



A Rising Tide: New Hacks Threaten Public Technologies

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Contents

4

Newly hacked technologies caused disruptions to public utilities

7

Solo cybercriminals exposed in several regions; ransomware and PoS malware continued to persist

14

Law enforcement efforts bore fruit as governments prioritized security

17

National and political impact—what made the OPM data breach the biggest incident thus far

20

Latest attacks on government entities emphasized political motives behind targeted campaigns

24


Vulnerabilities threatened public-facing websites, mobile devices

26

Angler Exploit Kit access numbers tripled, faster integration of exploits into kits seen

31

Threat landscape in review



It's no longer science fiction. Attacking commercial airlines, hijacking home routers, shutting down a TV network's broadcast—this quarter's security stories show that attackers are finding more inventive ways to infiltrate and abuse existing technologies. We've seen similar attacks in the past, but their ramifications weren't as prominent as they are now. Cybercriminals used to heavily rely on stealing data and money. Attackers targeted large enterprises and organizations for potentially much larger returns. As more and more public-facing technologies get developed for Internet connectivity, we are witnessing a recurrence in attacks that are more strongly felt.

Attackers are finding new means to target everyday technologies that are often overlooked. They come up with methods to manipulate routers, endangering user privacy. Advancements in point-of-sale (PoS) malware are causing more businesses to lose revenue. Attackers keep testing for vulnerabilities and looking for practical applications for their observations. If the ongoing studies in transportation security are any indication, attacks may be heading in a direction that could turn hacking into a more regular and actual physical concern. A successful airline hack, for example, could mean serious trouble in the skies. What more if attackers set their sights on everyday smart vehicles?

All these don't mean that cybercriminals are abandoning their old operations. Their use of traditional malware is still alive and well, as evidenced by their heavy presence in specific regions worldwide. Basic malware components and tools have become so available and simple to use that any fledgling cybercriminal can run his own malicious enterprise.

Although law enforcement is catching up—with Silk Road mastermind Ross Ulbricht's indictment as beacon—there's still a lot to do in terms of security. With the constant advancements in current technologies comes a new wave of security challenges. Given how most of these are accessible to the public, it's easier to feel their full effect.

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.

Newly hacked technologies caused disruptions to public utilities

Hacks on home routers, a full-scale act of hacktivism against a major TV network, and even attacks on commercial planes. If there's anything this quarter has taught us, it's that cyberthreats are real.

Chris Roberts, a researcher known for his work on airplane security, made headlines this May after allegations of hacking into a plane's in-flight entertainment system. According to a Federal Bureau of Investigation (FBI) report, Roberts caused "one of the airplane's engines to climb, resulting in a lateral or sideways movement during a flight."^{1,2} Roberts got kicked off a United Airlines flight in April after tweeting about the aircraft's security vulnerabilities, which then led to further investigations on the possibility of accessing and hacking in-flight networks.³ In June, an attack on Poland's national airline's network made the news, as dozens of its flights were grounded for several hours, which affected more than 1,400 passengers.⁴

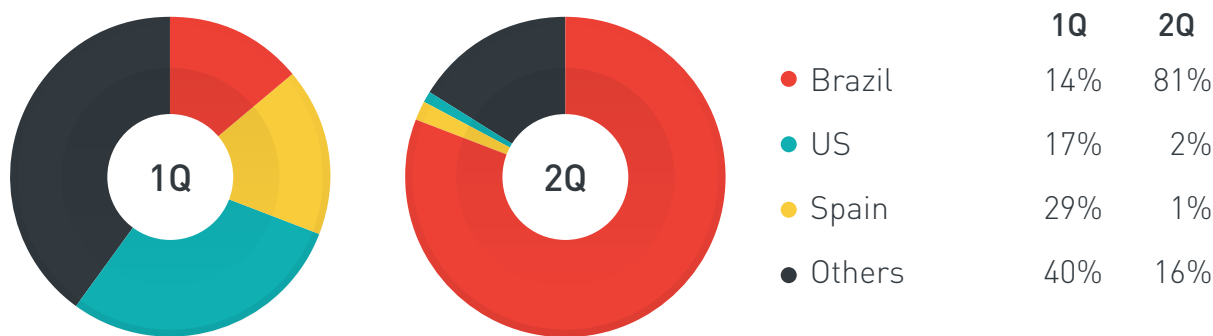
Our own research noted how simple it is to compromise automated vehicular systems with the right tools and aptitude. In the fourth quarter of 2014, our report on Automatic Identification System (AIS), which is used to monitor ships at sea, noted how it's possible for attackers to falsify maritime readings and cause panic and potential disasters. Our researchers' work on smart cars also justified that hacks on private transportation means are possible.

We researched various attacks that specifically targeted home routers this quarter, too. Domain Name System (DNS)-aided attacks are no longer new. Using DNS changers to target home routers has made a comeback though. This quarter, cybercriminals set their sights on routers to tamper with the information these relayed to connected devices, thus facilitating data theft.⁵

Malware that infect routers and modify their DNS settings allow cybercriminals to perform malicious activities like steering victims to bad sites. These malicious sites can be phishing pages or even fake sites that solely exist to serve malware.

We saw an increase in the number of DNS changer detections, particularly in Brazil.⁶ These attempted to gain control of routers by way of changing their DNS settings.

DNS changer detections seen (1Q and 2Q 2015)



Brazil accounted for 81% of the total global number of DNS changer detections this quarter, a far cry from its mere 14% share of the global pie in the previous quarter.

The increase in number of attacks involving routers is alarming because these devices play an important role in home networks. The more Internet-enabled home devices are connected to home routers, the more viable the routers are as attack targets. Attackers who gain control of vulnerable routers, after all, gain visibility on all of the devices connected to them as well as all of the information they relay.

We’ve seen DNS changers poison searches or modify router settings to redirect victims to malicious pages in the past. The more devices are connected to infected routers, the more potential fraud victims there will be.

Unlike typical cybercriminal operations and attacks whose effects are only felt “behind the scenes,” the hacking incidents we saw this quarter were more evident and “real,” so to speak. French TV station, TV5MONDE, for instance, suffered a four-hour-long public broadcast disruption and complete internal network shutdown.⁷ Its site and social media accounts weren’t spared as well.

“

Like any other system, there are bugs somewhere in this [airplane] system; no human-built system is 100% error free. It will be up to governments and regulators to force vendors (both of airplanes and in-flight entertainment systems) to move beyond simple security-through-obscurity and demonstrate that existing systems are secure, and to fix any vulnerability that does come to light. Who knows? Perhaps the systems that are in place have been designed in a robust and secure manner and do a good job of keeping attackers out.

”

—Martin Rösler

Senior Director, Threat Research

Solo cybercriminals exposed in several regions; ransomware and PoS malware continued to persist

This quarter, we saw how solo cybercriminal operations used malware like FighterPOS to spread mayhem. A cybercriminal named “Lordfenix” in Brazil was one of them. Another lone cybercriminal named “Frapstar” from Canada also profited from peddling stolen information.

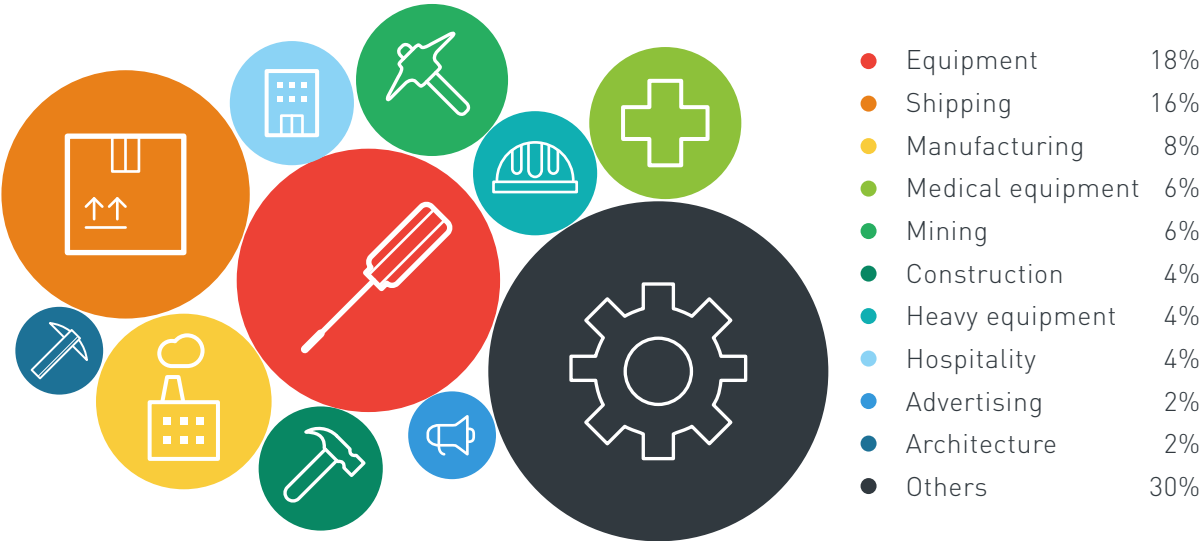
Cybercriminals always update malware code; their actions this quarter were no different. Modifying existing malware is, after all, the fastest way to launch attacks. And anyone armed with the basic tools and know-how can successfully do so, even a solo cybercriminal.

Such was the case of the two solo cybercriminals behind HawkEye keylogger attacks. Each used run-of-the-mill data-stealing malware to hijack business transactions and steal information from small and medium-sized businesses (SMBs).⁸ Each repurposed existing malware, toolkits, and techniques to target victims from India, Egypt, Iran, Pakistan, Taiwan, and the United States (US), among other countries.

Countries where HawkEye victims were located (2Q 2015)



Industries most affected by HawkEye (2Q 2015)



HawkEye’s victims mostly comprised SMBs spread across various industries.

Traditional malware like simple keyloggers are constantly modified to suit intended targets. The modus operandi used to distribute them, meanwhile, directly correlated with their operators’ geographic locations.

Frapstar, a lone criminal operator from Canada, earned a lot of money from selling the information he stole.⁹ So did a 20-year-old college student from Brazil known as Lordfenix who profited from selling banking malware.¹⁰ Our research revealed that Lordfenix has created more than 100 banking Trojans since April 2013 that each sold for around R\$1,000 (roughly US\$320). Frapstar, meanwhile, was very active in known cybercriminal and hacking forums—the usual platforms for selling sensitive data dumps.

FighterPOS entered the picture this April. Also backed by a solo cybercriminal operation, FighterPOS was able to steal 22,000 unique credit card numbers from and infect more than 100 PoS terminals in countries led by Brazil (with a 96% share).¹¹ FighterPOS’s sole operator also appeared to have had a long history in carding, payment scams, and malware creation.

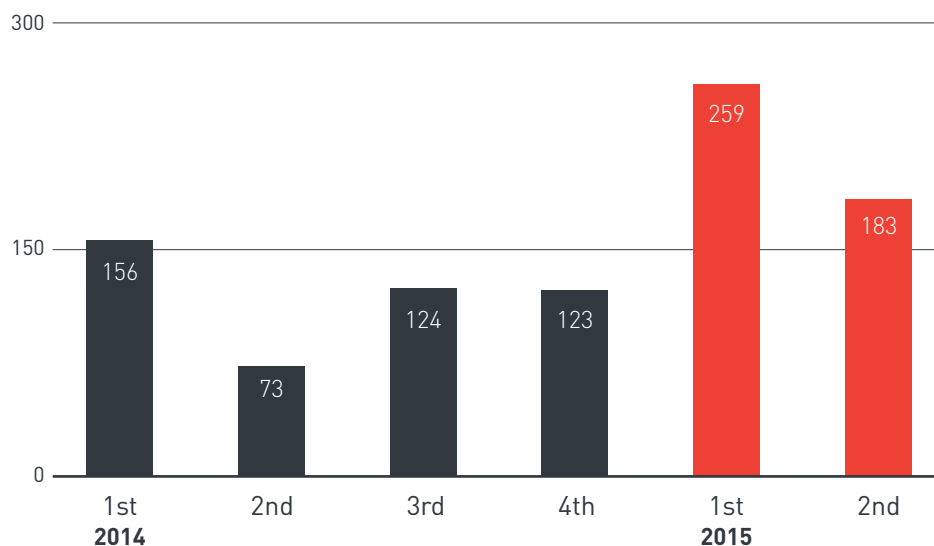
This June, newly discovered MalumPOS targeted systems running Oracle® MICROS, potentially affecting 330,000 hospitality, food and beverage, and retail establishments primarily in the US. As many more PoS variants come to the fore, it’s only a matter of time before other enterprising cybercriminals take its source code for their own use.

Cybercriminal operations/operators seen (2Q 2015)

Operation/Operator	Affected countries
HawkEye	India, Egypt, Iran, Pakistan, Taiwan, US, Hong Kong, Russia, France, Germany
Lordfenix	Brazil
Frapstar	US, Canada*
Teenage Chinese mobile ransomware developers	China
TorrentLocker	Australia, Spain, Germany, France, UK, Turkey, Poland, US, Italy, Taiwan, New Zealand, Netherlands
CryptoWall 3.0	US, Canada, India, UK, France, Japan, Taiwan, South Korea, Australia

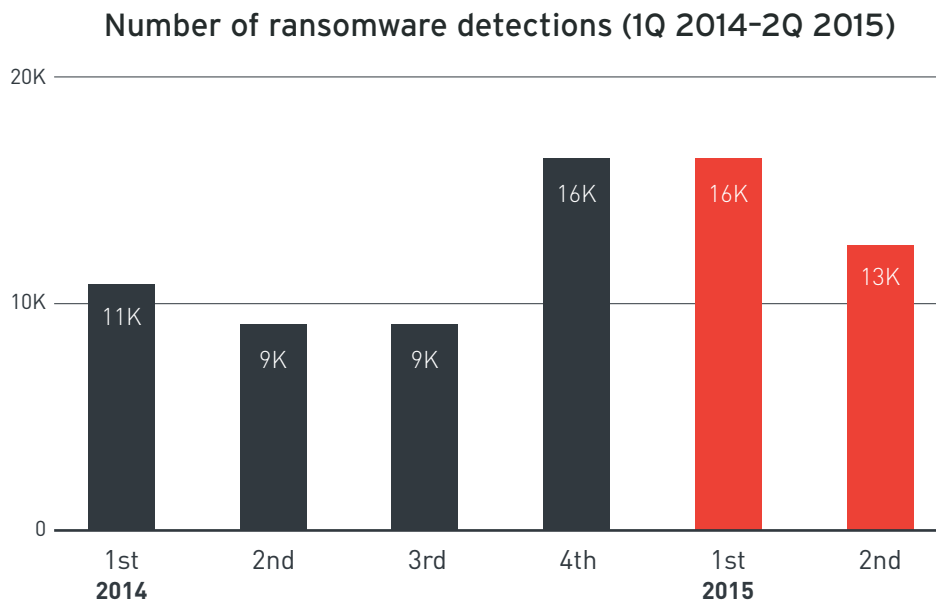
**Note: Frapstar could be selling information in countries other than those mentioned in the table above.*

Number of PoS malware detections (1Q 2014-2Q 2015)



The slight decline in PoS malware detections could be due to the threat reaching its saturation point. The latest iterations of the threat throughout the first half of the year could just be last-ditch efforts to capitalize on the gains they bring.

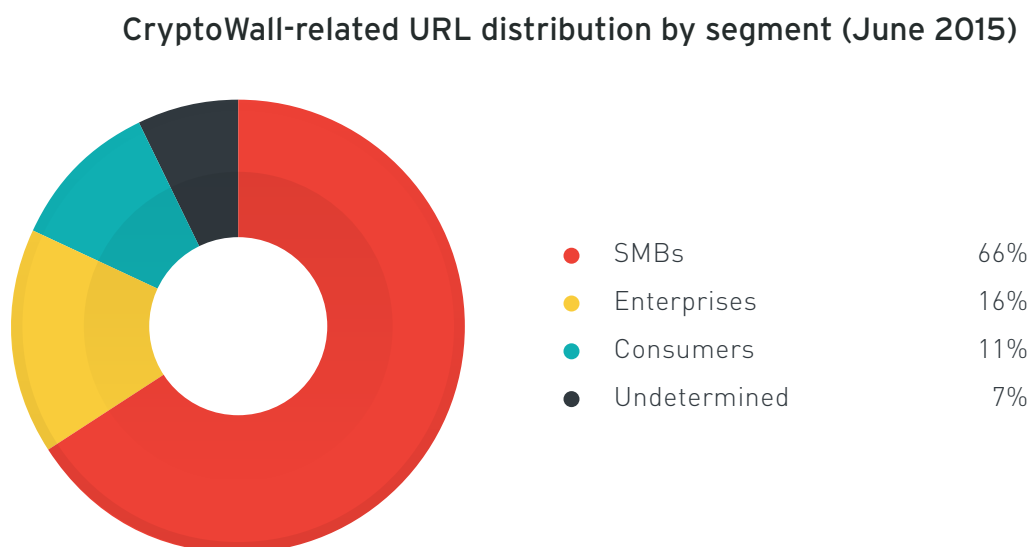
The ransomware detection volume, meanwhile, may appear to have declined quarter over quarter, but in-depth analysis showed that the threat isn't disappearing anytime soon. It's just becoming more regionalized.



The volume of ransomware detections has been decreasing since the first quarter of 2015.

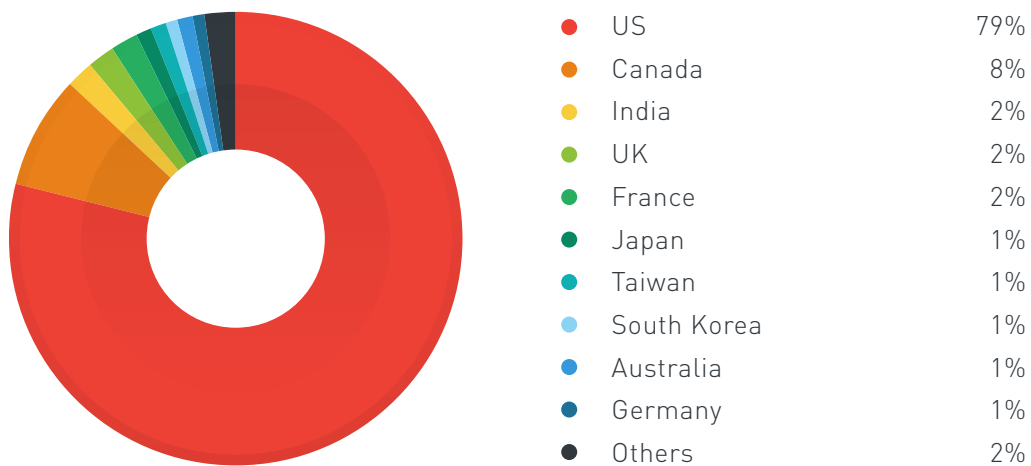
The risks that ransomware pose should be studied from different angles. Their ability to infect computers is just one piece of the puzzle. Just this June, we closely monitored two notable ransomware variants—CryptoWall and TorrentLocker.

CryptoWall 3.0, the latest crypto-ransomware variant, spread via spam and was even seen in cahoots with FAREIT.¹²



SMBs were most affected by CryptoWall based on data gathered in June 2015.

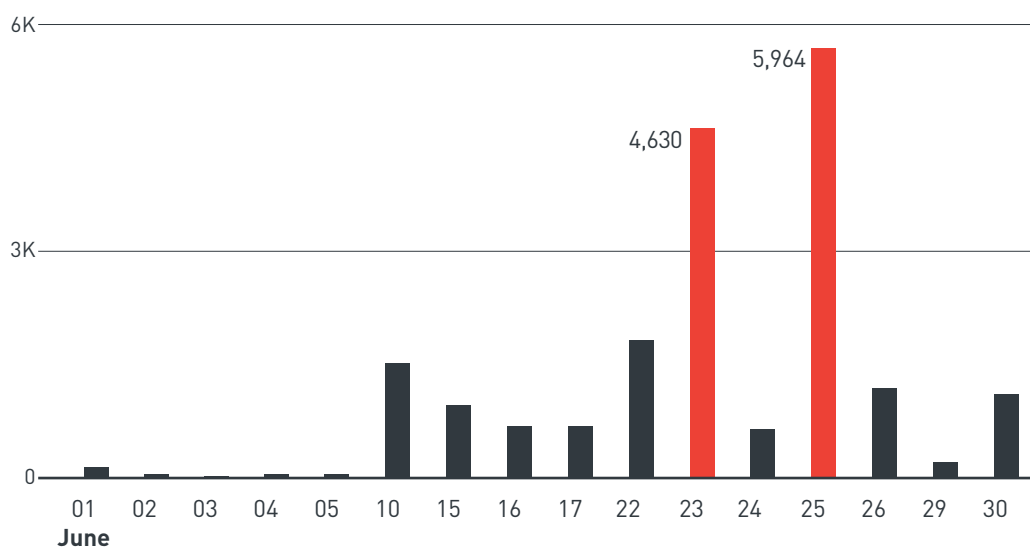
Top 10 countries where CryptoWall victims were located (June 2015)



A majority of the CryptoWall victims were from the US, accounting for nearly 80% of the total number of detections.

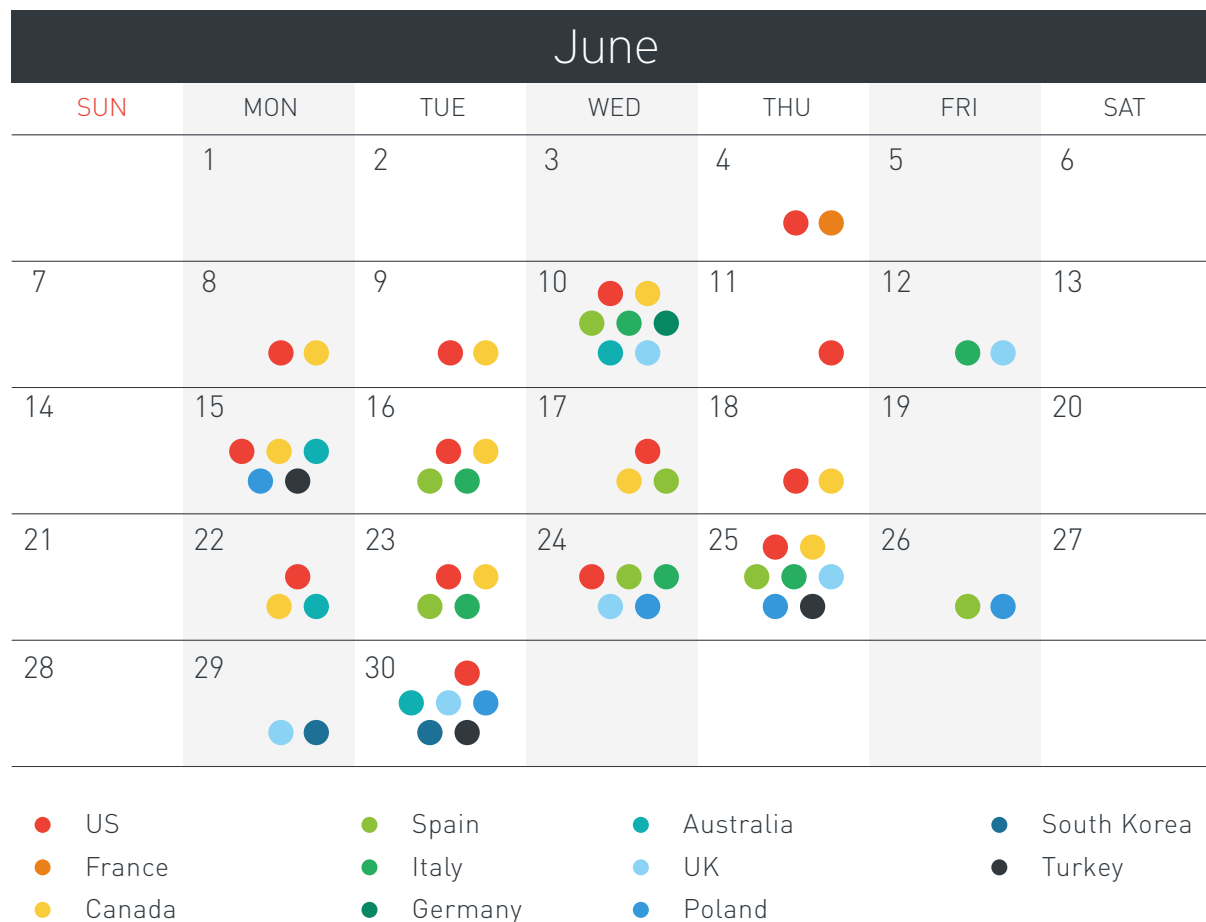
More than 10,000 TorrentLocker-related URLs were accessed by users this June alone. On 23 and 25 June, the number of URLs accessed reached more than 4,000 a day. This means that more and more users are clicking links embedded in emails, showing just how important having a multilayer approach to ransomware security is.

Number of user clicks to TorrentLocker-hosting URLs (June 2015)



Just this June, we blocked more than 10,000 user clicks to TorrentLocker-related URLs. We saw the highest number of user clicks to related URLs on the 23rd and 25th of that month.

Regional ransomware outbreaks (June 2015)



The calendar above shows evidence of specific intentions to deliver ransomware to specific countries. These ransomware include TorrentLocker and CryptoWall variants.

This quarter, we also saw a surge in the volume of TorrentLocker-related emails sent to users in certain countries, particularly the United Kingdom (UK) and Turkey.¹³ These emails used popular postal or courier and telecommunications firms (SDA Express, Pozcta, Correo, and Turkcell) as social engineering bait. Unlike older variants though, more recent iterations changed malware-storage sites. They no longer favored SendSpace and Mediafire. They used Yandex Disk and Google Drive™ instead.

Mobile ransomware also plagued users in China driven by an unusual group of suspects. Underground research revealed the existence of more than a thousand variants of a piece of Android™ ransomware. A closer look at these variants revealed that they all came from a single source code that was widely distributed in underground forums. This code was created by a new generation of cybercriminals aged 16 to 21.¹⁴ They seemed bolder and more reckless, leaving traces of their real identities online, along with their malicious code creations. They even offered tutorial services to wanna-be cybercriminals underground. And unlike more experienced cybercriminals, newbies favored that payments be made via Alipay, WeChat, and bank transfer—a departure from the current trend (using cryptocurrencies to cover traces of illegal activities).

“

Moving forward, we're probably going to see an incorporation of old and new threats, blended for the same objective. Defenders have to start considering new and upcoming threats while addressing old threats and keeping an eye out on potential targeted attacks. I would recommend using a clearly defined strategy to combat threats. Aside from looking into particular events within a host, make sure you can correlate them with network events, too.

”

—Jay Yaneza

Threats Analyst

Law enforcement efforts bore fruit as governments prioritized security

More organized law enforcement efforts were seen this quarter, as botnet takedowns and real-world implications were made evident by cybercriminal arrests. These just showed that acts of cybercrime that make a real-world impact have real-world consequences.

One of the more notable developments we saw was coordination across law enforcement agencies. Trend Micro aided law enforcement agencies in taking down two notorious botnets that were heavily involved in full-scale cybercriminal operations—SIMDA and Beebone.

In a public-private partnership (PPP), Trend Micro, the FBI, Europol, the US Department of Homeland Security (DHS), and other security vendors took part in taking down a longstanding botnet operation known as “Beebone” this April.^{15, 16} Beebone malware, which we detect as VOBFUS variants, are polymorphic malware created to download other malware.¹⁷

That same month, another collaborative effort to take down the SIMDA botnet involving Trend Micro, INTERPOL, Microsoft, Kaspersky, and Japan’s Cyber Defense Institute resulted in a triumph for the security industry.¹⁸ SIMDA botnet activity was believed to have spanned the globe, with redirection servers in 14 countries and victims from at least 62 countries.¹⁹

Digging into the Deep Web

This February, federal prosecutors formally indicted alleged Silk Road mastermind, 31-year-old Ross Ulbricht.²⁰ A few months later, in May, Ulbricht was sentenced to life imprisonment without parole.²¹ Silk Road was the largest Dark Web marketplace for illegal drugs that assured its users of privacy and anonymity.

Ulbricht’s sentencing shone a light on the otherwise deep and dark mysteries behind the Deep Web, along with the other nefarious activities that surround it. Over the course of two years, the Trend Micro Forward-Looking Threat Research (FTR) Team delved into an extensive exploration of the Deep Web and its effects

on the real world.²² The paper we released some months back revealed that drugs happen to be the most popular merchandise sold in the Deep Web. The Deep Web, as it turned out, was also home to several bitcoin and money-laundering services for cybercriminal operators.

Ulbricht's sentencing should serve as a clear warning to all those who are thinking of following his footsteps. We have yet to see a drastic change in the cybercriminal underground, but given that the likes of Ulbricht operate within the Deep Web—a law enforcement challenge we discussed in June—much more work needs to be done in darknet investigations.

Snapshot of product and service prices in the Deep Web (2Q 2015)

Item	Price
German PayPal accounts with at least US\$500 balance	US\$250
100 unverified PayPal accounts	US\$100
100 unverified eBay accounts	US\$100
100 unverified credit cards with Card Verification Value (CVV2) code	US\$150
Fake European passports	€500–750
Fake US passports	€800
US credit cards with US\$2,000 balance	US\$90
European credit cards with €5,000 balance	US\$210

Source:

http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf

Striking a balance between privacy and security

The botnet takedowns and cybercriminal arrests this quarter proved that security is a US government priority. Just this June, the US government signed the newly legislated “USA Freedom Act,” which aims to allow citizens to freely use communication technologies while limiting the data-collection activities of intelligence agencies.²³ The US also took another bold step for security by rolling out the mandatory use of HTTPS across federal websites, ensuring secure and private access for all visitors.²⁴ This was definitely a positive change though it isn't a cure-all for online threats.

That same month, member states of the Council of the European Union (EU) agreed to new European data protection laws that could see tough new regulations unified across the whole region.²⁵

“

One of the biggest problems that legislation has with cybercrime is that it evolves very quickly. Most laws would take maybe 3–5 years to pass. So, the most relevant will be general laws that have been around for a long time. The US has been successful in arresting people charged with organized crime or racketeering. These laws are not specifically ‘cyber’ in nature, but having them helped. What should generally be done is to standardize laws across countries.

At the end of the day, the Internet is global. Therefore, cybercrime is global so it would be a lot easier to prosecute people if the law on hacking a server is exactly the same in Germany as it is in Ireland or France. There’ll be fewer complications as incidents like these happen. Then again, what’s most important is to make communication within PPPs easier. If communication is easy, law enforcement agencies and security researchers can easily share information.

—**Robert McArdle**

Senior Threat Research Manager

”

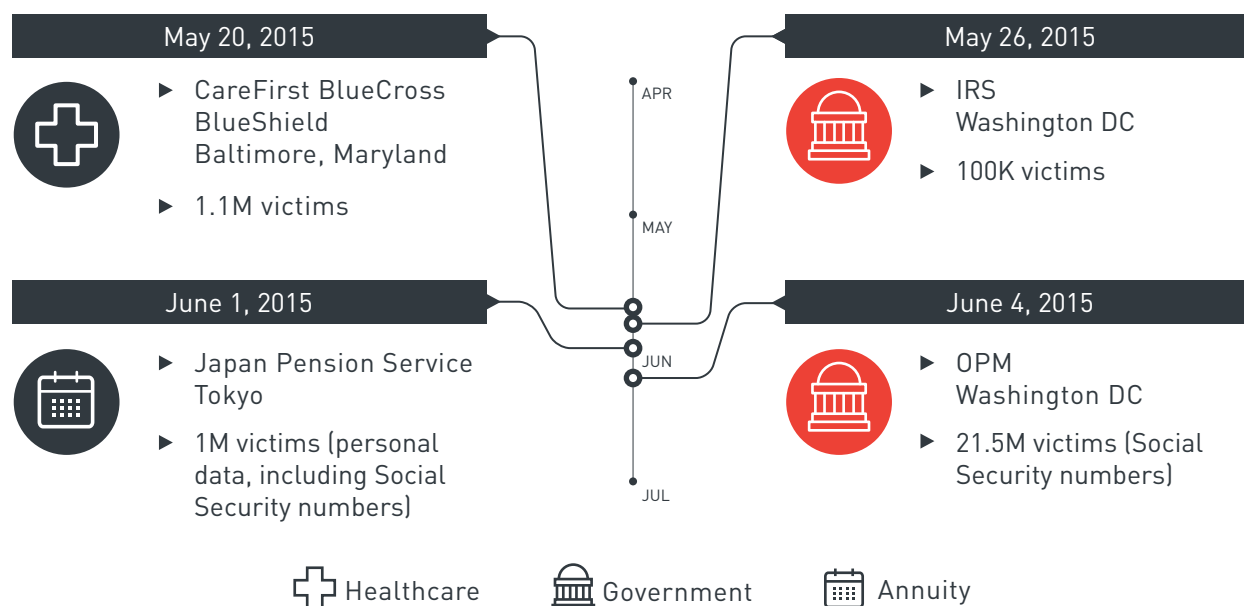
National and political impact— what made the OPM data breach the biggest incident thus far

US officials declared an investigation on a massive data breach on the systems that belong to the Office of Personnel Management (OPM) in the latter part of June this year.²⁶ OPM, a human resources (HR) department of the federal government, conducts background checks on all state employees. An estimated 21 million former and current federal employees, including rejected applicants, had their personal information exposed as a result of the breach.²⁷

The attackers' target of choice isn't new. We already know that HR departments are often the initial targets of island-hopping or "leapfrogging" attacks whose "real" targets are the departments' affiliates.²⁸ The amount of data collected is enough to warrant serious concern, but given the comprehensiveness of the information stolen, this breach's impact is indisputable. The attackers were able to access millions of forms for National Security positions in the US (SF-86 forms). These contained Social Security numbers, job assignments, and background information on family members and friends, among other details. The information lost also reportedly included security investigations on federal employees and contractors, which could be used for identity theft, extortion, and phishing. An even graver consequence could be threats against national security using the stolen information.²⁹

The Internal Revenue Service (IRS) joined the list of breached organizations as well, as attackers siphoned data off its "Get Transcript" Web application this May. This incident granted attackers access to over 100,000 taxpayer records, including Social Security information, dates of birth, and street addresses.^{30, 31} Japan's Pension Service also lost data in an attack when an employee opened a malicious email attachment this June.³²

Reported major data breaches (2Q 2015)



Government entities were the primary attack targets this quarter. The OPM breach was the biggest incident to date, as it exposed more than 20 million records.

Source: <https://www.privacyrights.org/data-breach>

“

In some ways, your personal information getting leaked is more dangerous. I can easily get my credit card changed but unless I move, I can't change my address. Neither can I change my birthday. Personally identifiable information (PII) don't only identify users, it's also frequently difficult, if not impossible, to change.

”

—**Raimund Genes**

Chief Technology Officer

Latest attacks on government entities emphasized political motives behind targeted campaigns

We saw the Pawn Storm attackers target members of the North Atlantic Treaty Organization (NATO) and the White House. Campaigns like ESILE or Lotus Blossom and Tropic Trooper, meanwhile, trailed their sights on Southeast Asian governments. Based on Smart Protection Network data, attackers are finding more use for macro malware in mostly politically motivated campaigns.

The quarter in campaigns: Pawn Storm, ESILE/Lotus Blossom, Tropic Trooper, and DUQU 2.0

This April, Trend Micro researchers saw new campaigns connected to Operation Pawn Storm, which zeroed in on NATO members and the White House. Pawn Storm attackers sent out specially crafted emails designed to trick targets into clicking malicious links. They injected exploits into legitimate government websites and new command-and-control (C&C) servers to target NATO members and governments in Europe, Asia, and the Middle East.³³

This May, Operation Tropic Trooper, so named after the attackers' choice of targets, went after government entities in Taiwan and the Philippines.³⁴ The campaign relied on old infiltration tactics, abusing two commonly exploited Windows® vulnerabilities, basic steganography, and effective social engineering.³⁵

Yet another targeted attack campaign figured in the news again this June. Dubbed “ESILE” or “Lotus Blossom,” this campaign reportedly carried out more than 50 attacks against military organizations in Southeast Asia over a three-year period.³⁶ Based on our own analysis, the malware used in the campaign dropped files with properties that have been carefully crafted to confuse security researchers.³⁷

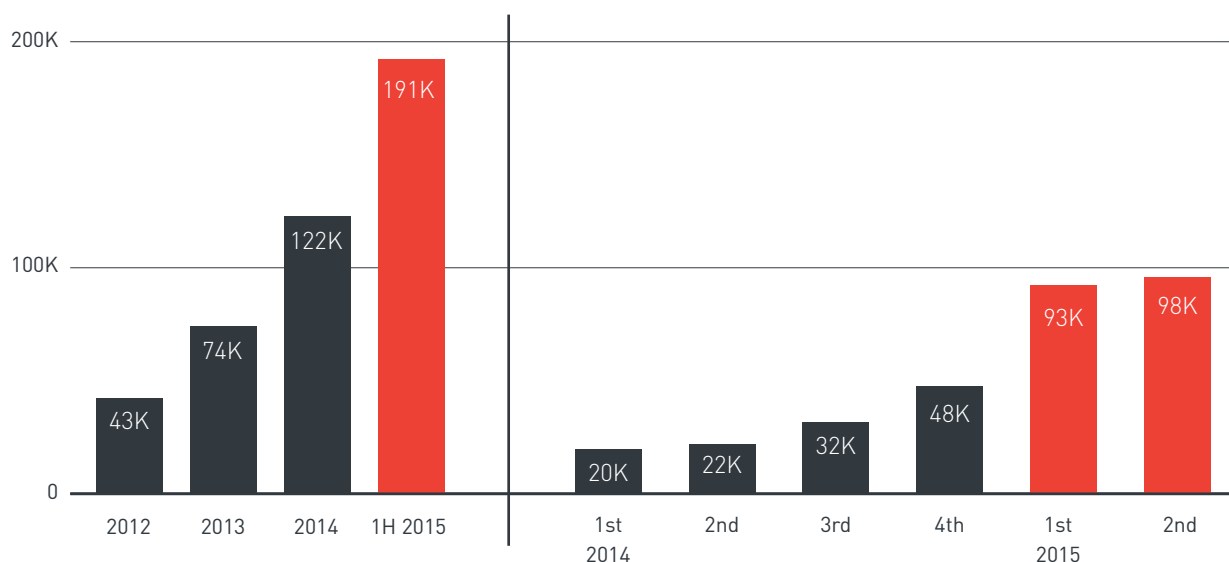
STUXNET successor, DUQU, first made headlines in October 2011 when researchers noted similarities between the two threats’ code.³⁸ Just this June, we saw those behind DUQU 2.0 exploit several zero-day vulnerabilities to attack chosen targets.³⁹ Security researchers believe DUQU 2.0 has ties to Israel and is being used to spy on discussions over Iran’s nuclear capabilities.⁴⁰

Macro malware now used in targeted attacks

Apart from “typical” use by cybercriminals in malware attacks, macro malware are now figuring in sophisticated targeted attack campaigns, too. Campaigns like Operation Woolen-Goldfish, for instance, employed spear-phishing emails that had Microsoft™ Excel® attachments laced with malicious macros.^{41, 42}

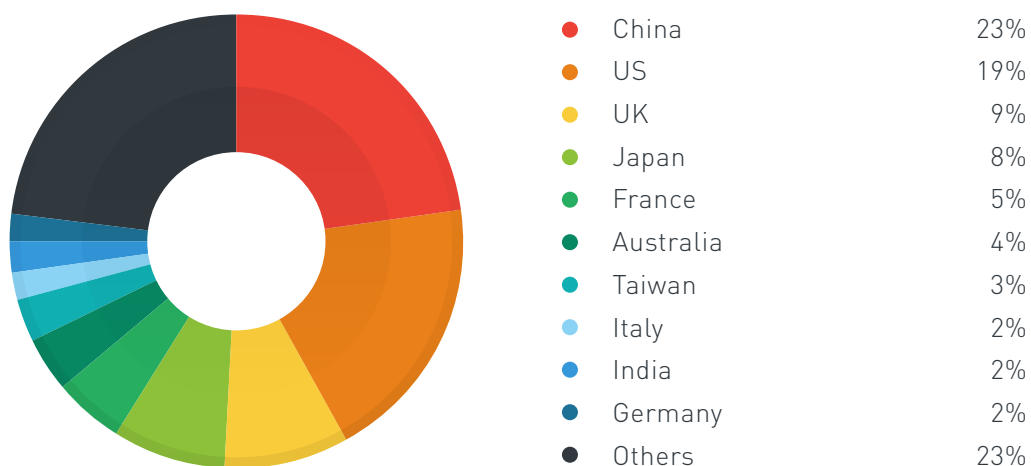
Due to the presence of these attacks, the importance of improving one’s security measures against targeted attacks is more important than ever. A more layered security strategy for email-based attacks is necessary, as these are the usual targeted attack vectors.

Macro malware detections (2012-1H 2015)



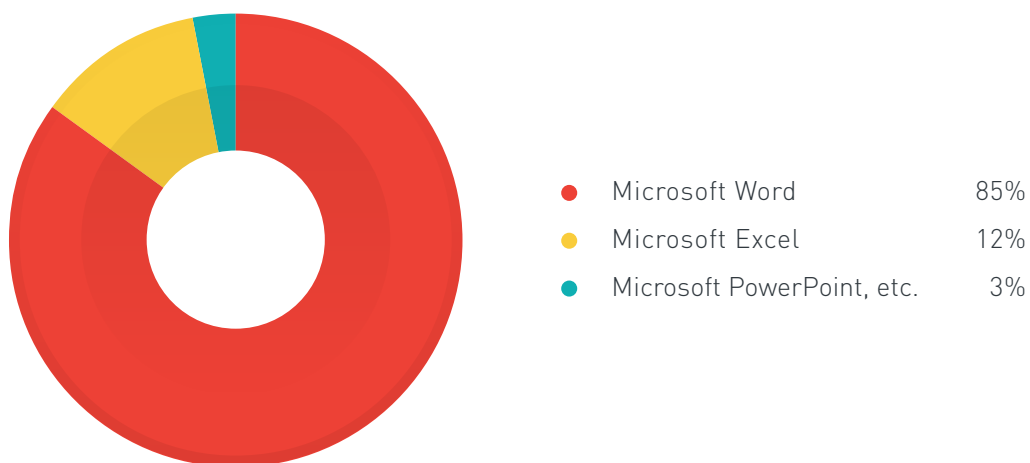
The number of macro malware detections slightly increased quarter over quarter, most likely due to a rise in the use of malvertisements that led to macro-malware-download sites in attacks.

Countries with the highest number of macro malware detections (2Q 2015)



The same four countries that posted the highest number of macro malware detections in the first quarter remained this past quarter's top-notchers.

Macro malware detection distribution per application (2Q 2015)



Most macro malware came with Microsoft Word® documents this quarter.

“

Traditionally speaking, targeted attacks against political targets and enterprises are fairly similar. However, there are some minor differences in motivation and end result. Political attacks are sometimes more known for employing zero days in conjunction with ‘traditional’ attack vectors. Attacks against enterprises, meanwhile, traditionally utilize ‘standard’ methodologies since they almost always rely on the human element, which is the weakest link in the chain.

”

—Kyle Wilhoit

Senior Threat Researcher

“

Secondary infections are flourishing due to three ominous phenomena. First, more hackers are targeting the information supply chain of organizations, leveraging island hopping to compromise internal hosts. Second, after a compromise, the use of steganography allows a second C&C channel to be established within compromised systems, allowing the adversary to effectively counter incident response. Finally, once the cybercriminal has stolen intellectual property or PII, they then use the organization’s brand to attack its constituency via watering-hole attacks. These have exponentially grown in the first six months of 2015.

”

—Tom Kellermann

Chief Cybersecurity Officer

Vulnerabilities threatened public-facing websites, mobile devices

This quarter showed us that vulnerabilities in Web apps were just as dangerous as those in software with very large user bases.

Security researchers discovered a vulnerability in Magento, a Web app that deals with banking-related information.⁴³ Roughly 20,000 websites that use the platform were reported to be vulnerable to the malicious code and could be prone to credit card theft. Magento serves over 240,000 sites worldwide, including eBay, the popular e-commerce service provider with an estimated user base of around 157 million active buyers. eBay has since resolved the issue.⁴⁴

This April, WordPress's content management system (CMS) was exploited by attackers who inserted a malicious JavaScript code into its administrator browser window.⁴⁵ Discovered by Finland-based researcher, Jouko Pynnönen, this allowed cross-site scripting (XSS) attacks via comment boxes in forums and discussion boards on WordPress sites, which make up a fourth of the Internet.

As always, mobile devices weren't spared from the same types of bugs as those seen for Web apps and software. Security researchers, for instance, announced a keyboard vulnerability seen in over 600 million Samsung mobile devices.⁴⁶ Based on our own analysis, the Samsung SwiftKey Vulnerability (CVE-2015-4640 and CVE-2015-4641), could allow would-be attackers to run malicious code via man-in-the-middle (MitM) attacks on vulnerable devices.^{47, 48, 49} Though a patch for this has been released, fragmentation still poses a challenge. The question as to whether users will receive patches or not due to device and mobile carrier differences remains.⁵⁰

A vulnerability in the Apache Cordova app framework was also uncovered this May. This allowed attackers to modify how apps behaved with just a click on a wrong URL.⁵¹ This highly severe vulnerability affected a majority of Cordova-based apps, which accounted for more than 5% of all Google Play™ apps. The vulnerability has been given the designation, "CVE-2015-1835," which could crash apps on affected devices.⁵²

This June, Mac OS® X flaws also affected iOS device users. Huge holes were found in the application sandboxes that "protected" both platforms. This vulnerability could allow potential attackers to create apps that steal keychain and 1Password content.⁵³

“

Attackers leverage vulnerabilities and weaknesses in all platforms. They just need a way to get in. Enterprises must be very watchful of vulnerabilities in the core software and plug-ins that they use. A focused and continuous vulnerability assessment program must be complemented by a configuration assessment program. Though vulnerabilities in standard software like Flash, Java, Firefox, and Internet Explorer® are used as a yardstick to draw the threat landscape, we shouldn't forget that vulnerabilities in custom applications (mainly Web apps) are also very high in number and a lot of them don't make it to the CVE list. Custom applications need customized checking. A good penetration test on custom applications always compensates for that.

”

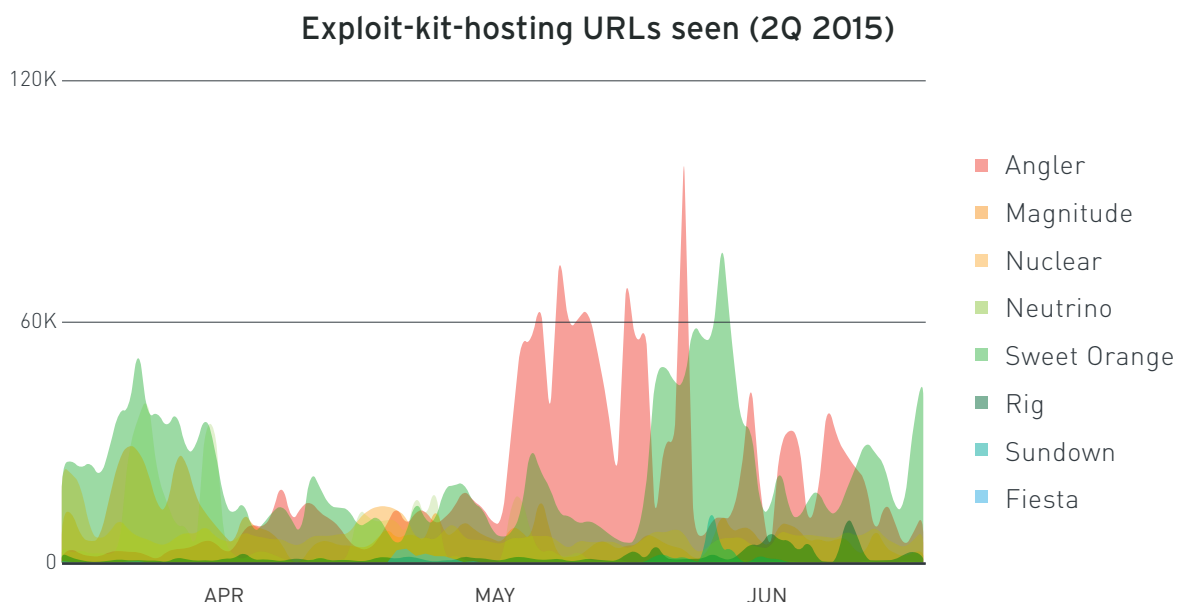
—Pawan Kinger

Director, Deep Security Labs

Angler Exploit Kit access numbers tripled, faster integration of exploits into kits seen

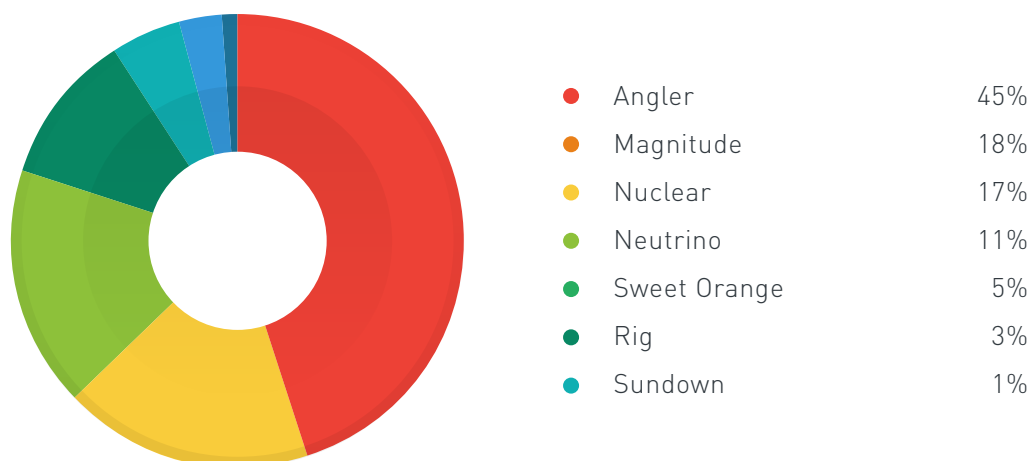
We saw a 67% growth in the overall exploit-kit-related detection numbers quarter over quarter. The Angler Exploit Kit numbers, meanwhile, tripled, as its creators more aggressively integrated new exploits for Adobe® Flash® vulnerabilities.

Much like the Angler Exploit Kit, the Magnitude and Nuclear exploit kits also more actively figured in Adobe Flash exploit attacks.



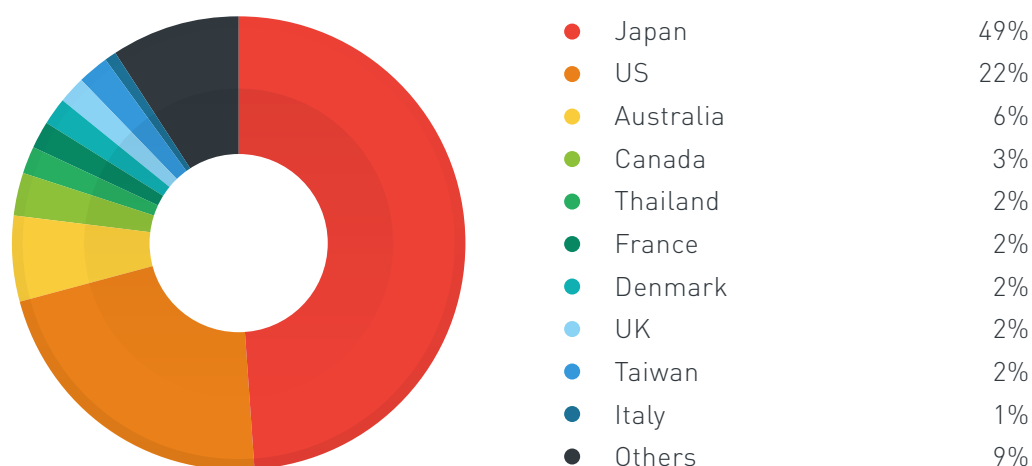
A spike was seen in the number of users accessing Angler Exploit Kit-hosting URLs from May to the start of June this year. An increase in the number of compromised and adult sites that served malvertisements, which led to Angler Exploit Kit download sites was seen during this period.

Exploit-kit-related URL access volume distribution (2Q 2015)



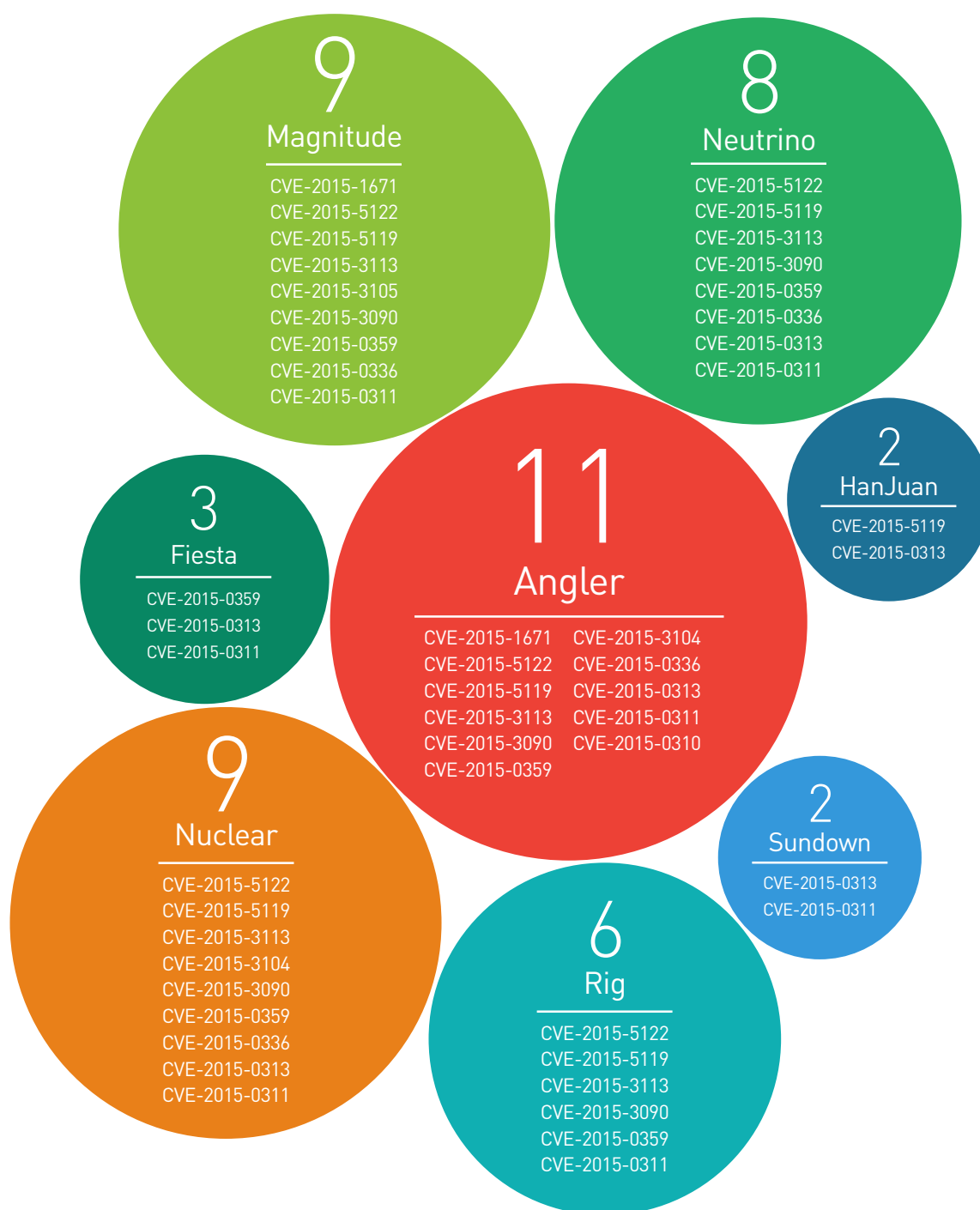
Angler Exploit Kit took Nuclear Exploit Kit's place this quarter in terms of number of user access to related URLs.

Countries most affected by exploit-kit-related attacks (2Q 2015)



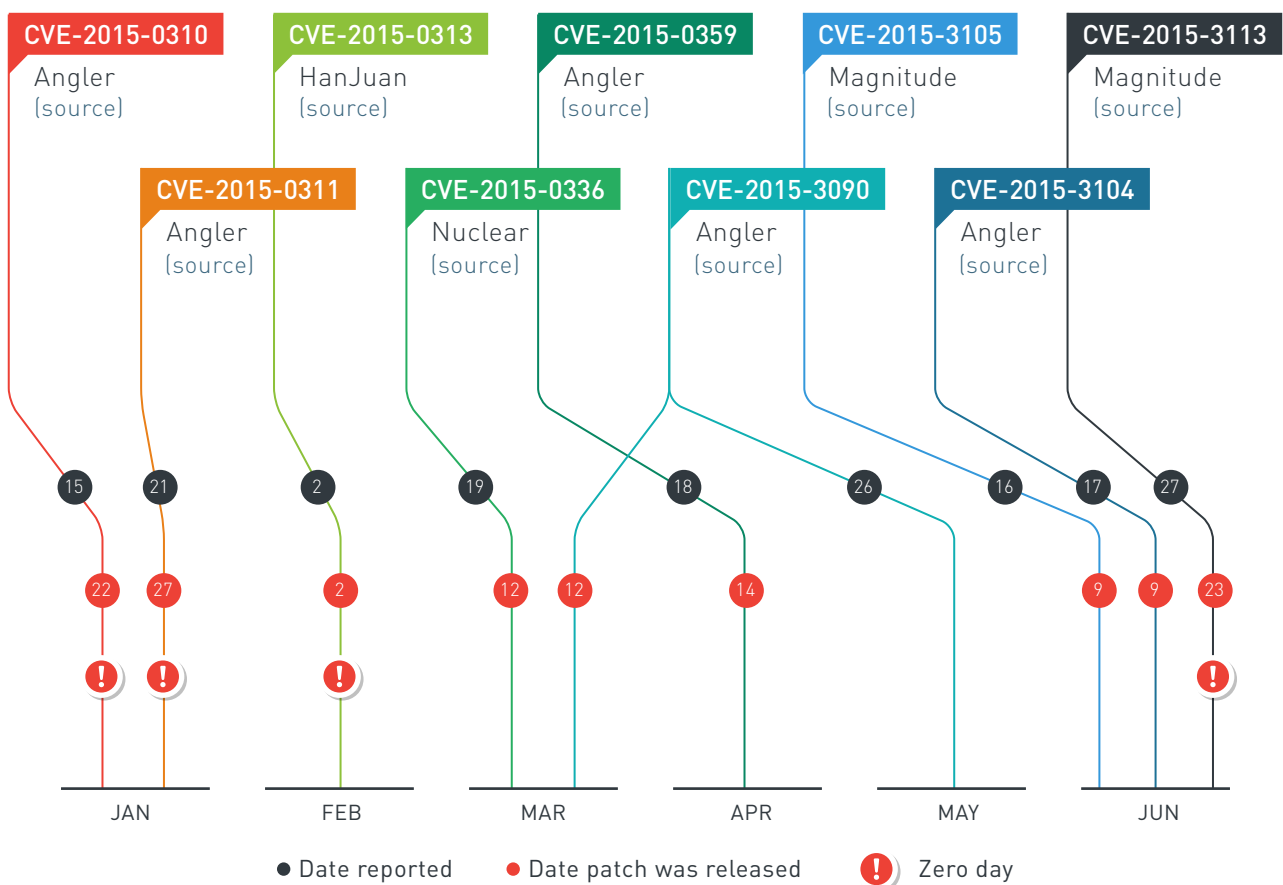
A spike in Angler Exploit Kit-related activity was seen in Japan. In fact, it was the most affected country in terms of user access to related URLs.

Developers of the Angler Exploit Kit proved more prolific and productive, adding several exploits to their creation. Ten of the 11 exploits added to the kit exploited Adobe Flash vulnerabilities, putting all sites that load content like videos with the software, at risk. The Angler and Magnitude exploit kits also integrated an exploit for a Silverlight® vulnerability (CVE-2015-1671).⁵⁴



Exploits for Adobe Flash vulnerabilities have been integrated into more and more exploit kits (especially Angler) since the start of this year. Angler was updated in April, May, and June. And just this July, security researcher, Kafeine, reported two Angler Exploit Kit-related zero-day attacks (one on 7 July and the other on 11 July).^{55, 56}

Timeline of Adobe Flash vulnerabilities integrated into exploit kits (1H 2015)



Exploits for Adobe Flash vulnerabilities have been integrated into more and more exploit kits (especially Angler) since the start of this year.

“

Angler Exploit Kit’s developers have been very actively and aggressively adding Adobe Flash exploits to it. Magnitude and Nuclear exploit kit developers are doing the same thing. It’s this agility that we should continue to study and monitor to better protect our customers.

”

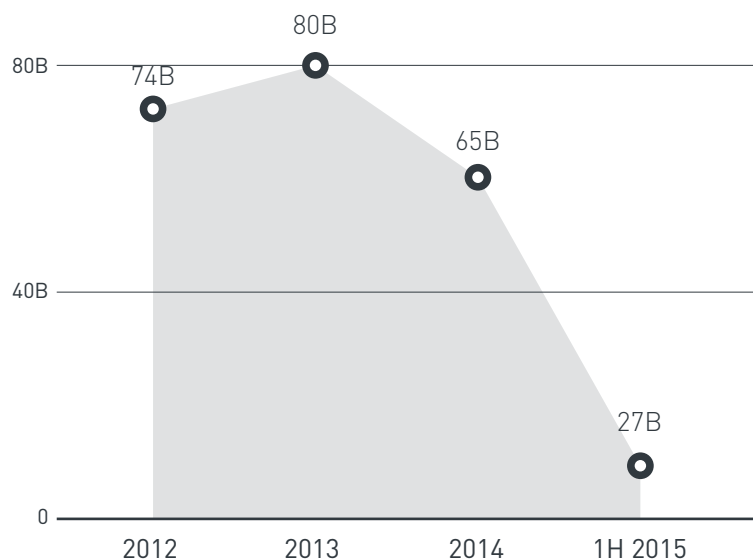
—Joseph C. Chen

Threats Analyst

Threat landscape in review

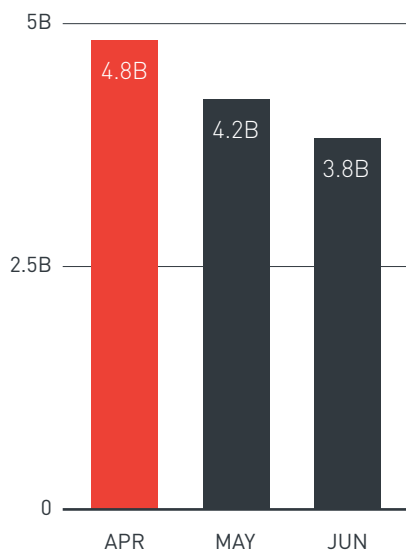
The overall Smart Protection Network numbers have been steadily declining since 2012. This could mean that cybercriminals and threat actors are veering away from a “strike anywhere” approach and so need not rely on victimizing masses to measure their success. Instead, they have been focusing on identifying the “right” targets, which often resulted in higher returns on investment (ROIs).

Total number of threats blocked (2012-1H 2015)



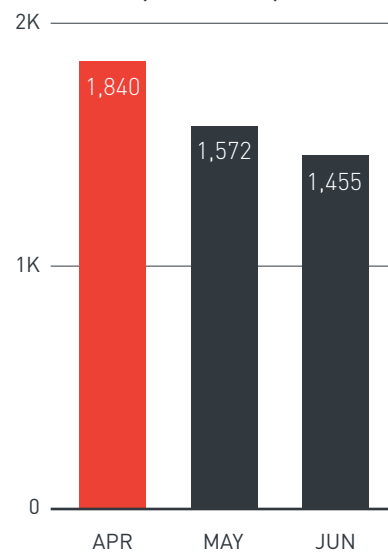
The number of threats detected by the Smart Protection Network declined by roughly 20% year over year.

Total number of threats blocked (2Q 2015)



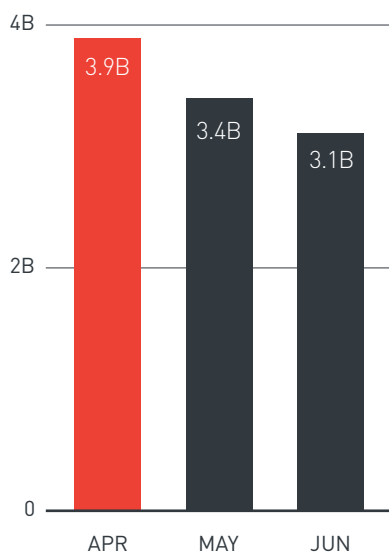
We blocked an average of 4.2 billion threats per month this quarter, indicating a slight decrease from the previous quarter's recorded average of 4.7 billion threats per month.

Trend Micro overall detection rate: Number of threats blocked per second (2Q 2015)



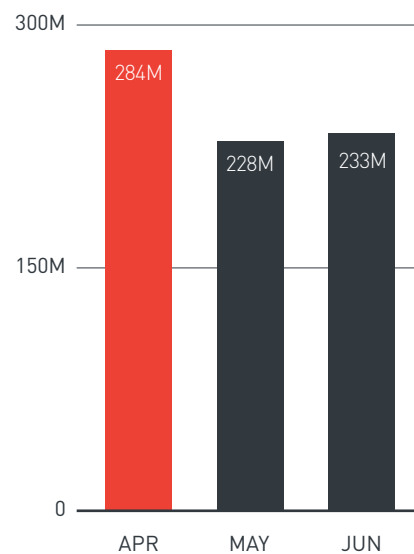
We blocked an average of 1,622 threats per second this quarter. This number decreased from the previous quarter's 1,800 threats per second.

Number of email reputation queries categorized as spam (2Q 2015)



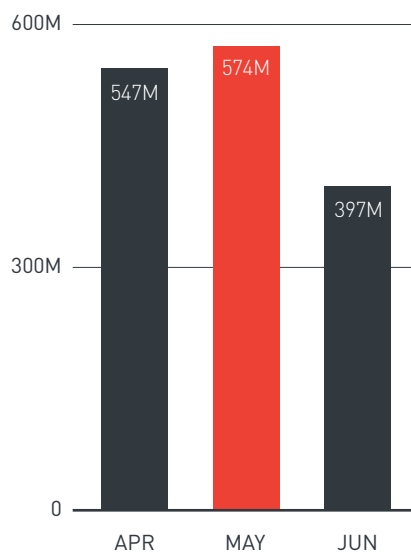
We prevented 10.5 billion emails from spam-sending IP addresses from reaching users' inboxes, indicating a rather significant decrease from the previous quarter's 12 billion emails. A possible cause for this decline is that spammers may be resorting to other messaging means, veering away from solely using email.

Number of user visits to malicious sites blocked (2Q 2015)



We blocked more than 745 million user visits to malicious sites this quarter, with numbers dropping from April to May then slightly increasing this June.

Number of malicious files blocked (2Q 2015)



We prevented more than a billion malicious files from infecting devices this quarter.

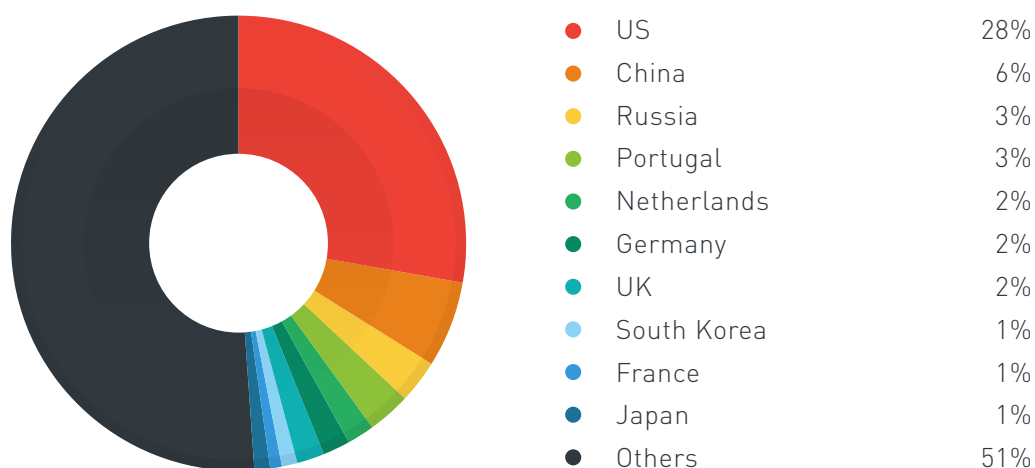
The number of malware dropped by 287 million from May to June.

Malicious domains users were prevented from visiting (2Q 2015)

Domain	Reason for blocking access to
sso.anbtr.com	Browser hijacker; dangerous
cnfg.toolbar-services.com	Browser hijacker; changes Web browsers' home and default search pages without user permission
jsgnr.eshopcomp.com	Displays lots of dangerous pop-up ads on-screen
initilizeinstall.net	Accesses several malware-laden sites
sp-storage.spccint.com	Site that malware communicate with
bugreport.yac.mx	Related to ADW_INCORE, which users unknowingly download when they visit malicious sites
checkver.dsiteproducts.com	Site that malware communicate with
reports.montiera.com	Site that malware communicate with
creative.ad120m.com	Distributes malicious and unwanted programs
log.data-url.com	Site that malware and other unwanted programs communicate with

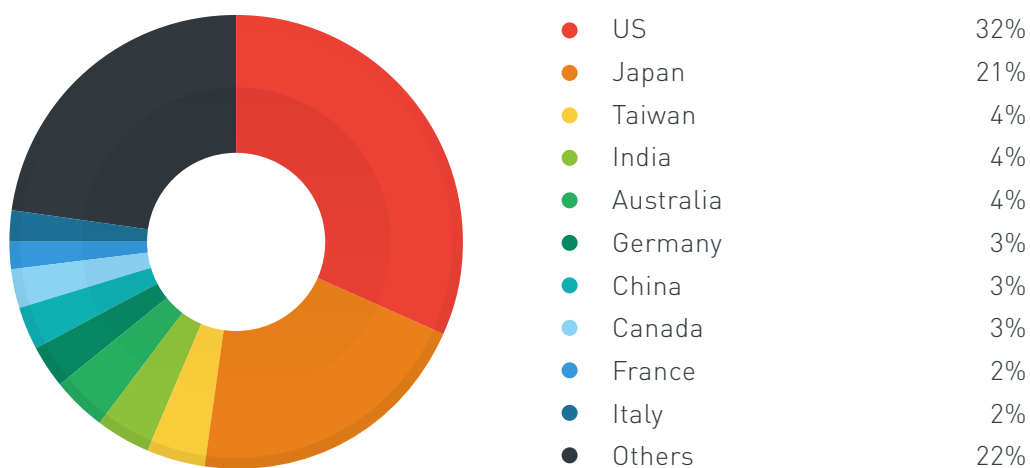
Browser hijackers made up the top most accessed malicious URLs.

Countries that hosted the highest number of malicious URLs (2Q 2015)



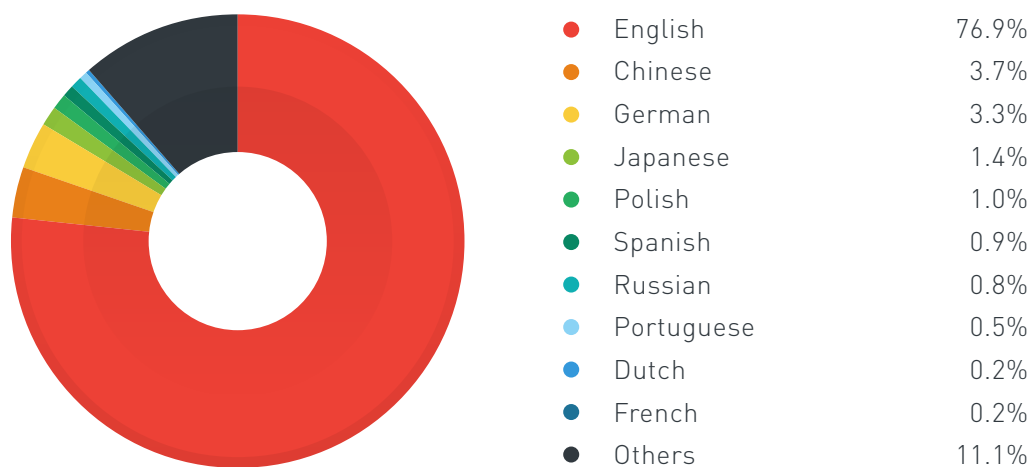
*The US continued to dominate the list of malicious-URL-hosting countries.
China and Russia, meanwhile, knocked the Netherlands off the top 3.*

Countries with the highest number of users who clicked malicious URLs (2Q 2015)



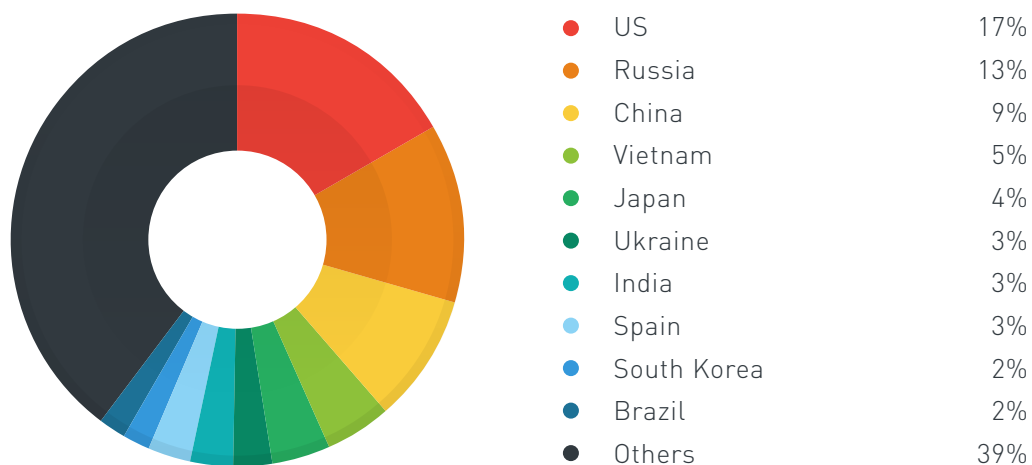
No significant changes were observed in the list of countries where most users who clicked malicious URLs were located.

Top spam languages (2Q 2015)



English remained the most-used spamming language. Chinese and German, meanwhile, gained much larger shares compared with previously recorded numbers.

Top spam-sending countries (2Q 2015)



The top 3 spam-sending countries stayed the same quarter over quarter.

Top malware families (2Q 2015)

Family	Volume
SALITY	88K
DOWNAD	77K
GAMARUE	58K
BROWSEVIEW	57K
DUNIH	47K
UPATRE	40K
DLOADR	40K
RAMNIT	39K
VIRUX	36K
ANDROM	29K

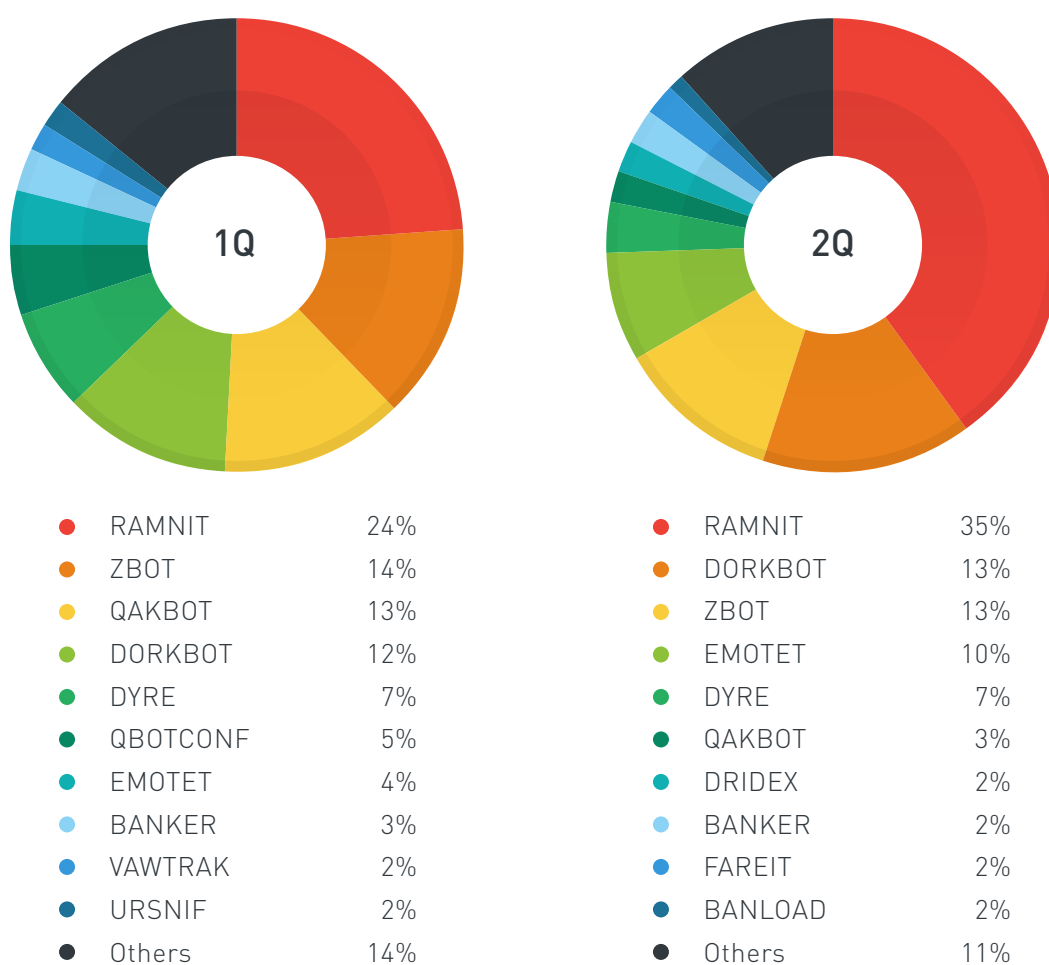
Top malware families by segment (2Q 2015)

Segment	Detection Name	Volume
Enterprise	DOWNAD	58K
	SALITY	33K
	DUNIH	28K
SMB	UPATRE	12K
	DLOADR	12K
	DOWNAD	11K
Consumer	GAMARUE	32K
	SALITY	31K
	VIRUX	17K

File infector, VIRUX, was a new addition to the top 3 malware affecting consumers this quarter. VIRUX spreads via removable drives and network shares.

Old online banking malware, EMOTET, continued to figure in highly localized operations in the past quarter. The number of EMOTET detections rose quarter over quarter, specifically affecting German users tricked into clicking a link embedded in supposed DHL notification emails.⁵⁷

Top 10 online banking malware families (1Q and 2Q 2015)



Top online banking malware, RAMNIT, steals sensitive information, including saved FTP credentials and browser cookies. It's primarily a file infector that infects even HTML files, hence the increase in its volume quarter over quarter.

Top adware families (2Q 2015)

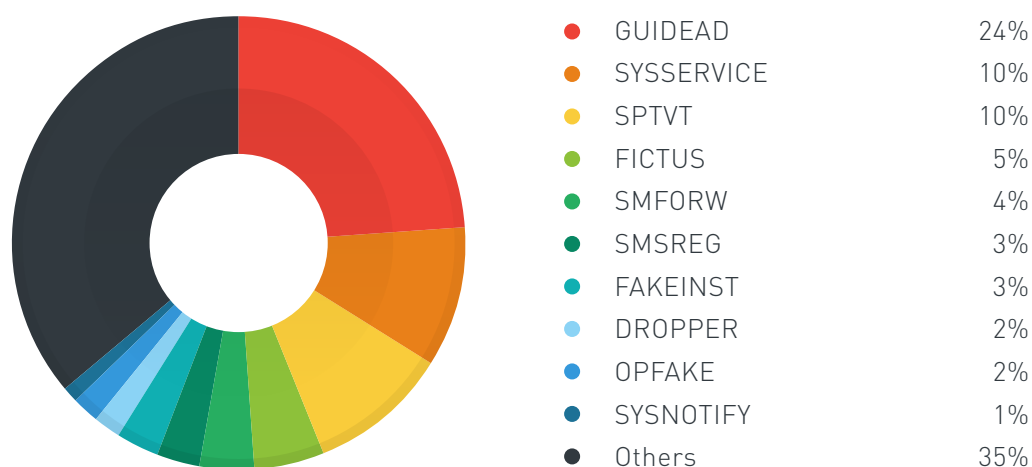
Family	Volume
OPENCANDY	423K
FAKEGOOG	208K
MYPCBACKUP	161K
ELEX	118K
CROSSRIDER	100K
DEALPLY	90K
SPROTECT	83K
MULTIPLUG	82K
TOMOS	78K
ADVSYSTEMPROTECTOR	76K

Top adware families by segment (2Q 2015)

Segment	Detection Name	Volume
Enterprise	OPENCANDY	50K
	FAKEGOOG	16K
	CROSSRIDER	15K
SMB	OPENCANDY	20K
	DEALPLY	7K
	FAKEGOOG	7K
Consumer	OPENCANDY	324K
	FAKEGOOG	161K
	MYPCBACKUP	122K

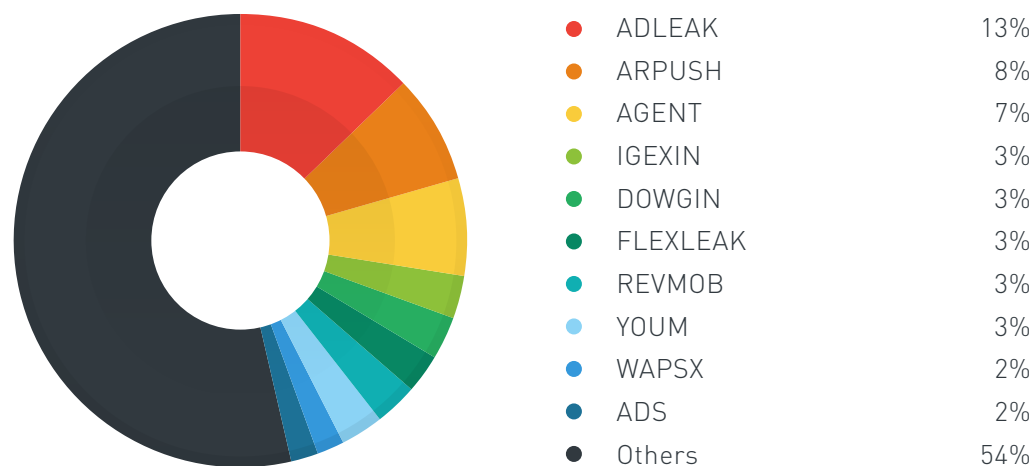
OPENCANDY and MYPCBACKUP come bundled with toolbars and other free software. The pop-up ads that they come with are, in general, annoying.

Top Android malware families (2Q 2015)



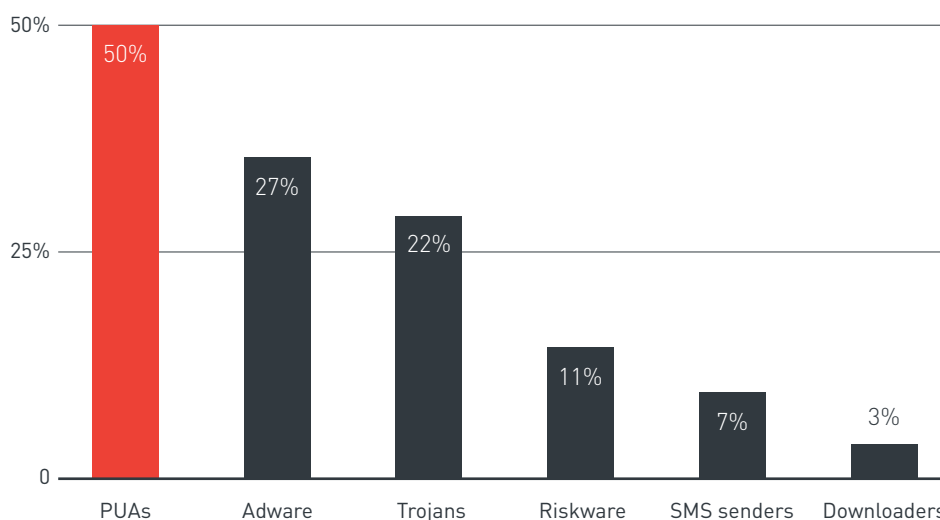
GUIDEAD variants don't have graphical user interfaces (GUIs) or icons. They just silently run in the background after installation.

Top Android adware families (2Q 2015)



As in the previous quarter, ADLEAK, a generic detection for apps that could put user privacy at risk, topped the list of adware.

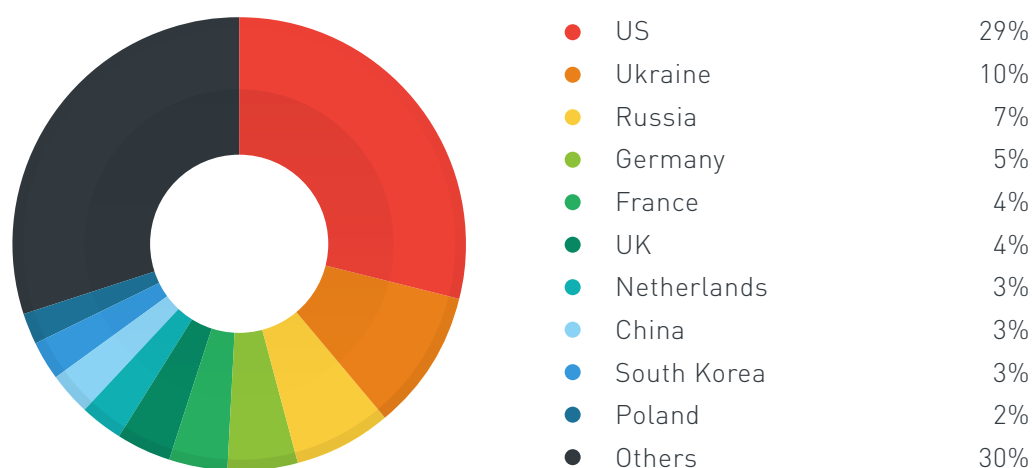
Top Android threat types seen (2Q 2015)



Half of the Android threats seen this quarter were potentially unwanted apps (PUAs). Riskware refer to apps that have functionality that can be used for malicious purposes.

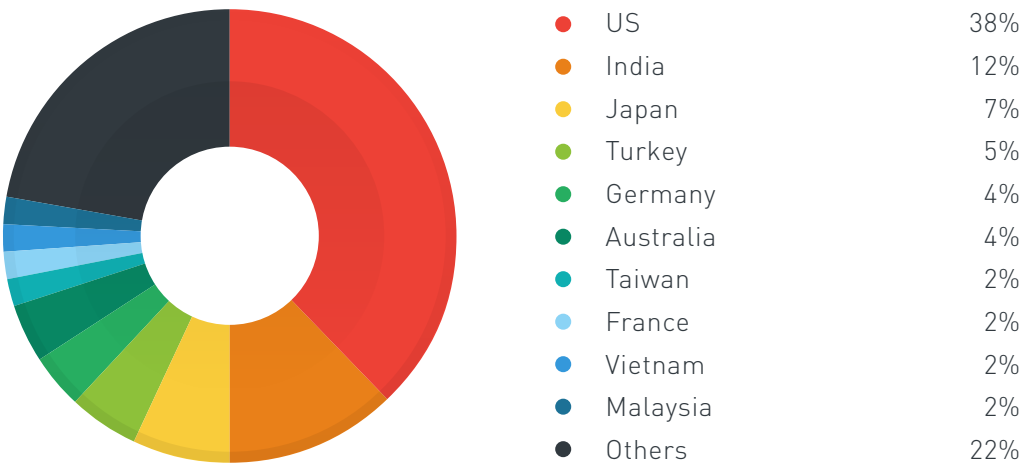
Note: A mobile threat family may exhibit the behaviors of more than one threat type.

Countries where the highest number of C&C servers were hosted (2Q 2015)



C&C servers were broadly distributed across countries like the US, the Ukraine, and Russia this quarter. Note that attackers don't necessarily have to reside in the same countries where their C&C servers are located, as these can be remotely manned. Most of the countries in the list above also figured as top malicious URL hosts, which could indicate hosting service and infrastructure abuse.

Countries with the highest number of C&C server connections (2Q 2015)



The US accounted for the highest number of C&C connections.

References

1. Evan Perez. (19 May 2015). *TrendLabs Security Intelligence Blog*. “FBI: Hacker Claimed to Have Taken Over Flight’s Engine Controls.” Last accessed on 28 July 2015, <http://edition.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/>.
2. Martin Rösler. (19 May 2015). *TrendLabs Security Intelligence Blog*. “Mile-High Hacking: Should You Worry?” Last accessed on 28 July 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/mile-high-hacking-should-you-worry/>.
3. Kim Zetter. (15 May 2015). *Wired*. “Feds Say That Banned Researcher Commandeered a Plane.” Last accessed on 28 July 2015, <http://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/>.
4. BBC. (21 June 2015). *BBC News*. “Polish LOT Aeroplanes Grounded by Computer Hack.” Last accessed on 28 July 2015, <http://www.bbc.com/news/world-europe-33219276>.
5. Jaydeep Dave. (20 May 2015). *TrendLabs Security Intelligence Blog*. “New Router Attack Displays Fake Warning Messages.” Last accessed on 28 July 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/new-router-attack-displays-fake-warning-messages/>.
6. Fernando Mercês. (28 May 2015). *TrendLabs Security Intelligence Blog*. “DNS Changer Malware Sets Sights on Home Routers.” Last accessed on 28 July 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/dns-changer-malware-sets-sights-on-home-routers/>.
7. Christopher Budd. (10 April 2015). *Trend Micro Simply Security*. “The TV5MONDE Attack: Four Hours That Changed the World.” Last accessed on 28 July 2015, <http://blog.trendmicro.com/the-tv5monde-attack-four-hours-that-changed-the-world/>.
8. Lord Alfred Remorin. (25 June 2015). *TrendLabs Security Intelligence Blog*. “Change of Supplier Fraud: How Cybercriminals Earned Millions Using a \$35 Malware.” Last accessed on 28 July 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/change-of-supplier-fraud-how-cybercriminals-earned-millions-using-a-35-malware/>.
9. Trend Micro. (26 May 2015). *TrendLabs Security Intelligence Blog*. “Attack of the Solo Cybercriminals—Frapstar in Canada.” Last accessed on 28 July 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/attack-of-the-solo-cybercriminals-frapstar-in-canada/>.
10. Trend Micro. (30 June 2015). *TrendLabs Security Intelligence Blog*. “Lordfenix: 20-Year-Old Brazilian Makes Profit Off Banking Malware.” Last accessed on 28 July 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/lordfenix-20-year-old-brazilian-makes-profit-off-banking-malware/>.
11. Trend Micro Senior Threat Researchers. (13 April 2015). *TrendLabs Security Intelligence Blog*. “One-Man PoS Malware Operation Captures 22,000 Credit Card Details in Brazil.” Last accessed on 28 July 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/fighterpos-fighting-a-new-pos-malware-family/>.
12. Peter Pi. (16 June 2015). *TrendLabs Security Intelligence Blog*. “Magnitude Exploit Kit Uses Newly Patched Adobe Vulnerability; US, Canada, and UK Are Most at Risk.” Last accessed on 28 July 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/magnitude-exploit-kit-uses-newly-patched-adobe-vulnerability-us-canada-and-uk-are-most-at-risk/>.
13. Paul Pajares. (1 July 2015). *TrendLabs Security Intelligence Blog*. “TorrentLocker Surges in the UK, More Social Engineering Lures Seen.” Last accessed on 28 July 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/torrentlocker-surges-in-the-uk-more-social-engineering-lures-seen/>.
14. Veo Zhang. (2 June 2015). *TrendLabs Security Intelligence Blog*. “Attack of the 90s Kids: Chinese Teens Take on the Mobile Ransomware Trade.” Last accessed on 28 July 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/attack-of-the-90s-kids-chinese-teens-take-on-the-mobile-ransomware-trade/>.
15. TrendLabs. (9 April 2015). *Trend Micro Security News*. “Beebone Botnet Takedown: Trend Micro Solutions.” Last accessed on 29 July 2015, <http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/151/beebone-botnet-takedown-trend-micro-solutions>.

16. Europol. (9 April 2015). *Europol*. “International Police Operation Targets Polymorphic Beebone Botnet.” Last accessed on 29 July 2015, <https://www.europol.europa.eu/content/international-police-operation-targets-polymorphic-beebone-botnet>.
17. US-CERT. (9 April 2015). *US-CERT*. “Alert (TA15-098A): AAHE.” Last accessed on 29 July 2015, <https://www.us-cert.gov/ncas/alerts/TA15-098A>.
18. INTERPOL. (13 April 2015). *INTERPOL*. “INTERPOL Coordinates Global Operation to Take Down SIMDA Botnet.” Last accessed on 29 July 2015, <http://www.interpol.int/News-and-media/News/2015/N2015-038>.
19. Trend Micro. (12 April 2015). *TrendLabs Security Intelligence Blog*. “SIMDA: A Botnet Takedown.” Last accessed on 29 July 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/simda-a-botnet-takedown/>.
20. Andy Greenberg. (4 February 2015). *Wired*. “Silk Road Mastermind Ross Ulbricht Convicted of All 7 Charges.” Last accessed on 29 July 2015, <http://www.wired.com/2015/02/silk-road-ross-ulbricht-verdict/>.
21. Sam Thielman. (29 May 2015). *The Guardian*. “Silk Road Operator Ross Ulbricht Sentenced to Life in Prison.” Last accessed on 29 July 2015, <http://www.theguardian.com/technology/2015/may/29/silk-road-ross-ulbricht-sentenced>.
22. Vincenzo Ciancaglini. (22 June 2015). *TrendLabs Security Intelligence Blog*. “Digging into the Deep Web.” Last accessed on 29 July 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/digging-into-the-deep-web/>.
23. TrendLabs. (5 June 2015). *Trend Micro Security News*. “The Patriot Act Revision: What Does It Mean to You?” Last accessed on 29 July 2015, <http://www.trendmicro.com/vinfo/us/security/news/online-privacy/patriot-act-revision-underway-what-does-it-mean-to-you>.
24. David Sancho. (18 June 2015). *TrendLabs Security Intelligence Blog*. “US Government, Wikipedia Go All-HTTPS. Should Site Owners Do It, Too?” Last accessed on 29 July 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/us-government-wikipedia-go-all-https-should-site-owners-do-it-too/>.
25. Warwick Ashford. (15 June 2015). *ComputerWeekly.com*. “EU Data Protection Regulation to Be Finalized by End of 2015.” Last accessed on 29 July 2015, <http://www.computerweekly.com/news/4500248164/EU-Data-Protection-Regulation-to-be-finalised-by-end-of-2015>.
26. TrendLabs. (5 June 2015). *Trend Micro Security News*. “US OPM Hack Exposes Data of 4 Million Federal Employees.” Last accessed on 29 July 2015, <http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/us-opm-hack-exposes-data-of-4-million-federal-employees>.
27. Ellen Nakashima. (9 July 2015). *The Washington Post*. “Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say.” Last accessed on 29 July 2015, <http://www.washingtonpost.com/blogs/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/>.
28. TrendLabs. (25 September 2014). *Trend Micro Security News*. “Utilizing Island Hopping in Targeted Attacks.” Last accessed on 29 July 2015, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/utilizing-island-hopping-in-targeted-attacks>.
29. Ashley Carmann. (13 July 2015). *SC Magazine*. “OPM Repercussions Might Never Be Fully Understood, Says Former White House Cybersecurity Advisor.” Last accessed on 31 July 2015, <http://www.scmagazine.com/opm-repercussions-might-never-be-fully-understood-says-former-white-house-cybersecurity-advisor/article/426140/>.
30. Christopher Budd. (27 May 2015). *Trend Micro Simply Security*. “The IRS Hack: What It Means and What It Means for You.” Last accessed on 29 July 2015, <http://blog.trendmicro.com/the-irs-hack-what-it-means-and-what-it-means-for-you/>.
31. Internal Revenue Service. (2 June 2015). *IRS*. “IRS Statement on the ‘Get Transcript’ Application.” Last accessed on 29 July 2015, <http://www.irs.gov/uac/Newsroom/IRS-Statement-on-the-Get-Transcript-Application>.
32. Reuters. (1 June 2015). *The Asahi Shimbun*. “Japan Pension System Hacked, 1.25 Million Cases of Personal Data Leaked.” Last accessed on 31 July 2015, http://ajw.asahi.com/article/behind_news/social_affairs/AJ201506010096.
33. Feike Hacquabord. (16 April 2015). *TrendLabs Security Intelligence Blog*. “Operation Pawn Storm Ramps Up Its Activities; Targets NATO, White House.” Last accessed on 29 July 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/operation-pawn-storm-ramps-up-its-activities-targets-nato-white-house/>.

34. Kervin Alintanahin. (May 2015). *Trend Micro Security Intelligence*. “Operation Tropic Trooper: Relying on Tried-and-Tested Flaws to Infiltrate Secret Keepers.” Last accessed on 29 July 2015, <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-tropic-trooper.pdf>.
35. TrendLabs. (14 May 2015). *Trend Micro Security News*. “How Operation Tropic Trooper Infiltrates Secret Keepers.” Last accessed on 29 July 2015, <http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-tropic-trooper-infiltrates-secret-keepers>.
36. Robert Abel. (17 June 2015). *SC Magazine*. “‘Lotus Blossom’ Cyber Attacks Hit Military, Government Targets in Southeast Asia.” Last accessed on 29 July 2015, <http://www.scmagazine.com/researchers-discover-50-cyber-attacks-in-lotus-blossom-campaign/article/421279/>.
37. Ming Yen Hsieh. (26 June 2015). *TrendLabs Security Intelligence Blog*. “The State of the ESILE/Lotus Blossom Campaign.” Last accessed on 29 July 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/the-state-of-the-esilelotus-blossom-campaign/>.
38. Karl Dominquez. (19 October 2011). *TrendLabs Security Intelligence Blog*. “Keeping Tabs on the Next STUXNET.” Last accessed on 29 July 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/keeping-tabs-on-the-next-stuxnet/>.
39. Jack Tang. (17 June 2015). *TrendLabs Security Intelligence Blog*. “Analysis of CVE-2015-2360—DUQU 2.0 Zero-Day Vulnerability.” Last accessed on 29 July 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/analysis-of-cve-2015-2360-duqu-2-0-zero-day-vulnerability/>.
40. Samuel Gibbs. (11 June 2015). *The Guardian*. “DUQU 2.0: Computer Virus ‘Linked to Israel’ Found at Iran Nuclear Talks Venue.” Last accessed on 29 July 2015, <http://www.theguardian.com/technology/2015/jun/11/duqu-2-0-computer-virus-with-traces-of-israeli-code-was-used-to-hack-iran-talks>.
41. Jay Yaneza. (4 May 2015). *TrendLabs Security Intelligence Blog*. “Macro Malware: When Old Tricks Still Work, Part 1.” Last accessed on 29 July 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/macro-malware-when-old-tricks-still-work-part-1/>.
42. Jay Yaneza. (7 May 2015). *TrendLabs Security Intelligence Blog*. “Macro Malware: When Old Tricks Still Work, Part 2.” Last accessed on 29 July 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/macro-malware-when-old-tricks-still-work-part-2/>.
43. TrendLabs. (1 July 2015). *Trend Micro Security News*. “eBay’s Magento E-Commerce Platform Hit by Payment Card Stealers.” Last accessed on 31 July 2015, <http://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/ebay-magento-ecommerce-platform-hit-by-payment-card-stealers>.
44. Charlie Osborne. (22 June 2015). *ZDNet*. “eBay Patches Input, XSS, CSRF Vulnerabilities in Magento E-Commerce Platform.” Last accessed on 31 July 2015, <http://www.zdnet.com/article/ebay-patches-input-xss-csrf-vulnerabilities-in-magento-e-commerce-platform/>.
45. Jaydeep Dave. (29 April 2015). *TrendLabs Security Intelligence Blog*. “WordPress Vulnerability Puts Millions of Sites at Risk; Trend Micro Solutions Available.” Last accessed on 31 July 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/wordpress-vulnerability-puts-millions-of-sites-at-risk-trend-micro-solutions-available/>.
46. NowSecure, Inc. (2015). *NowSecure*. “Samsung Keyboard Security Risk Disclosed: Over 600M+ Devices Worldwide Impacted.” Last accessed on 31 July 2015, <https://www.nowsecure.com/keyboard-vulnerability/>.
47. The MITRE Corporation. (2015). *CVE*. “CVE-2015-4640.” Last accessed on 31 July 2015, <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4640>.
48. The MITRE Corporation. (2015). *CVE*. “CVE-2015-4641.” Last accessed on 31 July 2015, <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4641>.
49. Trend Micro. (19 June 2015). *TrendLabs Security Intelligence Blog*. “The Samsung SwiftKey Vulnerability—What You Need to Know and How to Protect Yourself.” Last accessed on 31 July 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/the-samsung-swiftkey-vulnerability-what-you-need-to-know-and-how-to-protect-yourself/>.

50. Christopher Budd. (18 June 2015). *Trend Micro Simply Security*. “Unpatchable Android?” Last accessed on 31 July 2015, <http://blog.trendmicro.com/unpatchable-android/>.
51. Seven Shen. (27 May 2015). *TrendLabs Security Intelligence Blog*. “Trend Micro Discovers Apache Cordova Vulnerability that Allows One-Click Modification of Android Apps,” Last accessed on 30 July 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-discovers-apache-vulnerability-that-allows-one-click-modification-of-android-apps/>.
52. The MITRE Corporation. (2015). *CVE*. “CVE-2015-1835.” Last accessed on 31 July 2015, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1835>.
53. Dan Goodin. (18 June 2015). *Ars Technica*. “Serious OS X and iOS Flaws Let Hackers Steal Keychain, 1Password Contents.” Last accessed on 31 July 2015, <http://arstechnica.com/security/2015/06/serious-os-x-and-ios-flaws-let-hackers-steal-keychain-1password-contents/>.
54. The MITRE Corporation. (2015). *CVE*. “CVE-2015-1671.” Last accessed on 5 August 2015, <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1671>.
55. Brooks Li. (7 July 2015). *TrendLabs Security Intelligence Blog*. “Hacking Team Flash Zero Day Integrated into Exploit Kits.” Last accessed on 29 July 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-flash-zero-day-integrated-into-exploit-kits/>.
56. Peter Pi. (11 July 2015). *TrendLabs Security Intelligence Blog*. “Another Zero-Day Vulnerability Arises from Hacking Team Data Leak.” Last accessed on 29 July 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/another-zero-day-vulnerability-arises-from-hacking-team-data-leak/>.
57. Michael Angelo Casayuran. (19 May 2015). *Trend Micro Threat Encyclopedia*. “DHL Spam Arrives with EMOTET.” Last accessed on 4 August 2015, <http://www.trendmicro.com/vinfo/us/threat-encyclopedia/spam/3561/dhl-spam-arrives-with-emotet>.

Created by:

TrendLabs

The Global Technical Support and 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

SHARE:

