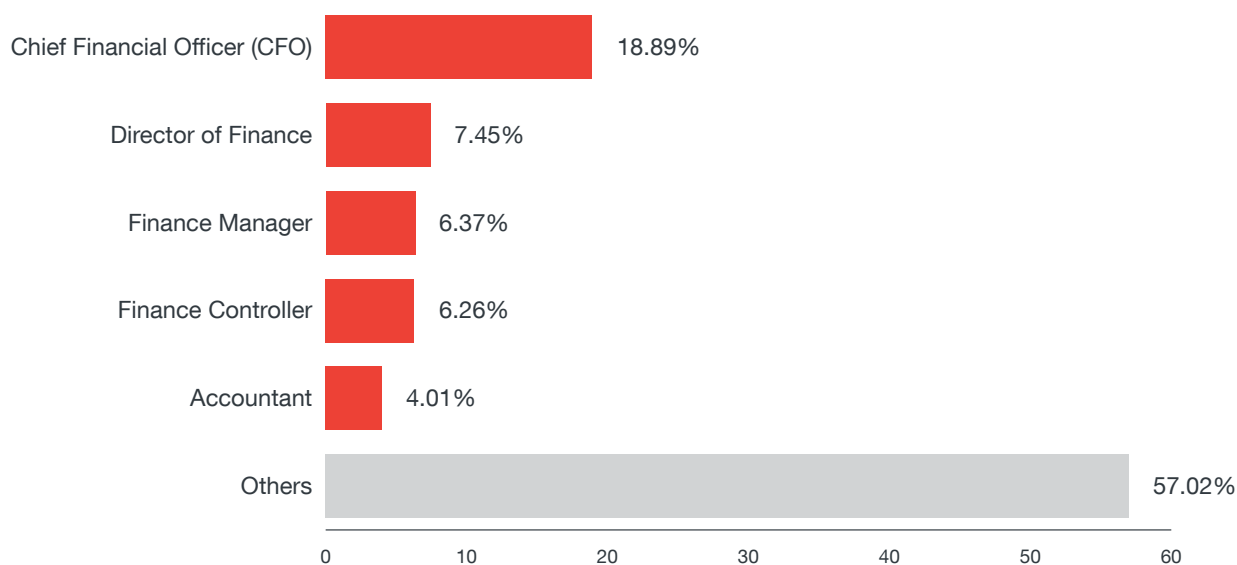


Figure 7. Percentage of BEC attack attempts that target specific positions, 1H 2017

Based on the samples we have acquired, words and phrases commonly associated with BEC-related emails include “Acquisition,” “Contract,” “Instructions,” “Invoice,” “Request,” and “Swift response needed.”



Figure 8. BEC email with “invoice” in the subject

Amid a heightened focus on CEO scams, there was also a resurgence of old techniques used in BEC. One of these is the supplier swindle scheme, in which cybercriminals spoof a company related to or doing business with their target, rather than a C-level executive from the same organization.³⁶ As for how the con is done, attackers may resort to using malware attached to social engineering emails.

Traditionally, the attachments in BEC scams are executable files. Unfortunately for the fraudsters, these are usually flagged and the recipients are discouraged from clicking them as there is a high chance that the files are malicious. As a result, BEC attacks have manifested a tendency to use HTML pages instead of executable files for their phishing email attachments.³⁷

Because it relies mostly on social engineering, BEC typically does not require sophisticated system penetration. It is imperative, then, for enterprises to employ email solutions that can provide protection against socially engineered messages and gateway solutions that can block emails containing malware such as keyloggers. Perhaps most importantly, enterprises are advised to train personnel from finance and other critical departments in spotting and reporting BEC attempts. High-ranking executives and rank-and-file employees alike, if uninitiated, could be duped into sending funds via wire transfer or revealing information necessary for cybercriminals to pull off their fraudulent schemes.

From small businesses to large corporations, enterprises can become unwitting victims in the multibillion-dollar scam that is BEC.

Cyberpropaganda Threatens Targeted Enterprises

Near the end of 2016, we made the observation that since the internet had become accessible to nearly half of the world's population, it had become easier for people with vested interest to use the internet to influence public opinion. We then predicted that cyberpropaganda would become more commonplace in 2017, what with the increased use, abuse, and misuse of social media.³⁸

The most recent notable cyberpropaganda incident occurred just two days before the May presidential election in France. Hackers leaked a 9GB archive of emails from the political party of the then frontrunner (now French president) Emmanuel Macron, apparently in an attempt to sabotage his campaign. On Twitter, misinformation on the leaks was spread through the #Macronleaks hashtag.³⁹ In response, Macron's party said that the attack was a last-hour effort to destabilize democracy.⁴⁰

While the primarily political nature of cyberpropaganda remains undeniable, we have to bear in mind that cyberpropaganda is no different from most other cybercriminal activities in that it is geared toward getting something in return. This could range from simple monetary gain to the sick satisfaction of inflicting misfortune for no apparent reason. In Macedonia, for example, teenagers continue to spread fake news after raking in thousands of dollars during the U.S. election season by creating and sharing sham stories in favor of the then candidate (now U.S. president) Donald Trump.⁴¹ And in London, a restaurant was hit in May by a fake news article claiming that it sold human meat, resulting in fewer patrons and threats of vandalism.⁴²

As mentioned in our research paper "The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public,"⁴³ Chinese, Russian, Middle Eastern, and English-based underground markets have a range of services that can push propaganda. These include tools for creating content, boosting social media reach, and directly influencing the outcome of online polls through vote buying.

Activity	Price (in USD, after currency conversion)		
	Chinese	Russian	Middle East
Content distribution	\$74 – 194		\$3 – 250
Content promotion via social media through various means	\$0.18 – 184,723	\$2 – 7,518	\$3 – 999
Online polls vote manipulation	\$30 – 52	\$1,002 – 2,506	
Content marketing	\$15 – 30		
Public opinion monitoring and influencing	\$1,905 – 4,286		
Content takedown	\$372 – 893		
Hiring a click farm	\$5,035 – 14,847		

Note: Currency conversion is based on the exchange rates on Aug. 1, 2017.⁴⁴

Table 1. Fake news-related activities and tools sold in underground markets

Given the tools available in underground markets, a barrage of bad publicity can be easily concocted and circulated. Whether or not the accompanying shares or likes are all manufactured, impressions made by real people can damage the reputation of an individual, a group, or a company.

Indeed, even enterprises are not safe from losses due to cyberpropaganda. For instance, a court hearing in May revealed that a teenager hacked the website of *The Sun* and redirected traffic to a fake story reporting that the newspaper owner and media mogul Rupert Murdoch had committed suicide.⁴⁵ As a result, the website of *The Sun* and its sister news sites were shut down for a few hours.

More than crisis management, the protection of valuable data and inspection of all points that could be compromised should be adopted as standard practices by enterprises in combating cyberpropaganda. If attackers are able to infiltrate the systems of a targeted enterprise, they could find files that they could use to launch a campaign to sway public opinion about the enterprise one way or the other.

Hacking Now Leading Cause of Data Breach

In 2015, we published a research paper, titled “Follow the Data: Dissecting Data Breaches and Debunking Myths,”⁴⁶ where we stated that the likeliest breach method was through device loss or theft. However, in the first half of 2017, the top cause of data breaches was hacking or malware. Of the 278 incidents reported in the U.S. during this period, hacking or malware accounted for 153.⁴⁷

The rise of hacking or malware as the primary breach method may be attributed to attackers finding more entry points into enterprise networks. In the case of the E-Sports Entertainment Association breach, which was carried out in December but was made public in January, a hacker leaked 1.5 million user records after the company refused to pay the demanded US\$100,000 ransom.⁴⁸

The biggest data breach in the first half of 2017, though, was the one in March that involved the spam operator River City Media. That incident led to the exposure of 1.37 billion email addresses due to an improperly configured backup system.⁴⁹ Parts of River City Media’s own operations were also leaked in the form of business plans, chat logs, accounts, and other data.

While victims of leaked personal information run the risk of bank account identity theft and other fraudulent schemes, targeted enterprises are often faulted further for their inability to protect customer data. Case in point: In May, the retail giant Target finally settled claims from its breach in 2013 for US\$18.5 million. However, that was not all that it had lost: Target said that it had incurred US\$202 million in expenses since the breach.⁵⁰

With the threat of data breaches (whether they are done through hacking or otherwise), enterprises should focus on securing all possible entry points, monitoring network communications, and encrypting high-value data. Since loss and theft are still major causes of data breaches, additional authentication techniques should be implemented to keep sensitive information from prying eyes. Inadequacies in security such as poorly configured networks and outdated systems can be exploited by attackers. If the attack is not detected, let alone thwarted, there will be ransom or damages to pay.

Threat Landscape in Review

In the first half of 2017, over 38 billion threats were blocked by the Trend Micro™ Smart Protection Network™⁵¹. That the vast majority of these were email threats is consistent with the persistence of ransomware and BEC, which primarily use spam as their propagation mechanism.

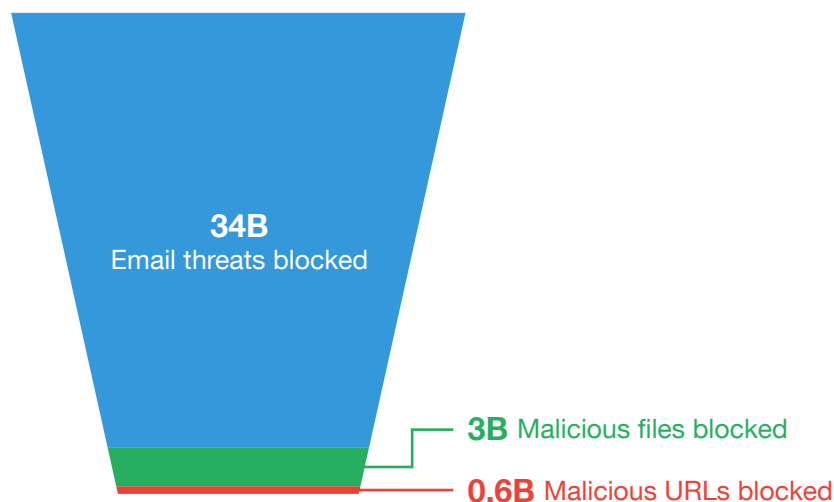


Figure 9. Threats blocked by Trend Micro products, based on Smart Protection Network feedback, 1H 2017

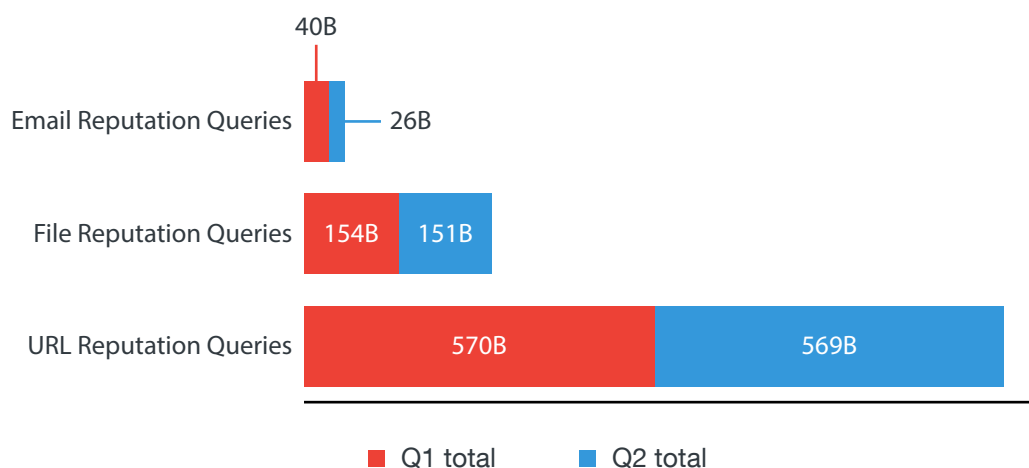


Figure 10. Volume of queries, based on Trend Micro Smart Protection Network feedback, 1H 2017

Most of the spam blocked by Trend Micro products carry file attachments that contain malware. In the first half of 2017, .PDF was the top file type for spam attachments; the ransomware families LOCKY and CRYPTJAFK were delivered as .PDF attachments via spam. .JS attachments were usually detected as CERBER variants.

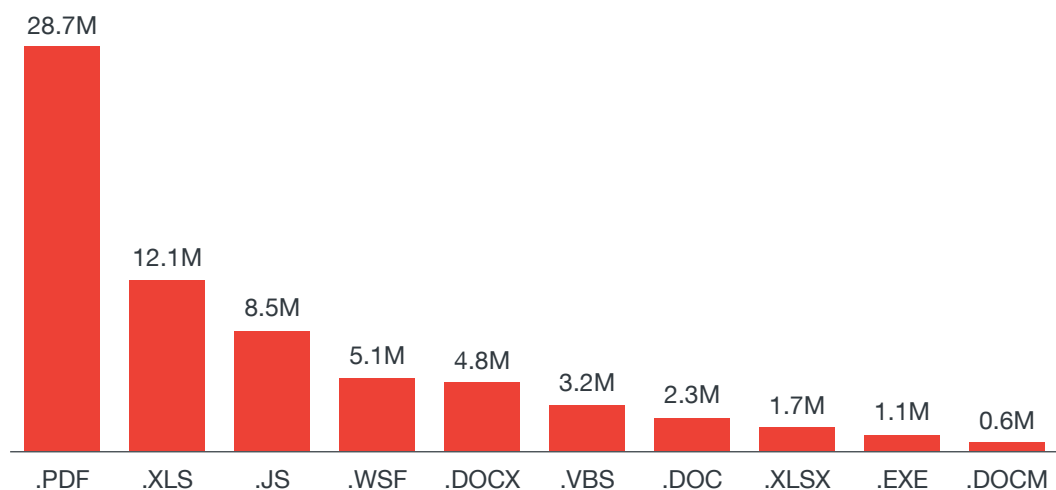


Figure 11. Top 10 file types for spam attachments, 1H 2017

JAN	CRYPFUN	REBOLOCK	VXLOCK	NETIX	13
	YUHAK	CRYPRAAS	HAVOC	MABORO	
	SPORA	EVILWARE	CRYPTOPIC	BLEEDGREEN	
	EXMAS				
FEB	CRYPPTY	CRYPCYR	CZCRYPT	VANGUARD	22
	OSX_CRYPPATCHER	TUSIKSLOCK	PYLEET	KASISKI	
	CRYPNTK	HERMES	ONCRYPT	JOBCRYPTER	
	FAKEGLOBE	WCRY	PABLUKLOCK	SERBRAN	
	SOFAD	CRYPTCONSOLE	URCRYP	EREBUS	
	CUTSOME	JAVAWARE			
MAR	NEDSOM	NARLAN	NXCRYP	CRYPDNC	23
	HAPPYDAYZZZ	BATHIDE	DARKLOCKER	METEORITAN	
	LELELOCK	KRYPTA	CRYPDEVIL	CRPTX	
	STUP	ROZALOCK	GGCRYP	KIRK	
	WEOGO	VORTEX	KAENLUPUF	CRYPJACKY	
	CRYPDANGER	CRYPDAMG	YAFCOOKIE		
APR	DEADSEC	EXTRACTOR	TESTLOCKER	DONTSLIP	24
	ZIPIAC	BTCWARE	CRYPCTF	KAHAS	
	PSHCRYPT	MEDLINZ	LOLI	GOSHIFR	
	CONFICKER	SHWERER	CRADLE	RUSHQL	
	SHIKEY	ALKA	TRESORAS	LAMBDALOCKER	
	GXFORTY	FLUFFY	JANLOCKER	SALSA	

MAY	MAYKOLIN	AMNESIA	CRYPEC	VCRYPT	37
	WANTMYFILES	CLOUDED	BITKANGROO	VIKI	
	CRYPJAFF	ANIMESCREENLOCK	UIWIX	LOCKOUT	
	FAKEWCRY	LOKTROM	DTOD	VISIONCRYPT	
	MEMELOCKER	WIDIALOCKER	EGLUELOCKER	XORDEOS	
	MOWARE	DEADDS	RIMALOCKER	THORNIA	
	MANCROS	ROBLOCKER	LIGHTNING	WIRA	
	QRLOCKER	MISORRY	FAKERA	TESLAWARE	
	GOMME	ZIPRAMEN	BRICKR	XORGOT	
	CUTWISH				
JUN	BLACKMAIL	BLUEHOWL	JOSKY	SNEKUD	49
	TUBELAW	DARKENCRYPTOR	DELS CARE	OGRE	
	ZILLA	MALHUNT	DESUI	DYNACRYPT	
	SAWORSED	MRLOCKER	BEETHOV	XXLECXX	
	SPECTRE	GPAA	CASHOUT	PROTONOSX	
	CRYPAYSAVE	XINTI	SKULLSCREEN	ADLITTLE	
	FREEZES CARE	SCARAB	LIXLOCKER	FAKECERBER	
	KTZWARE	WINBAM	REETNER	QUAKEWAY	
	PSCRYPT	DARKSCARE	GRIFFINLOCK	MARKOLOCK	
	KRYPTONITE	GOJDUE	EXECUTIONER	RUBY	
	KARO	VIACRYPT	RANPHP	TRIPM	
	BUBBLE	PIRATE	RANSIX	PYTHOCRYPT	
	WIRUSLOCKER				

Table 2. New ransomware families, 1H 2017

Exploit kits are no longer as important to cybercriminals as they were several years ago. Cybercriminals have apparently turned to other reliable means, such as spam, phishing, and exploiting vulnerabilities. Security improvements in internet browsers, exploit kits' playground, have also contributed to the continuing decline of exploit kits' access.

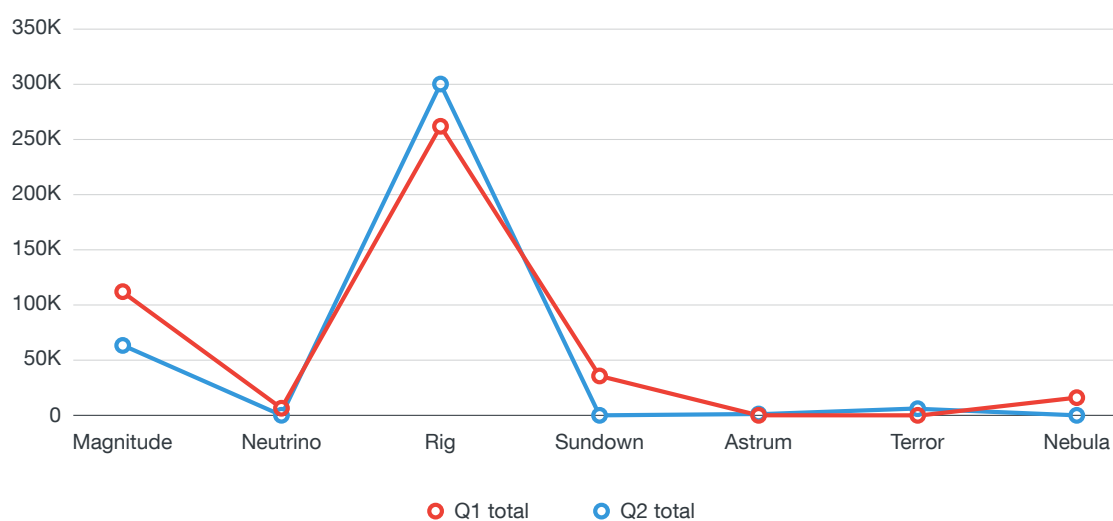


Figure 12. Instances of access to URLs hosting exploit kits, 1H 2017

E-Sports Entertainment Association (ESEA)	1.5 million player profiles	Jan. 8, 2017
CoPilot Provider Support Services Inc.	220,000 patient profiles	Jan. 19, 2017
Arby's Corporate Restaurants	350,000 credit and debit card issued by the Public Service Credit Union (PSCU)	Feb. 9, 2017
Spiral Toys	800,000 user credentials and 2 million message recordings	Feb. 27, 2017
Goldenvoice/Coachella Music Festival	950,000 Coachella.com accounts	March 2, 2017
Center for Election Systems at Kennesaw State University	7.5 million voter records	March 3, 2017
River City Media	1.37 billion records	March 8, 2017
Dun & Bradstreet	33.7 million personnel information	March 15, 2017
America's Job Link Alliance	2.1 million user records	March 27, 2017
IRS Data Retrieval Tool	100,000 personal records	April 7, 2017
Schoolzilla	1.3 million records of students	April 12, 2017
Deep Root Analytics	198 million records of registered voters	June 19, 2017

Figure 13. Notable data breaches, 1H 2017

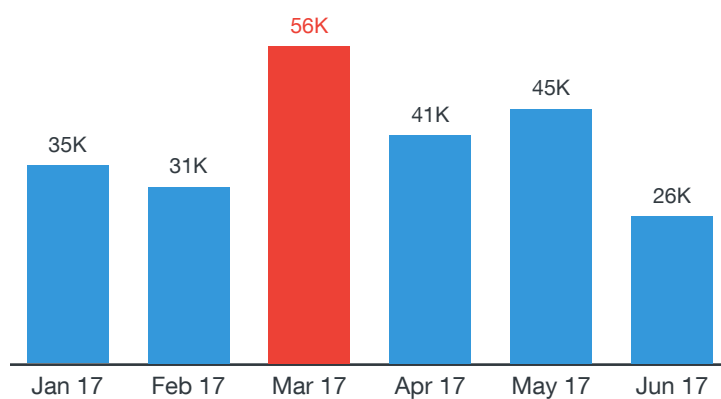


Figure 14. Unique mobile ransomware sourced by Mobile App Reputation Service (MARS), 1H 2017

Note: This shows the unique samples of ransomware discovered/added to MARS each month.

References

1. Christopher Budd. (23 August 2016). *Trend Micro Simply Security*. “2016 – The Year of Online Extortion: Proven.” Last accessed on 2 August 2017 at <http://blog.trendmicro.com/2016-year-online-extortion-proven/>.
2. CBS News. (16 May 2017). *CBS News*. “North Korean hackers behind global cyberattack?” Last accessed on 2 August 2017 at <http://www.cbsnews.com/news/cyberattack-wannacry-ransomware-north-korea-hackers-lazarus-group/>.
3. Alexander Smith, Saphora Smith, Nick Bailey, and Petra Cahill. (17 May 2017). *NBC News*. “Why ‘WannaCry’ Malware Caused Chaos for National Health Service in U.K.” Last accessed on 30 August 2017 at <https://www.nbcnews.com/news/world/why-wannacry-malware-caused-chaos-national-health-service-u-k-n760126>.
4. BBC. (15 May 2017). *BBC News*. “Ransomware cyber-attack: Who has been hardest hit?” Last accessed on 2 August 2017 at <http://www.bbc.com/news/world-39919249>.
5. Ibid.
6. Jonathan Berr. (16 May 2017). *CBS News*. “‘WannaCry’ ransomware attack losses could reach \$4 billion.” Last accessed on 2 August 2017 at <http://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/>.
7. Trend Micro. (25 April 2017). *Trend Micro Security News*. “Ransomware Recap: Expanding Distribution Methods.” Last accessed on 2 August 2017 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-expanding-distribution-methods>.
8. Trend Micro. (19 May 2017). *Trend Micro Security News*. “Ransomware Recap: The Week of WannaCry.” Last accessed on 2 August 2017 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-the-week-of-wannacry>.
9. Ibid.
10. Jasen Sumalapao. (25 March 2016). *TrendLabs Security Intelligence Blog*. “PETYA Crypto-ransomware Overwrites MBR to Lock Users Out of Their Computers.” Last accessed on 2 August 2017 at <http://blog.trendmicro.com/trendlabs-security-intelligence/petya-crypto-ransomware-overwrites-mbr-lock-users-computers/>.
11. Nicole Perlroth, Mark Scott, and Sheera Frenkel. (27 June 2017). *The New York Times*. “Cyberattack Hits Ukraine Then Spreads Internationally.” Last accessed on 2 August 2017 at <https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html>.
12. Ibid.
13. Trend Micro. (28 June 2017). *Trend Micro Security News*. “Ransomware Recap: Petya Ransomware Outbreak Shakes Europe.” Last accessed on 2 August 2017 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-petya-ransomware-outbreak-shakes-europe>.
14. Trend Micro. (27 June 2017). *TrendLabs Security Intelligence Blog*. “Large-Scale Petya Ransomware Attack In Progress, Hits Europe Hard.” Last accessed on 2 August 2017 at <https://blog.trendmicro.com/trendlabs-security-intelligence/large-scale-ransomware-attack-progress-hits-europe-hard/>.
15. Ibid.
16. Trend Micro. (28 June 2017). *Trend Micro Security News*. “Frequently Asked Questions: The Petya Ransomware Outbreak.” Last accessed on 2 August 2017 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/frequently-asked-questions-the-petya-ransomware-outbreak>.
17. Gilbert Sison. (28 March 2017). *TrendLabs Security Intelligence Blog*. “Cerber Starts Evading Machine Learning.” Last accessed on 2 August 2017 at <http://blog.trendmicro.com/trendlabs-security-intelligence/cerber-starts-evading-machine-learning/>.
18. Gilbert Sison. (2 May 2017). *TrendLabs Security Intelligence Blog*. “Cerber Version 6 Shows How Far the Ransomware Has Come (and How Far it’ll Go).” Last accessed on 2 August 2017 at <http://blog.trendmicro.com/trendlabs-security-intelligence/cerber-ransomware-evolution/>.

19. Trend Micro. (2 March 2017). *Trend Micro Security News*. "Ransomware Recap: Patcher Ransomware Targets MacOS." Last accessed on 2 August 2017 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-patcher-ransomware-targets-macos>.
20. Mobile Threat Response Team. (5 July 2017). *TrendLabs Security Intelligence Blog*. "SLocker Mobile Ransomware Starts Mimicking WannaCry." Last accessed on 2 August 2017 at <http://blog.trendmicro.com/trendlabs-security-intelligence/slocker-mobile-ransomware-starts-mimicking-wannacry/>.
21. Trend Micro. (6 December 2016). *Trend Micro Security News*. "The Next Tier – 8 Security Predictions for 2017." Last accessed on 3 August 2017 at <https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2017>.
22. Trend Micro. (15 June 2017). *Trend Micro Security News*. "Erebus Linux Ransomware: Impact to Servers and Countermeasures." Last accessed on 17 August 2017 at <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/erebus-linux-ransomware-impact-to-servers-and-countermeasures>.
23. Trend Micro. (17 May 2017). *TrendLabs Security Intelligence Blog*. "After WannaCry, UIWIX Ransomware and Monero-Mining Malware Follow Suit." Last accessed on 17 August 2017 at <http://blog.trendmicro.com/trendlabs-security-intelligence/wannacry-uiwix-ransomware-monero-mining-malware-follow-suit/>.
24. Trend Micro. (24 March 2017). *Trend Micro Security News*. "Ransomware Recap: New Disguises and a Change of Cryptocurrency." Last accessed on 17 August 2017 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-new-disguises-and-a-change-of-cryptocurrency>.
25. Zero Day Initiative. (2017). *Zero Day Initiative*. "Published Advisories." Last accessed on 3 August 2017 at <http://www.zerodayinitiative.com/advisories/published/2017/>.
26. Dan Goodin. (15 April 2017). *Ars Technica*. "NSA-leaking Shadow Brokers just dumped its most damaging release yet." Last accessed on 3 August 2017 at <https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/>.
27. Trend Micro. (21 May 2017). *Trend Micro Business Support*. "Preventing WannaCry (WCry) ransomware attacks using Trend Micro products." Last accessed on 3 August 2017 at <https://success.trendmicro.com/solution/1117391-updates-on-the-latest-wcry-wannacry-ransomware-attack-and-trend-micro-protection>.
28. Trend Micro. (6 December 2016). Op. cit.
29. Trend Micro. (18 December 2016). *Trend Micro Security News*. "A Rundown of the Biggest Cybersecurity Incidents of 2016." Last accessed on 3 August 2017 at <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/a-rundown-of-the-biggest-cybersecurity-incidents-of-2016#WorstTroublemakerMirai>.
30. Trend Micro. (9 May 2017). *TrendLabs Security Intelligence Blog*. "Persirai: New Internet of Things (IoT) Botnet Targets IP Cameras." Last accessed on 3 August 2017 at <http://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/>.
31. Federico Maggi, Davide Quarta, Marcello Pogliani, Mario Polino, Andrea M. Zanchettin, and Stefano Zanero. (2017). *Trend Micro Security News*. "Rogue Robots: Testing the Limits of an Industrial Robot's Security." Last accessed on 3 August 2017 at <https://documents.trendmicro.com/assets/wp/wp-industrial-robot-security.pdf>.
32. Trend Micro. (3 May 2017). *Trend Micro Security News*. "Rogue Robots: Testing the Limits of an Industrial Robot's Security." Last accessed on 3 August 2017 at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/rogue-robots-testing-industrial-robot-security>.
33. International Federation of Robotics. (25 February 2016). *IFR Press Releases*. "Survey: 1.3 million industrial robots to enter service by 2018." Last accessed on 3 August 2017 at <https://ifr.org/ifr-press-releases/news/-survey-13-million-industrial-robots-to-enter-service-by-2018->.
34. Federal Bureau of Investigation Internet Crime Complaint Center (IC3). (4 May 2017). *Public Service Announcement – Federal Bureau of Investigation*. "Business E-mail Compromise E-mail Account Compromise The 5 Billion Dollar Scam." Last accessed on 3 August 2017 at <https://www.ic3.gov/media/2017/170504.aspx>.

35. "How HTML Attachments and Phishing Are Used In BEC Attacks" in the Trend Micro Security Intelligence Blog is an independent research using a different data set, and does not have a direct correlation with the data set in this paper <http://blog.trendmicro.com/trendlabs-security-intelligence/html-attachments-phishing-used-bec-attacks/>.
36. Trend Micro. (11 January 2016). *Trend Micro Security News*. "Security 101: Business Email Compromise (BEC) Schemes." Last accessed on 3 August 2017 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/business-email-compromise-bec-schemes>.
37. Lord Alfred Remorin. (27 July 2017). *TrendLabs Security Intelligence Blog*. "How HTML Attachments and Phishing are Used in BEC attacks." Last accessed on 3 August 2017 at <http://blog.trendmicro.com/trendlabs-security-intelligence/html-attachments-phishing-used-bec-attacks/>.
38. Trend Micro. (6 December 2016). Op. cit.
39. Lion Gu, Vladimir Kropotov, and Fyodor Yarochkin. (2017). *Trend Micro*. "The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public." Last accessed on 3 August 2017 at https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf.
40. Lily Hay Newman. (1 July 2017). *Wired*. "The Biggest Cybersecurity Disasters of 2017 So Far." Last accessed on 3 August 2017 at <https://www.wired.com/story/2017-biggest-hacks-so-far/>.
41. Samanth Subramanian. (15 February 2017). *Wired*. "Inside the Macedonian Fake-News Complex." Last accessed on 3 August 2017 on <https://www.wired.com/2017/02/veles-macedonia-fake-news/>.
42. BBC. (19 May 2017). *BBC Newsbeat*. "Restaurant hit by 'human meat' fake news." Last accessed on 3 August 2017 at <http://www.bbc.co.uk/newsbeat/article/39966215/restaurant-hit-by-human-meat-fake-news-claims>.
43. Lion Gu, Vladimir Kropotov, and Fyodor Yarochkin. (2017). Op. cit.
44. XE. (1 August 2017). *XE*. "Current and Historical Rate Tables." Last accessed on 4 August 2017 at <http://www.xe.com/currencytables/?from=USD&date=2017-08-01>.
45. BBC. (24 May 2017). *BBC News*. "Irish teen hacked Sun website with fake news of Murdoch death." Last accessed on 3 August 2017 at <http://www.bbc.com/news/world-europe-40029530>.
46. Numaan Huq. (2015). *Trend Micro Security News*. "Follow the Data: Dissecting Data Breaches and Debunking Myths." Last accessed on 3 August 2017 at <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/follow-the-data>.
47. Privacy Rights Clearinghouse. (2017). *Privacy Rights Clearinghouse*. "Data Breaches." Last accessed on 25 July 2017 at <https://www.privacyrights.org/data-breaches>.
48. Shaun Prescott. (10 January 2017). *PC Gamer*. "Over 1.5 million user records leaked after ESEA website hacked." Last accessed on 3 August 2017 at <http://www.pcgamer.com/over-15-million-user-records-leaked-after-esea-website-hacked/>.
49. Mark Wycislik-Wilson. (6 March 2017). *BetaNews*. "Huge database leak reveals 1.37 billion email addresses and exposes illegal spam operation." Last accessed on 3 August 2017 at <https://betanews.com/2017/03/06/river-city-media-spam-database-leak/>.
50. Reuters. (24 May 2017). *NBC News*. "Target Settles 2013 Hacked Customer Data Breach for \$18.5 Million." Last accessed on 3 August 2017 at <http://www.nbcnews.com/business/business-news/target-settles-2013-hacked-customer-data-breach-18-5-million-n764031>.
51. Trend Micro. Smart Protection Network. *Trend Micro*. Last accessed on 22 August 2017 at https://www.trendmicro.com/en_us/business/technologies/smart-protection-network.html.



Created by:

TrendLabs

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

TREND MICRO™

Trend Micro Incorporated, a global 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



Securing Your Journey
to the Cloud