TrendLabs^{SM} 3Q 2014 Security Roundup

TREND MICRO™

Vulnerabilities Under Attack

Shedding Light on the Growing Attack Surface

Distributed by:

ITU

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.

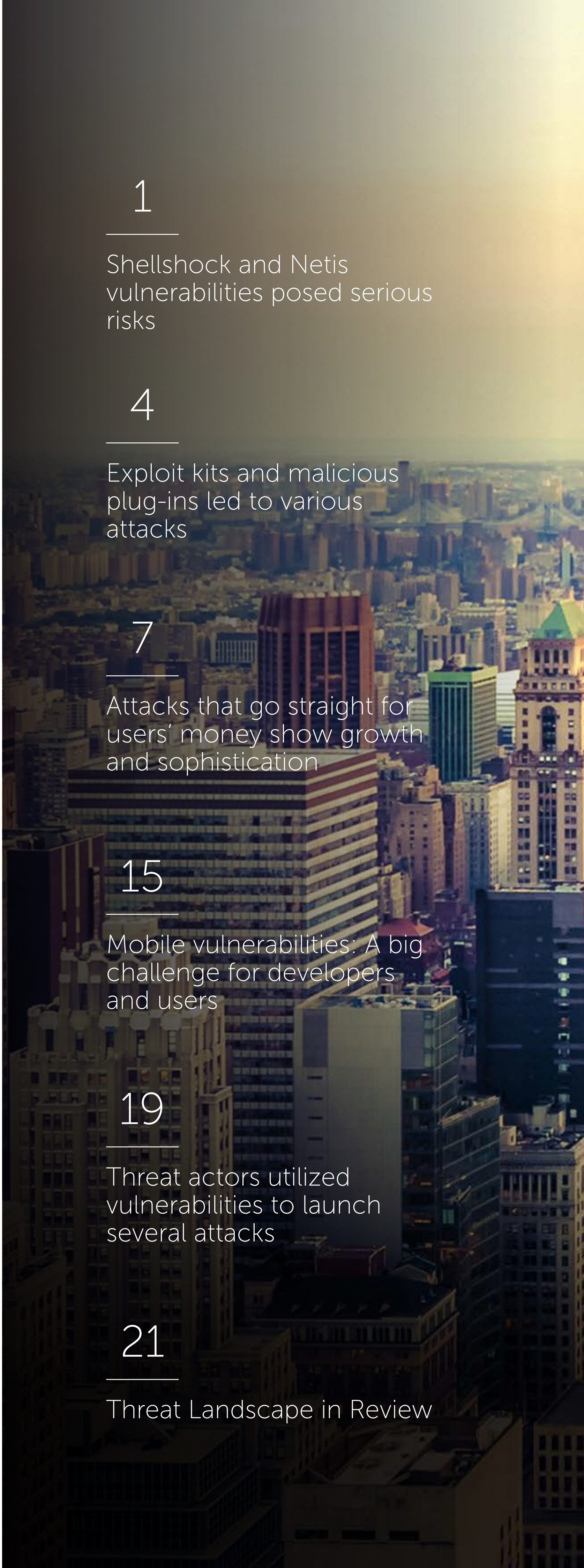
Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences 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.

ITU LEGAL NOTICE

The International Telecommunication Union (ITU) distributes the present publication as is and makes no representations or warranties of any kind, express, implied or otherwise concerning the publication, including without limitation warranties of title, ownership of intellectual property rights, merchantability, fitness for a particular purpose, noninfringement, accuracy or the absence of errors.

The name, abbreviation, title and logo of the ITU are the property of the ITU. All rights thereto are reserved.



Introduction

Following second quarter's infamous Heartbleed vulnerability, the industry found another serious vulnerability in open-source software: Shellshock. This vulnerability in the Bash shell, a common interface for directing commands to computers, Shellshock threatened to wreak havoc on Linux and UNIX computers and systems. This vulnerability allows attackers to run arbitrary commands through the Bash shell that can be used to gain access to sensitive user information or remotely take control over computers.

The third quarter showed us loopholes in often overlooked targets, such as routers and point-of-sale (PoS) systems. Routers and PoS systems, which can be used as attack vectors to steal information, play a critical role in handling information within a network as well as storing user information. Combining these points of entry with the possibility of human error (i.e., falling for social engineering lures, being tricked by fake emails, among others) spells out a massive attack surface, where everything can be vulnerable.

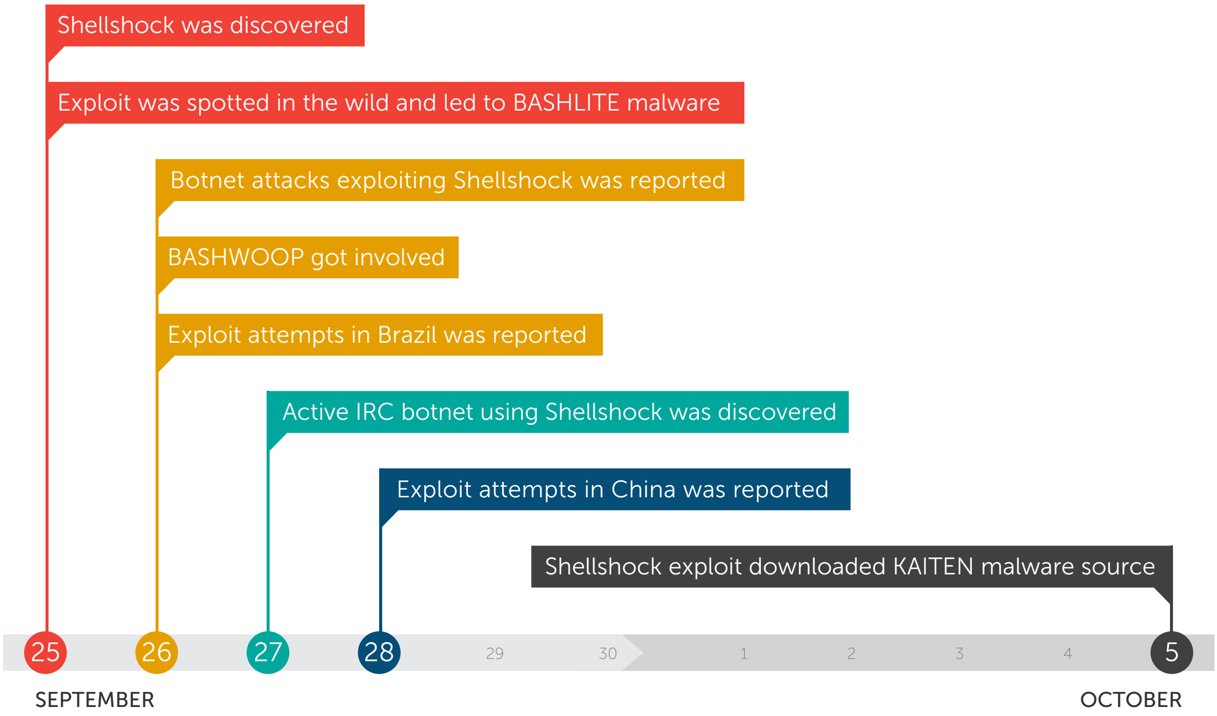
A good mix of secured systems and proper patch management can be considered a defense strategy against such attacks. Couple this with employee training and awareness on security can also help minimize the growing attack surface as more and more vulnerabilities continue to be uncovered.

NOTE: *All mentions of "detections" within the text refer to instances when threats were found on users' computers 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.*

Shellshock and Netis vulnerability posed serious risks

Another critical vulnerability, with impact similar to Heartbleed, surfaced at the latter part of September. The flaw, known as Shellshock, was found in most Linux and UNIX operating systems, as well as in Mac OS X.[1,2] This vulnerability posed an immediate threat to over half a billion servers and devices worldwide.[3,4] End users may not be directly at risk from Shellshock, but the Web servers and other systems they use could be, such as those that use the Secure Shell (SSH) network protocol. Exploiting this vulnerability is easy to carry out; the bug further emphasizes that open source components are now prime targets for attacks.[5] The handling of Shellshock reiterates the lesson from Heartbleed: open source software is in dire need of an advanced response framework similar to what other established software vendors built to handle these situations that endanger the global Internet.

Shellshock was notable last quarter due to the fact that it was not considered as an attack surface prior to its discovery. We spotted multiple attempts to exploit this vulnerability in different countries soon after it was discovered. Having gone unnoticed for years, this incident suggests that there might be more vulnerabilities in Bash or in applications previously thought safe.[6]


Shellshock was discovered
Exploit was spotted in the wild and led to BASHLITE malware
Botnet attacks exploiting Shellshock was reported
BASHWOOP got involved
Exploit attempts in Brazil was reported
Active IRC botnet using Shellshock was discovered
Exploit attempts in China was reported
Shellshock exploit downloaded KAITEN malware source
25
26
27
28
29
30
1
2
3
4
5
SEPTEMBER
OCTOBER

Shellshock Exploitation Timeline

Shellshock was exploited immediately after its discovery. It was used to spread DDoS malware, to build a botnet, and to gather information on vulnerable servers.

Weeks before the Shellshock was found, a hard-coded backdoor was found in Netis routers that allowed cybercriminals to easily run arbitrary codes.[7] Routers used as attack vectors are not essentially new, but the results from a scanning report[8] asserted that its impact cannot be underestimated.[9]

China registered the highest number of vulnerable Netis routers on a global scale, close to 99% of the total number of devices in current use. From the time we first reported this incident, the number of infected routers peaked at almost 1.9M units on August 30 and significantly dropped at the start of the following month. The lowest number registered was at 197K on September 9 but steadily rose to 800K by month end.

Netis patched the vulnerability in early September, although the update may prove to be ineffective because it only closed the port and hid its controls.[10]

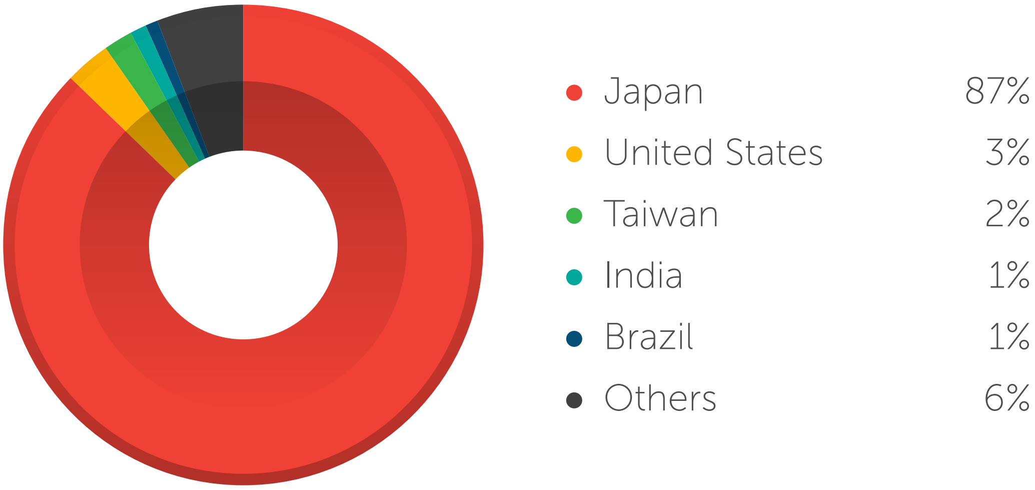
"Shellshock will continue to affect thousands of web applications in near and long term. The vulnerability is complex and has several attack vectors. It is already known that attacks can be carried out via HTTP, FTP, DHCP, CUPS, etc. It's just a matter of research that attackers will find more attack vectors. Also, the exposure via Web will continue to exist because of poor patching cycles, lack of awareness, etc.

The possibility of seeing another vulnerability as big as Shellshock in the future is likely. Heartbleed and Shellshock provided new avenues for attackers to look at. While the consumer malware still targets Microsoft™ Windows®-based machines, the server attacks are getting a lot of attention in the non-Windows world. The number of vulnerabilities in Apache software, JBoss, is very high compared to server vulnerabilities in Windows operating systems."

— Pawan Kinger
Director, Deep Security Labs

Exploit kits and malicious plug-ins led to various attacks

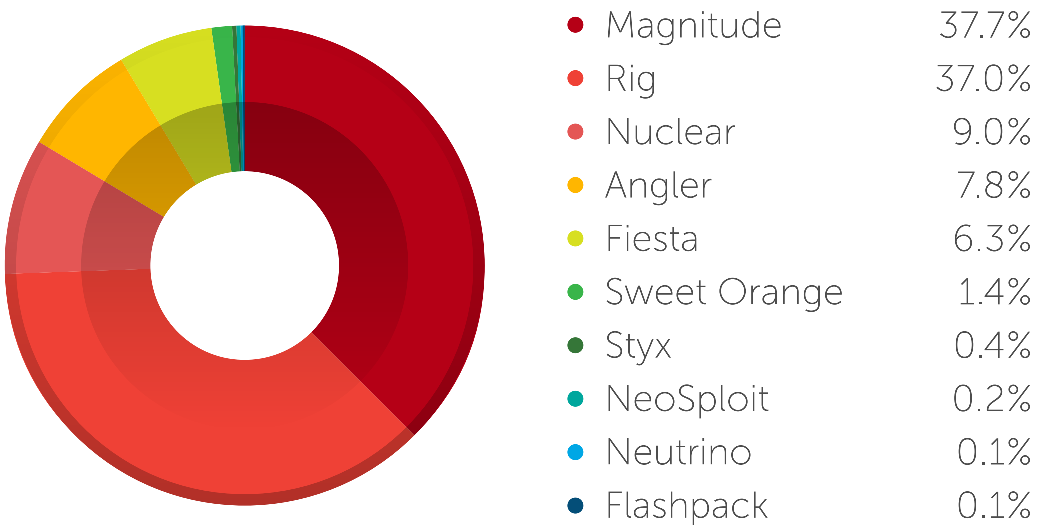
Exploit kits were heavily utilized last quarter, with FlashPack and Nuclear exploit kits seen in August and September, respectively. The FlashPack exploit kit used a compromised website add-on,[11] while the Nuclear exploit kit included Microsoft Silverlight in its roster of targeted software, expanding its attack surface.[12]



Distribution of Machines Infected by FlashPack

During a 17-day (Aug 1-17) monitoring, more than 60,000 users have been affected by this attack. This particular attack targeted Japanese users through a compromised website add-on.

Cybercriminals are not going to abandon using exploit kits anytime soon. Exploit kits are primarily used to create Web threats that deliver malicious payloads onto victims' computers and are sold in underground communities. The Magnitude exploit kit was the most frequently seen exploit kit in the third quarter.



Top Exploit Kits Based on Hits, 3Q 2014

Next to the Magnitude exploit kit, the Rig exploit kit's prevalence can be attributed to campaigns that changed their services from the FlashPack exploit kit by the end of August.

Another noteworthy vulnerability was the WordPress plugin that led to the compromise of the Gizmodo Brazilian regional site along with two different news websites. The vulnerability led site visitors to unknowingly download backdoor unto their machines, leaving around 7,000 users affected in just two hours.[13,14,15]

Google Chrome™ users were targeted by a malicious extension, which led to a chain of downloaded and dropped files that use legitimate-sounding file names like *flash.exe*.[16] Aside from dropping malicious files, the browser extension also disguises itself as an Adobe® Flash® Player extension.

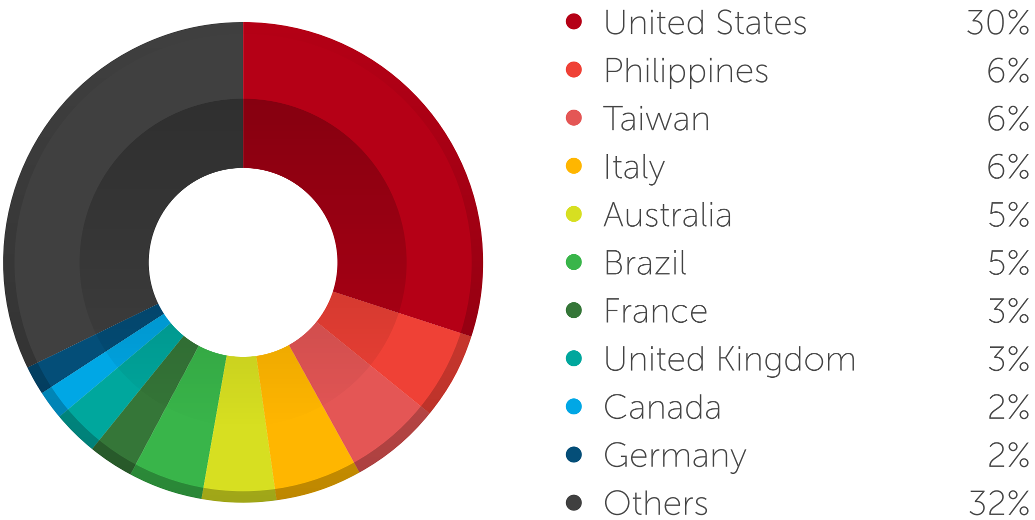
> “Exploit kits are notably more popular this year than the last. We’ve seen multiple exploit kit families get discontinued, revived, and later on, reengineered. Because of this cycle, I believe that exploit kits will continue to be used by cybercriminals who are out to make a quick buck. So far, the most abused platforms we’ve seen are limited to browsers. This means that a possible “combo kit” that detects Adobe Flash, Java and Microsoft Silverlight would be a highly successful infection vector.”

— Jay Yaneza

Senior Technical Manager

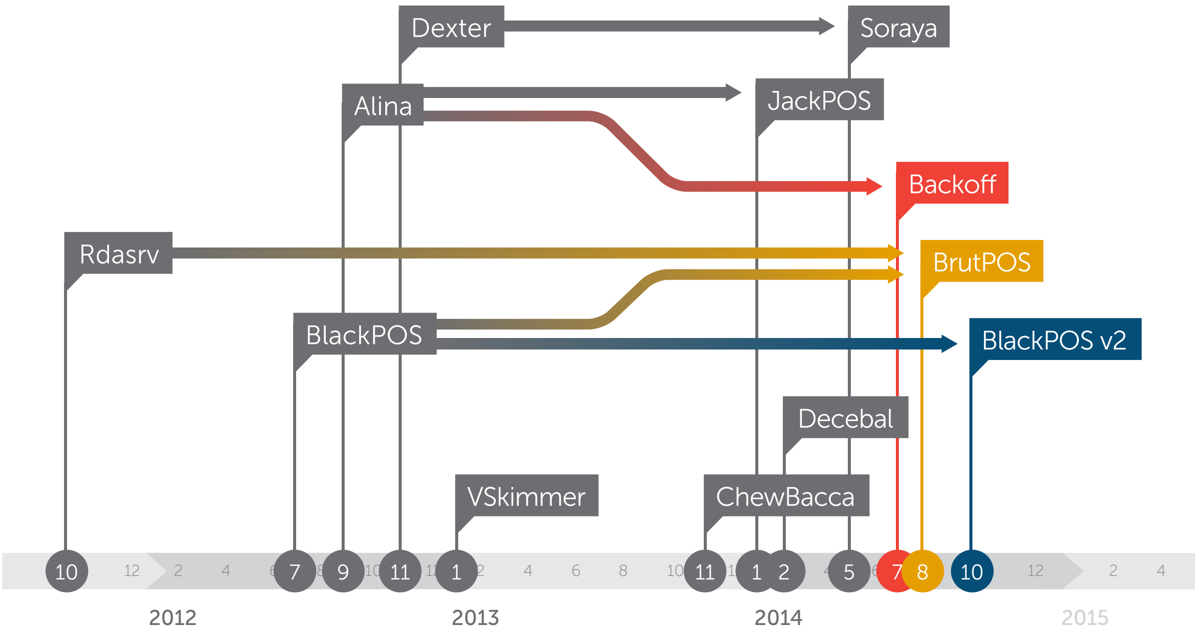
Attacks that go straight for users' money show growth and sophistication

Early this year, one of the largest retail companies in the U.S. disclosed that approximately 40 million consumer credit and debit card information was compromised as a result of a breach in its systems.[17] Not long afterward, Home Depot topped that record when it disclosed that more than 100 million customer records that included credit card information was stolen as a result of a payment systems breach.[18] The threat actors behind these breaches attacked the retailers' point-of-sale (PoS) systems. BlackPOS was implicated in the incident reported early this year, while BlackPOS version 2 was used in the Home Depot breach. This further indicates that PoS networks are highly accessible and vulnerable. Our findings reveal that the United States is at the top of a list of countries with the most PoS malware infections.



PoS Malware Infections by Country, 3Q 2014

The United States tops the list of countries with the most PoS malware infections. This may be due to the wide use of magnetic stripe cards.



Timeline and Relationships of PoS Malware

The arrows that connect the different malware refer to the evolved versions of the respective malware.

TIBRUN

a.k.a. BrutPOS

Known to target recognized PoS software, such as MICROS RES. Attackers using this PoS malware select its targets as opposed to launching attacks at random. BrutPOS was discovered in July 2014.

POSLOGR

a.k.a. Backoff

Involved in the Backoff PoS malware attack discovered in August 2014. This can steal financial information from infected devices. This malware was linked to the Home Depot data breach.

MEMLOG

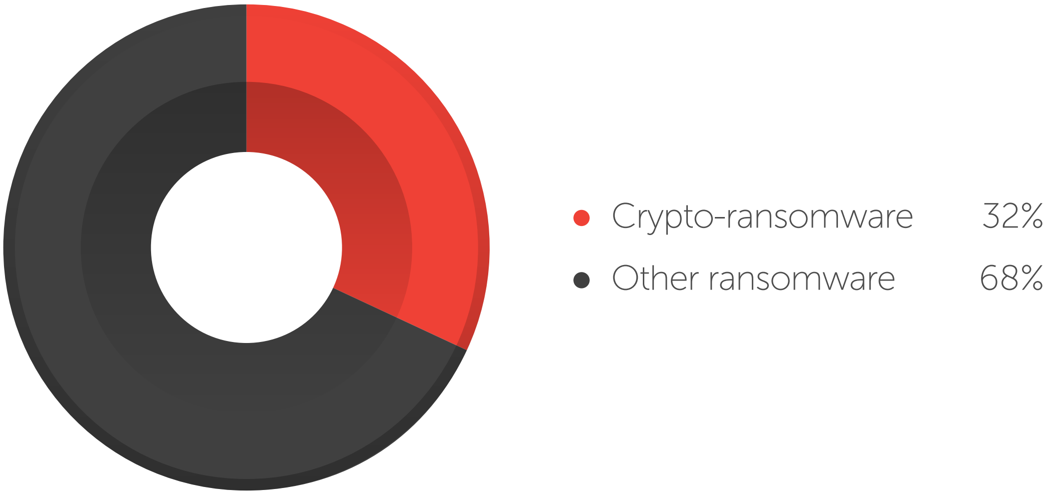
a.k.a. BlackPOS Version 2

This new variant of BlackPOS malware targets certain retail accounts. It also poses as an AV software service to evade detection.

New PoS Malware Seen in 3Q 2014

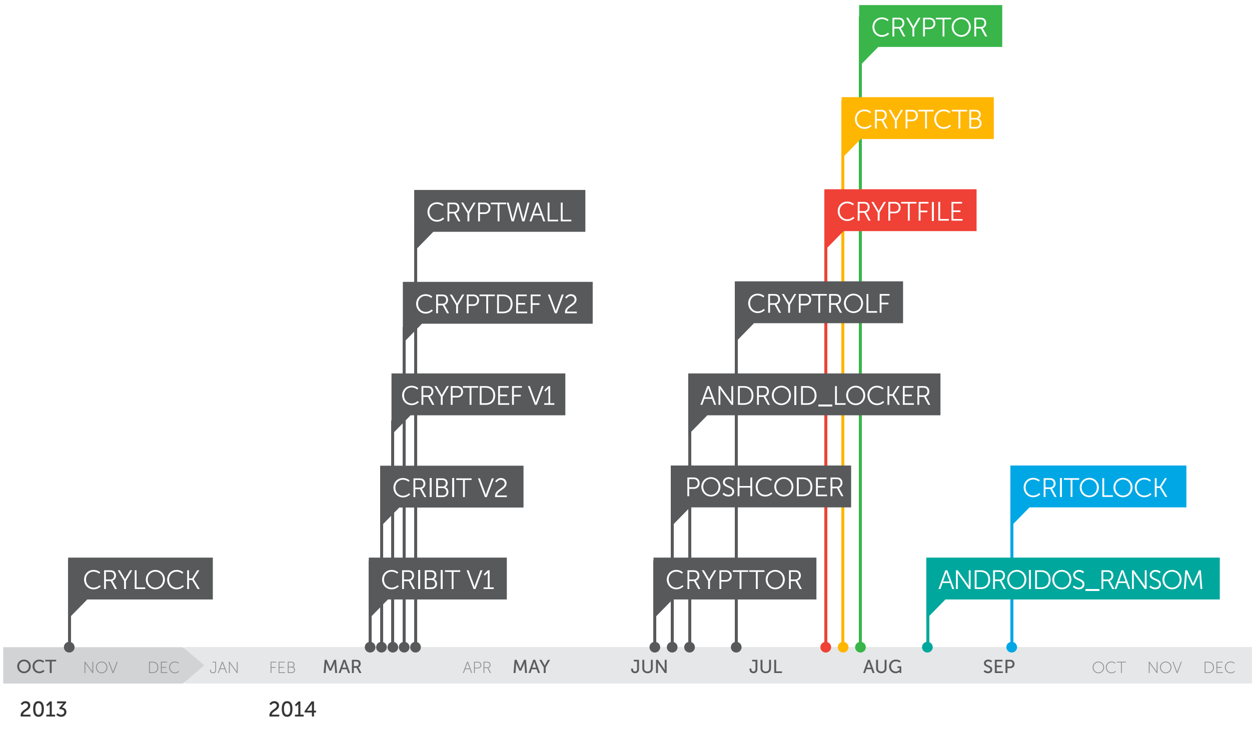
Ransomware forces users to pay money to regain access to their files. From being a scareware, some ransomware variants evolved into what we now know as crypto-ransomware. This is a sub-type that delivers on the threat by actually encrypting hostaged files. In the third quarter, crypto-ransomware accounted for more than a third of all ransomware found in the wild.

The crypto-ransomware variants we saw in the third quarter improved its capability to encrypt files, as well as evade detection.[19] So far, the most well-known crypto-ransomware family is CryptoLocker, which has affected users since late 2013.



Crypto-ransomware vs. Other ransomware

The crypto-ransomware share of infections increased from 19% to more than 30% in the last 12 months.



Timeline of the Emergence of Crypto-ransomware Variants in the Wild

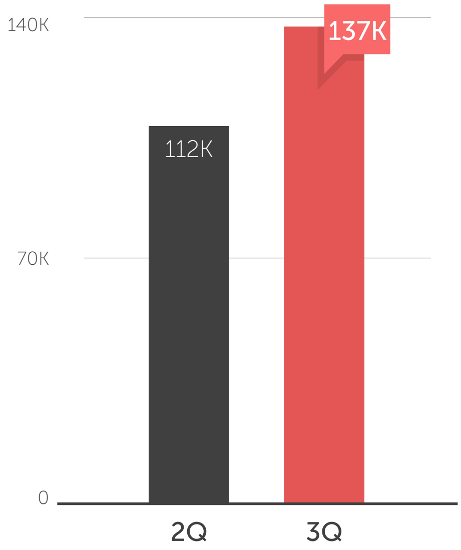
Compared to 2013, we saw an average of 4 to 5 crypto-ransomware variants in 2014.

MONTH	DETECTION NAME		BEHAVIOR
July	Cryptoblocker	TROJ_CRYPTFILE	Uses AES in its encryption code; creator seems to be new to ransomware.
	Cryptroni/ Critroni	TROJ_CRYPCTB	Use of elliptic curve cryptography. Uses Tor to mask its C&C communications.
	Xibow/BAT ransomware	BAT_CRYPTOR	Use of legitimate application GnuPG to encrypt files.
August	Mobile Ransomeware	ANDROIDOS_ RANSOM	Kills all running apps, encrypts data in SD card.
September	Cryptographic Locker	TROJ_CRITOLOCK	Uses .NET Framework to run, also uses AES.

Crypto-ransomware Variants Seen in 3Q 2014

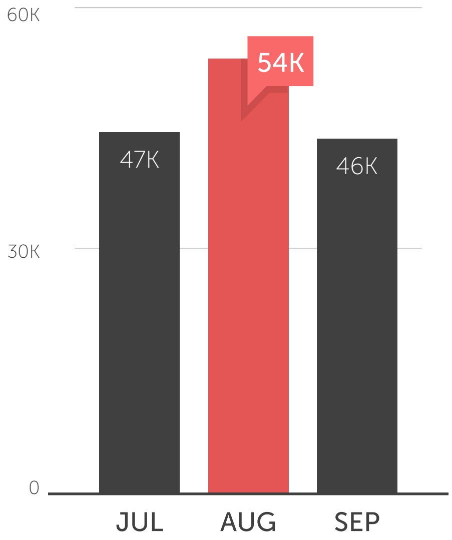
Crypto-ransomware variants seen in the last quarter used different encryption algorithms. TROJ_CRYPCTB used the most sophisticated cryptographic technique.

The online banking malware infections totaled to more than 137K this quarter and spread across the United States and Vietnam, among other countries. Compared with 200K infections in 3Q 2013,[20] the decline may possibly be due to the disrupted activities of the Gameover botnet.[21] This disruption had a significant effect on the scale of the ZBOT threat.



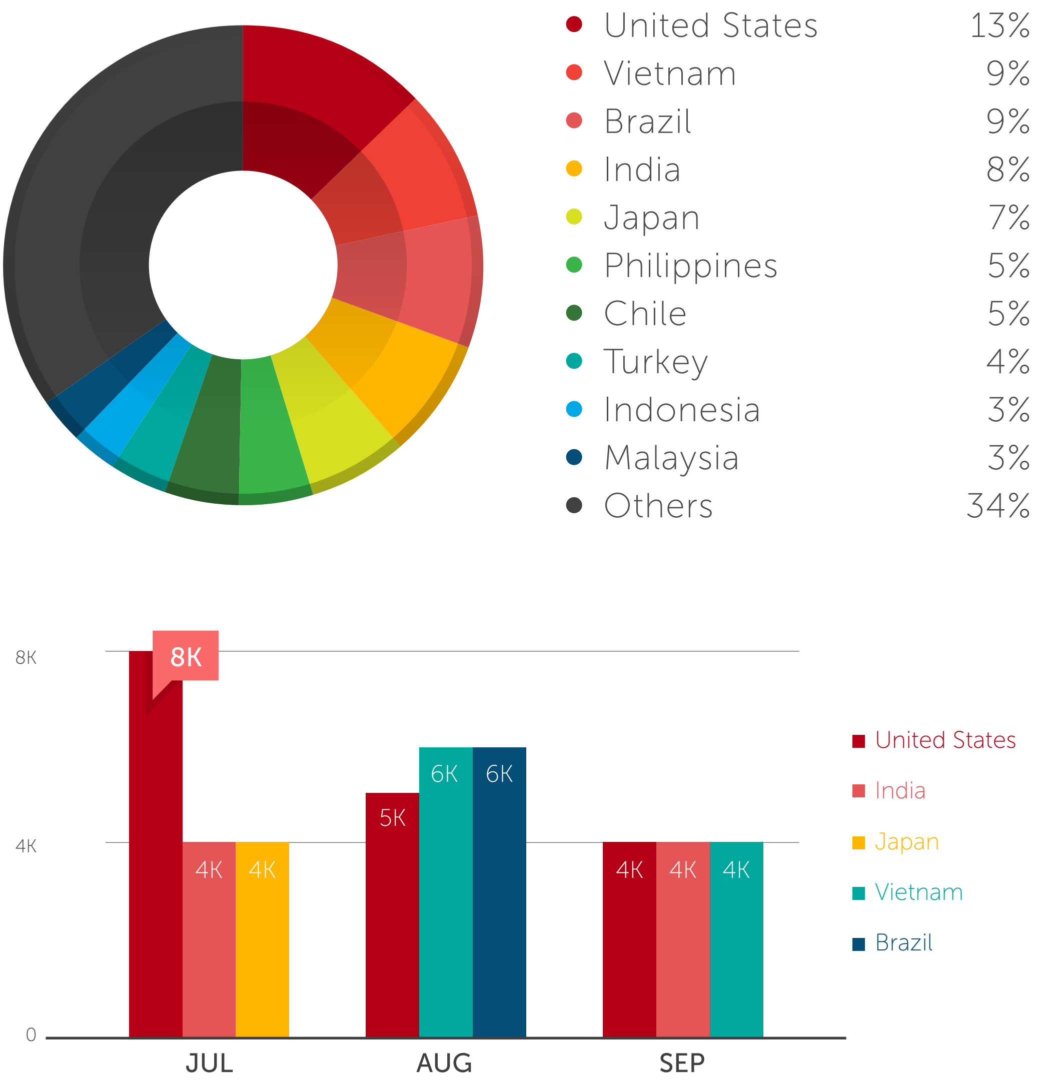
Online Banking Malware Infections Comparison, 2Q and 3Q 2014

Similar to the observed trend in the second and third quarters of 2013, online banking malware infections rose in the third quarter of 2014. The increase may be attributed to the holiday shopping season.



Online Banking Malware Infections, 3Q 2014

Online banking malware was most prevalent in August at around 54K infections. The total volume of online banking malware refers to the number of unique infections per month.

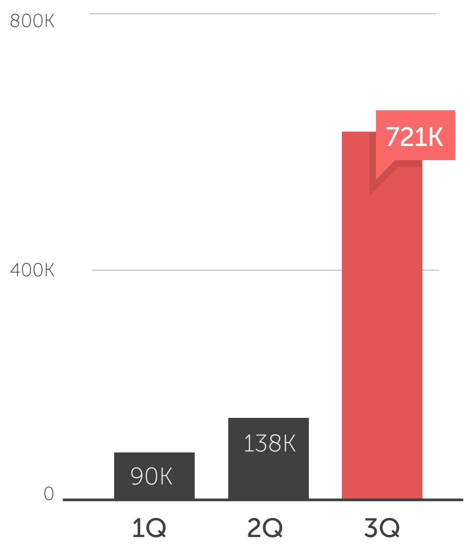


Countries Most Affected by Online Banking Malware, 3Q 2014

From being the top country most affected by online banking malware in the second quarter, Japan significantly dropped places because of the solutions created for VAWTRAK.

The high volume of online banking malware infections in the United States in July was due to ZBOT. Infections in Brazil and Vietnam rose last quarter. Both India and Vietnam infections were attributed to RAMNIT.

Phishing is still a viable means to get users' money. Social engineering lures coupled with spam contributed largely to phishing attacks. New techniques continue to emerge as various industries improved security against phishing attacks.[22]



Number of Phishing URLs Blocked, 3Q 2014

A huge increase in the number of phishing URLs was recorded in the last quarter. The increase may be due to a number of factors - new phishing techniques, new targets, uninformed users - to name a few. We saw phishing attacks targeting known brands such as Apple, PayPal, eBay, Google, and Twitter.

"Recently, the PoS RAM Scraper malware landscape has been going through numerous changes in quick progression. The malware itself is rapidly evolving: new families are emerging. We discovered existing families are being reengineered to become more efficient, and that victims are progressively getting larger in size. Attackers will adapt to security features put in place because that is their trade.

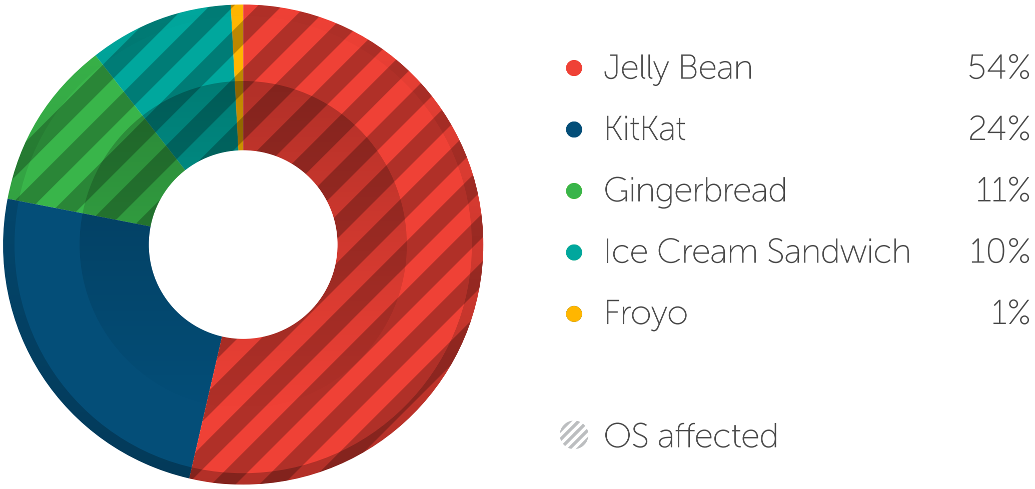
Worrisome developments have transpired in the last few months. New stolen credit card monetization methods are emerging, such as spoofing attacks that target EMV (EuroPay, MasterCard, and Visa credit cards with chip-and-PIN) technology. These are different from PoS-related attacks as EMV attacks bypass banks' fraud controls.

Unless retailers and merchants implement specialized hardware/software to protect card data in RAM, the data still remains vulnerable to PoS RAM scraper malware and EMV-related attacks. There is a slow shift toward implementing PoS ecosystems that support this data protection in RAM, and it'll be a couple of years before it is fully implemented everywhere. In the meantime, it is inevitable that cybercriminal gangs will continue their attacks."

— Numaan Huq
Senior Threat Researcher

Mobile vulnerabilities: A big challenge for developers and users

As in previous quarters, critical vulnerabilities were found in Android™. Unfortunately, released solutions are not available for all versions of the OS, further adding to the security issues of older Android devices. Take, for one, the FakeID vulnerability that allows apps to impersonate legitimate ones.[23] The Same Origin Policy bypass vulnerability also opens up Android's default browser to serious risks: attackers could potentially gather data from users who input their information on legitimate websites.[24] Although Google has released patches for these vulnerabilities, these does not always reach the majority of users because mobile patch deployments rely on device manufacturer and telecom providers.



Android Operating Systems Affected by FakeID and Android Browser Vulnerabilities

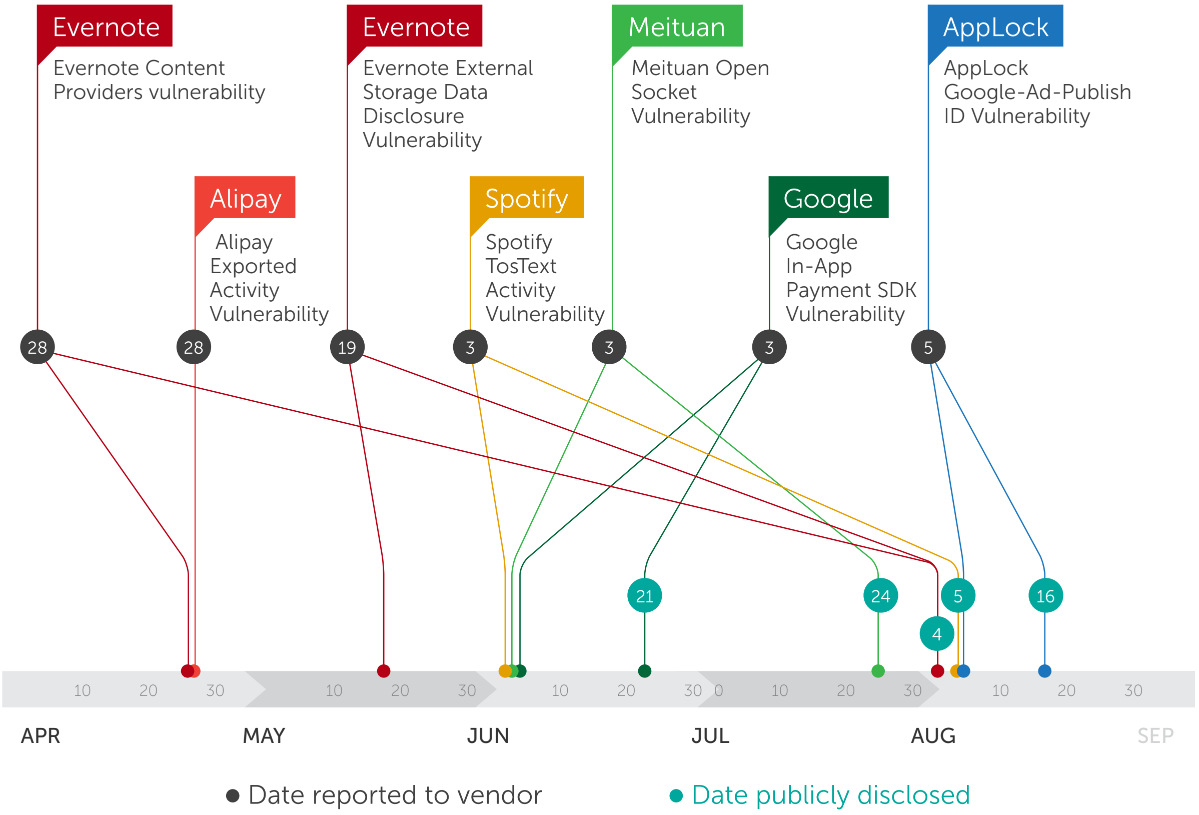
Over 75% of Android users are affected by both FakeID and Android browser flaws. Only KitKat is considered least affected. Note that the numbers above are based on Google Play OS distribution dashboard as reported in October 2014.

Source: *http://developer.android.com/about/dashboards/index.html*

The FakeID vulnerability may be exploited in the future just like how the Master Key vulnerability was exploited. While the FakeID vulnerability has yet to be exploited, this may soon change if it follows the same trend as the Master Key vulnerability.

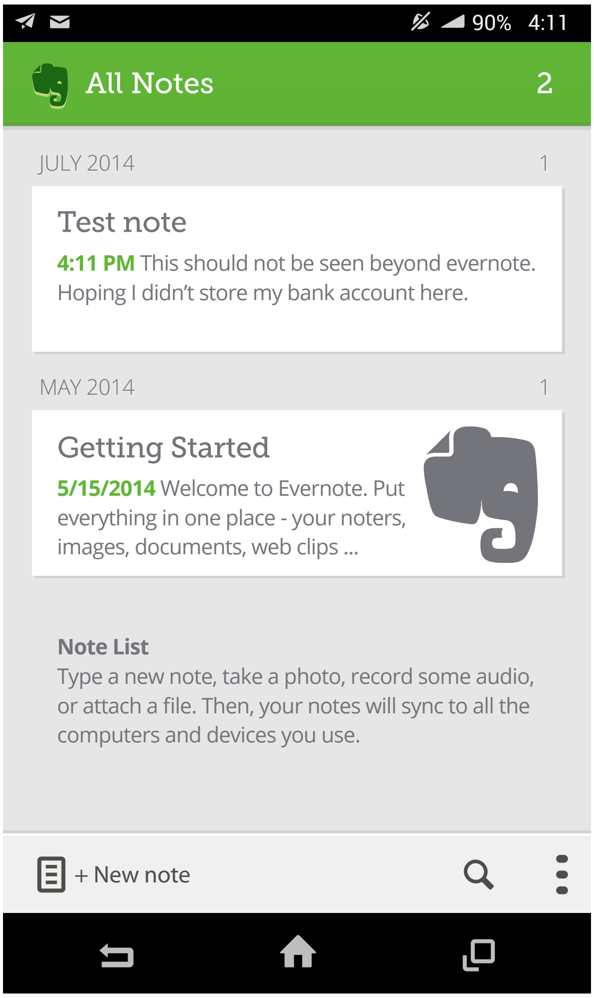
Legitimate Android apps were not spared either. We uncovered vulnerabilities in in-app payment software development kits (SDKs), namely, Google Wallet and the Chinese payment platform Alipay.[25,26] Vulnerabilities in popular apps like Evernote and Spotify were also exposed. The flaw we found in Spotify may be potentially abused by cybercriminals to launch phishing attacks, leading to data loss or theft.[27] Spotify quickly responded to our discovery by fixing the app version.

Evernote for Android, on the other hand, patched a vulnerability that may lead to user data being captured or used to launch attacks.[28] As more vulnerabilities in Android are discovered and while the Android update fragmentation still existing, the more likely cybercriminals will use exploits in mobile devices.



Timeline of Reported Vulnerabilities

All vulnerabilities listed above have been patched at the time of disclosure except the AppLock vulnerability.



JULY 2014 1

Test note

4:11 PM This should not be seen beyond evernote. Hoping I didn't store my bank account here.

MAY 2014 1

Getting Started

5/15/2014 Welcome to Evernote. Put everything in one place - your noters, images, documents, web clips ...

Note List

Type a new note, take a photo, record some audio, or attach a file. Then, your notes will sync to all the computers and devices you use.

In the Evernote Content Providers Vulnerability, users running Evernote below version 5.8.5 are exposed to the vulnerable component that may allow other apps to read or write certain data on the affected app.

Last quarter also showed that iOS devices are not at all safe from the threats that plague Android. In September, we found IOS_APPBUYER.A that ran on jailbroken devices. IOS_APPBUYER.A is a malware that hooks network APIs to steal users' Apple IDs and passwords. It spoofs proprietary protocols used by Apple to purchase apps from the Apple Store using the stolen Apple IDs and passwords.

This proves that even though iOS may be considered a secure mobile ecosystem, cybercriminals are still trying to find ways to infiltrate and bypass the iOS security measures.

"More and more mobile vulnerabilities, especially critical ones, will be discovered. To win customer trust, phone manufacturers and ROM/app providers will pay more serious attention to vulnerability response. Also, the bad guys are probably on to it. They will likely invest more in this area even for zero-day attacks. The mobile industry may not be mature enough in terms of vulnerability response, but there is progress. I have seen some app builders setting up response processes and teams. Google has made enhancements in releasing patches and hotfixes to help Android users get updates. Some mobile manufacturers are reacting faster than before in releasing OS-related patches."

— Leo Zhang

Mobile Threat Security Manager

Threat actors utilized vulnerabilities to launch several attacks

In the third quarter, we saw targeted attack malware families, KIVARS and MIRAS, infect 32- and 64-bit systems.[29,30] As more and more companies are adopting 64-bit OSes, currently at 81% market share,[31] threat actors are looking for ways to be able to inject code in 64-bit systems to widen the scope of their attack. This tells us that the probability of targeted attacks using 64-bit malware may increase over time.

Various targeted attacks revealed that attackers use different techniques in order to gain control over compromised machines. Apart from spear phishing, we noted that publicly available blogs were used as C&C servers in August.[32] Along with the external attacks, incidents of targeted attacks orchestrated from the inside were also seen.

One incident where a breach was caused from within the company was the Amtrak data breach. A former employee was found to have sold passengers' personally identifiable information (PII) since 1995.[33] A data management policy should thus be strictly enforced to defend against external- and internal-facing loopholes.

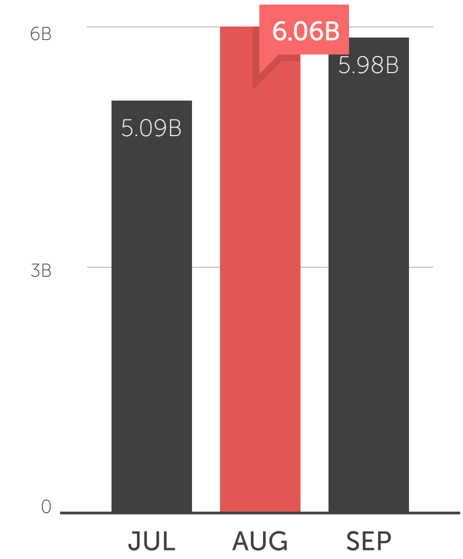
As such, network administrators should be able to spot such indicators of compromise (IOCs) and implement effective network monitoring.

> “A threat actors’ strategy is all about precision, covert operations, and adaptations. Traditional security, such as firewall, intrusion prevention, and policy enforcement, will all be less useful to find attacks made against networks. The security industry must set up new concepts to differentiate unusual and suspicious events from low-risk events, and use correlated threat intelligence to successfully identify and thwart targeted attacks.”

— Ziv Chang
Senior Threat Researcher

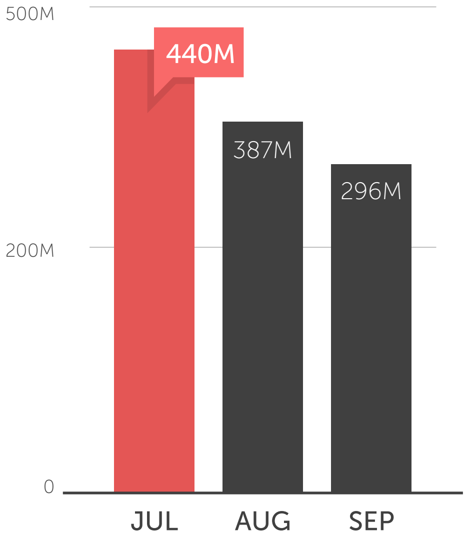
Threat Landscape in Review

Malware, Spam, and URLs



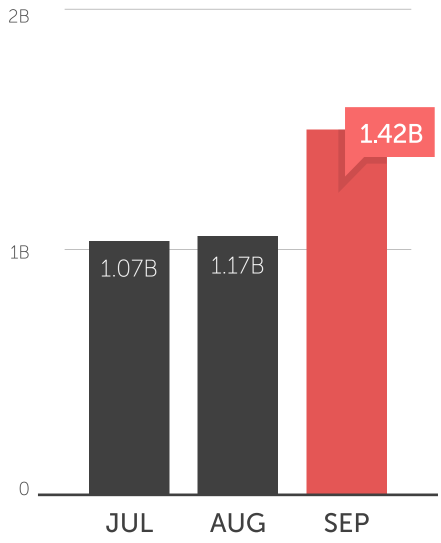
IP Address Queries Identified by the Trend Micro Smart Protection Network as Spam-sending IPs, 3Q 2014

The number of hits blocked from spam-sending IP addresses increased from last quarter's 13.5 billion.



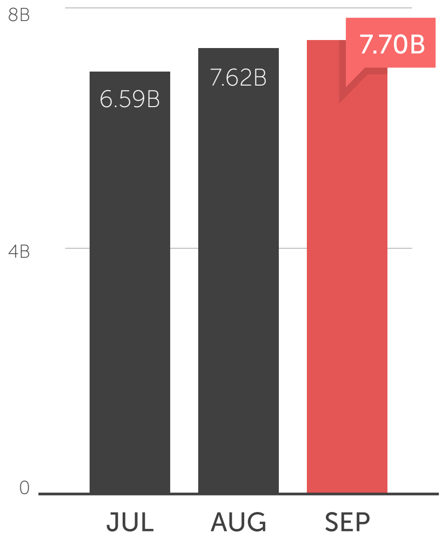
Visits to Malicious Sites Blocked by the Trend Micro Smart Protection Network, 3Q 2014

The number of hits to malicious sites blocked in July rose against the previous month's 412 million. September registered a significant drop.



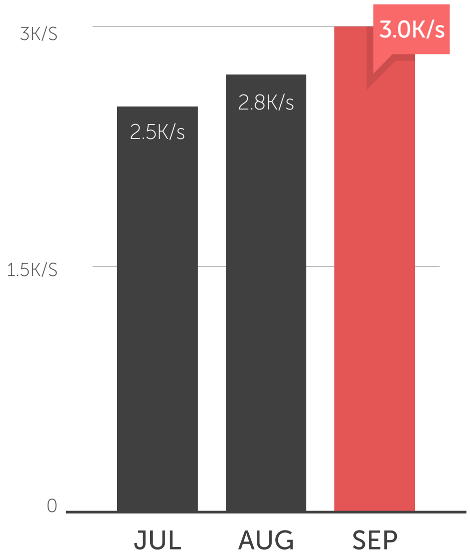
Malicious Files Detected by the Trend Micro Smart Protection Network, 3Q 2014

The number of malicious files blocked in September is the highest since April 2014.



Threats Blocked by the Trend Micro Smart Protection Network, 3Q 2014

We blocked an average of 7.3 billion threats per month this quarter, indicating a 2B increase from last quarter's 5.8 billion.



Trend Micro Smart Protection Network Overall Detection Rate, 3Q 2014

We blocked an average of 2.8 threats per second in the third quarter, compared to 2.3 threats per second blocked in the second quarter.

NAME	VOLUME
ADW_INSTALLCORE	333K
ADW_SPROTECT	294K
ADW_OPENCANDY	268K

NAME	VOLUME
PE_SALITY	104K
WORM_DOWNAD	80K
WORM_GAMARUE	56K

Top 3 Adware, 3Q 2014

ADW_INSTALLCORE remained the top adware for the quarter. ADW_SPROTECT was a new addition to the top 3.

Top 3 Malware, 3Q 2014

PE_SALITY, a file infector malware family, was the top malware for the quarter. Variants of this malware family are known to terminate anti-malware processes, adding to the difficulty of removing it in systems.

	NAME	VOLUME
Enterprise	WORM_DOWNAD	57K
	PE_SALITY	34K
	LNK_DUNIHI	29K
SMB	WORM_DOWNAD	12K
	PE_SALITY	8K
	TROJ_PIDIEF	8K
Consumer	PE_SALITY	44K
	PE_VIRUX	28K
	WORM_GAMARUE	28k

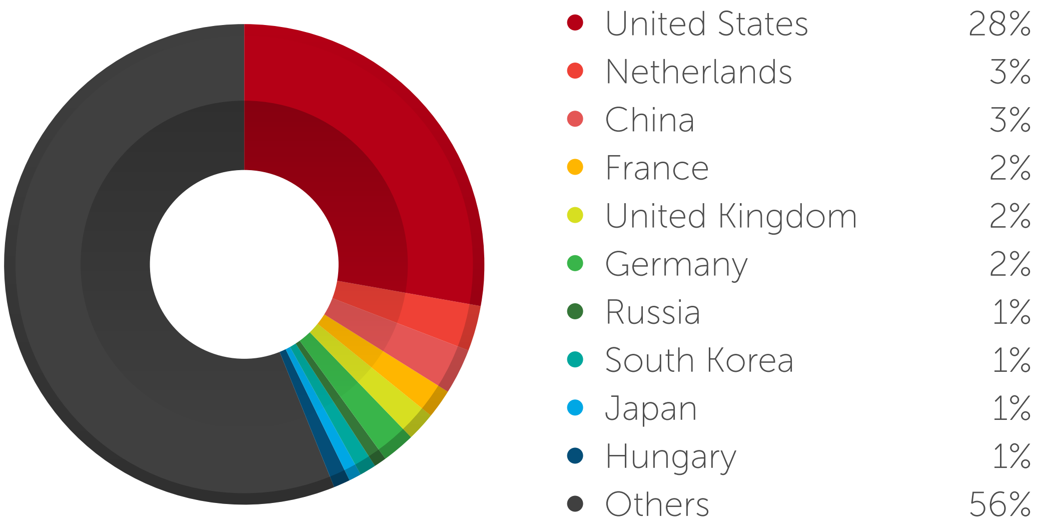
Top 3 Malware by Segment, 3Q 2014

WORM_DOWNAD continues to be a threat to enterprises, but is on a steady decline since 2013.

DOMAIN	REASON FOR BLOCKING ACCESS TO
flyclick.biz	Redirects to different ad sites that are recently registered. Domain registrations for said ad sites are less than a year.
cnfg.toolbarservices.com	Contains pop-ups and browser hijackers.
ads.alpha00001.com	Contains records related to browser hijacker that redirects user without their consent, changes home page, etc.
www .ody.cc	Related to the malware TROJ_VSTART.SMA.
optproweb.info	Downloads malicious files.
sugoi.pomf.se	Is used to upload malicious files.
s.ad120m.com	Contains malicious pop-up advertisements.
grade-well.com	Contains malicious records about Proxy Tunnel Trojan.
trafficconverter.biz	Related to the malware WORM_NGRBOT.EOQD.
downloaddspider.com	Downloads malicious files.

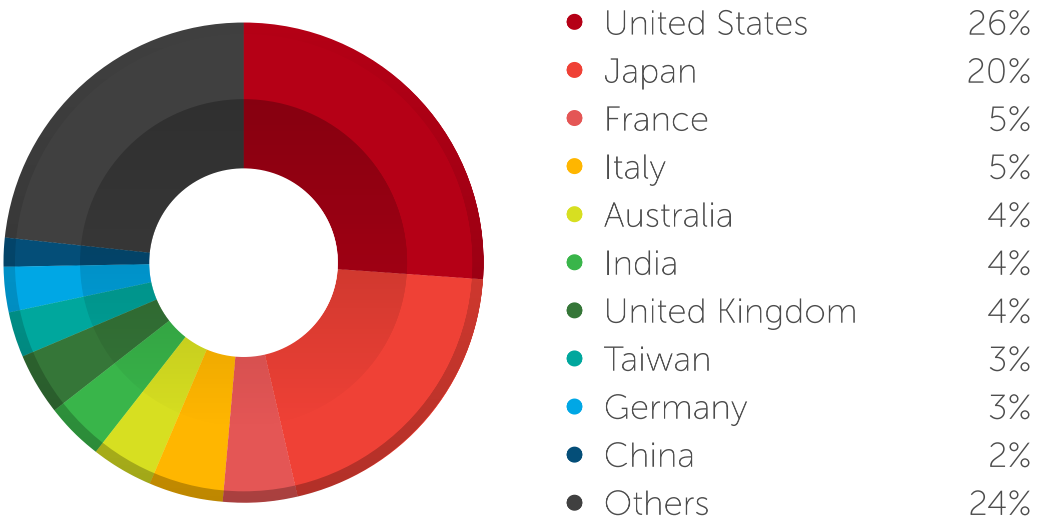
Top 10 Malicious Domains the Trend Micro Smart Protection Network Blocked Accessed To, 3Q 2014

Flyclick.biz rose to the top of the list from being at the 7th place as it redirected users to different ad sites.



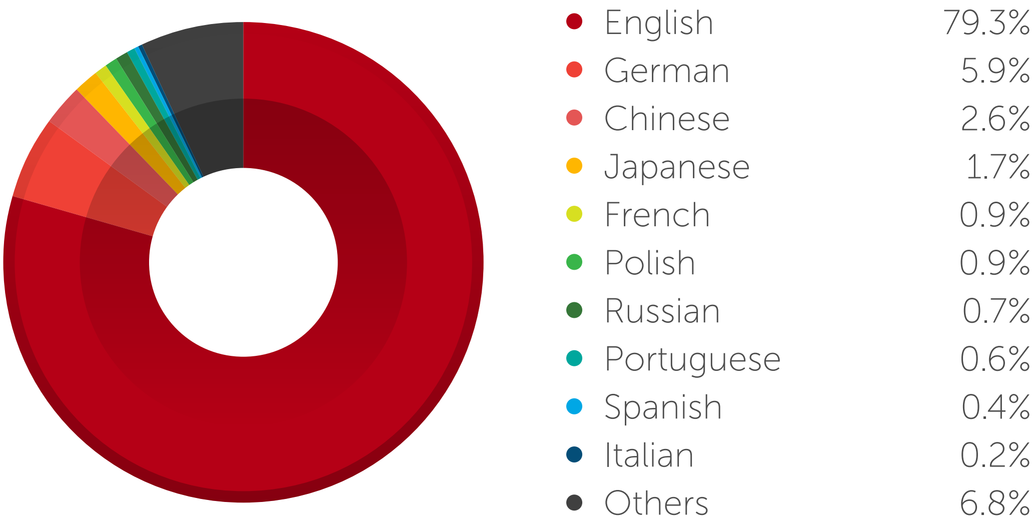
Top 10 Malicious URL Country Sources, 3Q 2014

The United States topped the quarter, showing a 3% increase from last quarter.



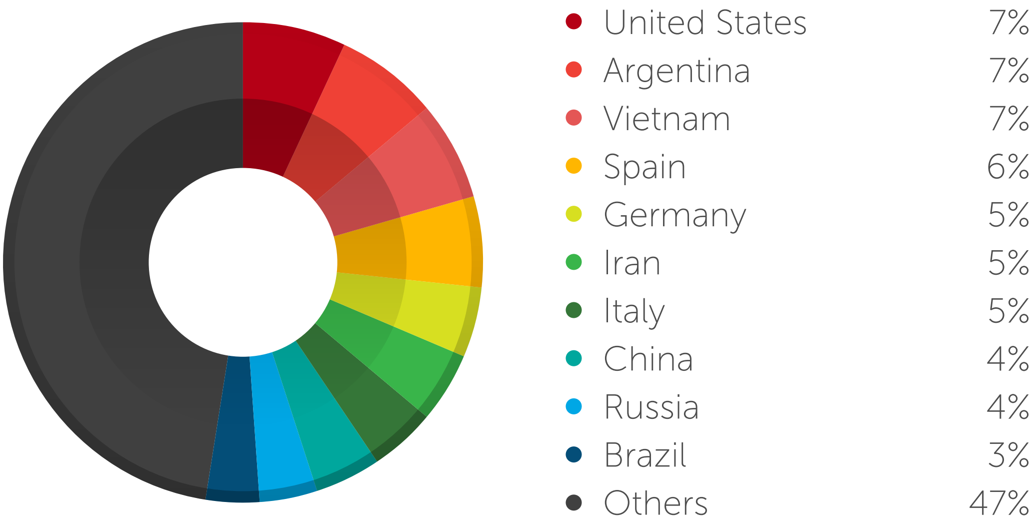
Countries with the Highest Number of Visits to Malicious Sites, 3Q 2014

The United States and Japan still top the list.



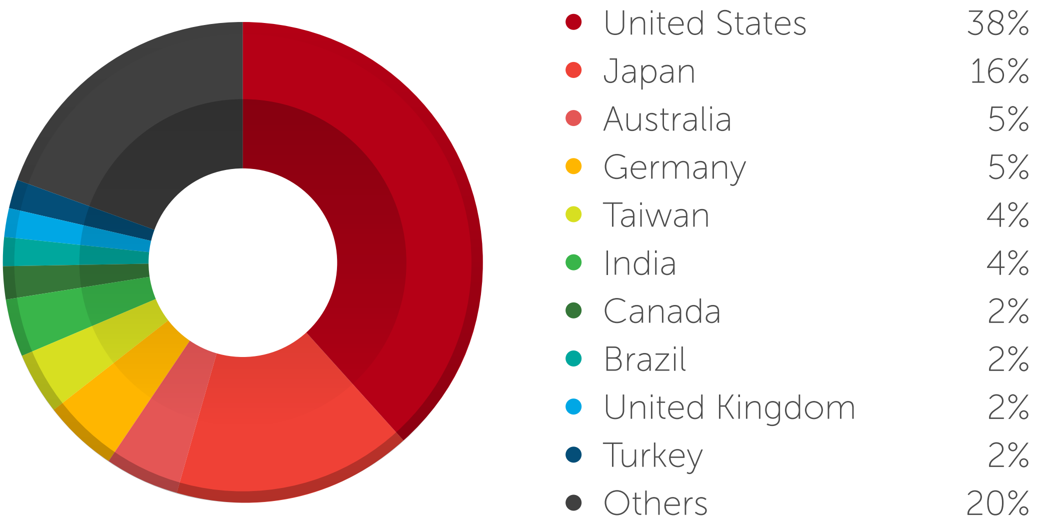
Most-used Spam Languages, 3Q 2014

Consistent with every quarter, English retained the top spot.



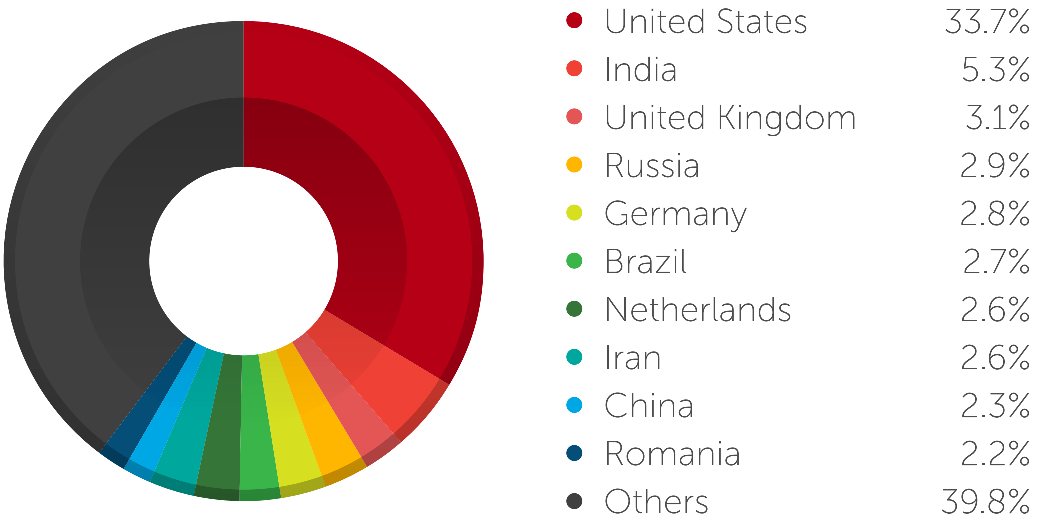
Distribution by Country of Spam Sent as Identified by the Trend Micro Smart Protection Network, 3Q 2014

The United States tops the list last quarter.



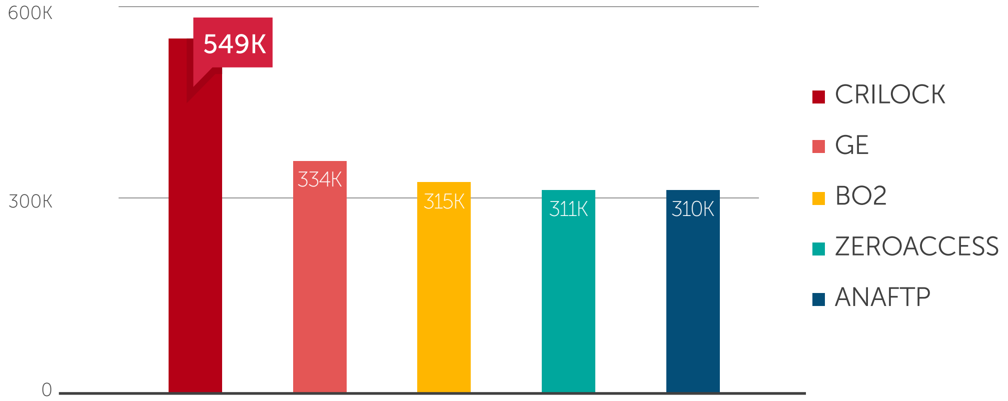
Connections from Endpoints to C&C Servers

The United States has the most number of affected endpoints, twice as much as that of Japan.



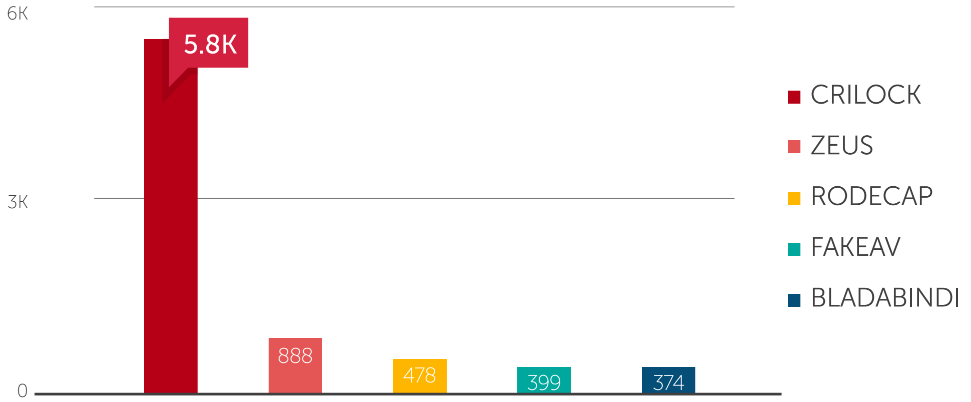
Location of C&C Servers

The United States hosted more than a third of all C&C servers in the third quarter.



Number of Infected Machines Connecting to Malware-related C&C Servers

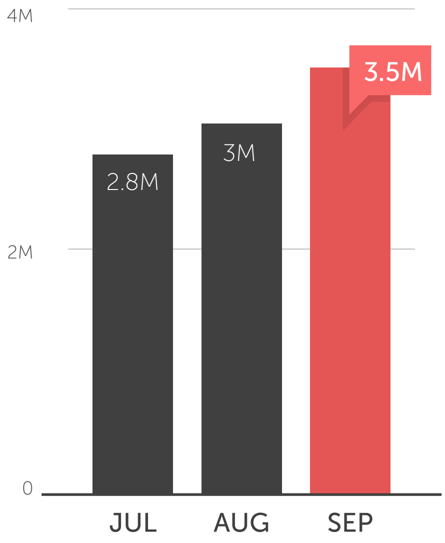
More than half a million infected machines were observed to be connecting to CRILOCK-related C&C servers.

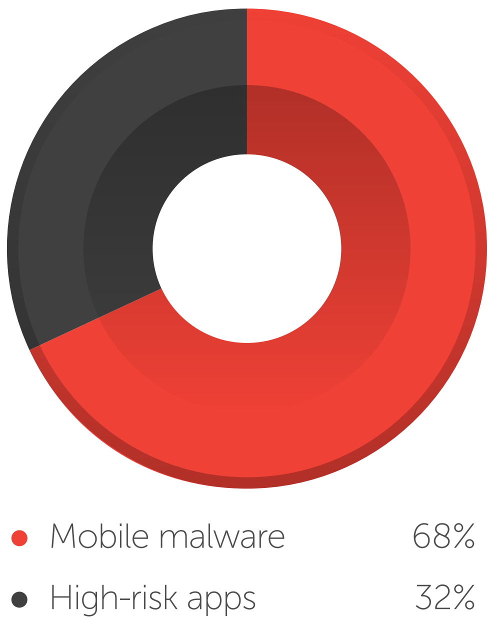


Number of Malware-related C&C Servers, 3Q 2014

Consistent with number of infected machines, the number of CRILOCK-related servers found is significantly higher than other malware families.

Mobile Threats

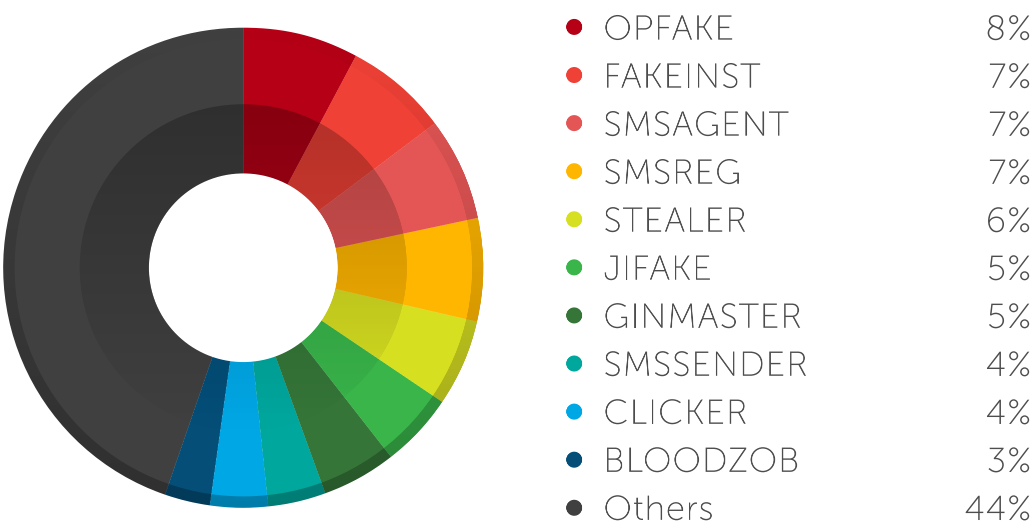




Cumulative Android Threat Volume as of 3Q 2014

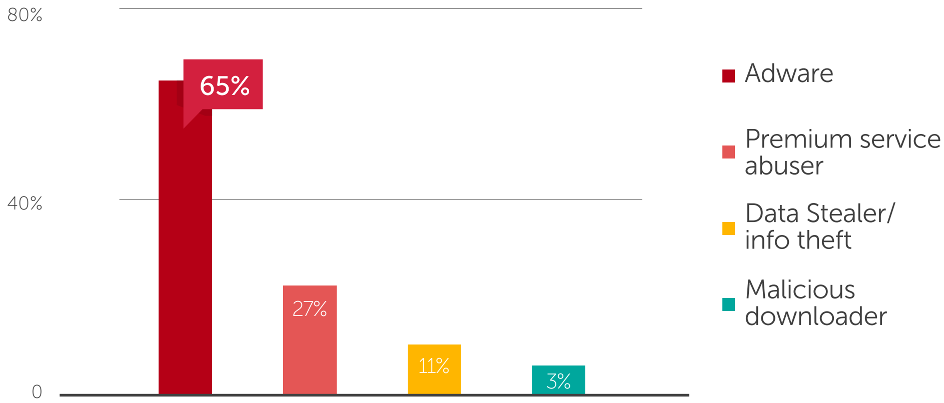
September saw the most number of added Android threats for both high-risk and malicious apps.

NOTE: *High-risk or potentially unwanted apps are those that can compromise user experience because they display unwanted ads, create unnecessary shortcuts, or gather device information without user knowledge or consent. Examples of these include aggressive adware.*



Top Android Malware Families, 3Q 2014

OPFAKE remained at the top last quarter. However, it registered a decline compared to its 14% share in the second quarter of 2014.

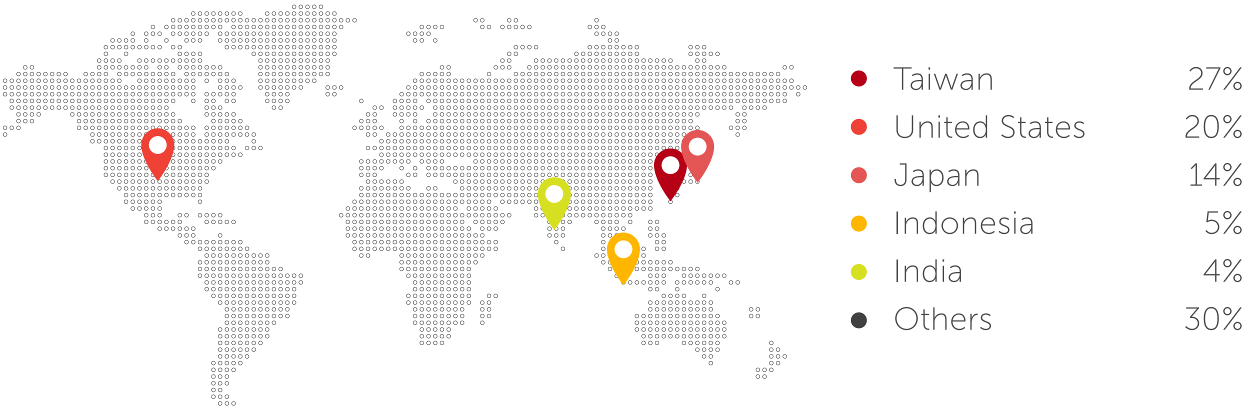


Top Android Threat Type Distribution, 3Q 2014

Adware is still the largest threat type, although there is a decrease, compared to the second quarter of 2014. Premium service abusers (PSA) and data stealers increased.

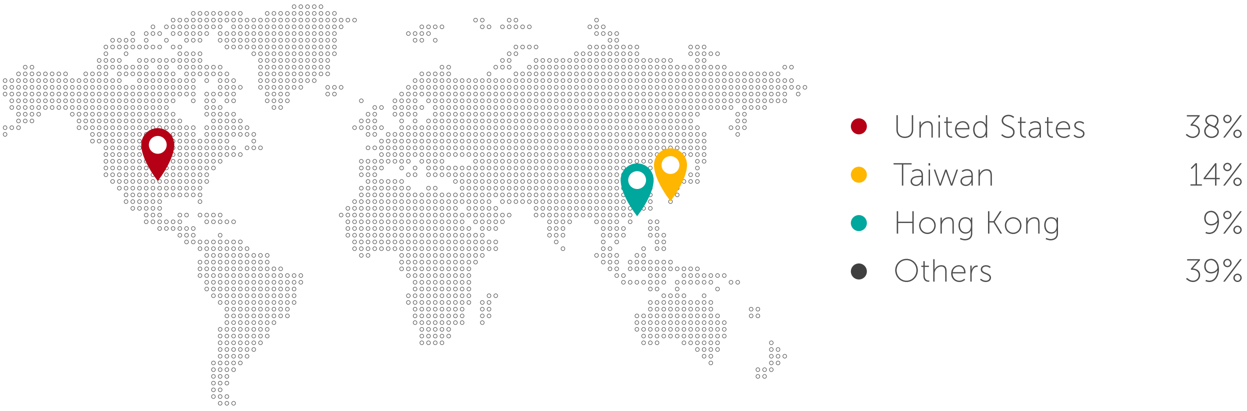
***NOTE:** PSAs register victims to overpriced services while adware aggressively push ads and could collect personal information without victim consent.The distribution numbers were based on the top 20 mobile malware and adware families that comprised 71% of the total number of mobile threats detected by the Trend Micro Mobile App Reputation Technology from July to September 2014. A mobile threat family may exhibit the behaviors of more than one threat type.*

Targeted Attacks and Data Breaches



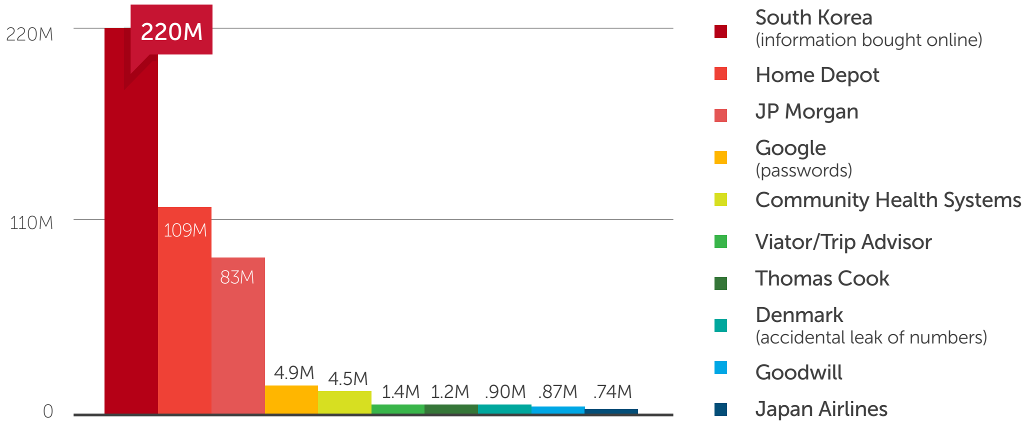
Targeted Attack Victim Locations, 3Q 2014

Taiwan and the United States were the two most targeted countries. The distribution of victim countries last quarter was rather broad, which shows that attacks are becoming more distributed globally.



Targeted Attack-related C&C Server Locations, 3Q 2014

Locations of C&C servers related to targeted attacks mostly comprised of the United States, Taiwan, and Hong Kong



Reported Data Breach Incidents in 3Q 2014

Sources:
http://koreajoongangdaily.joins.com/news/article/Article.aspx?aid=2993858
https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf
http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/?_php=true&_type=blogs&_r=0
http://www.cbsnews.com/news/russian-hackers-steal-5-million-gmail-passwords/
https://www.trustedsec.com/august-2014/chs-hacked-heartbleed-exclusive-trustedsec/
http://www.viator.com/about/media-center/press-releases/pr33251
http://www.telegraph.co.uk/technology/news/10990756/Former-Thomas-Cook-subsidiary-fined-150000-over-internet-security-breach.html
http://cphpost.dk/news/security-breach-leaks-900-000-cpr-numbers.10100.html
http://www.goodwill.org/press-releases/goodwill-provides-update-on-data-security-issue/
https://www.jal.co.jp/en/info/other/140924.html

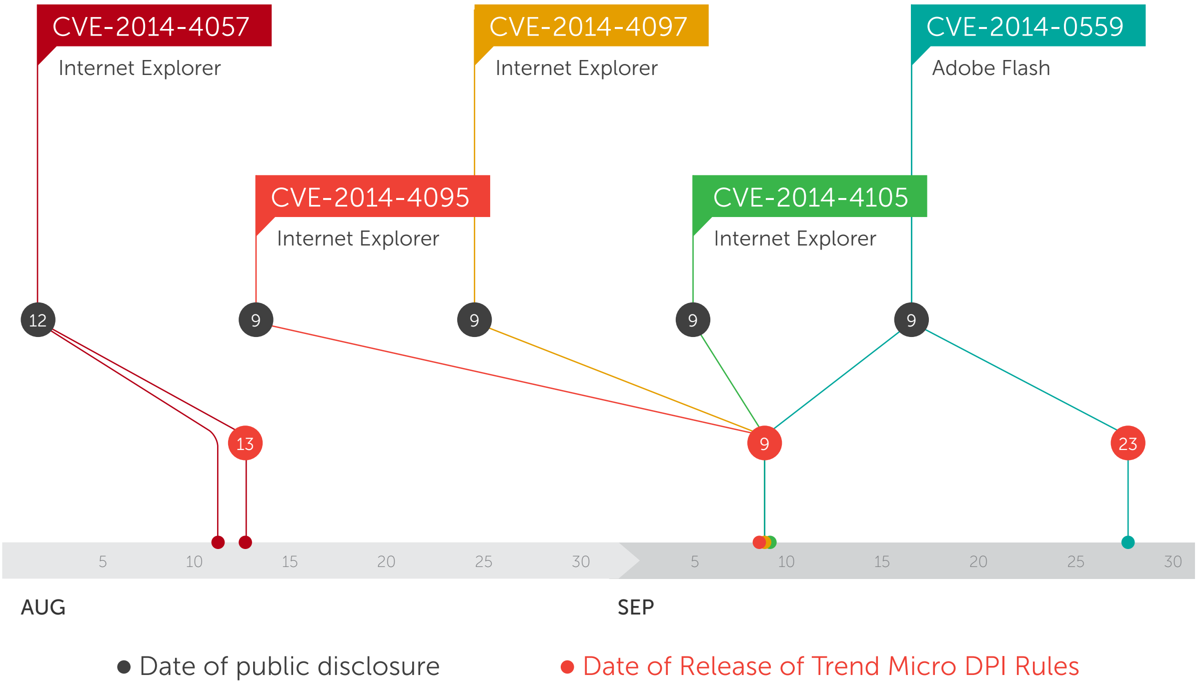
Digital Life and Internet of Everything

Last quarter we highlighted various aspects of users' digital lives with respect to the continuous growth of the IoE/IoT phenomenon. We tackled the use of smart meters within a smart grid scenario that opens up new attack vectors.[34,35] The security implications of smart wearable devices also came into focus as the quarter signaled a rise in new gadget types, which we divided into three major categories: "In" devices, "out" devices, and "in and out" devices.[36] Because it is equally important to consider how to manage all these wearables, we also discussed how the Administrator of Things (AoT) plays a crucial role in the security of every smart household.[37] We also stressed the importance of safe password management.[38]

Social engineering also played a big role in users' digital lives. The infamous iCloud photo leak[39] was an unfortunate incident that cybercriminals took advantage of as bait for users who scoured the Internet for the leaked celebrity photos.[40] Another effective social engineering lure was the rumored Windows 9 developer preview release that led to a wave of downloaded adware.[41]

Other Vulnerabilities Discovered

Apart from the aforementioned high-profile exploits, Trend Micro discovered and disclosed five critical vulnerabilities found in two programs. Four were seen affecting Internet Explorer®, while one affected Adobe Flash Player.[42]



Critical Vulnerabilities Trend Micro Discovered in 3Q 2014

References

1. Trend Micro. (September 26, 2014). *TrendLabs Security Intelligence Blog*. "Shellshock Vulnerability Used in Botnet Attacks." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/bash-bug-vulnerability-used-in-botnet-attacks/.

2. Trend Micro (September 26, 2014). *TrendLabs Security Intelligence Blog*. "Shellshock Updates: BASHLITE C&Cs Seen, Shellshock Exploit Attempts in Brazil." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/shellshock-updates-bashlite-ccs-seen-shellshock-exploit-attempts-in-brazil/.

3. Trend Micro. (September 25, 2014). *TrendLabs Security Intelligence Blog*. "Bash Vulnerability (Shellshock) Exploit Emerges in the Wild, Leads to BASHLITE Malware." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/bash-vulnerability-shellshock-exploit-emerges-in-the-wild-leads-to-flooder/.

4. Pavan Thorat and Pawan Kinger. (September 25, 2014). *TrendLabs Security Intelligence Blog*. "Bash Vulnerability Leads to Shellshock: What it is, How it Affects You." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/shell-attack-on-your-server-bash-bug-cve-2014-7169-and-cve-2014-6271/.

5. Trend Micro. (September 26, 2014). *TrendLabs Security Intelligence Blog*. "Shellshock – How Bad Can It Get?" Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/shellshock-how-bad-can-it-get/.

6. Trend Micro. (September 26, 2014). *TrendLabs Security Intelligence Blog*. "Shellshock Updates: BASHLITE C&Cs Seen, Shellshock Exploit Attempts in Brazil." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/shellshock-updates-bashlite-ccs-seen-shellshock-exploit-attempts-in-brazil/.

7. Tim Yeh. (August 25, 2014). *TrendLabs Security Intelligence Blog*. "Netis Routers Leave Wide Open Backdoor." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/netis-routers-leave-wide-open-backdoor/.

8. ShadowServer Foundatoin. ShawdowServer.org. "Vulnerable Netis Router Scanning Project." Last accessed November 7, 2014, https://netisscan.shadowserver.org/.

9. Jonathan Leopando. (September 2, 2014). *TrendLabs Security Intelligence Blog*. "ShadowServer Scans Confirm Scale of Netis Threat." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/shadowserver-scans-confirm-scale-of-netis-threat/.

10. Tim Yeh. (October 3, 2014). *TrendLabs Security Intelligence Blog*. "Netis Router Backdoor "Patched" But Not Really." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/netis-router-backdoor-patched-but-not-really/.

11. Joseph C Chen. (August 21, 2014). *TrendLabs Security Intelligence Blog*. "Website Add-on Targets Japanese Users, Leads To Exploit Kit." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/website-add-on-targets-japanese-users-leads-to-exploit-kit/.

12. Brooks Li. (September 23, 2014). *TrendLabs Security Intelligence Blog*. "Nuclear Exploit Kit Evolves, Includes Silverlight Exploit." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/nuclear-exploit-kit-evolves-includes-silverlight-exploit/.

13. Fernando Mercês. (July 30, 2014). *TrendLabs Security Intelligence Blog*. "Gizmodo Brazil Compromised, Leads to Backdoor." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/gizmodo-brazil-compromised-leads-to-backdoor/.

14. Fernando Mercês. (August 7, 2014). *TrendLabs Security Intelligence Blog*. "More Details Regarding the Gizmodo Brazil Compromise." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/more-details-regarding-the-gizmodo-brazil-compromise/.

15. Fernando Mercês. (October 3, 2014). *TrendLabs Security Intelligence Blog*. "Anatomy of a Compromised Site: 7,000 Victims in Two Hours." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/anatomy-of-a-compromised-site-7000-victims-in-two-hours/.

16. Sylvia Lascano. (September 4, 2014). *TrendLabs Security Intelligence Blog*. "Malware Bypasses Chrome Extension Security Feature." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/malware-bypasses-chrome-extension-security-feature/.

17. Numaan Huq. (September 11, 2014). *TrendLabs Security Intelligence Blog*. "An Explosion of Data Breaches and PoS RAM Scrapers." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/2014-an-explosion-of-data-breaches-and-pos-ram-scrapers/.

18. Jonathan Leopando. (September 9, 2014). *TrendLabs Security Intelligence Blog*. "Home Depot Breach Linked to BlackPOS Malware." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/home-depot-breach-linked-to-blackpos-malware/.

19. Eduardo Altares II. (July 30, 2014). *TrendLabs Security Intelligence Blog*. "New Crypto-Ransomware Emerge in the Wild." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/new-crypto-ransomware-emerge-in-the-wild/.

20. Trend Micro Incorporated. (2013). "TrendLabs 2013 3Q 2013 Security Roundup: The Invisible Web Unmasked." Last accessed November 12, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-trendlabs-3q-2013-security-roundup.pdf.

21. Alvin Bacani. (August 5, 2014). *TrendLabs Security Intelligence Blog*. "Gameover Increases Use of Domain Generation Algorithms." Last accessed November 12, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/gameover-increases-use-of-domain-generation-algorithms/.

22. Paul Pajares. (September 5, 2014). *TrendLabs Security Intelligence Blog*. "Phishing Safety: Is HTTPS Enough?" Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/phishing-safety-is-https-enough/.

23. Simon Huang. (August 12, 2014). *TrendLabs Security Intelligence Blog*. "The Dangers of the Android FakeID Vulnerability." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/the-dangers-of-the-android-fakeid-vulnerability/.

24. Simon Huang. (September 29, 2014). *TrendLabs Security Intelligence Blog*. "Same Origin Policy Bypass Vulnerability Has Wider Reach Than Thought." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/same-origin-policy-bypass-vulnerability-has-wider-reach-than-thought/.

25. Weichao Sun. (August 21, 2014). *TrendLabs Security Intelligence Blog*. "Vulnerability in In-App Payment SDKs May Lead to Phishing." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/vulnerability-in-in-app-payment-sdks-may-lead-to-phishing/.

26. Weichao Sun. (July 29, 2014). *TrendLabs Security Intelligence Blog*. "Vulnerabilities in Alipay Android App Fixed." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/vulnerabilities-in-alipay-android-app-fixed/.

27. Simon Huang. (August 5, 2014). *TrendLabs Security Intelligence Blog*. "Vulnerability in Spotify Android App May Lead to Phishing." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/vulnerability-in-spotify-android-app-may-lead-to-phishing/.

28. Weichao Sun. (August 4, 2014). *TrendLabs Security Intelligence Blog*. "Evernote Patches Vulnerability in Android App." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/evernote-patches-vulnerability-in-android-app/.

29. Kervin Alintanahin. (July 2, 2014). *TrendLabs Security Intelligence Blog*. "KIVARS With Venom: Targeted Attacks Upgrade with 64-bit "Support"." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/kivars-with-

venom-targeted-attacks-upgrade-with-64-bit-support/.

30. Abraham Camba. (September 15, 2014). *TrendLabs Security Intelligence Blog*. " 64-bit Version of MIRAS Used in Targeted Attack." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/64-bit-version-of-miras-used-in-targeted-attacks/.

31. Steam. SteamPowered.com. "team Hardware & Software Survey: October 2014." Last accessed November 7, 2014, http://store.steampowered.com/hwsurvey/.

32. Dove Chiu. (August 4, 2014). *TrendLabs Security Intelligence Blog*. "Backdoor Techniques in Targeted Attacks." Last accessed November 7, 2014, *http://blog.trendmicro.com/trendlabs-security-intelligence/backdoor-techniques-in-targeted-attacks/*.

33. Masayoshi Someya. (August 18, 2014). *TrendLabs Security Intelligence Blog*. "Risks from Within: Learning from the Amtrak Data Breach." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/risks-from-within-learning-from-the-amtrak-data-breach/.

34. Rainer Link. (July 1, 2014). *TrendLabs Security Intelligence Blog*. "Introduction to Smart Meters." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/introduction-to-smart-meters/.

35. Rainer Link. (July 23, 2014). *TrendLabs Security Intelligence Blog*. "Smart Grid Attack Scenarios." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/smart-grid-attack-scenarios/.

36. David Sancho. (September 4, 2014). *TrendLabs Security Intelligence Blog*. "The Security Implications of Wearables, Part 1." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/the-security-implications-of-wearables-part-1/.

37. Geoff Grindrod. (August 19, 2014). *TrendLabs Security Intelligence Blog*. "The Administrator of Things (AoT) – A Side Effect of Smartification." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/the-administrator-of-things-aot-a-side-effect-of-smartification/.

38. David Sancho. (August 6, 2014). *TrendLabs Security Intelligence Blog*. "Sending Mixed Messages With Passwords." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/sending-mixed-messages-with-passwords/.

39. Arabelle Mae Ebora. (September 3, 2014). *TrendLabs Security Intelligence Blog*. "iCloud Hacking Leak Now Being Used As Social Engineering Lure." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/icloud-hacking-leak-now-being-used-as-social-engineering-lure/.

40. David Raven and Jess Wilson. (September 2, 2014). Mirror.co.uk. "Jennifer Lawrence leaked nude photos: Apple launches investigation into hacking of iCloud." Last accessed November 7, 2014, http://www.mirror.co.uk/3am/celebrity-news/jennifer-lawrence-leaked-nude-photos-4155078.

41. Gideon Hernandez. (August 27, 2014). *TrendLabs Security Intelligence Blog*. "Cybercriminals Leverage Rumored Windows 9 Developer Preview Release With Social Engineering." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/cybercriminals-leverage-rumored-windows-9-developer-preview-release-with-social-engineering/.

42. Weimin Wu. (September 24, 2014). *TrendLabs Security Intelligence Blog*. "Trend Micro Uncovers 14 Critical Vulnerabilities in 2014 So Far." Last accessed November 7, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-uncovers-14-critical-vulnerabilities-in-2014-so-far/.

Created by:

TrendLabs

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

TREND MICRO™

Securing Your Journey to the Cloud