

Bad Ads and Zero Days: Reemerging Threats Challenge Trust in Supply Chains and Best Practices

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

Web Advertising Business Model Flaws Put User Security at Risk

11

Crypto-Ransomware Infection Volume Soared, Threatened Enterprises

17

Macro Malware, Old but Still Effective

21

Decade-Old FREAK Security Flaw Brought on Patch Management Challenges

26

Health Care Industry Suffered Massive Breaches, Other Industries Debilitated by PoS Malware Attacks

30

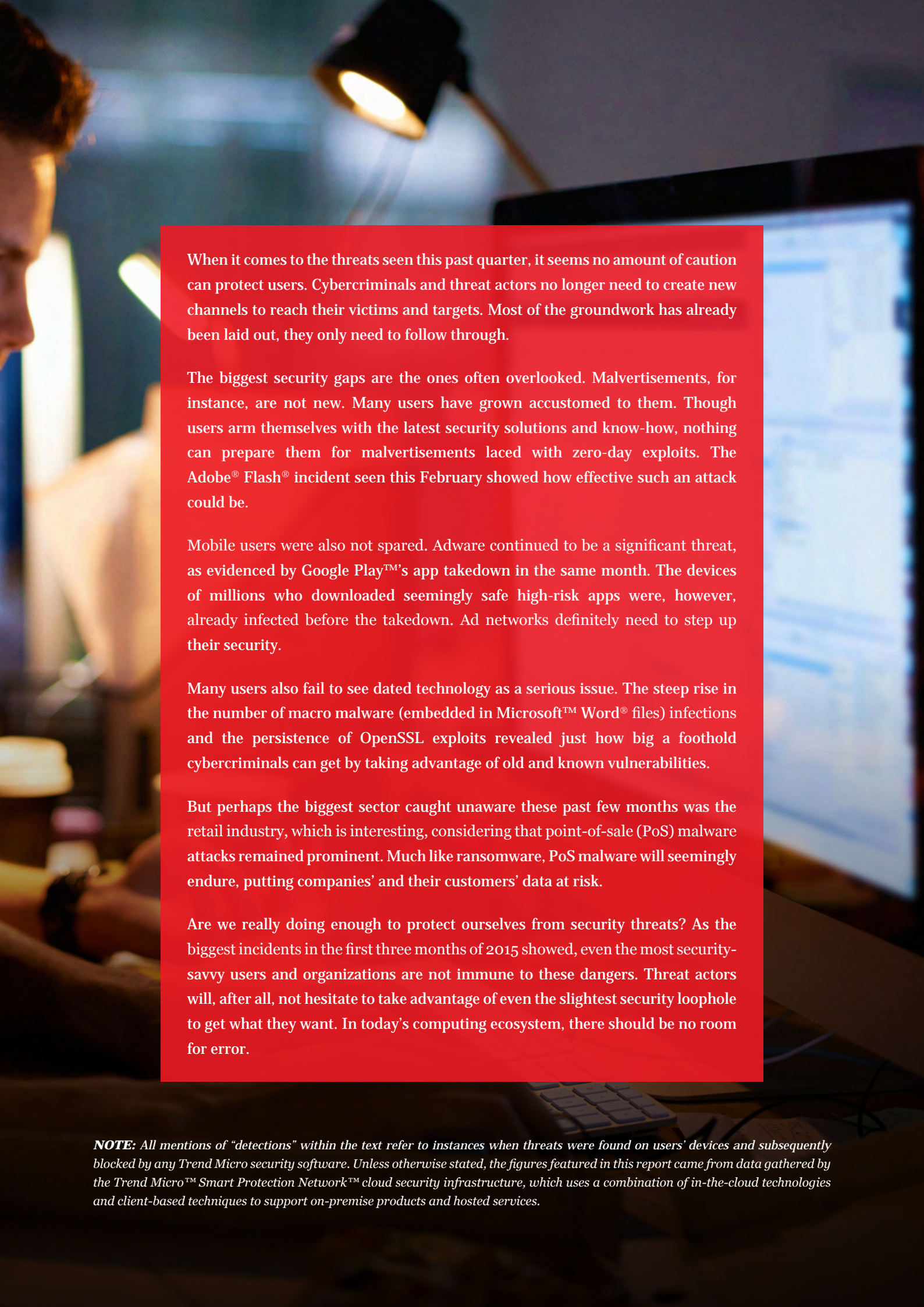
Old Threat Actors Reemerged with New Targeted Attack Campaign Tools, Tactics, and Procedures

32

Exploit Kits Continued to Grow in Sophistication

36

Threat Landscape in Review



When it comes to the threats seen this past quarter, it seems no amount of caution can protect users. Cybercriminals and threat actors no longer need to create new channels to reach their victims and targets. Most of the groundwork has already been laid out, they only need to follow through.

The biggest security gaps are the ones often overlooked. Malvertisements, for instance, are not new. Many users have grown accustomed to them. Though users arm themselves with the latest security solutions and know-how, nothing can prepare them for malvertisements laced with zero-day exploits. The Adobe® Flash® incident seen this February showed how effective such an attack could be.

Mobile users were also not spared. Adware continued to be a significant threat, as evidenced by Google Play™'s app takedown in the same month. The devices of millions who downloaded seemingly safe high-risk apps were, however, already infected before the takedown. Ad networks definitely need to step up their security.

Many users also fail to see dated technology as a serious issue. The steep rise in the number of macro malware (embedded in Microsoft™ Word® files) infections and the persistence of OpenSSL exploits revealed just how big a foothold cybercriminals can get by taking advantage of old and known vulnerabilities.

But perhaps the biggest sector caught unaware these past few months was the retail industry, which is interesting, considering that point-of-sale (PoS) malware attacks remained prominent. Much like ransomware, PoS malware will seemingly endure, putting companies' and their customers' data at risk.

Are we really doing enough to protect ourselves from security threats? As the biggest incidents in the first three months of 2015 showed, even the most security-savvy users and organizations are not immune to these dangers. Threat actors will, after all, not hesitate to take advantage of even the slightest security loophole to get what they want. In today's computing ecosystem, there should be no room for error.

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 software. 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.

Web Advertising Business Model Flaws Put User Security at Risk

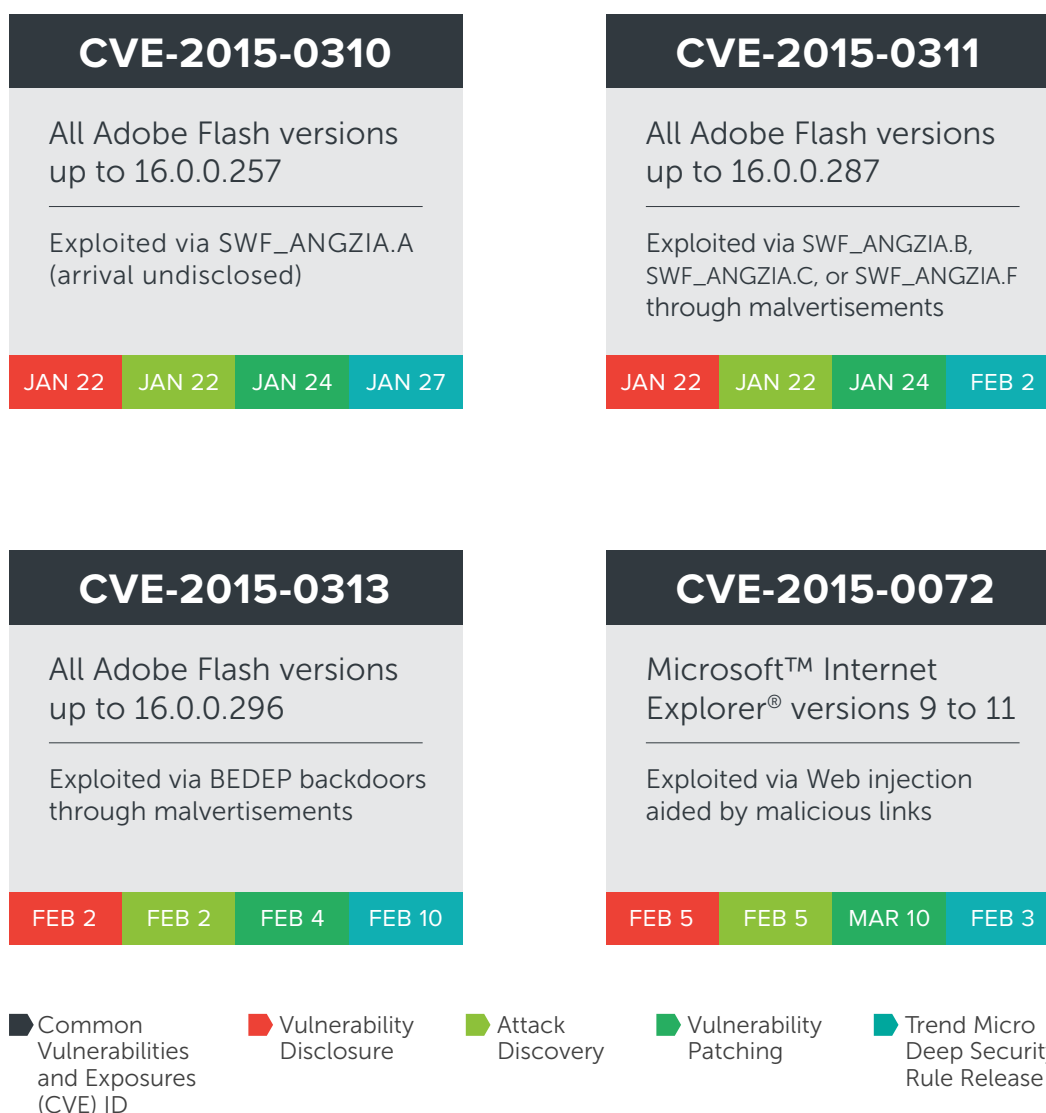
Online ads became a favored exploit carrier, most likely riding on the fact that users cannot control what ads they see. Site owners, like their visitors, also suffered, as they had no control over what ads were actually shown on their sites.

Zero-day exploits targeting Adobe software got a recent upgrade as they were used in malvertising attacks. An example of such an exploit (CVE-2015-0313), which has become part of the Angler Exploit Kit, was uncovered early this February. It used malvertisements and so no longer required victims to visit or stumble upon malicious pages to get their computers infected.

Recent malvertising attacks have become a more serious threat with the use of zero-day exploits. The malvertisement-zero-day combination undermined two of the most common security best practices today—only visiting trusted sites and keeping applications updated with the latest patches.

The online advertising industry, said a U.S. Senate Committee on Homeland Security and Governmental Affairs report, is tricky to navigate around. “The complexity of the online advertising industry makes it difficult to identify and hold accountable the entities responsible for damages resulting from malware attacks.”^{1, 2} Malvertising is a problem not only for end users but also site owners. Websites could also be laced with malicious advertisements without their owners’ consent or knowledge.

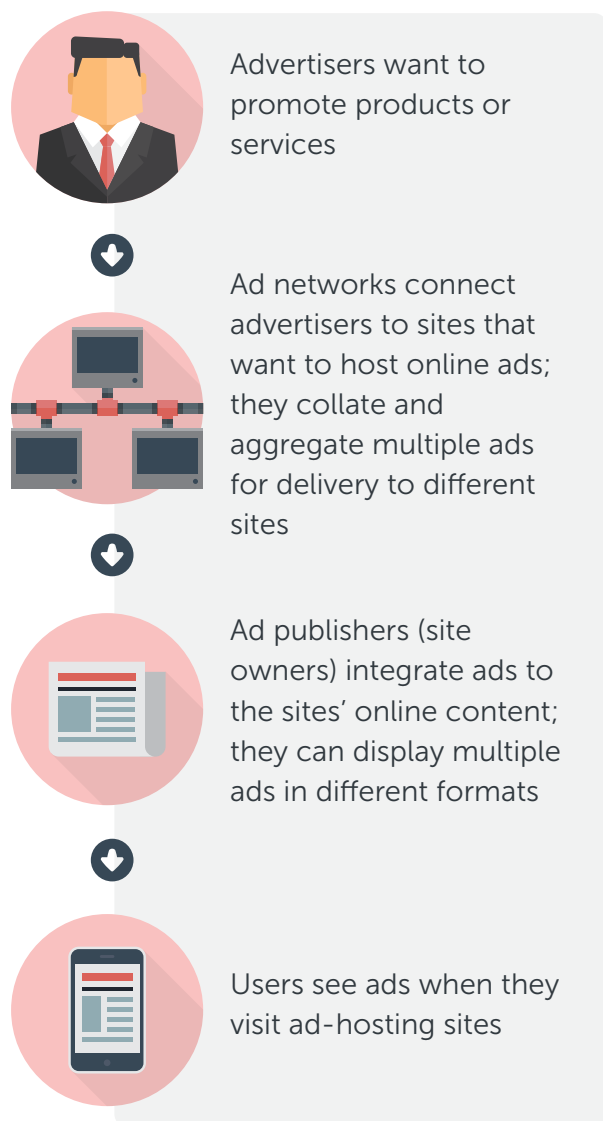
Notable Vulnerabilities in 1Q 2015



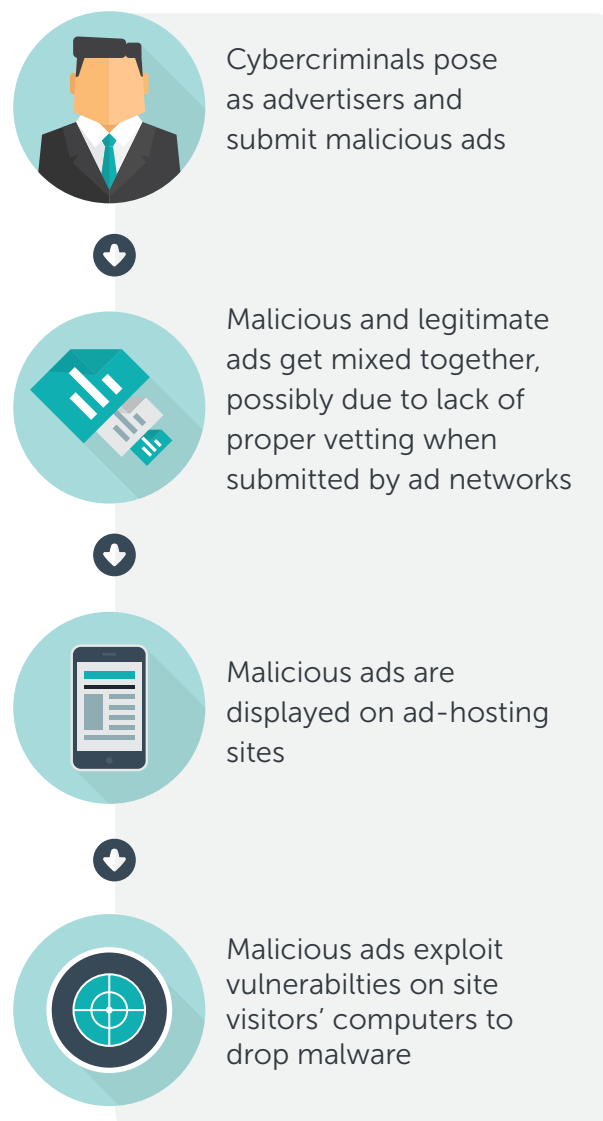
Out of the four zero-day exploits disclosed this past quarter, two used malvertisements as infection vector.

How Malvertising Works

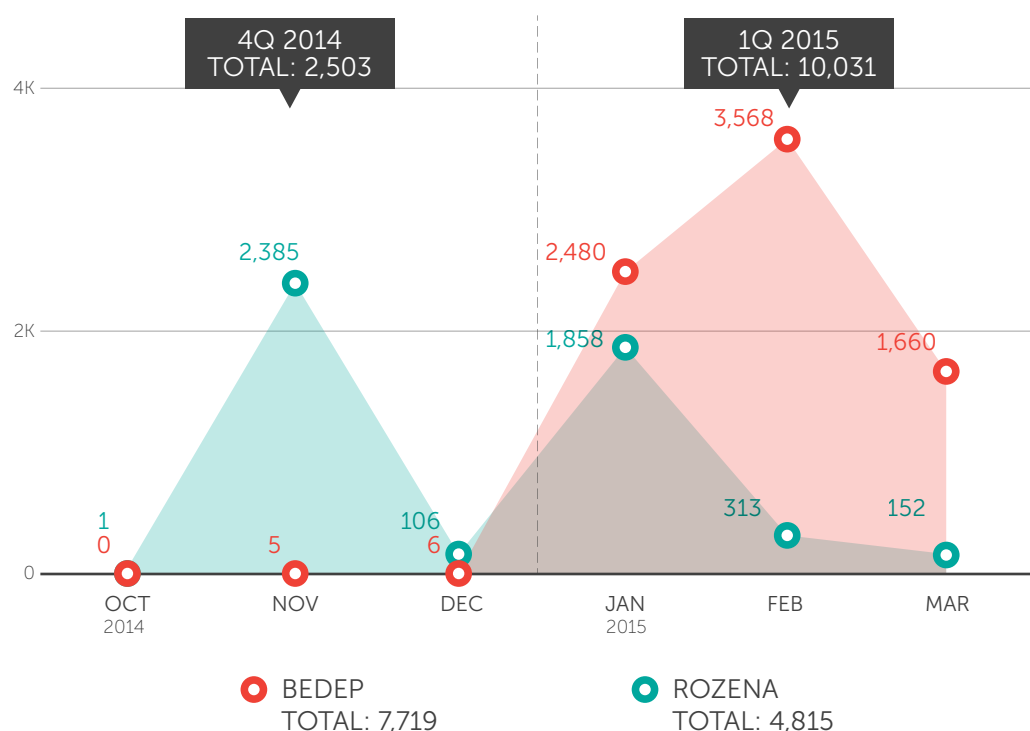
How Online Advertising Works



How Online Malvertising Works



Number of BEDEP and ROZENA Infections Distributed via Malvertisements from 4Q 2014 to 1Q 2015



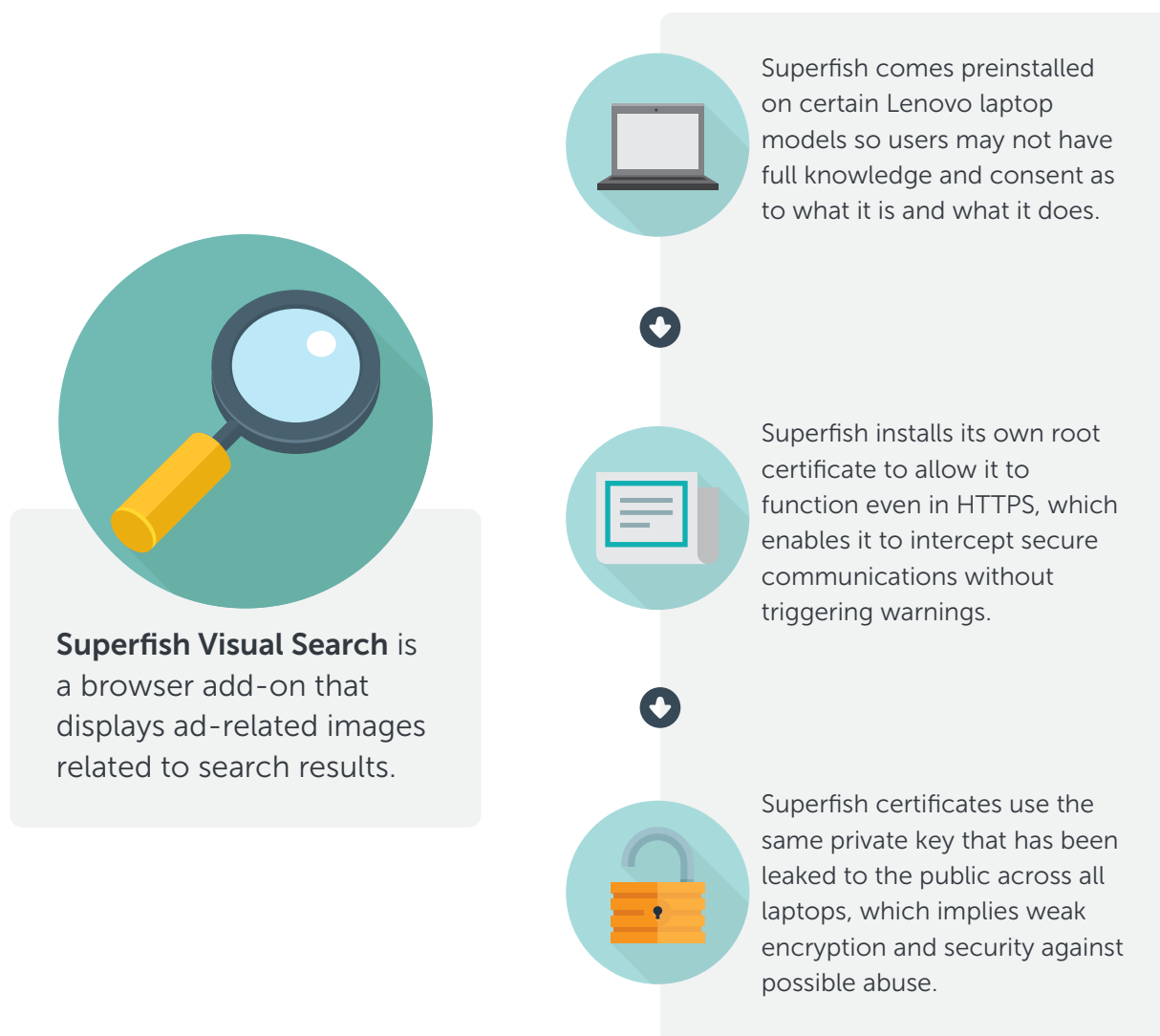
Malvertisements redirected victims to sites that automatically infected their computers with various kinds of malware.

A zero-day Adobe Flash exploit distributed via malvertisements spread BEDEP malware.³ Unwitting users who downloaded BEDEP malware were put at risk of becoming unwilling participants in attackers' botnet operations, apart from becoming fraud victims and downloading other malware.⁴

The advertising-related threats this quarter also included Superfish, a browser add-on that came preinstalled in at least 52 consumer-grade Lenovo®

laptop models shipped between September and December 2014.^{5, 6} Categorized as a piece of bloatware or unnecessary software that eat up a lot of disk space and come preinstalled in computers, Superfish had the capability to alter search results (displayed as images) based on users' browsing histories.⁷ It not only behaved like adware but also allowed cybercriminals to snoop in on supposedly secure communications.

How Does Superfish Work?



Apart from being preinstalled on computers and behaving like adware, Superfish posed a serious threat. Its weak certificate put even secure communications at great risk.

Adware did not only go after users, as several Google Play apps that used the MDash software development kit (SDK) also aggressively displayed harmful ads on all affected mobile devices.⁸ MDash (ANDROIDOS_ADM DASH.HRX) was said to have

infected millions of devices before apps laced with it were removed from Google Play. Over 2,000 apps sporting similar behaviors were also found on the store.

Number of MDash-Laced Apps Found on Google Play Before and After the Takedown



Around 2,000 MDash-laced apps were found on Google Play early this March, most of which were taken down within a month after the notification.

The threats seen this past quarter abused the online advertising platform to compromise users and site owners' data security. Malvertisements proved effective vehicles for zero-day exploits, as seen in the recent Adobe zero-day attacks. Superfish

put even supposedly secure communications in danger of landing in attackers' hands. And proving again that no device is safe from threats, attackers used MDash and similar apps to steal precious information from victims.

“For regular people, malvertisements represent one of the worst threats out there. More than any other threat, malvertisements can hurt people even when they’re doing all the right things. Malvertisements can affect people who don’t click links, have fully updated security solutions, and only go to trusted sites. In short, there’s no amount of caution that can protect you from malvertisements, just luck.”

—Christopher Budd,
Threat Communications Manager

“Users have steadily been moving away from exposing advertising materials in both online and traditional media. If the trend of advertising abuse continues, we can expect to see browser makers directly incorporate ad-blocking functionality to their products, which is only available as third-party plug-ins today. The only potential means to avert this sea of change is for advertising networks to step up their game when it comes to verifying the content they serve using prerelease sandboxing, for example, and effectively authenticating the sites they serve.”

—Rik Ferguson,
Vice President of Security Research

Crypto-Ransomware Infection Volume Soared, Threatened Enterprises

Crypto-ransomware expanded their target base, no longer just going after consumers but also trailing their sights on enterprises and niche user types.

Almost half of all ransomware infectors in the first quarter of 2015 have been classified as the more lethal type—crypto-ransomware. Today's more potent ransomware no longer just locked victims out of their computers like their Police Trojan

predecessors. Their more lethal descendants—crypto-ransomware—encrypted files held for ransom to ensure payment, putting users at greater risk.

Comparison of Known Crypto-Ransomware Variants

1 **GulCrypt** TROJ_GULCRYPT.A

Uses .RAR to password-protect archived files; password is PGP encrypted

Downloaded by TROJ_CRYPTOP.KLS along with other components

2 **Fud@india.com (Bandarchor)** TROJ_CRYPAURA.F

Uses old techniques though new variants are frequently released (targets more file types; switched from Russian to English ransom notes)

Distributed via spam and vulnerability exploitation

3 **CryptoFortress** TROJ_CRYPFORT.A

Mimics TorrentLocker's user interface (UI); extensively uses wildcards to search for filename extensions; encrypts files in network shares

Included in the Nuclear Exploit Kit

4 **TeslaCrypt** TROJ_CRYPAURA.F

Uses a UI similar to that of CryptoLocker; encrypts game-related files apart from documents

Included in the Angler Exploit Kit

5 **VaultCrypt** BAT_CRYPVAULT.A

Uses GnuPG to encrypt files; downloads hacking tools to steal browser-cached login credentials; uses *sDelete* 16 times to hinder victims from recovering files from backup; mostly targets Russians

Distributed via spam with a JavaScript™ downloader

6 **Troidesh** TROJ_CRYPSHED.A

Renames files to {*encoded filename*}.xtbl; steals IP addresses;

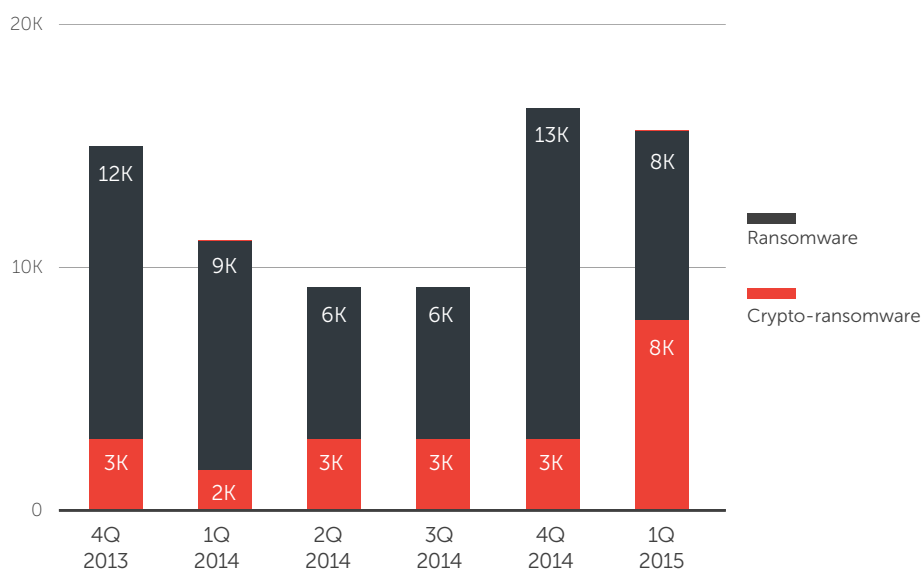
Included in the Nuclear Exploit Kit

FEATURES	1	2	3	4	5	6
New family?	Yes	No	Yes	Yes	Yes	Yes
Data stolen	Not applicable	Computer name and machine globally unique identifier (GUID)	Not applicable	IP address	Browser-cached login credentials using a hacking tool known as "Browser Password Dump by Security Xploded" (HKTL_BROWPASS)	IP address
C&C communication	No	Yes (to a hard-coded command-and-control [C&C] server)	No	Yes (via Tor2web)	Yes (via Onion City - Tor2web)	Yes (via Tor)
Ransom note filename	{user name}_.files	fud.bmp (as wallpaper)	READ IF YOU WANT YOUR FILES BACK.html	HELP_TO_SAVE_YOUR_FILES.txt; HELP_TO_SAVE_YOUR_FILES.bmp (as wallpaper)	VAULT.txt	README(1 to 10).txt
Extension name appended to encrypted files	.rar	.id-{id#}_fud@india.com*	.ftrss	.ecc	.VAULT	Renames files to {encoded filename}.xtbl
Deletes shadow copies?	No	No	Yes	Yes	Yes	No
Number of files targeted	11	102 (from 39 in older variants)	132+	185	15	342
Ransom asked for	€300	US\$500 worth of Bitcoins (BTC)	1 BTC	1.5 BTC (US\$1,000 if paying via PayPal)	US\$247 worth of BTC (increases after seven days)	Unknown since victims need to contact threat actors via email first; no reported ransom payers yet
Uses the Deep Web for payment sites	Mail2Tor (Tor email service)	No (via email)	Tor	Tor	Tor	No (via email)
Freemium features?	Yes (via email)	No	Yes	Yes	Yes	No

(* id# refers to the number that identifies victims during decryption transactions.)

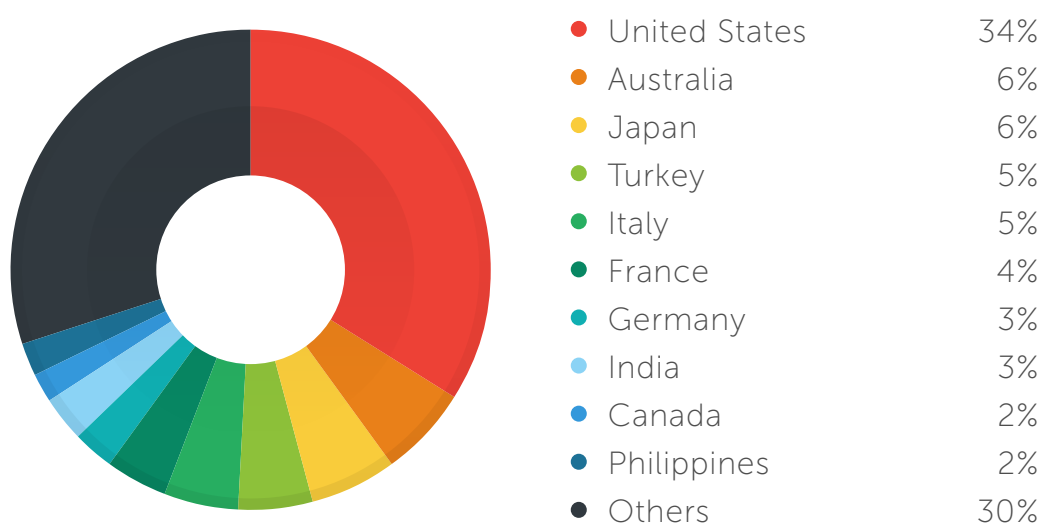
Six families were added to the growing list of notable crypto-ransomware, which sported varying levels of demand severity and sophistication.

Number of Ransomware Infections



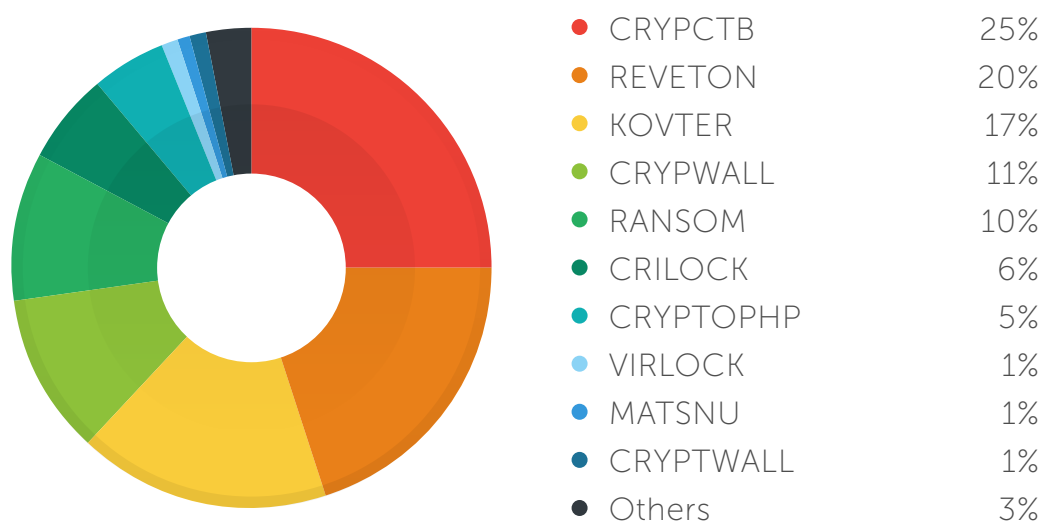
After declining in volume from the first to the third quarter of 2014, most likely due to the arrest of Blackhole Exploit Kit author (Paunch) toward the end of 2013, the ransomware volume regained steam before 2014 ended. (The Blackhole Exploit Kit was known for distributing ransomware.)

Countries That Posted the Highest Number of Ransomware Infections in 1Q 2015



The United States accounted for the bulk of ransomware infections, most likely due to the addition of new crypto-ransomware variants like CTB-Locker early this year, which targeted U.S. residents.

Top-Ranking Ransomware Families

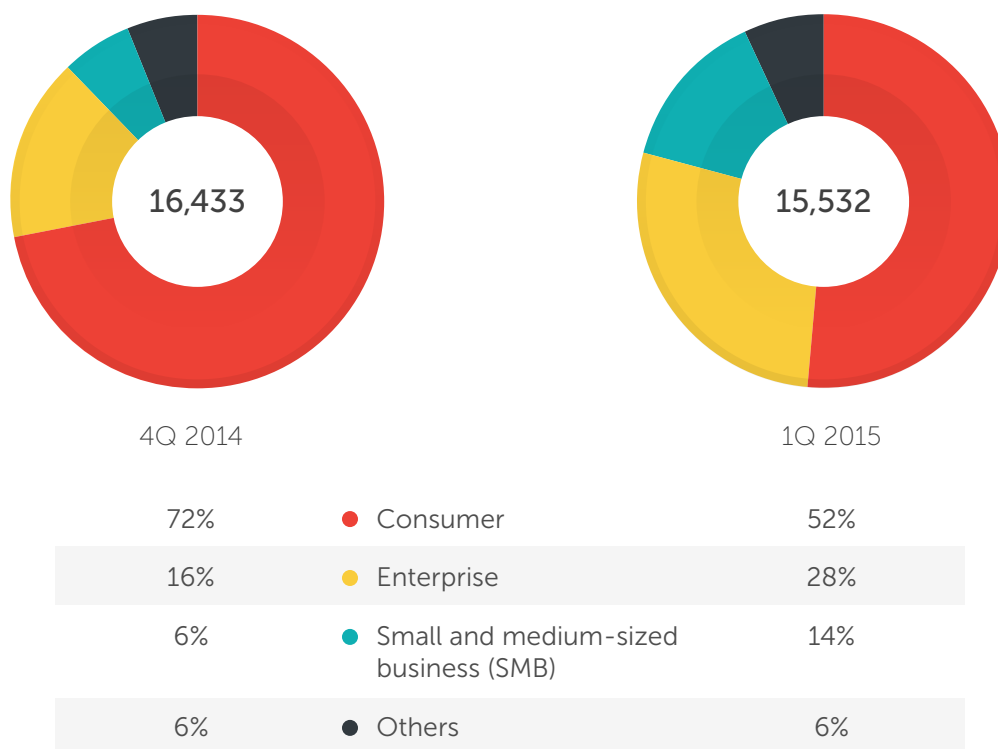


CRYPTCTB, which accounted for 25% of the entire ransomware pie, is the Trend Micro detection name for CTB-Locker variants, which plagued users in the first two months of this year.

Though Paunch's arrest in 2013 led to the decrease in the number of ransomware infections, the incident did not deter other cybercriminals from distributing more lethal variants of the threat.⁹ Users today are, in fact, being plagued by even more lethal ransomware variants.

Even more alarming though, ransomware no longer just threatened consumers but also enterprises. CryptoFortress, a CryptoLocker "copycat" (TROJ_CRYPTFORT.A), could encrypt files in shared folders.¹⁰ CRYPWEB, meanwhile, could encrypt Web server databases.¹¹ Enterprises need to take ransomware as a serious threat to their infrastructure and business.

Number of Ransomware Infections by Segment in 4Q 2014 and 1Q 2015



The number of ransomware infections affecting enterprises almost doubled this past quarter. This could be attributed to the increased number of ransomware targeting businesses as opposed to normal users.

Apart from enterprises, online gamers also joined the list of crypto-ransomware targets. Teslacrypt (TROJ_CRYPTESLA.A) could encrypt Steam® game and software data as well as documents, along with users' media and backup files.^{12, 13} Apart from targeting gamers, even police officers in Massachusetts have been duped into paying up to US\$500 in ransom just to regain access to their encrypted files.¹⁴

Users from Australia and New Zealand (ANZ) suffered from ransomware attacks as well. TorrentLocker attacks, as seen this January, inched their way from market to market. Other crypto-ransomware variants seen this past quarter also

showed marked improvements. CRYPURA, for instance, held a total of 102 file types for ransom, as opposed to its usual 39.

Ransomware can be likened to FAKEAV in that they scared practically anyone into paying the price to regain access to their computers and files. Time will tell whether ransomware will pose as many problems as FAKEAV did. Unlike FAKEAV though where user education proved very effective—as long as users ignored annoying pop-up messages, they stayed safe—the same cannot be said for ransomware. Ransomware do not leave users a choice. Their only hope is to be able restore ransomed files from secure backup locations.

“Crypto-ransomware provide a great means for cybercriminals to monetize attacks. Those behind the first variants earned millions of dollars in just a few months. The fact that ransomware can be easily turned into crypto-ransomware with the addition of crypto-libraries could have contributed to the threat’s growth. Crypto-algorithms are irreversible. Victims who don’t keep backups would then have no choice but to pay up to retrieve their important files.”

—Anthony Melgarejo,
Threat Response Engineer

Macro Malware, Old but Still Effective

The resurgence of macro malware could very well be cybercriminals' way of taking advantage of lack of user awareness. Very few users, after all, truly understand what macros are and how they work.

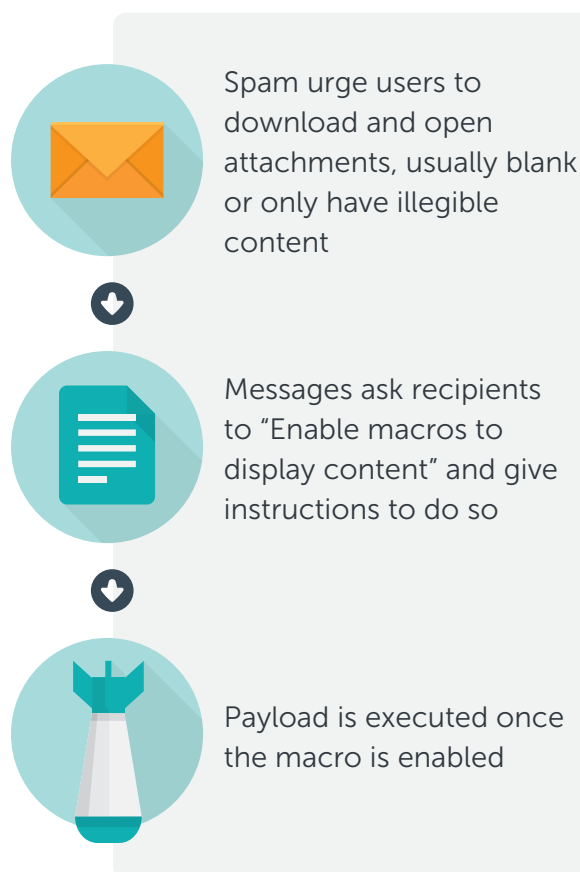
A resurgence of macro malware was seen toward the end of 2014, as evidenced by an increase in the number of spam with malicious-macro-laden attachments and the emergence of new variants. Macro malware often used key phrases and popular search terms to entice targets to download and run them.¹⁵ Even infamous banking malware, VAWTRAK, used malicious macros to infect computers, a far cry from its known arrival methods. It used spam that convinced recipients to enable macros in order to properly view specially crafted Word file attachments. Doing so executes macro malware (W2KM_VLOAD.A), which download VAWTRAK variants.¹⁶ Other threats that previously used macro malware as infection vector include data stealers, DRIDEX and ROVNIX.^{17, 18}

Cybercriminals could be relying on catching users unaware, hence the success of macro malware attacks. They took advantage of the fact that users do not have an idea what macros are and what they do. So when asked to enable macros to properly view attachments to very convincing spam, they do.

Macros are becoming more highly favored attack vectors due to their ability to bypass traditional antimalware solutions. Because running macro malware requires manual intervention, sandboxing technologies may not effectively thwart the threat. Users of email-scanning solutions may be less

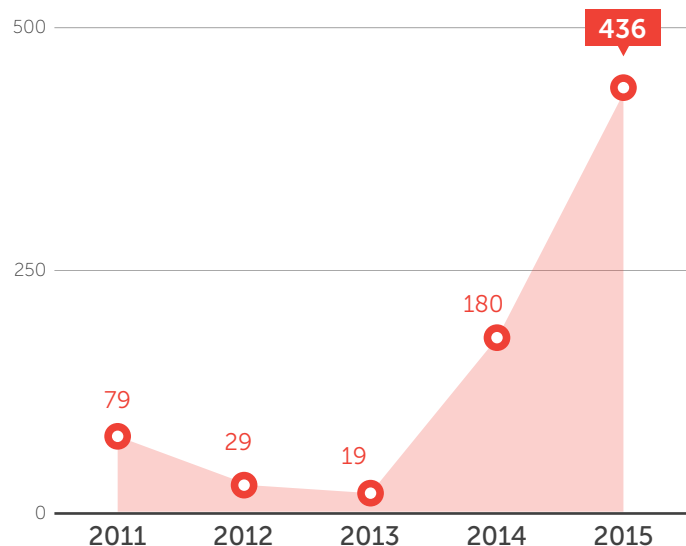
prone to macro malware infections, as these detect executables rather than scan for embedded malicious macros that can be easily obfuscated and thus remain unnoticed by antimalware solutions.

How Macro Malware Work



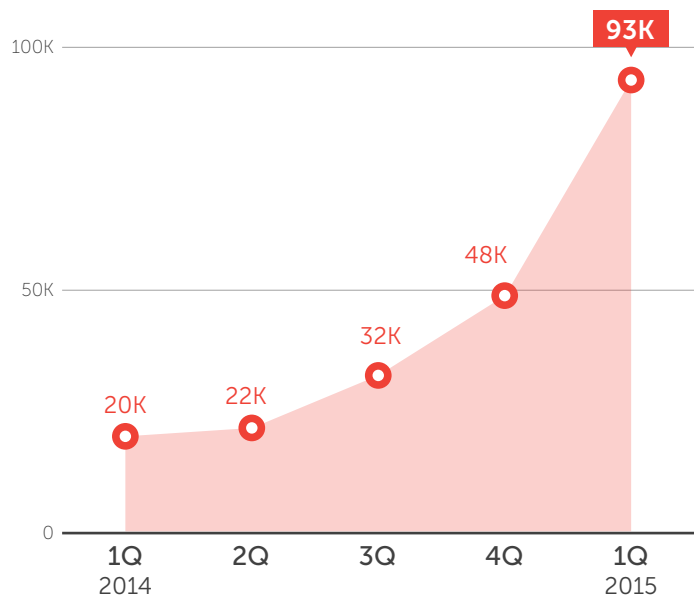
Social engineering played a big role in recent macro malware attacks. Users were tricked into enabling macros to properly view attachments without knowing they ran malicious routines in the background.

New Macro Malware Found as of 1Q 2015



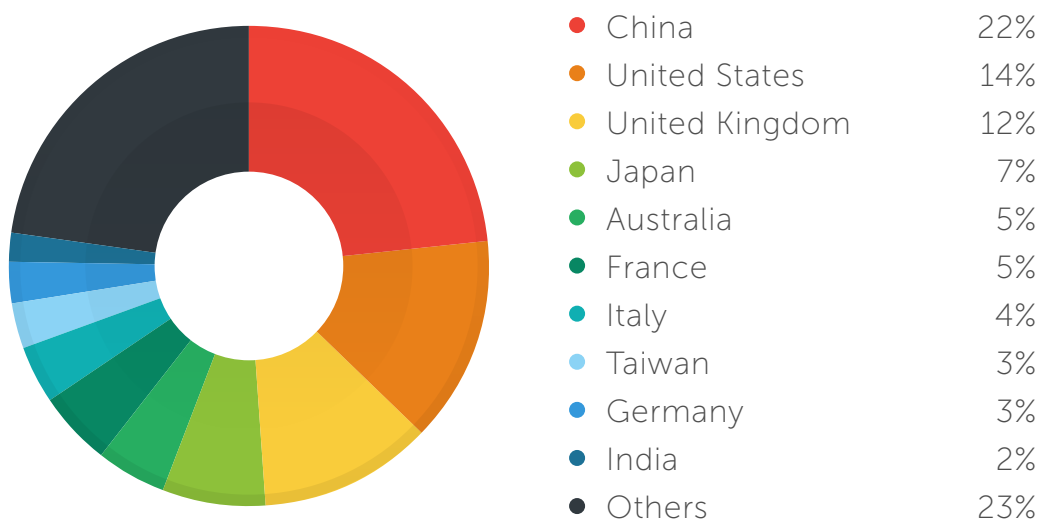
A resurgence of macro malware was seen since 2014. Even banking Trojan, VAWTRAK, has started using them.

Number of Macro Malware Infections as of 1Q 2015



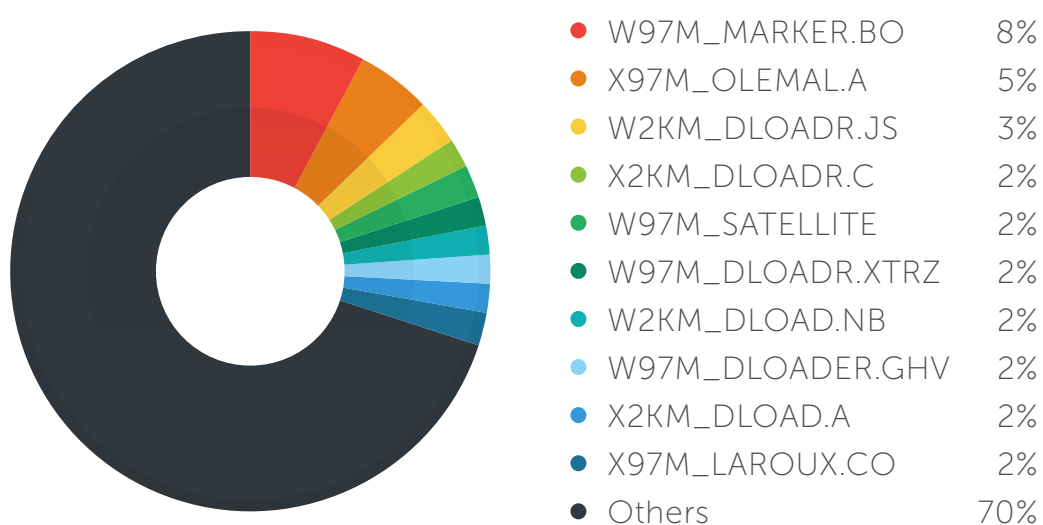
The number of macro malware infections has been constantly increasing since the first quarter of 2014. This could be attributed to the release of new variants and the rise in number of spam carrying malicious-macro-laden attachments.

Countries That Posted the Highest Number of Macro Malware Infections in 1Q 2015

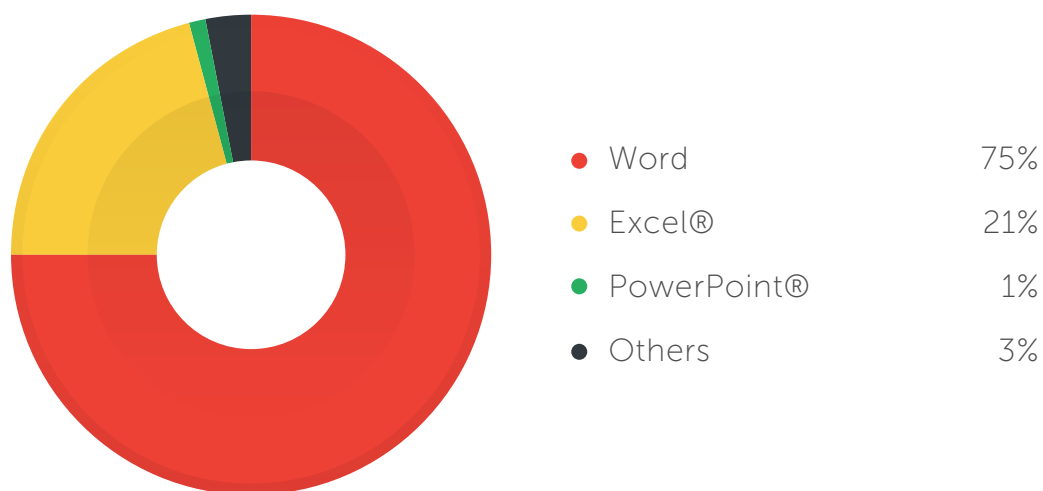


China topped the list of countries that posted the highest number of macro-malware-infected computers in the first three months of 2015. Though Microsoft has disabled macros by default on Office, users of older versions are still at risk.

Top-Ranking Macro Malware Variants in 1Q 2015

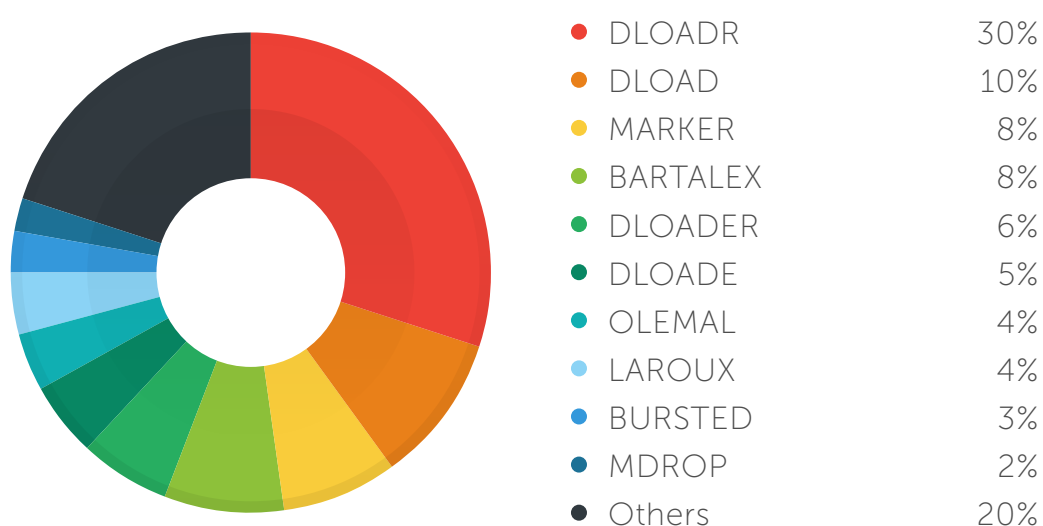


Applications Most Abused to Carry Malicious Macros in 1Q 2015



Microsoft Word documents and Excel spreadsheets proved to be cybercriminals' favorite malicious macro carriers.

Top-Ranking Macro Malware Families in 1Q 2015



Macro malware have become favored attack vectors because they can easily evade standalone antimalware solutions installed on most computers. The top-ranking macro malware families were downloaders, which could indicate that other malware use them as means to infect systems.

“Macro malware’s recent success could be attributed to their use of effective social engineering lures and the fact that they can be easily obfuscated. They are also normally embedded in Office files, which are treated more leniently by malware-scanning solutions. Even worse, macros can be enabled via batch and script files, which also evade antimalware detection.”

—**Anthony Melgarejo,**
Threat Response Engineer

Decade-Old FREAK Security Flaw Brought on Patch Management Challenges

FREAK and GHOST spooked users of vulnerable computers and applications. These brought about out-of-cycle patch management challenges for IT administrators, owing to the variety of platforms and devices that need to be secured. More exploitable flaws across platforms and devices are expected to surface as the year progresses.

FREAK, short for “Factoring RSA Export Keys,” a vulnerability that forces affected secure sites and applications to use weaker encryption, was discovered this March. All OpenSSL versions released prior to 1.0.1k and Apple Transport Layer

Security (TLS)/Secure Sockets Layer (SSL) clients were found vulnerable to man-in-the-middle (MiTM) attacks.¹⁹ Affected Windows® users were put at risk of having their confidential data stolen.²⁰

	Currently Vulnerable	Change Since March 3
HTTPS servers in Alexa’s top 1M domain names	8.5%	Down from 9.6%
HTTPS servers with browser-trusted certificates	6.5%	Down from 36.7%
All HTTPS servers	11.8%	Down from 26.3%

The number of servers affected by the FREAK vulnerability has decreased since the flaw’s discovery this March.²¹

GHOST, a buffer overflow vulnerability in Linux™ (glibc or the GNU C Library versions prior to 2.2) also surfaced this January. The flaw is triggered by calling certain functions in glibc that allow the execution of arbitrary code. Fortunately, it is not easy to exploit and can affect a very small number of systems.²²

Similar to client- and server-side vulnerabilities, Web application flaws need to be patched before they are abused. These can, after all, put business-

relevant data stored in possibly vulnerable back-end databases at risk.

Trend Micro Deep Security data revealed that cross-site scripting (XSS) and SQL injection attacks were used most to target Web applications in corporate servers. Open Web Application Security Project (OWASP) data supports this finding.

Top Web Application Vulnerabilities Found in 1Q 2015

SQL Injection Presents serious threats to any database-driven Web application; stems from insufficient or nonvalidated inputs passed on by users via affected Web applications to database servers in the form of SQL commands; can allow attackers to read, modify, add to, or delete data from databases, which can have disastrous consequences	CRITICAL
Nonpersistent XSS Allows attackers to inject malicious scripts (generally client side) into Web applications; XSS takes advantage of applications that do not validate, filter, or encode user-supplied data; often involves tricking victims into clicking legitimate-looking links that in reality provide additional data to launch attacks	HIGH
Path Traversal Exploits insufficient security validation in Web applications so attackers can access files from restricted system paths by navigating servers' file systems; also known as "dot dot slash" or "directory traversal" attacks	
Possible sensitive resource found Allows attackers to obtain information on resources that may or may not be linked to applications' structure like old backup, server configuration, server or database log, database configuration, database dump, or sensitive application files in order to carry out more sophisticated attacks	
Directory indexing Affects Web servers that display the index page of their virtual directory or subdirectory when accessed by user agents; allows attackers to mount further attacks by analyzing vulnerable Web applications' directory structure and content or gain unauthorized access to directory files	MEDIUM
Detailed application error messages Allows attackers to gain access to sensitive information, including internal Web application logic, packaged with HTML codes that users see when Web application errors or exceptions occur	
Sensitive form data transmitted without SSL Allows attackers to obtain sensitive data transmitted via applications that do not use SSL	
Include file source code disclosure Allows attackers to gain access to and abuse sensitive application logic information found in source codes	LOW
Local path disclosure Caused by the generation of unexpected outputs; Web applications that disclose local paths may give attackers an idea on webroot folders and such that they can use to craft customized attacks in order to access internal system files	
Internal IP address leaked Can disclose information about internal networks' IP-addressing scheme that can be used to craft customized attacks	

Nonpersistent XSS is the most common Web application vulnerability. According to OWASP, "XSS flaws occur whenever an application takes untrusted data and sends it to a Web browser without proper validation." This could allow attackers to execute malicious scripts by tricking users into clicking specially crafted links.

Deep Security data also revealed that PHP server vulnerabilities were most prevalent among organizations. In fact, all 10 top server vulnerabilities had ties to PHP server-side scripting language designed for Web development

and sometimes as a general-purpose programming language. Most of these vulnerabilities, rated “high” to “critical,” have been patched in the latest PHP versions.

Top Platform Vulnerabilities Found in 1Q 2015

CVE ID	Severity Rating	Affected Software	Description	Solution
CVE-2012-2688	Critical	PHP	Unspecified	Upgrade to PHP 5.3.15 or 5.4.5 or later
CVE-2012-2376	Critical	PHP	Allows attackers to execute arbitrary code	Patches or upgrades have yet to be released to address this
CVE-2011-3268	Critical	PHP	Allows attackers to execute arbitrary code or crash affected applications	Upgrade to PHP 5.3.7 or later
CVE-2014-9427	High	PHP	Allows attackers to crash affected applications, obtain sensitive information from the php-cgi process memory, or trigger unexpected code execution	Contact application vendors for information on fixing this flaw
CVE-2013-1635	High	PHP	Allows attackers to bypass intended access restrictions	Upgrade to PHP 5.3.22 or 5.4.13 or later
CVE-2011-1092	High	PHP	Allows attackers to crash affected applications	Upgrade to PHP 5.3.6 or later
CVE-2012-1823	High	PHP	Allows attackers to execute arbitrary code	Upgrade to PHP 5.4.2 or later
CVE-2012-2311	High	PHP	Allows attackers to execute arbitrary code	Upgrade to PHP 5.3.13 or 5.4.3 or later
CVE-2012-2386	High	PHP	Allows attackers to crash affected applications	Upgrade to PHP 5.3.14 or 5.4.4 or later
CVE-2011-1153	High	PHP	Allows attackers to obtain sensitive information and stage denial-of-service (DoS) attacks	Upgrade to PHP 5.3.6 or later

PHP was the most vulnerable platform this past quarter, as flaws were discovered in different versions of the scripting language. Users and IT administrators alike should keep their applications updated with the latest patches or upgrade to the latest versions. Note that Deep Security has solutions in place to address related vulnerabilities.

As more and more vulnerabilities in open source OSs and applications are discovered, IT administrators will find it increasingly difficult to mitigate risks associated with them. A major

underlying issue could be the lack of direct accountability in disclosing or patching flaws, adding to the challenge of securing all potentially vulnerable OSs and applications.

“The FREAK attack was yet another reminder that no matter how secure we think our systems and networks are, there’s always something new to discover. Legacy systems should be upgraded as much as possible. Companies must retain the source codes of custom applications that vendors build for them. Like Heartbleed, FREAK should reiterate the fragility of OpenSSL. It’s an outdated technology and must be replaced with much better encryption libraries. Organizations that rely on open source software and libraries must review and tighten their security policies. They should use security solutions that assess IP and domain reputation, monitor network traffic via breach detection systems, and use intrusion prevention to block known and unknown threats, among others.”

—Pawan Kinger,
Director of Deep Security Labs

Health Care Industry Suffered Massive Breaches, Other Industries Debilitated by PoS Malware Attacks

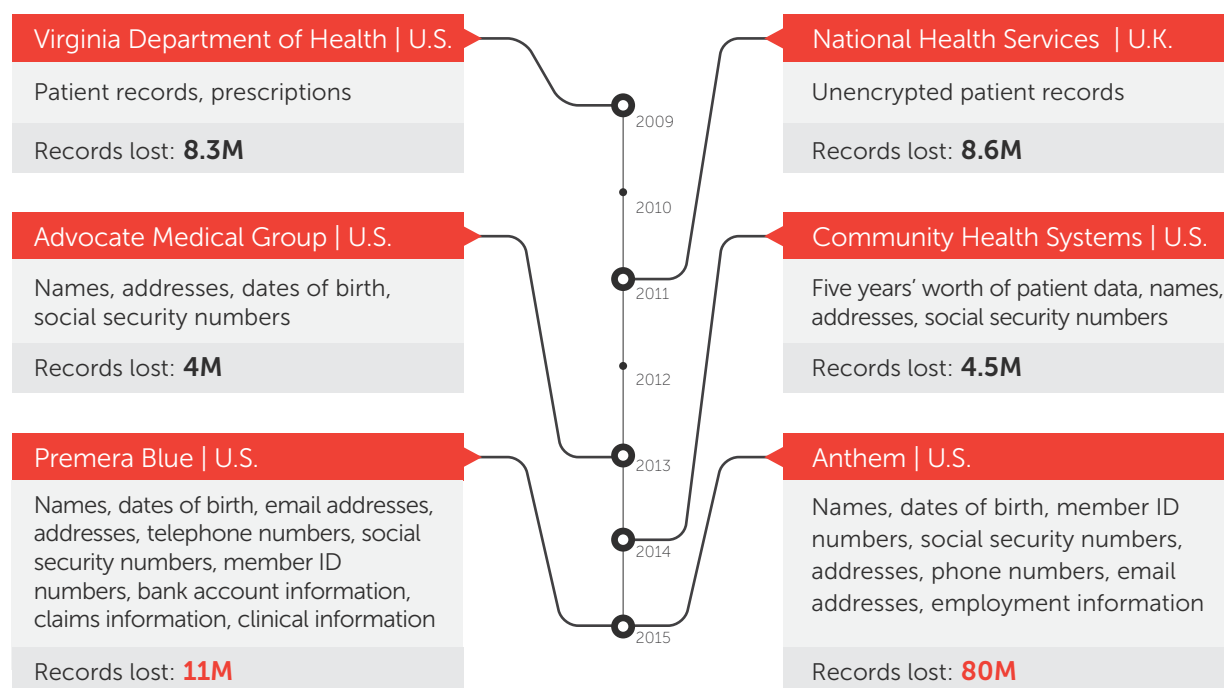
Lax security and failure to use best-of-breed solutions despite the massive amount of confidential data stored in health care service providers' networks could be the main reasons why they have become favored attack targets.

Major health care service providers, Premera Blue Cross and Anthem, suffered data breaches that exposed millions of their customers' financial and medical records this March.²³ The Anthem breach reportedly affected 80 million of its customers and employees.²⁴ An attack on Premera Blue Cross that was discovered this January, meanwhile, exposed the records of 11 million of its customers. Both data

breaches ousted NHS, which exposed more than 8.6 million of its records, from being the worst-hit health care service provider since 2011.²⁵

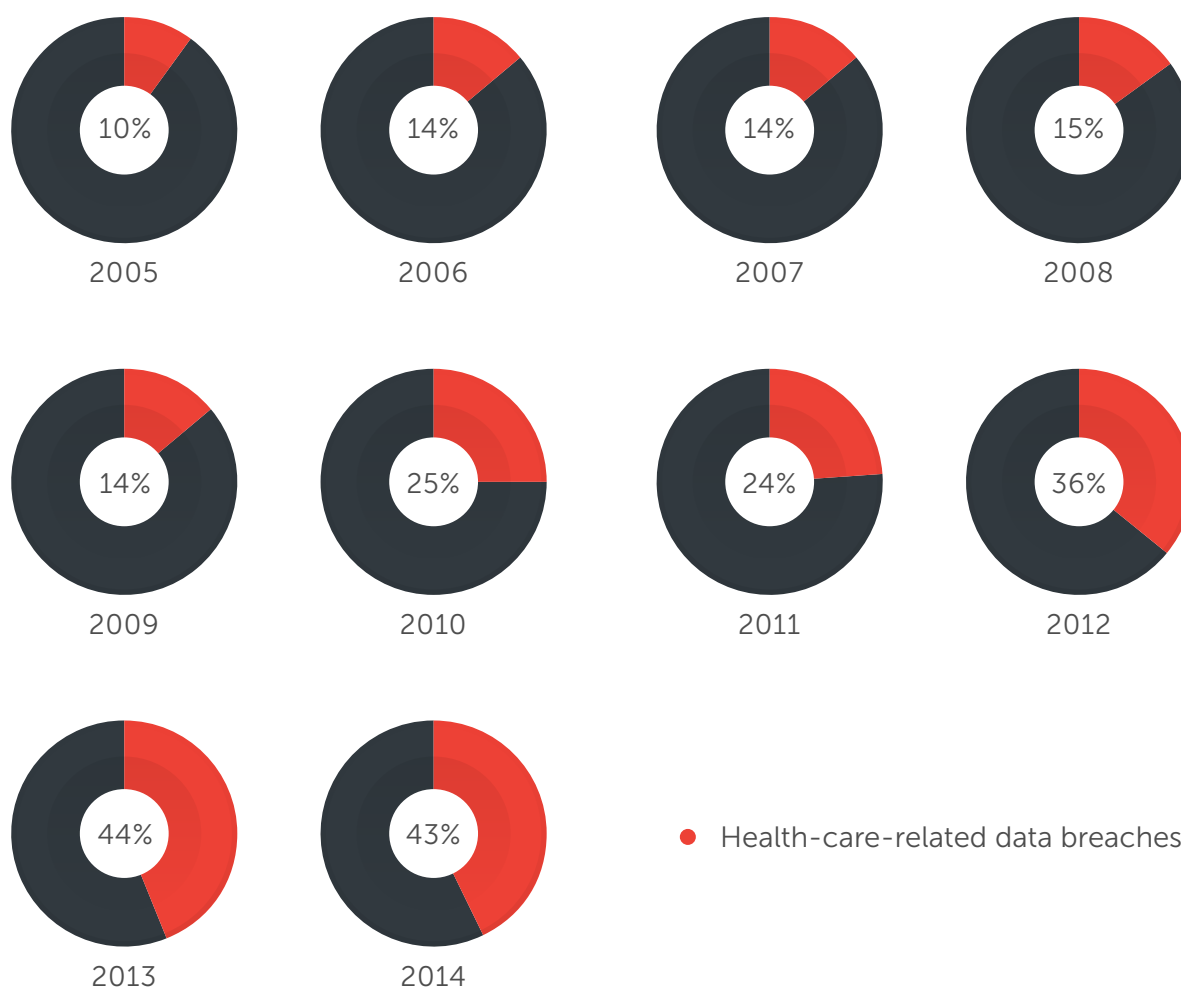
Health care service providers hold more information on customers than any other type of organization but do not necessarily use the most effective means to secure their data.²⁶

Most Notable Health Care Service Provider Data Breach Attacks from 2009 to 2015



The Anthem and Premera data breaches, both discovered early this year, have been the worst found to date.²⁷ The last breach of this type was seen in 2011 when laptops that may have contained unencrypted patient records were stolen from NHS. (Note: Coverage was limited to organizations that lost at least 4 million records.)

How Many of the Data Breaches Seen from 2005 to 2014 Were Health Care Related?

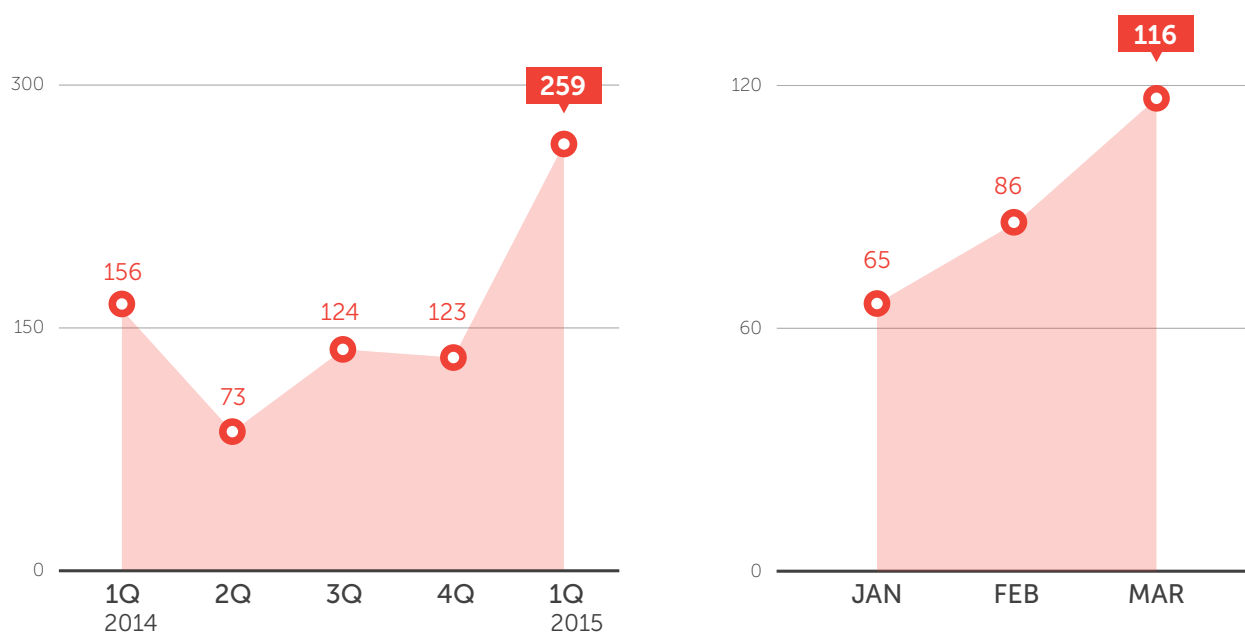


The number of health care service provider breach victims has grown almost fourfold in 2014 from 2005. The health care industry even suffered more than the business and military and government sectors between 2012 and 2014.²⁸

In the retail and service industry, PoS RAM scrapers continued to increase in number. Weak PoS system security allowed RAM scrapers to become viable means to breach networks though not necessarily to stage targeted attacks. PoS malware provided attackers instant gratification in the form of huge profits.

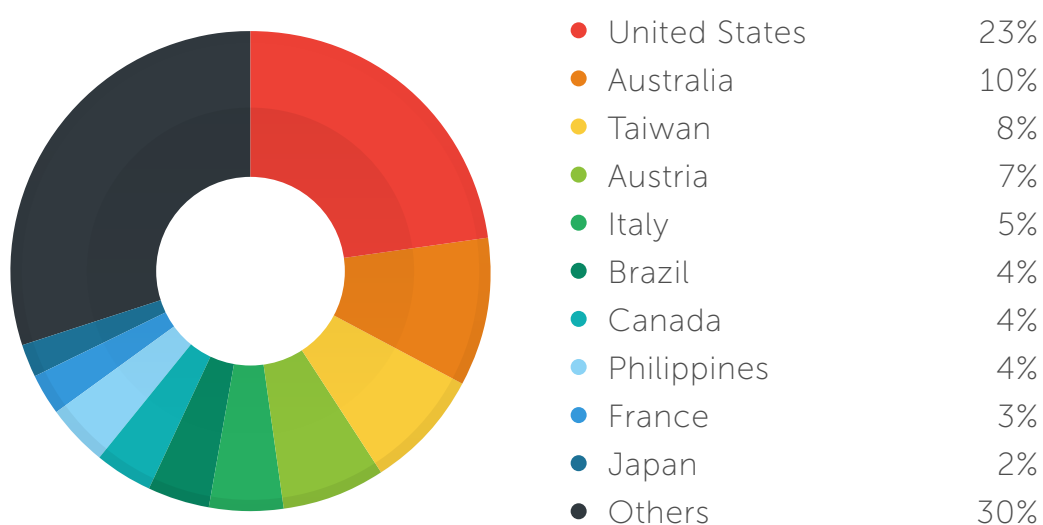
A variety of old and new PoS RAM scraper variants continued to plague users. FighterPoS joined the growing list of notorious PoS malware this February while oldie-but-goodie BlackPOS continued to haunt companies, accounting for a sizable chunk of the total number of infections.²⁹

Number of PoS-RAM-Scraper-Infected Systems



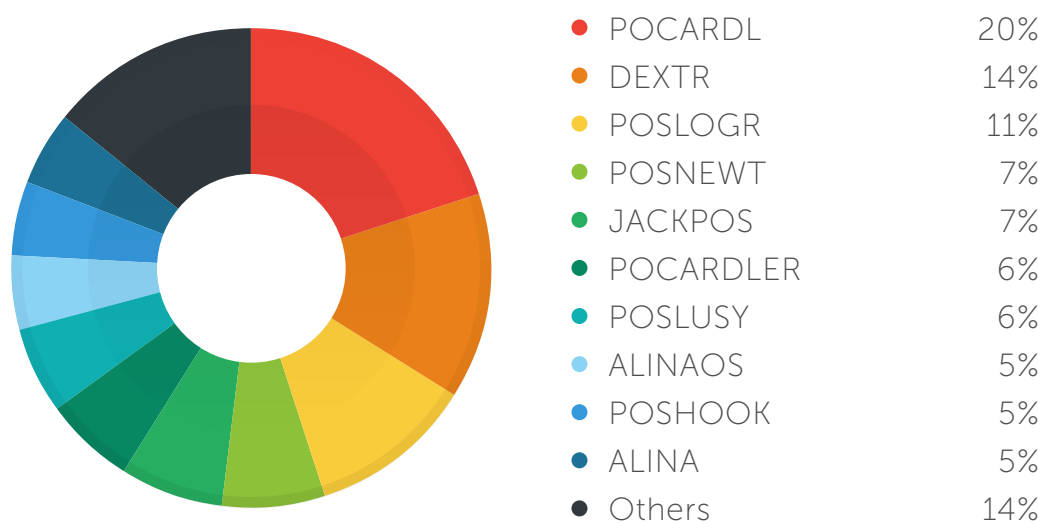
The number of PoS-RAM-scraper detections more than doubled since we started tracking them last year, which could be attributed to improvements to existing PoS malware, as in BlackPOS's case.³⁰

Countries That Posted the Highest Number of PoS RAM Scraper Infections in 1Q 2015



The United States was targeted most by PoS malware attacks, owing to its large base of potential victims. In fact, 80% of the country's population constantly used payment cards as opposed to cash.³¹

Top-Ranking PoS RAM Scraper Families in 1Q 2015



POCARDL, which stole payment card credentials, first seen in October 2012, was the most prominent PoS RAM scraper family in the first three months of 2015.³²

“PoS malware are going to be mainstays in the security industry just like scareware, FAKEAV, and ransomware. This is especially true for countries like the United States where most people prefer cards over cash.”

—Jay Yaneza,
Cyberthreat Researcher

Old Threat Actors Reemerged with New Targeted Attack Campaign Tools, Tactics, and Procedures

Rocket Kitten and those behind Operation Pawn Storm set their sights on new targets, proving that targeted attacks continue to persist and evolve.

Operation Pawn Storm, an ongoing economic and political cyber-espionage operation exploited vulnerable iOS™ devices to infiltrate target networks.³³ Though not the first campaign to make use of mobile malware to stage targeted attacks, Pawn Storm was the first to specifically set sights on iOS. The actors behind it used two malicious iOS apps—XAgent (IOS_XAGENT.A) and a fake version of MadCap (IOS_XAGENT.B)—that were

comparable to SEDNIT variants on Windows computers.

In keeping with continuous enhancements in the realm of targeted attacks, Rocket Kitten improved their tools, tactics, and procedures (TTPs).³⁴ The actors behind the operation abused OneDrive® to host WOOLERG keyloggers.

Notable Mobile-Related Targeted Attacks Seen Since 2011

Pawn Storm Economic and political espionage attacks instigated by a group of threat actors primarily targeting military, embassy, and defense contractor personnel from the United States and its allies; first to specifically use iOS malware to infiltrate target networks	2011
Luckycat Linked to 90 attacks against various industries and/or communities in Japan and India; used remote-access-tool (RAT)-like Android™ malware that gathered information and uploaded/downloaded files to/from infected devices	2012
Chuli Targeted Tibetan and Uyghur activists; used social engineering tricks to exploit vulnerable Windows and Mac OS X systems; spread ANDROIDOS_CHULI.A using hacked email accounts of target activists	2013
Xsser mRAT Believed to be a campaign launched by Chinese-speaking attackers against Chinese protesters; cross-platform malware, Xsser mRAT (ANDROIDOS_Code4HK.A), affected Android and iOS devices; ANDROIDOS_Code4HK.A exposed victims' text, email, and instant messages, location data, usernames and passwords, call logs, and contact lists	2014
Regin Targeted governments, financial institutions, telecommunications operators, research organizations, and other entities in various countries; abused Global System for Mobile Communications (GSM) base station controllers to collect credentials needed to manipulate a Middle Eastern country's GSM network	

Attackers target mobile devices because everyone uses them. Unsafe mobile habits practiced on personal time can easily leak into the workplace, thanks to the bring-your-own-device (BYOD) trend.³⁵

How the Pawn Storm Actors Bypassed Enterprise App Stores' Security Measures



While the exact methods of installing XAgent malware remain unknown, they can affect even nonjailbroken devices if their carrier apps are signed with Apple's enterprise certificate. Social engineering lures can also increase chances of device infection.

Exploit Kits Continued to Grow in Sophistication

Exploit kits constantly add exploits for more and more vulnerabilities to their arsenals, adding to their allure to all kinds of attackers who are always on the lookout for the best value for their money. Their involvement in the past quarter's malvertising attacks also proved a viable means of exploit delivery.

More than 70 exploit kits found in the wild can take advantage of more than 100 vulnerabilities.³⁶ Since Paunch's arrest in 2013, the number of exploit kits in use has significantly dropped. What they lack in volume though, they are making up for in sophistication. Exploit kits are, after all, continuously being updated so they can take advantage of more and more vulnerabilities.

The Hanjuan Exploit Kit, for instance, was used in the previously mentioned Adobe Flash zero-day

attack. The Nuclear Exploit Kit, meanwhile, was most used in the first three months of 2015.

Japan was attackers' most favored country target, as evidenced by several malvertising attacks particularly going after Japanese users.³⁷

As in the past, the most popular kits had exploits for Adobe Flash and Internet Explorer, most likely due to the software's huge user bases.

Vulnerabilities Used in Exploit Kits

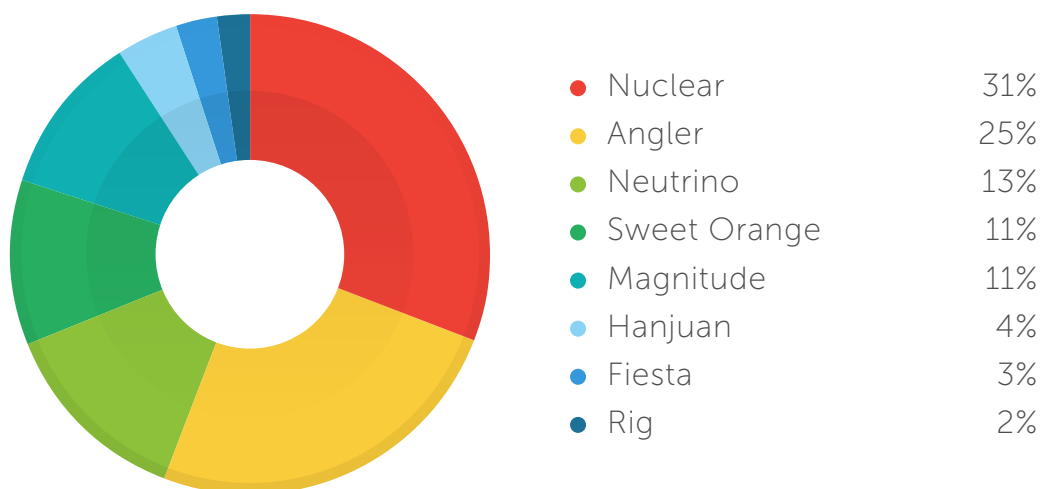
	Nuclear	Sweet Orange	FlashPack	Rig	Angler	Magnitude	Fiesta	Styx	Hanjuan
Internet Explorer	CVE-2013-2551	CVE-2013-2551 CVE-2014-0322 CVE-2014-6332	CVE-2013-2551 CVE-2013-3918 CVE-2014-0322	CVE-2013-2551	CVE-2013-2551	CVE-2013-2551	CVE-2013-2551	CVE-2013-2551	
Microsoft Silverlight®	CVE-2013-0074			CVE-2013-0074	CVE-2013-0074		CVE-2013-0074	CVE-2013-0074	
Adobe Flash	CVE-2014-0515 CVE-2014-0569 CVE-2014-8439 CVE-2015-0311	CVE-2014-0515 CVE-2014-0569	CVE-2013-0634 CVE-2014-0497 CVE-2014-0515 CVE-2014-0569	CVE-2014-0569 CVE-2015-0311	CVE-2014-0515 CVE-2014-0569 CVE-2015-0311	CVE-2014-0515	CVE-2014-0497 CVE-2014-0569 CVE-2015-0311	CVE-2014-0515	CVE-2015-0313
Adobe Acrobat® Reader	CVE-2010-0188						CVE-2010-0188		
Oracle Java™	CVE-2012-0507		CVE-2013-2460 CVE-2013-5471		CVE-2013-2465		CVE-2012-0507 CVE-2014-2465		
XMLDOM ActiveX	CVE-2013-7331			CVE-2013-7331	CVE-2013-7331			CVE-2013-7331	

Adobe Flash exploits were available across all kits used in the most notable attacks in the first quarter of 2015.

Number of Times Exploit Kit Servers Were Accessed in 4Q 2014 and 1Q 2015

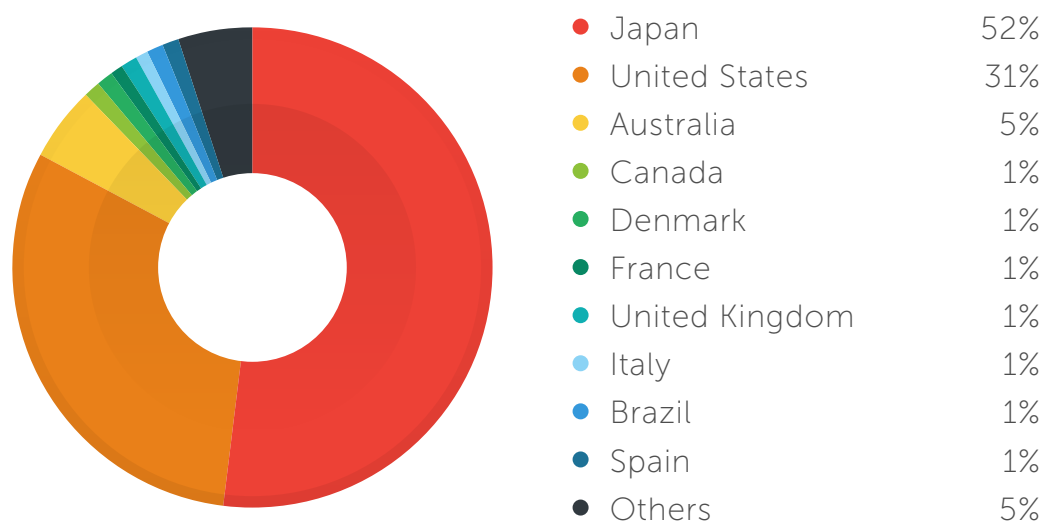
	Sweet Orange	Angler	Magnitude	Rig	Nuclear	Neutrino	Fiesta	Hanjuan	Total
4Q 2014	1,077,223	363,982	155,816	140,604	14,671	26,943	25,133	No data	1,804,372
1Q 2015	264,897	590,063	255,593	42,424	740,037	321,712	61,952	103,924	2,380,602
Growth	-75.4%	62.1%	64.0%	-69.8%	4,944.2%	1,094%	146.5%	No data	31.9%

Exploit Kits That Were Most Accessed by Users in 1Q 2015



A 30% increase in exploit-kit-related activities was seen this quarter. The Nuclear Exploit Kit recorded the highest number of user hits, most likely due to related malvertising attacks seen. The declining number of hits to the Sweet Orange Kit, meanwhile, could be attributed to the malicious ad cleanup certain advertising networks took on their platforms.

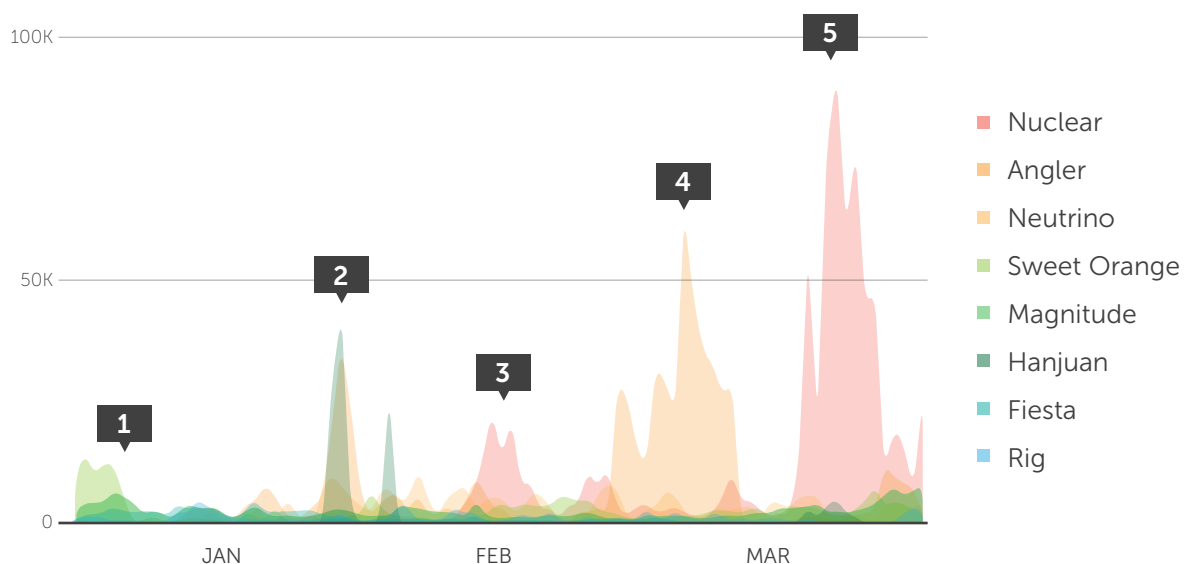
Countries Most Affected by Exploit-Kit-Related Attacks



Japan was the most affected country most likely due to the spate of exploit-kit-related malvertising attacks specifically targeting Japanese users early this year.

Though the volume of newly released exploit kits decreased, a sizable number remained active this past quarter. Could this be the calm before a storm? Are exploit kit developers lying low and quietly enhancing their offerings before going to market?

Known Daily Exploit Kit Activity in 1Q 2015



(Note: The spikes in the chart above correspond to the numbered details below.)

Actions taken by AOL to pull out malvertisements from its platform caused the decline in Sweet Orange Exploit Kit (1) activity. Angler (2 and 4) and Hanjuan (2) were used to push zero-day BEDEP malware to computers from late January to early February, which contributed to the increased number of times their servers were accessed. The Nuclear Exploit Kit (3 and 5), meanwhile, was used in a malvertising attack via pornographic sites.

“More and more exploit attacks are using malvertisements instead of compromised sites or spam. Abusing legitimate advertising networks, after all, allowed them to mask their malicious intent. Attackers constantly improve their tools and tactics to increase their campaigns’ effectiveness and grow their business. We are likely to see more such attacks as 2015 progresses.”

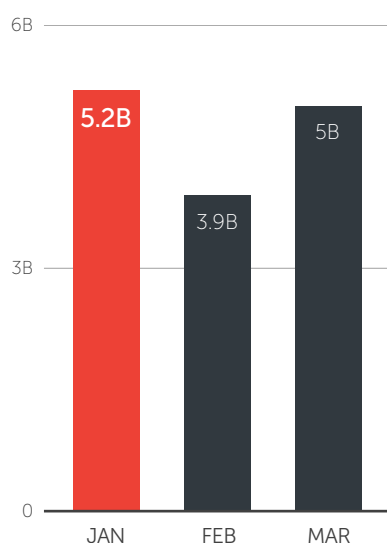
—**Joseph C. Chen,**
Engineer

Threat Landscape in Review

The overall threat volume generally decreased compared with that recorded in the fourth quarter of 2014. Unlike the lower number of malicious domains we blocked user access to and malware we prevented from infecting devices though,

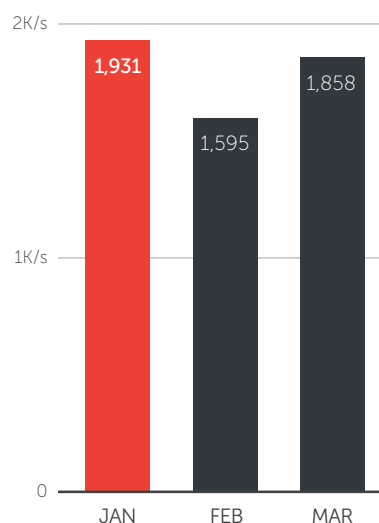
the spam volume spiked. This could indicate a return to email as the most-favored infection vector to deliver old threats like macro malware to vulnerable computers.

Total Number of Threats Blocked in 1Q 2015



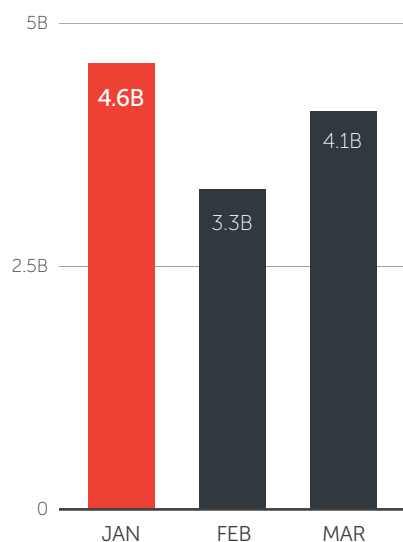
We blocked an average of 4.7 billion threats per month this past quarter, indicating a 1.5-billion increase from the number recorded in the last quarter of 2014.

Trend Micro Detection Rate: Number of Threats Blocked per Second in 1Q 2015



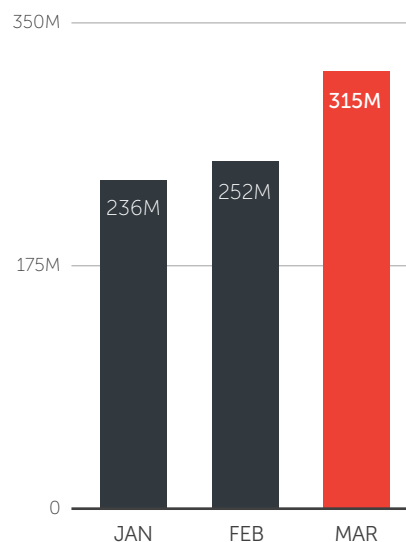
We blocked an average of 1,800 threats per second this past quarter. This showed an increase of 600 threats per second from the previously recorded 1,200 threats per second.

Number of Email Reputation Queries Blocked as Spam in 1Q 2015



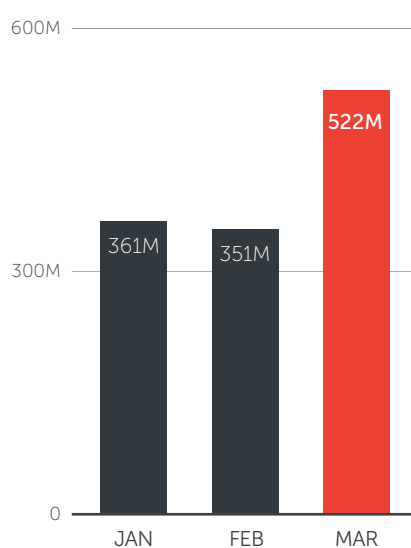
We prevented a total of 12 billion emails from spam-sending IP addresses from reaching users' inboxes.

Number of Malicious Site User Visits Blocked in 1Q 2015



We recorded more than 800 million user visits to malicious sites this past quarter, increasing month over month.

Number of Malicious Files Blocked in 1Q 2015



We prevented more than a billion malicious files from infecting devices this past quarter. The number of malware nearly doubled from this February to March.

The KRYPTIK family of Trojans that mostly affected consumers joined the list of top-ranking malware this past quarter. These Trojans, previously noted for scaring users into submission by splashing warnings on their screens, attempt to download other malicious files onto already-infected computers. They did not succeed in knocking down SALITY and DOWNAD, however, from their top 2 perches.

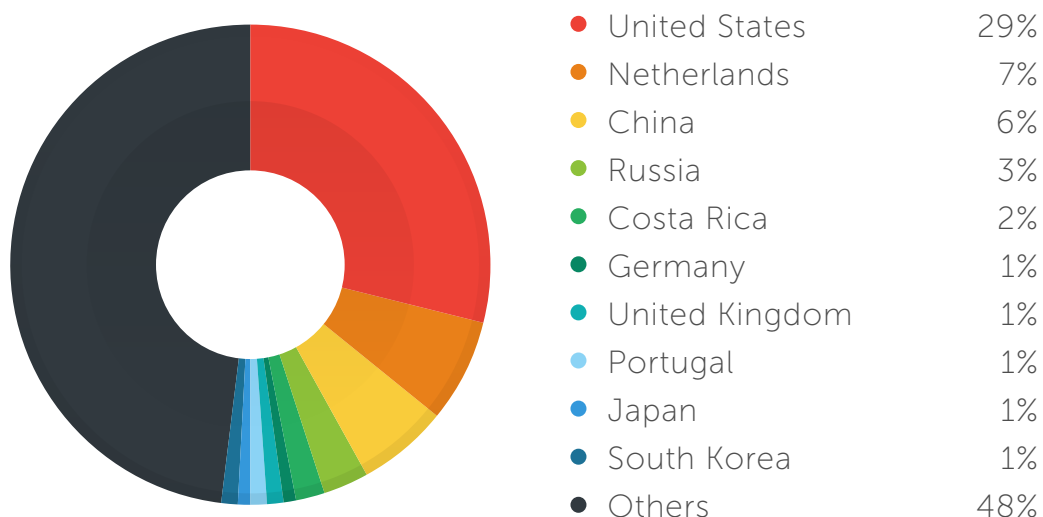
Many of the top domains we blocked user access to this past quarter were adware related. This could very well have ties to the surge in number of malvertising attacks seen. Incidentally, adware also topped the list of mobile threat types. In sum, we have recorded more than 5 million Android threats to date, nearing our predicted total of 8 million by the end of 2015.

Top Malicious Domains Users Were Prevented from Visiting in 1Q 2015

Domain	Reason for Blocking Access To
files-download-131.com	Downloads potentially unwanted files (PUAs) ³⁸
enhizlitakip.com	Related to a Turkish Twitter follower scam
cnfg.toolbarservices.com	Related to adware posing as a browser toolbar
s.trk-u.com	Related to adware posing as a browser toolbar
s.ad120m.com	Site a TROJ_GEN variant communicates with
sso.anbtr.com	Site PE_SALITY.RL communicates with
f0fff0.com	Opens pop-up pages that download adware
fa8072.com	Opens pop-up pages that download adware
creative.ad120m.com	Site a TROJ_GEN variant communicates with
lovek.info	Has ties to click fraud

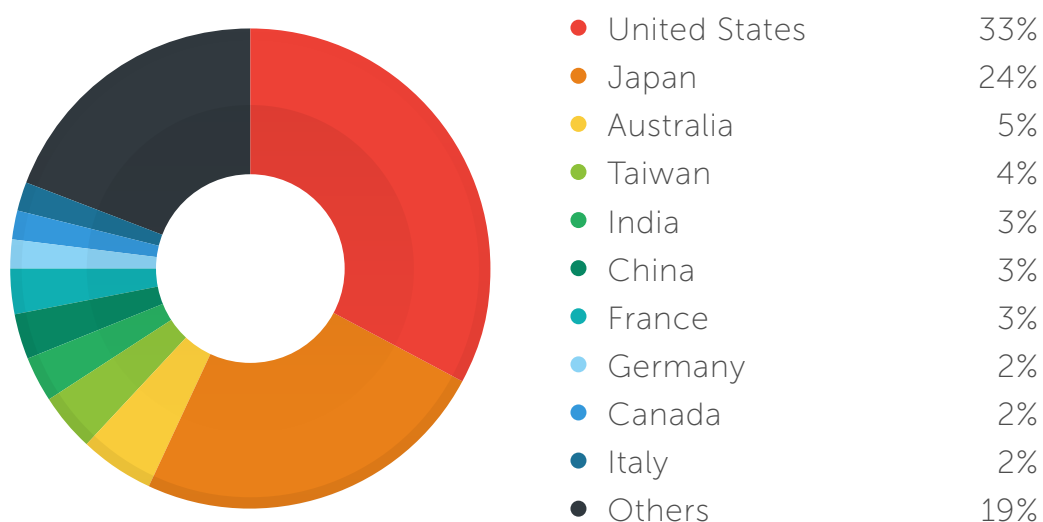
Most of the malicious domains we blocked user access to this past quarter were involved in serving adware and had ties to other scams.

Countries That Hosted the Highest Number of Malicious URLs in 1Q 2015



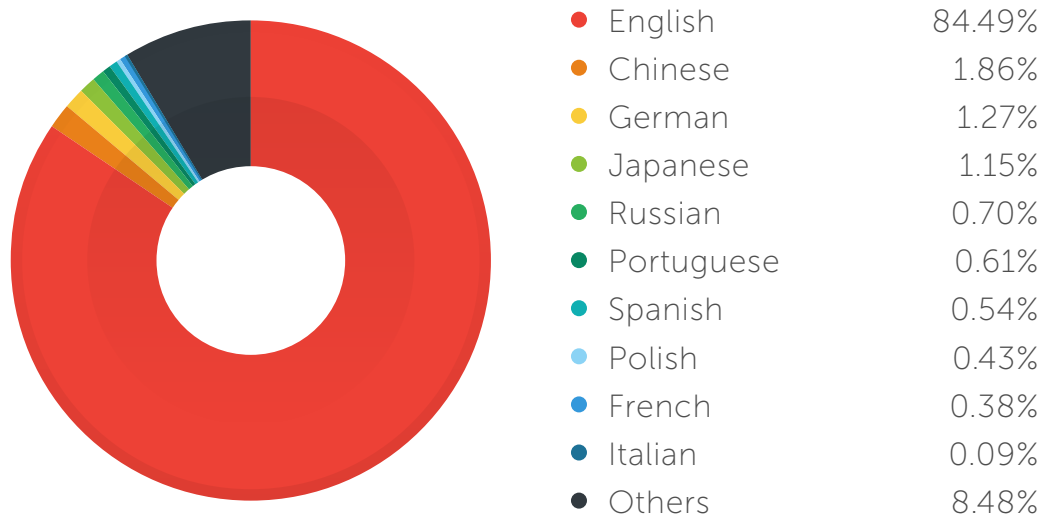
The United States continued to top the list malicious-URL-hosting countries. France and Hungary were knocked off the list by Costa Rica and Portugal.

Countries That Posted the Highest Number of Users Who Clicked Malicious URLs in 1Q 2015



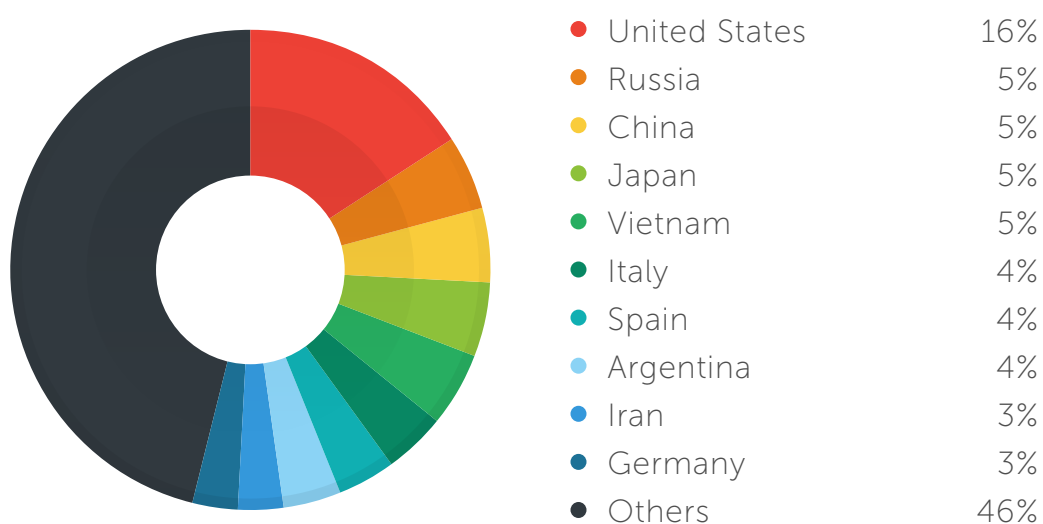
In keeping with being the top malicious-URL-hosting country, the United States also posted the highest number of user clicks to malicious links.

Top Spam Languages in 1Q 2015



English remained the most-used language in spam.

Top Spam-Sending Countries in 1Q 2015



Consistent with the top spamming language being English, the United States topped the list of spam-sending countries. Iran knocked the Ukraine off the list.

Top Malware Families in 1Q 2015

Detection Name	Volume
SALITY	86K
DOWNAD	83K
KRYPTIK	71K
BROWSEVIEW	69K
GAMARUE	65K
DUNIHI	49K
VIRUX	42K
UPATRE	41K
FORUCON	39K
RAMNIT	29K

Top Malware Families by Segment in 1Q 2015

Segment	Detection Name	Volume
Enterprise	DOWNAD	62K
	SALITY	35K
	DUNIHI	29K
SMB	DOWNAD	12K
	DLOADR	11K
	UPATRE	10K
Consumer	KRYPTIK	61K
	GAMARUE	38K
	SALITY	36K

Though KRYPTIK quickly rose to join the list of top malware this past quarter, it still did not manage to oust long-standing chart toppers, SALITY and DOWNAD.

Top Adware Families in 1Q 2015

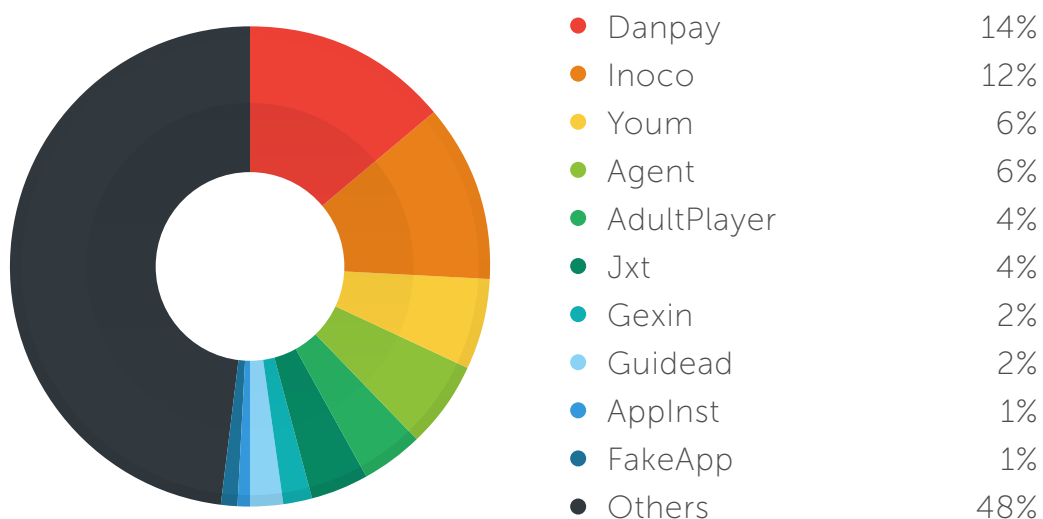
Detection Name	Volume
OPENCANDY	454K
DEALPLY	224K
MYPCBACKUP	183K
MYPCBaACKUP	142K
PULSOFT	122K
TOMOS	113K
MULTIPLUG	109K
INSTALLCORE	102K
ELEX	90K
SPROTECT	67K

Top Adware Families by Segment in 1Q 2015

Segment	Detection Name	Volume
Enterprise	OPENCANDY	68K
	DEALPLY	46K
	TOMOS	18K
SMB	OPENCANDY	29K
	DEALPLY	23K
	MYPCBACKUP	8K
Consumer	OPENCANDY	346K
	MYPCBACKUP	156K
	DEALPLY	135K

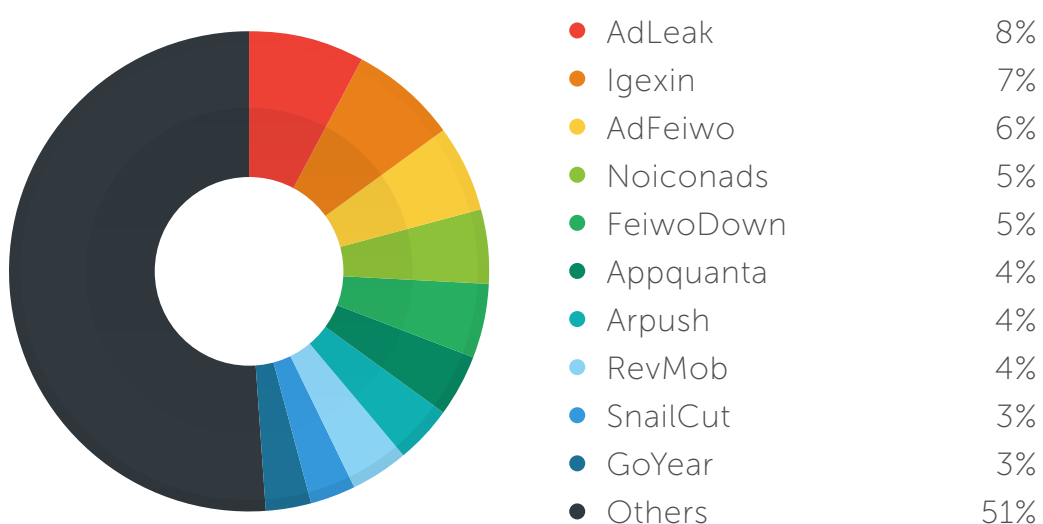
Top-ranking adware, OPENCANDY, consistently topped the list of device infectors across user segments.

Top Android Malware Families in 1Q 2015



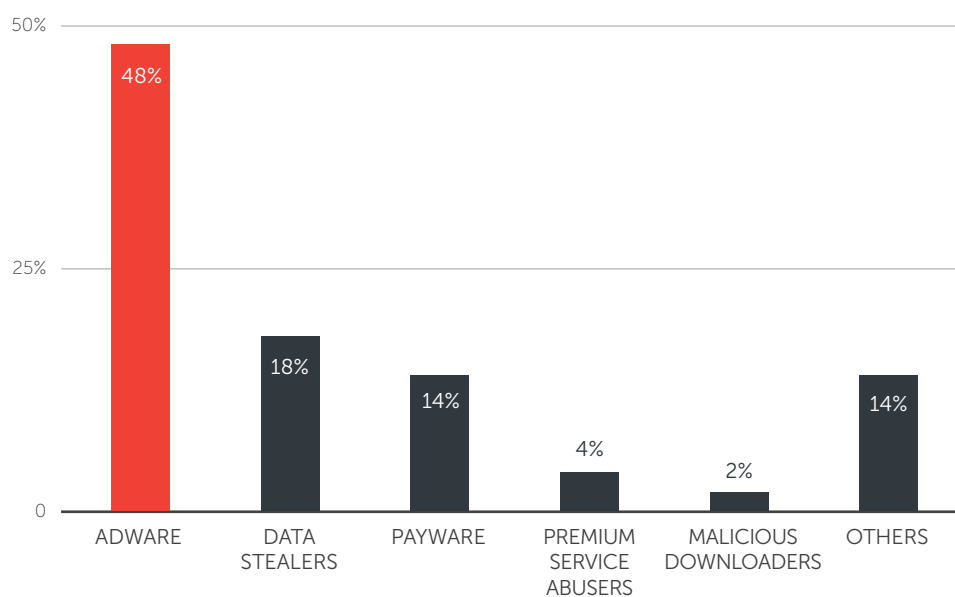
Danpay was the most notorious Android malware family this past quarter. Its routines include accessing C&C servers to wait for malicious commands while silently downloading other apps onto already-infected devices.

Top Android Adware Families in 1Q 2015



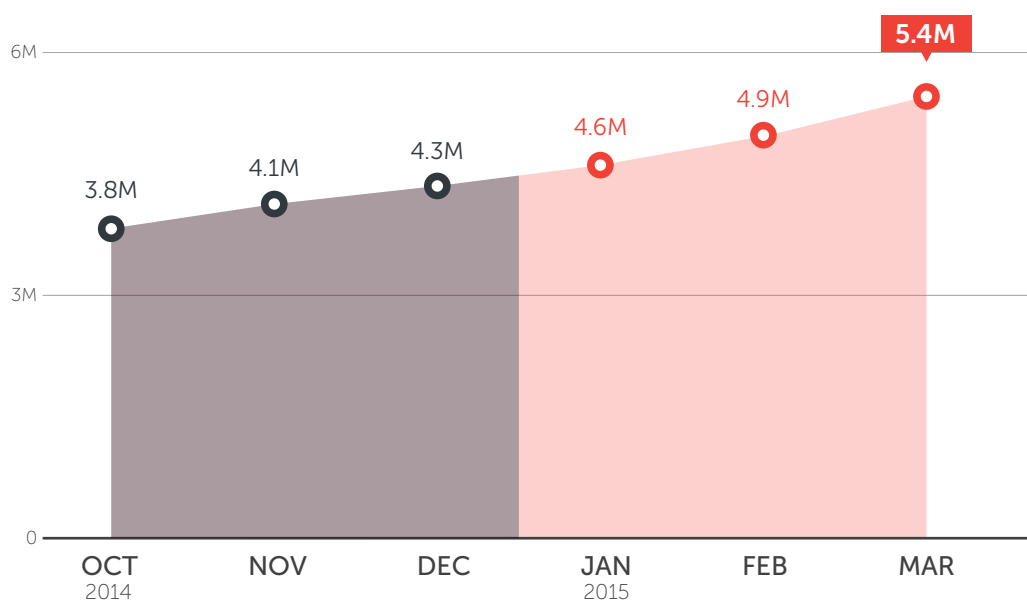
AdLeak, a generic Trend Micro detection name for apps that could put user privacy at risk, topped the list of mobile adware this past quarter.

Top Android Threat Types Seen in 1Q 2015



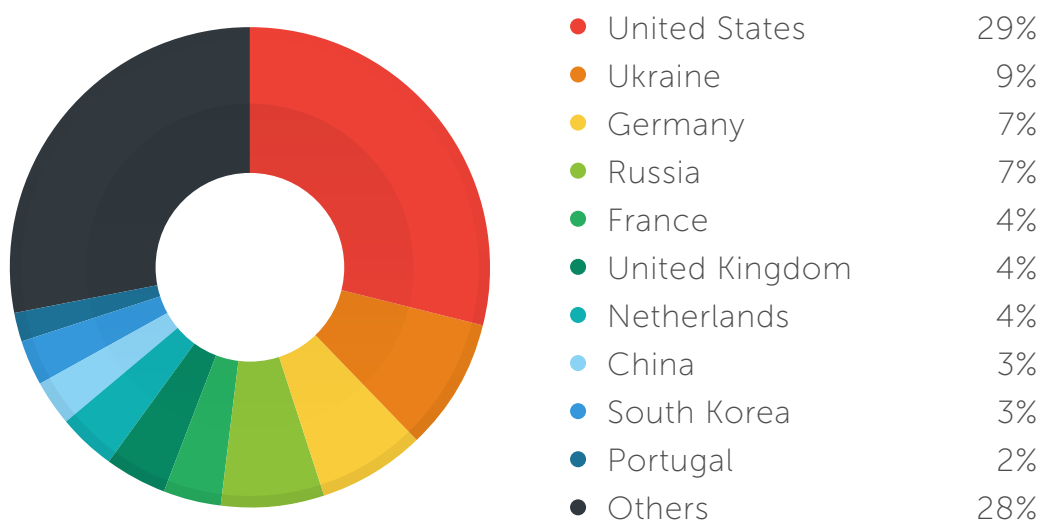
Adware continued to be the top threat type to Android devices. Payware refer to PUAs that manipulate users into agreeing to pay fraudulent fees or charges. PUAs are not inherently malicious but may have functionalities that can compromise users' data security or hamper their mobile experience.

Cumulative Android Threat Growth as of 1Q 2015



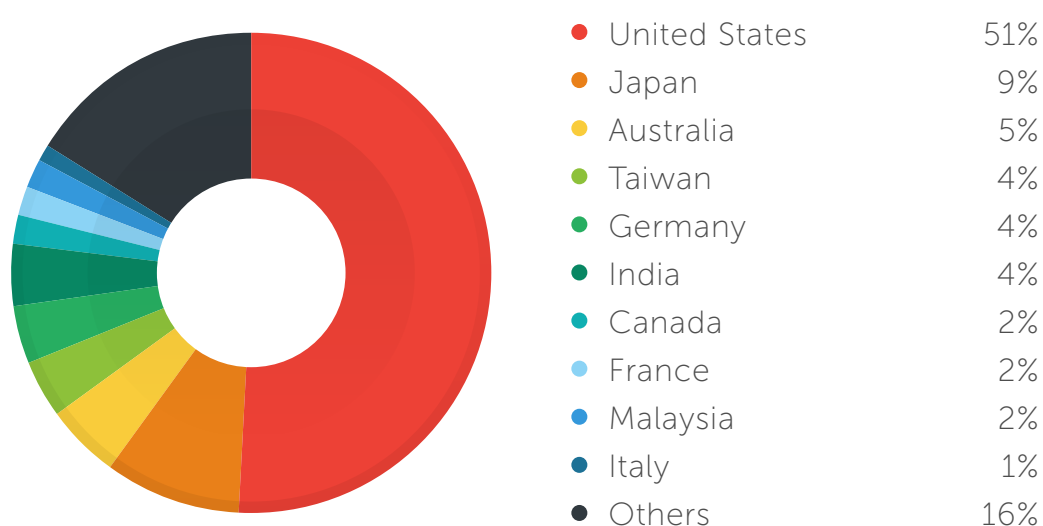
A majority of the Android threats we detected this past quarter were PUAs.

Countries Where the Highest Number of C&C Servers Were Hosted in 1Q 2015



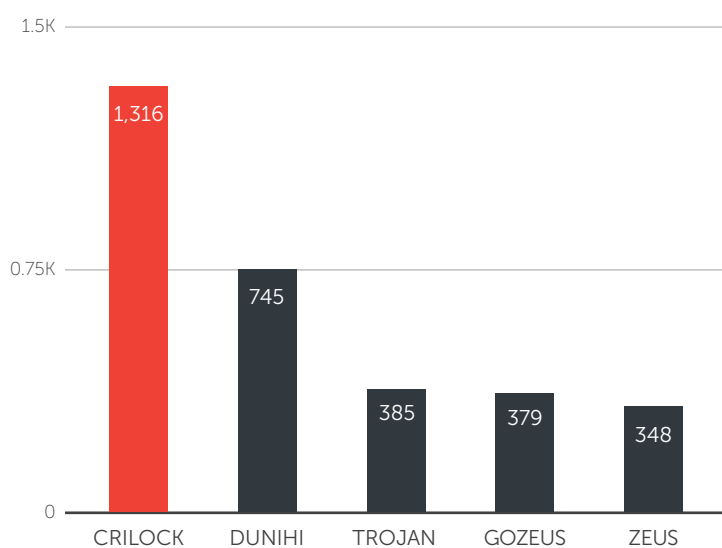
C&C servers were broadly distributed across countries like the United States, the Ukraine, and Germany. Note that attackers do not necessarily have to reside in these countries to access their C&C servers, as these can be remotely manned. Most of the countries in this list also figured in that of top malicious-URL-hosting countries. This could indicate hosting service and infrastructure abuse in these countries.

Countries with the Highest Number of C&C Server Connections in 1Q 2015



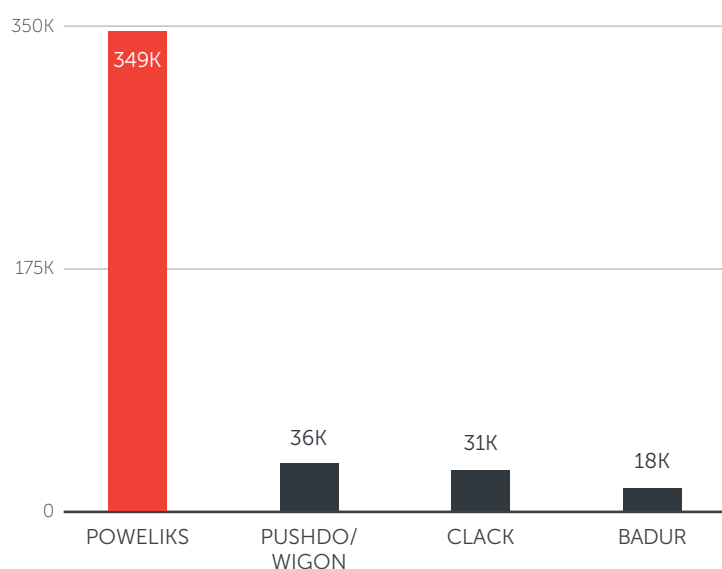
The United States posted the highest number of C&C connections. Coincidentally, it also topped the list of countries with the highest number of user clicks to malicious URLs. This could indicate that most of the access attempts recorded were botnet related.

Malware Families with the Highest Number of Related C&C Servers in 1Q 2015



Variants of the ransomware, CRILOCK, accessed the highest number of C&C servers this past quarter.

Malware Families with the Highest Number of Victims in 1Q 2015



POWELIKS recorded the highest number of victims this past quarter, likely due to its stealth mechanism, allowing it to stay hidden in infected systems.

References

1. U.S. Senate Committee on Homeland Security & Governmental Affairs. (14 May 2014). *U.S. Senate Committee on Homeland Security & Governmental Affairs*. "Permanent Subcommittee on Investigations Releases Report: 'Online Advertising and Hidden Hazards to Consumer Security and Data Privacy.'" Last accessed on 7 May 2015, <http://www.hsgac.senate.gov/media/permanent-subcommittee-on-investigations-releases-report-online-advertising-and-hidden-hazards-to-consumer-security-and-data-privacy->.
2. Brooks Li and Joseph C. Chen. (16 March 2015). *TrendLabs Security Intelligence Blog*. "Exploit Kits and Malvertising: A Troublesome Combination." Last accessed on 16 April 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/exploit-kits-and-malvertising-a-troublesome-combination/>.
3. Peter Pi. (2 February 2015). *TrendLabs Security Intelligence Blog*. "Trend Micro Discovers New Adobe Flash Zero-Day Exploit Used in Malvertisements." Last accessed on 16 April 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-discovers-new-adobe-flash-zero-day-exploit-used-in-malvertisements/>.
4. Alvin Bacani. (5 February 2015). *TrendLabs Security Intelligence Blog*. "BEDEP Malware Tied to Adobe Zero Days." Last accessed on 16 April 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/bedep-malware-tied-to-adobe-zero-days/>.
5. Trend Micro Incorporated. (20 February 2015). *TrendLabs Security Intelligence Blog*. "Superfish Adware in Lenovo Consumer Laptops Violates SSL, Affects Companies via BYOD." Last accessed 16 April 2015, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/superfish-adware-in-lenovo-consumer-laptops-violates-ssl>.
6. Lenovo. (19 February 2015). *Lenovo*. "Lenovo Statement on Superfish." Last accessed on 16 April 2015, http://news.lenovo.com/article_display.cfm?article_id=1929.
7. Vangie Beal. (2015). *Webopedia*. "Bloatware." Last accessed on 20 April 2015, <http://www.webopedia.com/TERM/B/bloatware.html>.
8. Seven Shen. (2 April 2015). *TrendLabs Security Intelligence Blog*. "The Fine Line Between Ad and Adware: A Closer Look at the MDash SDK." Last accessed on 16 April 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/the-fine-line-between-ad-and-adware-a-closer-look-at-the-mdash-sdk/>.
9. Trend Micro Incorporated. (13 February 2013). *TrendLabs Security Intelligence Blog*. "Key Figure in Police Ransomware Activity Nabbed." Last accessed on 23 April 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/key-figure-in-police-ransomware-activity-nabbed-2/>.
10. David John Agni. (2015). *Threat Encyclopedia*. "TROJ_CRYPTFORT.A." Last accessed on 16 April 2015, http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/TROJ_CRYPTFORT.A.
11. Francis Xavier Antazo. (2015). *Threat Encyclopedia*. "PHP_CRYPTWEB.A." Last accessed on 16 April 2015, http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/PHP_CRYPTWEB.A.
12. Anthony Joe Melgarejo. (1 April 2015). *TrendLabs Security Intelligence Blog*. "Crypto-Ransomware Sightings and Trends for 1Q 2015." Last accessed on 16 April 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/crypto-ransomware-sightings-and-trends-for-1q-2015/>.
13. David John Agni. (2015). *Threat Encyclopedia*. "TROJ_CRYPTESLA.A." Last accessed on 16 April 2015, http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/TROJ_CRYPTESLA.A.
14. Shirley Siluk. (13 April 2015). *CIO Today*. "Ransomware Hackers Hitting Police Departments." Last accessed on 16 April 2015, http://www.cio-today.com/article/index.php?story_id=033001297WKR.
15. Maydalene Salvador. (24 March 2015). *TrendLabs Security Intelligence Blog*. "Macro-Based Malware Increases Along with Spam Volume, Now Drops BARTALEX." Last accessed on 16 April 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/macro-based-malware-increases-along-with-spam-volume-now-drops-bartalex/>.
16. Trend Micro Incorporated. (16 February 2015). *TrendLabs Security Intelligence Blog*. "Banking Malware VAWTRAK Now Uses Malicious Macros, Abuses Windows PowerShell." Last accessed on 17 April 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/banking-malware-vawtrak-now-uses-malicious-macros-abuses-windows-powershell/>.
17. Rhena Inocencio. (5 November 2014). *TrendLabs Security Intelligence Blog*. "Banking Trojan DRIDEX Uses Macros for Infection." Last accessed on 6 May 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/banking-trojan-dridex-uses-macros-for-infection/>.

18. Joie Salvio. (19 November 2014). *TrendLabs Security Intelligence Blog*. "ROVNIX Infects Systems with Password-Protected Macros." Last accessed on 6 May 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/rovnix-infects-systems-with-password-protected-macros/>.
19. Trend Micro Incorporated. (4 March 2015). *TrendLabs Security Intelligence Blog*. "FREAK Vulnerability Forces Weaker Encryption." Last accessed on 17 April 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/freak-vulnerability-forces-weaker-encryption/>.
20. Karthikeyan Bhargavan, Antoine Delignat-Lavaud, Cédric Fournet, Markulf Kohlweiss, Alfredo Pironti, Pierre-Yves Strub, Santiago Zanella-Béguelin, Jean-Karim Zinzindohoué, and Benjamin Beurdouche. (2015). *MiTLS*. "SMACK: State Machine Attacks." Last accessed on 17 April 2015, <https://www.smacktls.com/#freak>.
21. "Tracking the FREAK Attack." (2015). Last accessed on 30 April 2015, <https://freakattack.com/>.
22. Pawan Kinger. (28 January 2015). *TrendLabs Security Intelligence Blog*. "Not So Spooky: Linux 'GHOST' Vulnerability." Last accessed on 17 April 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/not-so-spooky-linux-ghost-vulnerability/>.
23. Trend Micro Incorporated. (20 March 2015). *Trend Micro Security News*. "Premiera Blue Cross Admits to Data Breach, Exposes Records of 11 Million Patients." Last accessed 17 April 2015, <http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/premera-blue-cross-data-breach-exposes-11m-patient-records>.
24. Christopher Budd. (5 February 2015). *Trend Micro Simply Security*. "The Anthem Data Breach: What You Need to Know." Last accessed on 17 April 2015, <http://blog.trendmicro.com/what-you-need-to-know-about-the-anthem-hack/>.
25. Jack Clark. (15 June 2011). *ZDNet*. "NHS Laptop Loss Could Put Millions of Records at Risk." Last accessed on 30 April 2015, <http://www.zdnet.com/article/nhs-laptop-loss-could-put-millions-of-records-at-risk/>.
26. Trend Micro Incorporated. (10 February 2015). *Trend Micro Security News*. "Millions Affected in Anthem Breach, Healthcare Companies Prime Attack Targets." Last accessed on 17 April 2015, <http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/millions-affected-in-anthem-breach-healthcare-companies-prime-attack-targets>.
27. Miriam Quick, Ella Hollowood, Christian Miles, and Dan Hampson. (30 March 2015). *Information Is Beautiful*. "World's Biggest Data Breaches." Last accessed on 23 April 2015, <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>.
28. Identity Theft Resource Center. (2015). *ITRC*. "2008 Data Breaches." Last accessed on 23 April 2015, <http://www.idtheftcenter.org/ITRC-Surveys-Studies/2008-data-breaches.html>.
29. Jay Yaneza. (3 March 2015). *TrendLabs Security Intelligence Blog*. "PwnPOS: Old Undetected PoS Malware Still Causing Havoc." Last accessed on 17 April 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/pwnpos-old-undetected-pos-malware-still-causing-havoc/>.
30. Rhena Inocencio. (29 August 2014). *TrendLabs Security Intelligence Blog*. "New BlackPOS Malware Emerges in the Wild, Targets Retail Accounts." Last accessed on 23 April 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/new-blackpos-malware-emerges-in-the-wild-targets-retail-accounts/>.
31. American Consumer Credit Counseling. (2015). *ConsumerCredit.com*. "Infographic: Cash Vs. Card." Last accessed on 23 April 2015, <http://www.consumercredit.com/financial-education/infographics/infographic-cash-vs-card.aspx>.
32. Trend Micro Incorporated. (2014). *Trend Micro Security Intelligence*. "Cybercrime Hits the Unexpected: TrendLabs 1Q 2014 Security Roundup." Last accessed on 23 April 2015, <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-cybercrime-hits-the-unexpected.pdf>.
33. Lambert Sun, Brooks Hong, and Feike Hacquebord. (4 February 2015). *TrendLabs Security Intelligence Blog*. "Pawn Storm Update: iOS Espionage App Found." Last accessed on 17 April 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-update-ios-espionage-app-found/>.
34. Cedric Pernet. (18 March 2015). *TrendLabs Security Intelligence Blog*. "Operation Woolen-Goldfish: When Kittens Go Phishing." Last accessed on 17 April 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/operation-woolen-goldfish-when-kittens-go-phishing/>.

35. Trend Micro Incorporated. (27 February 2015). *Trend Micro Security News*. "Pawn Storm in iOS Apps and Other Cases of Mobile Links in Targeted Attacks." Last accessed on 23 April 2015, <http://www.trendmicro.com/vinfo/us/security/news/mobile-safety/pawn-storm-in-ios-apps-and-other-cases-of-mobile-links-in-targeted-attacks>.
36. Trend Micro Incorporated. (16 March 2015). *Trend Micro Security News*. "Exploit Kits: Past, Present and Future." Last accessed 17 April 2015, <http://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/exploit-kits-past-present-and-future>.
37. Peter Pi. (20 March 2015). *TrendLabs Security Intelligence Blog*. "Freshly Patched Adobe Exploit Added to Nuclear Exploit Kit." Last accessed on 23 April 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/freshly-patched-flash-exploit-added-to-nuclear-exploit-kit/>.
38. Trend Micro Incorporated. (2015). *Threat Encyclopedia*. "Potentially Unwanted Application." Last accessed on 30 April 2015, <http://www.trendmicro.com/vinfo/us/security/definition/potentially-unwanted-app>.

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