

TrendLabs 1Q 2013 SECURITY ROUNDUP

Zero-Days Hit Users Hard at the Start of the Year

Contents

Vulnerabilities and Exploits:
Multiple Zero-Days in Widely
Used Software 2

Cybercrime: Old Threats Return 4

 Digital Life Security Issues.....9

Mobile Threats:
Web Threats Affect Mobile Users, Too 11

APTs and Targeted Attacks: In Stealth Mode..... 15

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.

While exploits and vulnerabilities are a common problem for users, zero-day exploits in high-profile applications are relatively rare. That was not the case in the first quarter of 2013. Multiple zero-day exploits were found targeting popular applications like Java and Adobe Flash Player, Acrobat, and Reader.

In addition, as predicted, we saw improvements in already-known threats like spam botnets, banking Trojans, and readily available exploit kits.

Other high-profile incidents include the South Korean cyber attacks in March, which reiterated the dangers targeted attacks pose. On the mobile front, fake versions of popular apps remained a problem though phishers found a new target in the form of mobile browsers.

Vulnerabilities and Exploits: Multiple Zero-Days in Widely Used Software

Java in the Spotlight

- Java again took center stage this quarter due to a couple of high-profile zero-day incidents.
- A zero-day exploit that sported REVETON and ransomware variants proved that even fully patched systems can be no match for an exploit sometimes.¹
- Within days, Java released a security update to address the issue. But instead of putting the issue to rest, the solution led to even more questions, leading groups, including the U.S. Department of Homeland Security, to recommend uninstalling Java from computers.²

1 <http://blog.trendmicro.com/trendlabs-security-intelligence/java-zero-day-exploit-in-the-wild-spreading-ransomware/>

2 <http://blog.trendmicro.com/trendlabs-security-intelligence/java-fix-for-zero-day-stirs-questions/>

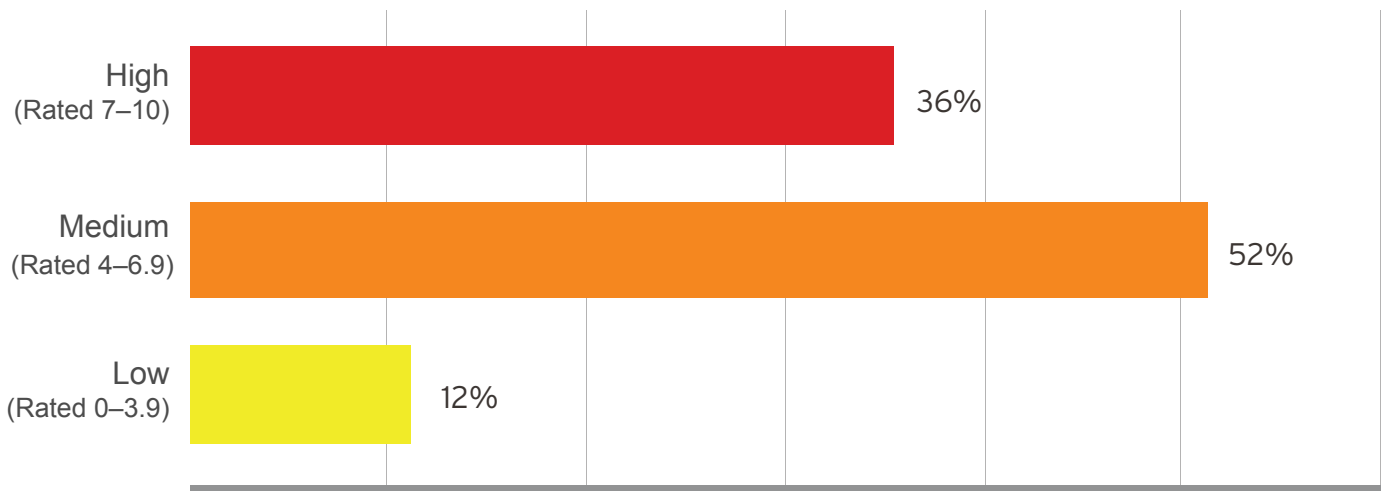
Adobe's Improvements Challenged

- Adobe was not exempted from zero-day attacks, as Adobe Flash Player and Reader fell prey to zero-day exploits in February.
- Two critical vulnerabilities in Adobe Flash Player were exploited, lending vulnerable computers to malware infection.
- Adobe Reader versions 9, 10, and 11 also fell prey to a zero-day attack, rendering even the vendor's sandbox technology vulnerable.³

3 <http://blog.trendmicro.com/trendlabs-security-intelligence/zero-day-vulnerability-hits-adobe-reader/>

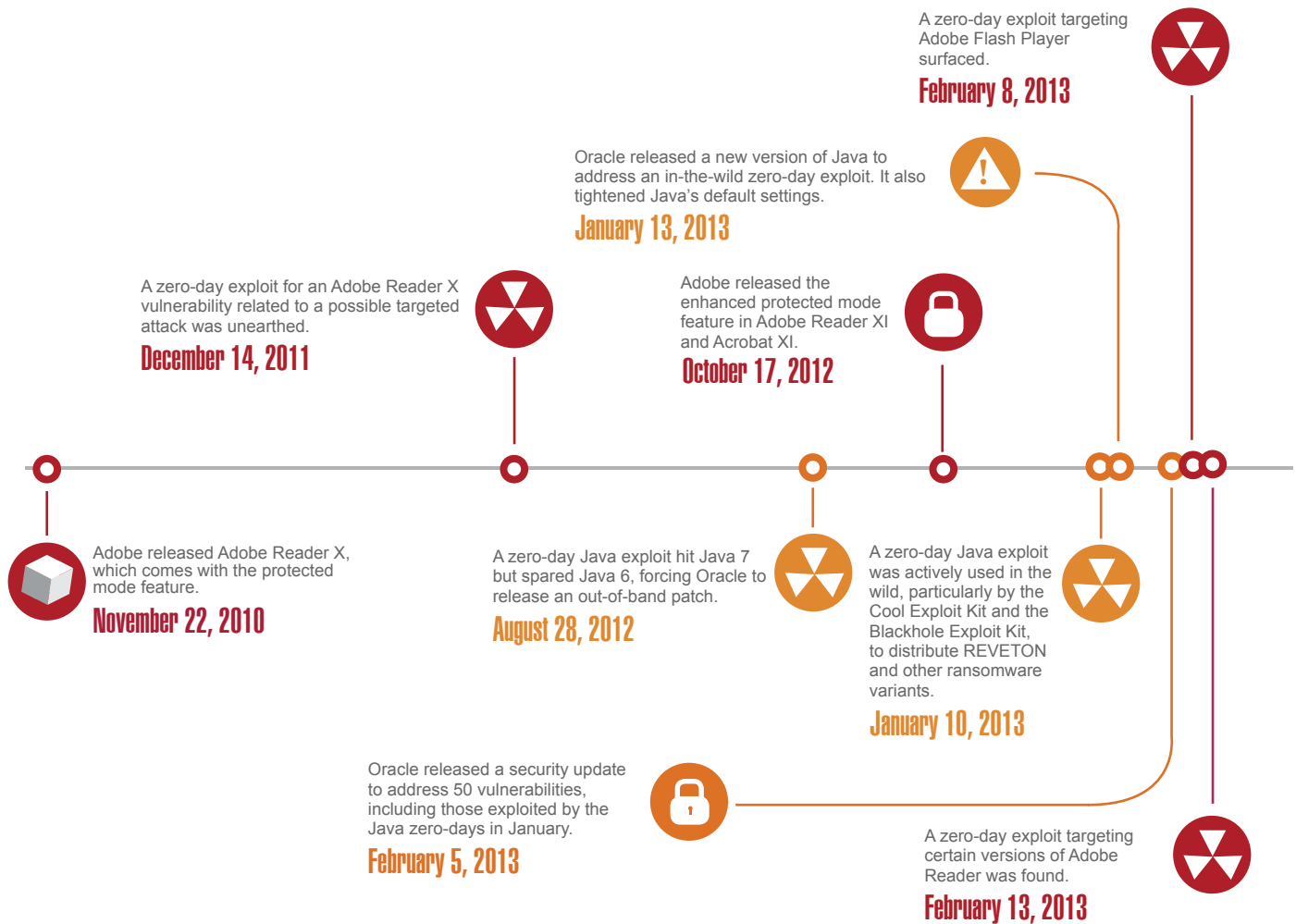
CVSS Score Distribution for Vulnerabilities Addressed

Source: CVE Database (cve.mitre.org)



The majority of the vulnerabilities disclosed in the first quarter were rated "medium" while about a third were rated "high."

Timeline of Adobe and Java Exploit Attacks Since Adobe Reader X



Adobe's protection features kept cybercriminals at bay for most of 2012 and in 2013, although these were first broken this quarter.

In the meantime, Java was exploited left and right, joining the ranks of some of the more exploited software to date.

Adobe's monthly patching cycle (as opposed to Oracle's quarterly cycle) allowed it to respond more quickly to privately reported vulnerabilities. Despite these steps by vendors, multiple zero-days riddled the first quarter's security landscape, highlighting the importance of cautious browsing and using proactive solutions.

Cybercrime: Old Threats Return

Exploit Kits Further Stir the Pot

- The Blackhole Exploit Kit now has exploits for Java vulnerabilities.⁴
- The Whitehole Exploit Kit, dubbed such for its adoption of the Blackhole Exploit Kit code with notable differences, also surfaced this quarter.⁵
- Not far behind was the Cool Exploit Kit, which is considered a high-end version of the Blackhole Exploit Kit.

⁴ <http://blog.trendmicro.com/trendlabs-security-intelligence/blackhole-exploit-kit-run-adopts-controversial-java-flaw/>

⁵ <http://blog.trendmicro.com/trendlabs-security-intelligence/whitehole-exploit-kit-emerges/>

Spam Botnets Refine Techniques

- Asprox, infamous for sending out tons of spam since 2007 and was supposedly taken down in 2008, has been “reborn” with a modular framework.⁷
- Unlike before, Asprox now uses compromised legitimate email accounts to evade spam filters and KULUOZ malware as droppers.⁸
- First spotted in 2011, the Andromeda botnet resurfaced this quarter with spam containing links to compromised sites that host the Blackhole Exploit Kit.⁹ Newly spotted Andromeda variants were found spreading via removable drives and dropping component files to evade detection.

⁷ <http://blog.trendmicro.com/trendlabs-security-intelligence/asprox-reborn/>

⁸ http://blog.trendmicro.com/trendlabs-security-intelligence/bkdr_kuluoz-at-a-spam-near-you/

⁹ <http://blog.trendmicro.com/trendlabs-security-intelligence/andromeda-botnet-resurfaces/>

Browser Crasher Transcends Platforms

- Users were hit by a threat we dubbed “browser crasher” because it causes browsers to hang or crash across different OSs.⁶
- Lured via Tweets with links that lead to a site embedded with a malicious JavaScript code, affected users saw a never-ending slew of pop-up messages.

⁶ <http://blog.trendmicro.com/trendlabs-security-intelligence/browser-crashers-hit-japanese-users/>

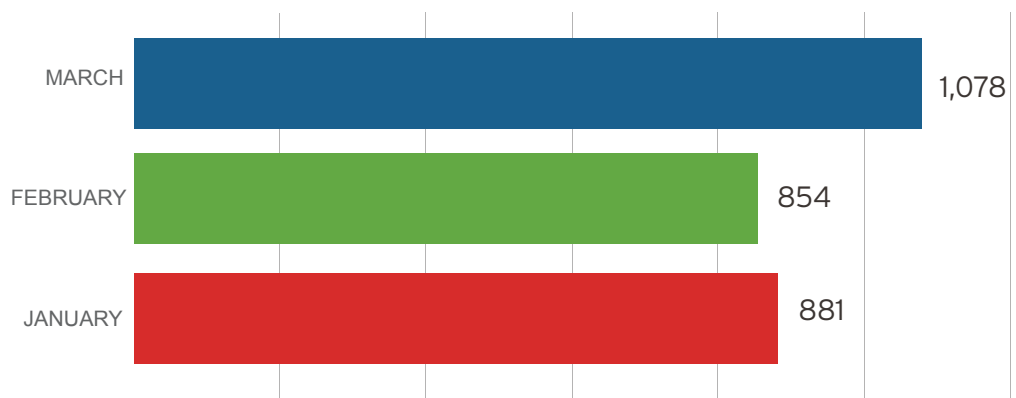
CARBERP Rears Its Ugly Head Again

- Banking Trojans known as CARBERP variants were first spotted in 2010.
- After a CARBERP command-and-control (C&C) server was sinkholed in 2010, variants of the malware that download new plug-ins to aid in data stealing surfaced.¹⁰
- Mobile versions of the malware also surfaced to prey on the growing number of people who use their phones or tablets to conduct banking transactions.¹¹

¹⁰ <http://blog.trendmicro.com/trendlabs-security-intelligence/carberp-sinkhole-findings/>

¹¹ <http://blog.trendmicro.com/trendlabs-security-intelligence/carberp-banking-malware-makes-a-comeback/>

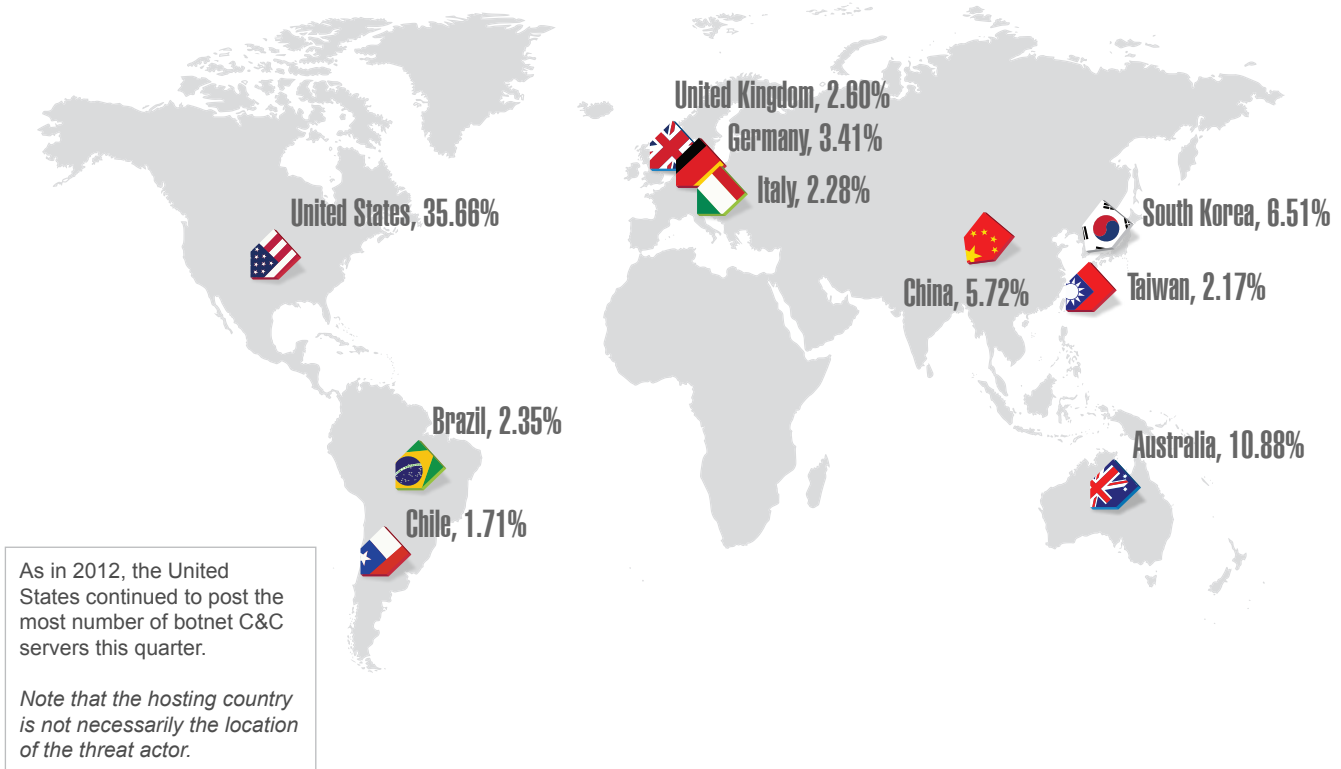
Number of Botnet C&C Servers Detected per Month



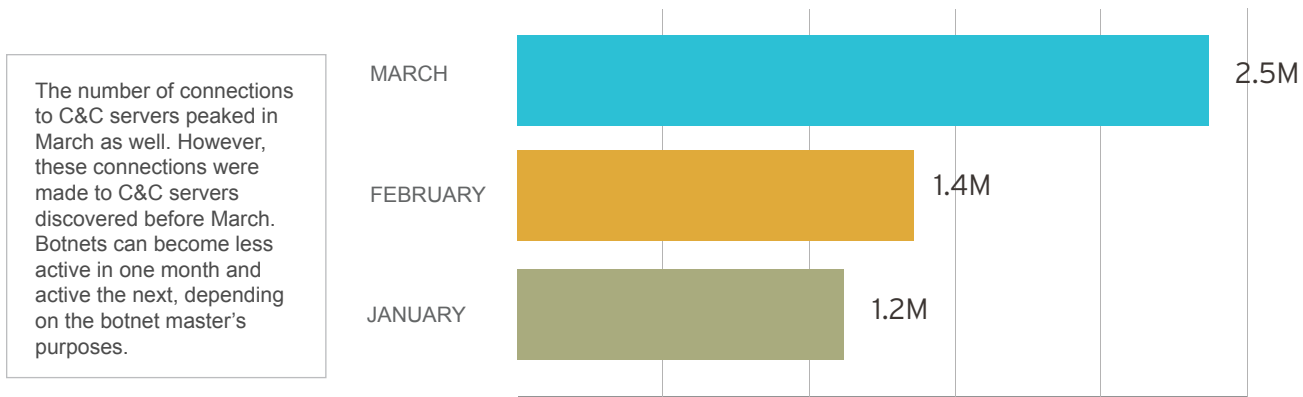
March showed the most number of C&C servers detected this quarter. Note that this is so far the biggest number of C&C servers we detected since June 2012.

The numbers in this chart refer to last-seen botnet C&C server detections as of April 10, 2013.

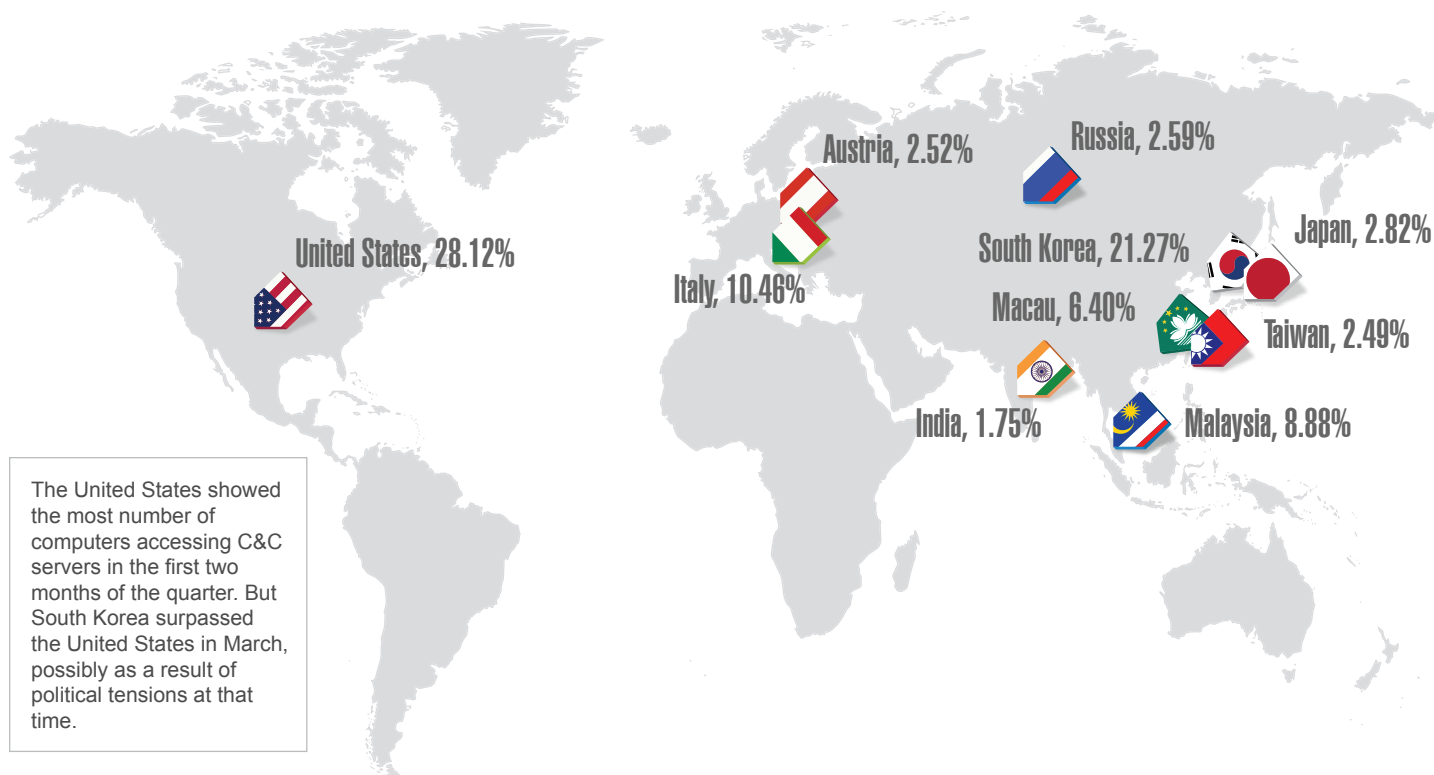
Top 10 Countries with the Most Number of Botnet C&C Servers



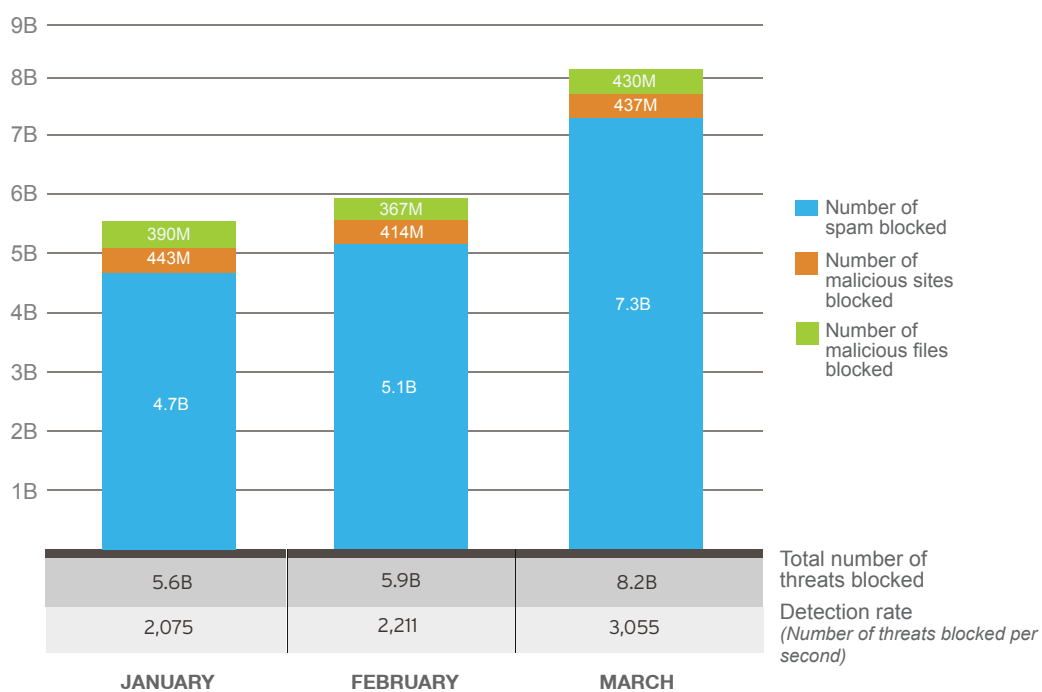
Number of Connections to Botnets per Month



Top 10 Countries with the Most Number of Botnet-Connected Computers



Overall Trend Micro Smart Protection Network Numbers



Top 3 Malware



WORM_DOWNAD remained the top malware this quarter, followed by TROJ_ZACCESS/SIREFEF, just like last year. But the number of adware surged led by ADW_PRICEGONG, which placed third to replace 2012's third-most prolific malware, PE_SALITY.

WORM_DOWNAD - **741K**

TROJ_ZACCESS/SIREFEF - **274K**

ADW_PRICEGONG - **234K**

ENTERPRISE		SMB		CONSUMER	
NAME	VOLUME	NAME	VOLUME	NAME	VOLUME
WORM_DOWNAD	364K	WORM_DOWNAD	81K	TROJ_ZACCESS/SIREFEF	163K
PE_SALITY	81K	PE_SALITY	17K	CRCK_KEYGEN	162K
PE_VIRUX	34K	TROJ_ZACCESS/SIREFEF	14K	ADW_PRICEGONG	157K

Top 10 Malicious Domains Blocked

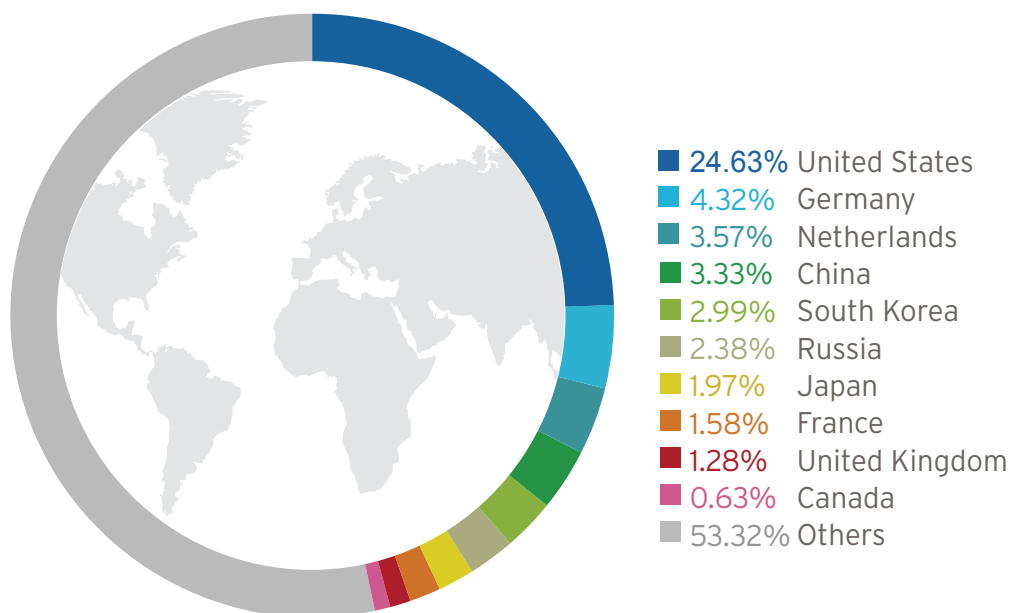
Almost all of the domains blocked this quarter were involved in malicious activities, specifically hosting and distributing malware. Only one of the top 10 was blocked due to malicious content related to child exploitation.

DOMAIN	REASON
trafficconverter.biz	Has a record for hosting and distributing worms
pu.plugrush.com	Has a poor reputation and record
ads.alpha00001.com	Reported as a C&C server and redirects to enterfactory.com, another malicious site
am10.ru	Has a record and reported in relation to pop-up messages and adware
www.trafficholder.com	Related to child exploitation
www.funad.co.kr	Related to a ADW_SEARCHSCOPE
www.ody.cc	Related to links with suspicious scripts and sites that host BKDR_HPGN.B-CN
cdn.bisped.com	Redirects to a malicious site and related to malicious files that distribute malware
h4r3k.com	Distributes Trojans
www.dblpmp.com	Contained spam and malware

Top 10 Malicious URL Country Sources

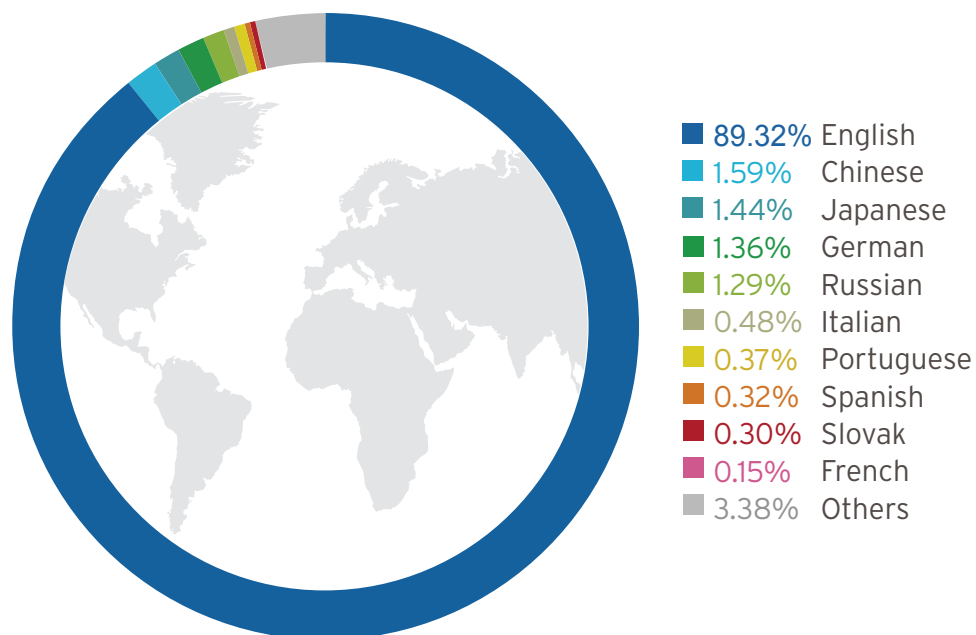
More than 20% of the malicious domains we blocked were hosted in the United States, consistent with our 2012 numbers. The United States and Germany hosted the most number of blocked malicious domains.

The data in this map refer to the number of malicious sites hosted in the countries. The malicious site owners are not necessarily from the identified countries but may have registered their domains in them.

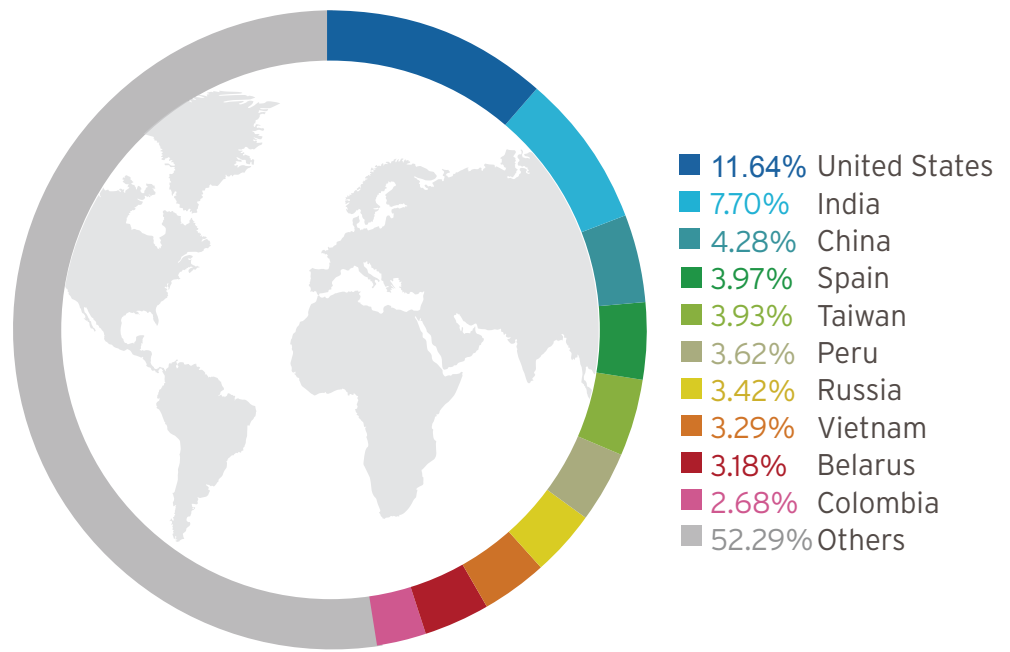


Top 10 Spam Languages

The majority of the spam was written in English, as it is the most widely used language in business, commerce, and entertainment. As such, spammers deemed spreading malicious messages in this language more profitable.



Top 10 Spam-Sending Countries



India, which led the pack of spam-sending countries in 2012, fell to second place after the United States. Some countries that used to be part of the top 10 list completely dropped out this quarter. It is clear though that spamming remains a global problem.

Digital Life Security Issues

Holidays and Historic Events Remain Effective Lures

- Historic moments like the papal conclave and the announcement of the new pope did not escape the attention of spammers and Blackhole Exploit Kit perpetrators.¹²
- The Google Glass competition in February also spurred the appearance of several web threats, including malicious links that led to survey scams.¹³
- The spam and malicious domain volumes also spiked days before Valentine's Day, again proving that cybercriminals still profit from these ruses.¹⁴

¹² <http://blog.trendmicro.com/trendlabs-security-intelligence/spammers-bless-new-pope-with-spam/>

¹³ <http://blog.trendmicro.com/trendlabs-security-intelligence/cybercriminals-hop-on-the-google-project-glass-bandwagon/>

¹⁴ <http://blog.trendmicro.com/trendlabs-security-intelligence/love-bugs-how-are-valentine-threats-looking-up/>

Hacking Gives Life to Zombies

- The Montana Emergency Alert System (EAS) was reportedly hacked and warned users that "bodies of the dead are rising from their graves and attacking the living."¹⁸
- Attacks like this shows that anything connected to the Internet, even public infrastructures, can be compromised and have disastrous results.

¹⁸ <http://blog.trendmicro.com/trendlabs-security-intelligence/zombies-are-funny-until-someone-loses-an-eye/>

Digital life refers to the entire ecosystem regarding the online activities of the general computing public, including behaviors, identities, privacy, social engineering, social media platforms, and the like.

Selling User Information Follows Its Own Business Model

- "Fullz," which refers to a collection of crucial information beyond names, addresses, and credit card numbers typically stolen from unsuspecting users and sold by scammers in underground forums.¹⁵
- Data can be stolen using different tools and/or techniques like spreading data-stealing malware, compromising "target-rich" organizations, and obtaining indiscriminately disclosed information.¹⁶
- Scammers who sell user information operate within a certain framework so they can gain new and retain existing customers to profit.¹⁷

¹⁵ <http://blog.trendmicro.com/trendlabs-security-intelligence/what-would-scammers-want-with-my-information/>

¹⁶ <http://blog.trendmicro.com/trendlabs-security-intelligence/business-models-behind-information-theft/>

¹⁷ <http://blog.trendmicro.com/trendlabs-security-intelligence/your-data-and-the-business-of-online-scam/>

Notable Social Engineering Lures Used

News events dominated the social engineering lures in the first quarter, with the election of a new pope making the loudest noise. Technology-related topics like Google Glass and Windows 8 were also frequently used.

CANDY CRUSH Windows 8
Pope Francis
 Google Glass Valentine's Day

Cybercriminal Underground Product/Service Prices (As of January 16, 2013)

Bank and e-commerce login credentials are highly prized in the underground compared with their social media counterparts. Besides peddling stolen data, it is interesting to note that cybercriminals also offer services like shipping gadgets.

PERSONAL DATA	PRICE
BANK LOGIN DATA	
Bank of America U.S.	
US\$7,000 balance	US\$300
US\$14,000 balance	US\$500
US\$18,000 balance	US\$800
HSBC U.S.	
US\$12,000 balance	US\$400
US\$28,000 balance	US\$1,000
HSBC U.K.	
US\$8,000 balance	US\$300
US\$17,000 balance	US\$700
GADGET SHIPMENT	
Laptop	
Apple	US\$240
HP/Dell/Toshiba/Samsung	US\$120
Vaio	US\$200
Mobile phone/Tablet	
iPhone 3GS	US\$120
iPhone 4G	US\$150
iPhone 4GS/iPad 2	US\$180
BlackBerry	US\$130
VERIFIED PAYPAL ACCOUNT (email and password)	
US\$1,500 balance	US\$150
US\$2,500 balance	US\$200
US\$4,000 balance	US\$300
US\$7,000 balance	US\$500

Mobile Threats: Web Threats Affect Mobile Users, Too

Phishing Hooks for Mobile Users

- Phishing is an emerging threat in the mobile space.¹⁹
- In 2012, the majority of mobile sites spoofed were banking sites.²⁰
- Financial service-related sites were most spoofed this quarter, proving that phishers, whether on computers or on mobile devices, will always go where the money is.

¹⁹ <http://about-threats.trendmicro.com/us/mobilehub/mobilereview/rpt-monthly-mobile-review-201302-mobile-phishing-a-problem-on-the-horizon.pdf>

²⁰ <http://blog.trendmicro.com/trendlabs-security-intelligence/when-phishing-goes-mobile/>

Mobile Backdoor Infects 1M Smartphones

- An Android malware variant that can send and receive commands was found on 1M smartphones.²¹
- The malware can update its script to evade anti-malware detection. Because of its backdoor routines, malicious users are able to control infected devices.
- Fortunately for Trend Micro customers, we have been detecting this malware since July 2012 despite the high number of infections in the first quarter.

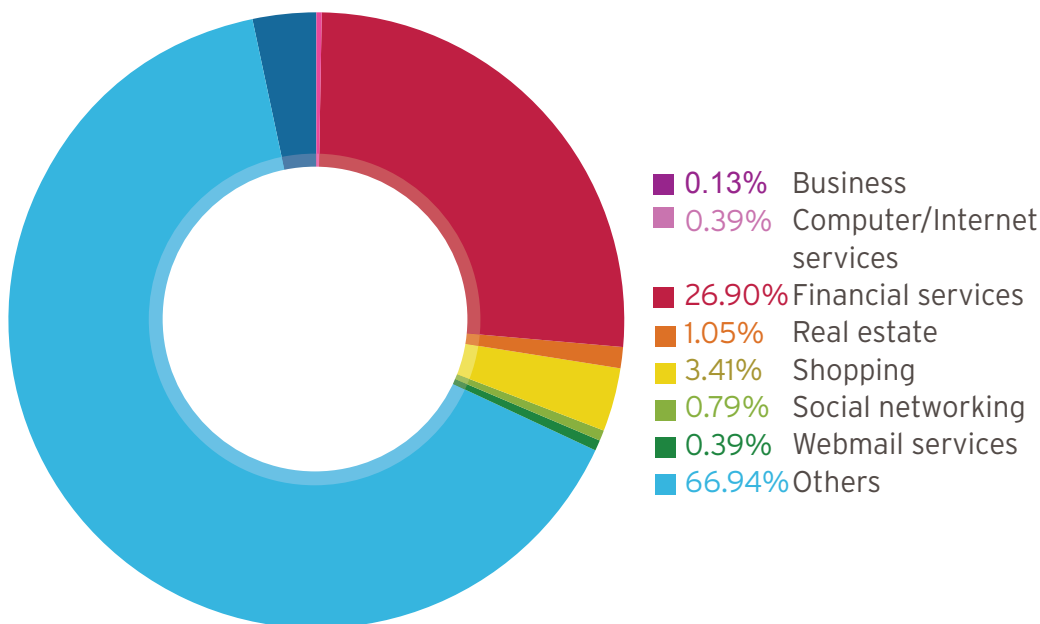
²¹ <http://blog.trendmicro.com/trendlabs-security-intelligence/android-malware-found-to-send-remote-commands/>

Fake Gaming Apps Become Threat Staples

- Mobile malware continued to take advantage of popular gaming apps this quarter.
- We spotted fake versions of Temple Run 2 and spoofed apps that offer cheats for the game Candy Crush Saga.²² These apps aggressively pushed ads and gathered personal information from infected mobile devices.

²² <http://blog.trendmicro.com/trendlabs-security-intelligence/fake-versions-of-temple-run-2-sprint-their-way-to-users/>; <http://blog.trendmicro.com/trendlabs-security-intelligence/dubious-developers-cash-in-on-candy-crush/>

Mobile Phishing Site Types Detected

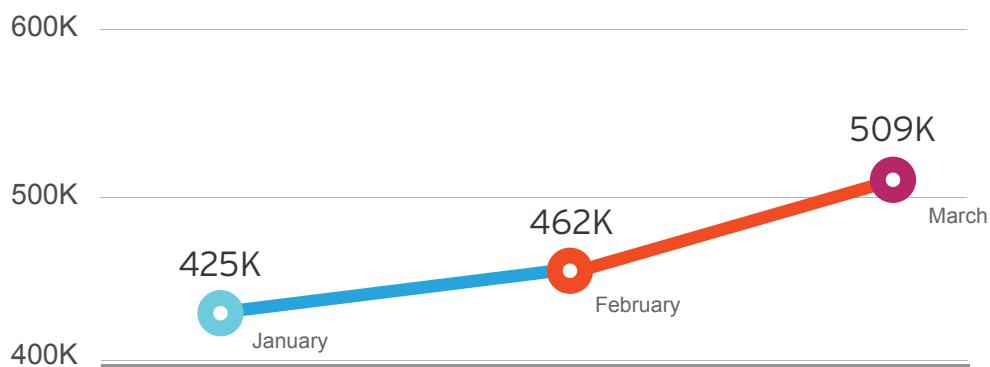


Financial sites were still the favorite phishing targets even in the mobile space this quarter. Note that the number of mobile phishing URLs increased by 54% from around 500 in the first quarter of 2012 to almost 800 in the same quarter of 2013.

The data in this figure refer to the number of malicious URLs that pointed to sites with mobile-related keywords.

The Android threat volume has reached the halfway mark in relation to our 2013 prediction—1M, indicating continued cybercriminal interest in the mobile space. The increase could be attributed to the fact that more than half of the global mobile device market share belongs to Google.

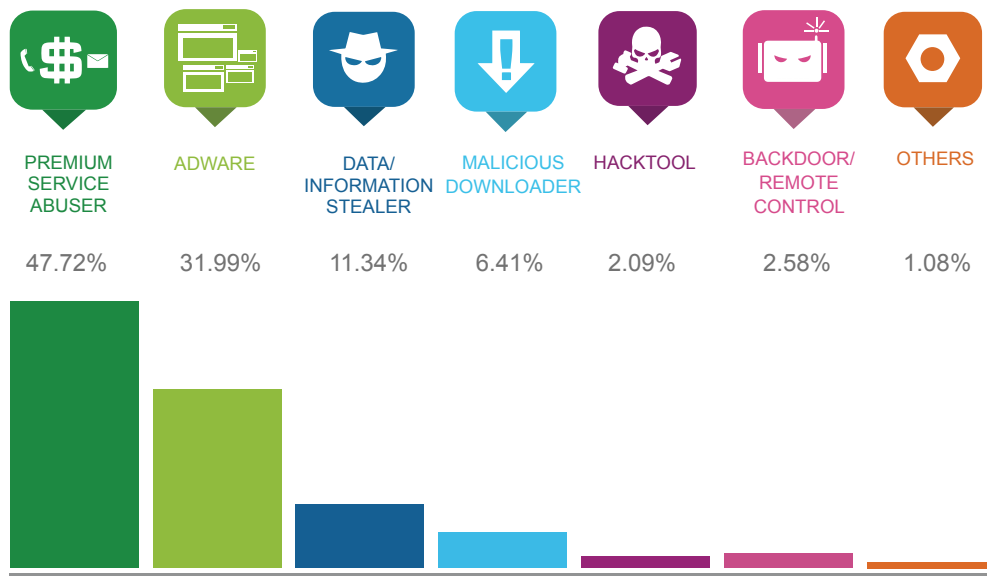
Android Threat Volume Growth



As in 2012, premium service abusers and adware remained the top Android threats this quarter. Premium service abusers are known for registering users to overpriced services while adware aggressively push ads and may even collect personal information without affected users' consent.

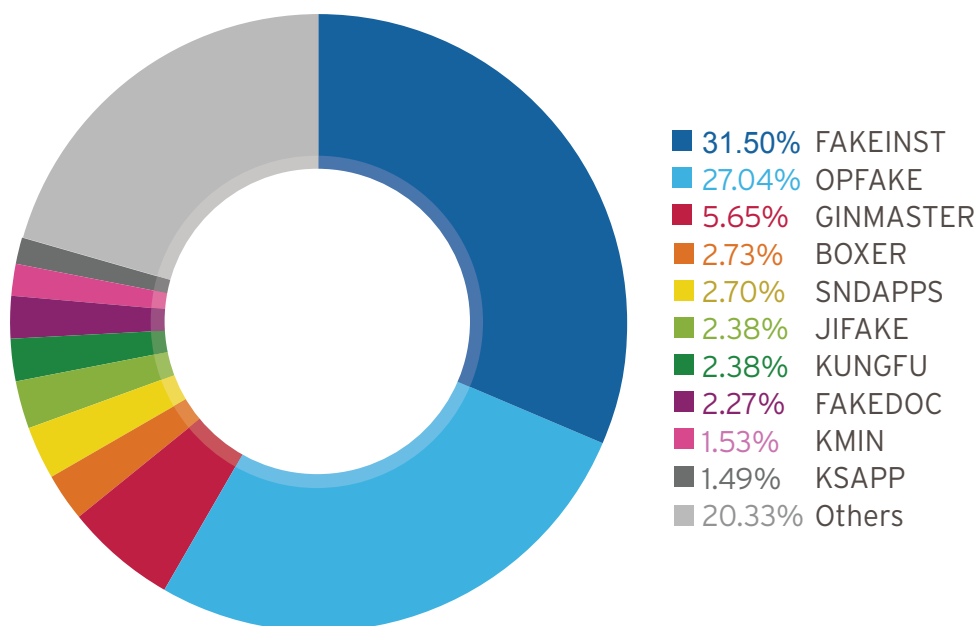
The distribution data was based on the top 20 mobile malware and adware families that comprise 88% of all the mobile threats detected by the Mobile Application Reputation Technology as of March 2013. Note that a mobile threat family may exhibit the behaviors of more than one threat type.

Distribution of Android Threat Types

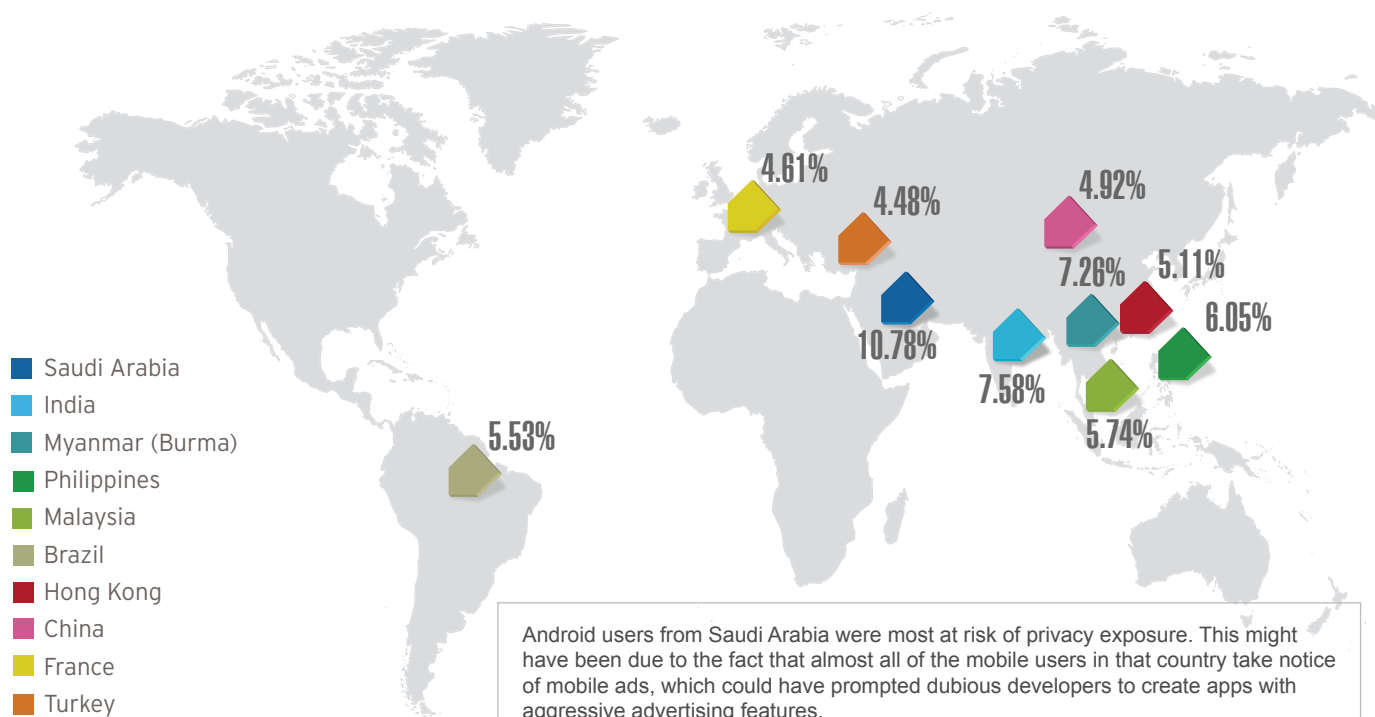


Top 10 Android Malware Families

Fake apps remained a significant mobile threat. Malicious apps that belong to the FAKEINST and OPFAKE families are known for imitating popular apps to lure users into downloading them.



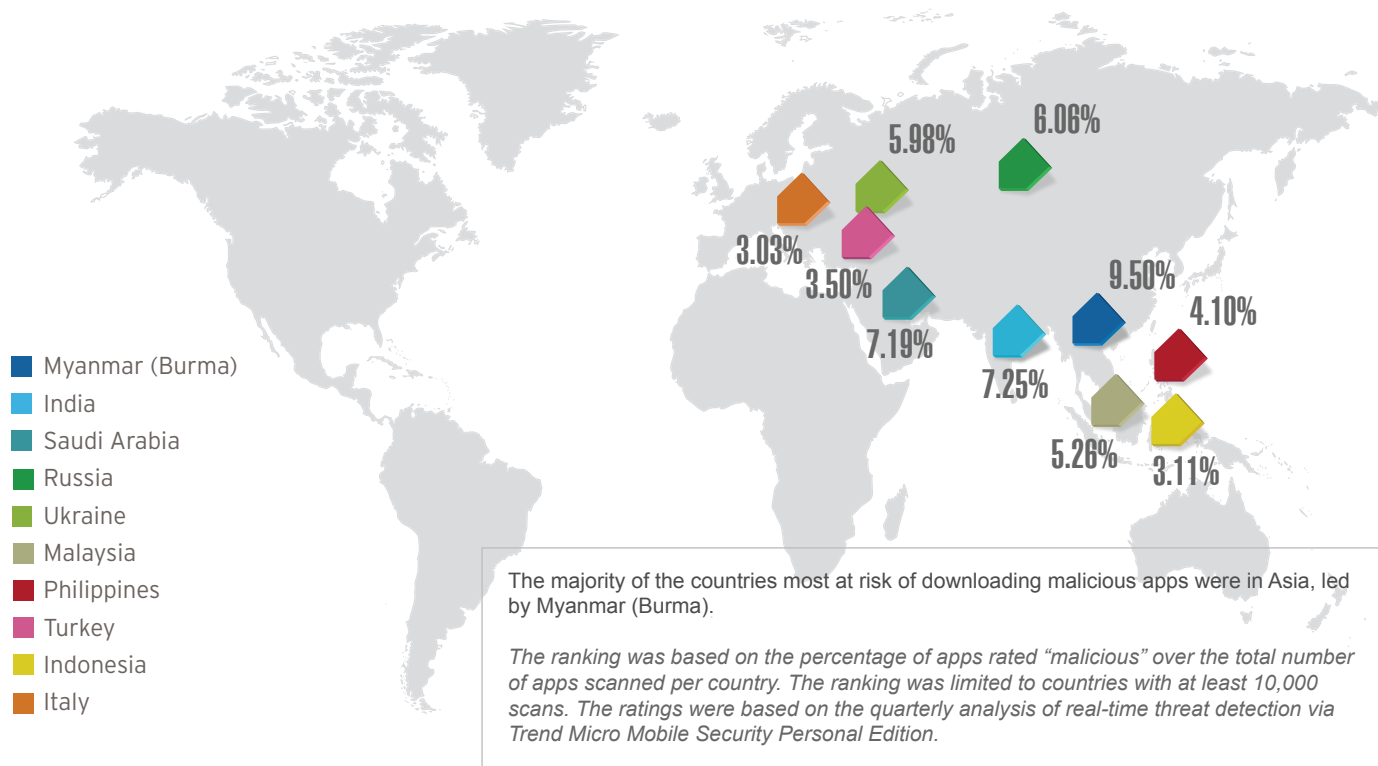
Countries Most at Risk of Privacy Exposure Due to App Use



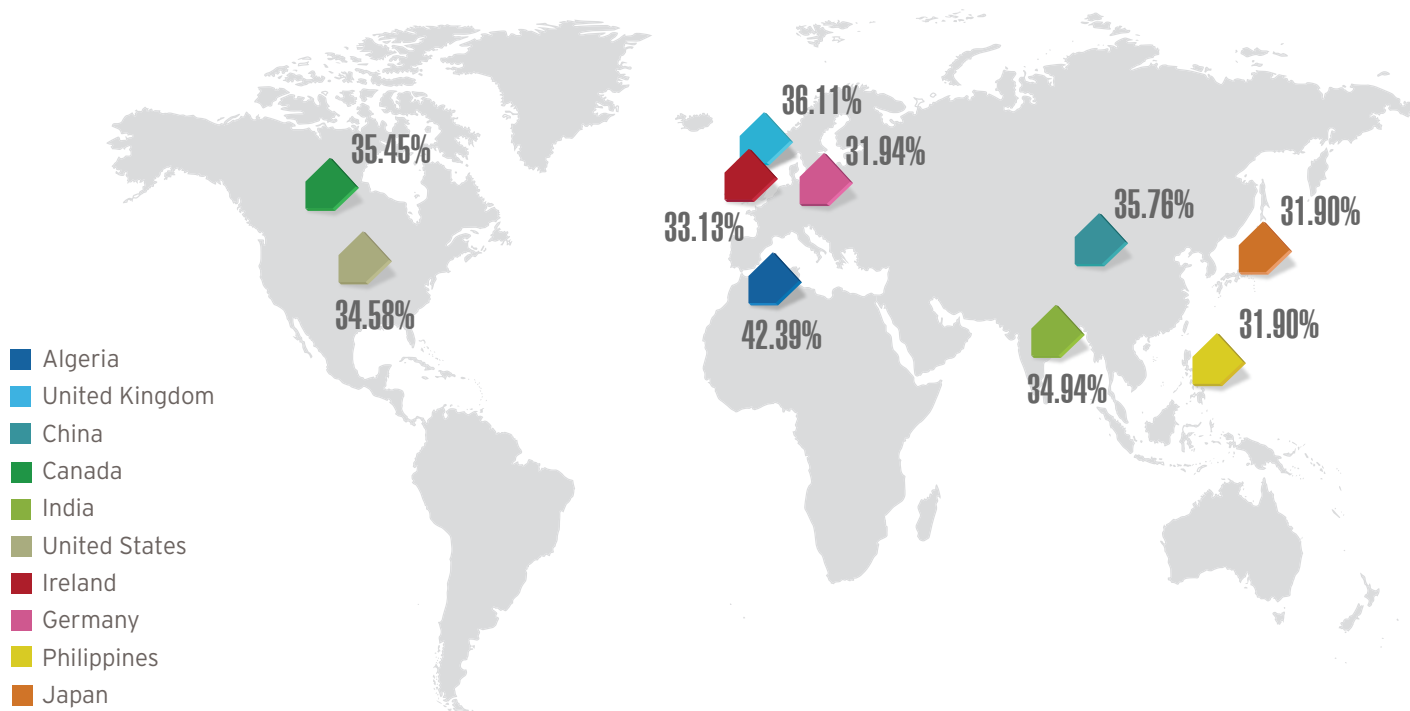
Android users from Saudi Arabia were most at risk of privacy exposure. This might have been due to the fact that almost all of the mobile users in that country take notice of mobile ads, which could have prompted dubious developers to create apps with aggressive advertising features.

The ranking was based on the percentage of apps categorized as "privacy risk inducers" over the total number of apps scanned per country. The ranking was limited to countries with at least 10,000 scans. The ratings were based on the quarterly analysis of real-time threat detection via Trend Micro™ Mobile Security Personal Edition.

Countries with the Highest Malicious Android App Download Volumes



Countries with the Highest Battery-Draining App Download Volumes



Users from Algeria downloaded the most number of battery-draining apps, closely followed by those from the United Kingdom and China. Having the ninth highest Internet penetration rate in Africa, Algeria may also become a likely web threat target.

The ranking was based on the percentage of apps categorized as "power hogs" over the total number of apps scanned per country. The ranking was limited to countries with at least 10,000 scans. The ratings were based on the quarterly analysis of real-time threat detection via Trend Micro Longevity.

APTs and Targeted Attacks: In Stealth Mode

MBR Wiper Attacks Target South Korea

- In mid-March, certain South Korean entities were targeted by a master boot record (MBR)-wiping Trojan.²³
- The attacks disrupted the targets' business by rendering systems, both clients and servers, unable to reboot.
- The samples we found either overwrite infected computers' MBR using certain strings or delete specific files and/or folders. Once overwritten, computer access either becomes limited or nonexistent.

²³ <http://blog.trendmicro.com/trendlabs-security-intelligence/summary-of-march-20-korea-mbr-wiper/>

FAKEM RAT Blends with Normal Traffic

- Like most remote access Trojans (RATs), FAKEM evades detection by blending in with normal network traffic.²⁴
- Unlike other RATs though, FAKEM traffic mimics Windows Messenger, Yahoo! Messenger, or HTML traffic to evade detection.²⁵

²⁴ <http://blog.trendmicro.com/trendlabs-security-intelligence/hiding-in-plain-sight-the-fakem-remote-access-trojan/>

²⁵ <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-fakem-rat.pdf>

RARSTONE Backdoor Imitates PlugX

- Like PlugX, the RARSTONE backdoor also loads an executable file in an infected computer's memory, apart from having its own set of unique tricks.²⁶
- RARSTONE hides its executable file by directly loading a backdoor in memory instead of dropping it onto the computer. Unlike PlugX though, it communicates via Secure Sockets Layer (SSL), which encrypts its traffic, allowing it to blend with normal traffic.

²⁶ http://blog.trendmicro.com/trendlabs-security-intelligence/bkdr_rarstone-new-rat-to-watch-out-for/

FAKEM Versus RARSTONE: RAT Techniques

FAKEM

RARSTONE



Arrives via spear-phishing emails



Arrives via spear-phishing emails



Usually disguised as files normally used in businesses (e.g., .DOC, .XLS, and .PDF)



Usually disguised as files normally used in offices (e.g., .DOC, .XLS, and .PDF)



Drops an .EXE file that initiates encrypted communication with C&C servers



Drops an .EXE file that drops a copy, which then opens a hidden Internet Explorer process and injects malicious code into a computer's memory; the code decrypts itself and downloads a .DLL file from a C&C server; the .DLL file is loaded in memory



Creates network traffic that mimics Yahoo! Messenger, Windows Messenger, and HTML traffic



Communicates with a C&C server using SSL



Despite certain differences in routine, both FAKEM and RARSTONE present novel ways to remain undetected by most anti-malware solutions.

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

TRENDLABSSM

TrendLabs is a multinational research, development, and support center with an extensive regional presence committed to 24 x 7 threat surveillance, attack prevention, and timely and seamless solutions delivery. With more than 1,000 threat experts and support engineers deployed round-the-clock in labs located around the globe, TrendLabs enables Trend Micro to continuously monitor the threat landscape across the globe; deliver real-time data to detect, to preempt, and to eliminate threats; research on and analyze technologies to combat new threats; respond in real time to targeted threats; and help customers worldwide minimize damage, reduce costs, and ensure business continuity.

