TrendLabs^SM 2Q 2014 Security Roundup

Turning the Tables on Cyber Attacks

Responding to Evolving Tactics

Distributed by:

Contents

Introduction

Recent events such as data breaches in the first half of 2014 strongly indicate that organizations need to start adopting a more strategic approach to protect digital information. This strategy includes protecting sensitive data such as intellectual property and trade secrets—often the crown jewels of any organization.

According to an Identity Theft Resource Center (ITRC) study, more than 10 million personal records have already been exposed as of July 15, 2014, with the majority of breaches occurring in the business sector.[1] The rising number of exposed personal records and data breaches raises the question, "How did organizations become so vulnerable?"

The main solution to these growing problems seems to be a change in mindset. According to our CTO, Raimund Genes, organizations first need to determine which information they regard as "core data," then focus on how to strongly protect it.[2] Organizations need to treat information security as part of their long-term business strategy instead of handling security issues as minor setbacks. And as the incidents seen this quarter show, organizations should strive for a more strategic security response.

Similar to having a business strategy to improve efficiency, a well-thought-out security strategy should also improve current protection practices for organizations to achieve long-term benefits and revenue. Failing to secure emerging and existing technologies can break a business, just like what happened to Code Spaces. Favorable organizational responses to attacks were also seen, although some bordered on the highly impractical. Organizations should keep in mind that no amount of mitigation would suffice if preventive security strategies are not put in place.

Meanwhile, on a broader scale, the battle against cybercrime can only be won through cooperation between private and public entities. In such partnerships, threat defense experts such as Trend Micro can, for instance, provide threat intelligence to law enforcement agencies in any country, which would aid the police in arresting cybercriminals. Our recent partnerships with law enforcement agencies in different parts of the world this quarter, in fact, show how security industry players can take a bold leap forward to respond to current threats to computing security.

NOTE: *All mentions of "detections" within the text refer to instances when threats were found on users' computers and were subsequently blocked by any Trend Micro security software. Unless otherwise stated, the figures featured in this report were based on 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.*

Critical vulnerabilities caused a stir among information security professionals and the public

Critical vulnerabilities hit different components of Internet-browsing and Web services ranging from server-side libraries to computer OSs, mobile apps, and browsers. Coordinated vulnerability disclosure and patch releases, however, raised the urgency and awareness of issues surrounding most of the vulnerabilities disclosed this quarter.

Heartbleed was the most critical vulnerability uncovered to date. On April 7, the OpenSSL Foundation announced the discovery of the two-year-old bug, which put millions of websites and their users at risk of possible cyber attacks.[3] Heartbleed paved the way for attackers to steal data such as passwords and credit card information from users conducting financial transactions via the Secure Sockets Layer (SSL) protocol on vulnerable websites.

Security warnings were issued regarding the Heartbleed bug, reminding system administrators how important keeping software updated is and telling them to revoke old security certificates and to issue new ones.[4] Months after the bug's public revelation, more than 300,000 Internet-connected systems remained unpatched.

The Heartbleed bug also affected 1,300 Android™ banking, shopping, payment, and other apps that accessed vulnerable servers.[5] An OpenSSL library specifically bundled with Android 4.1.1 was found susceptible to the bug, which could open up affected devices to server-side attacks.

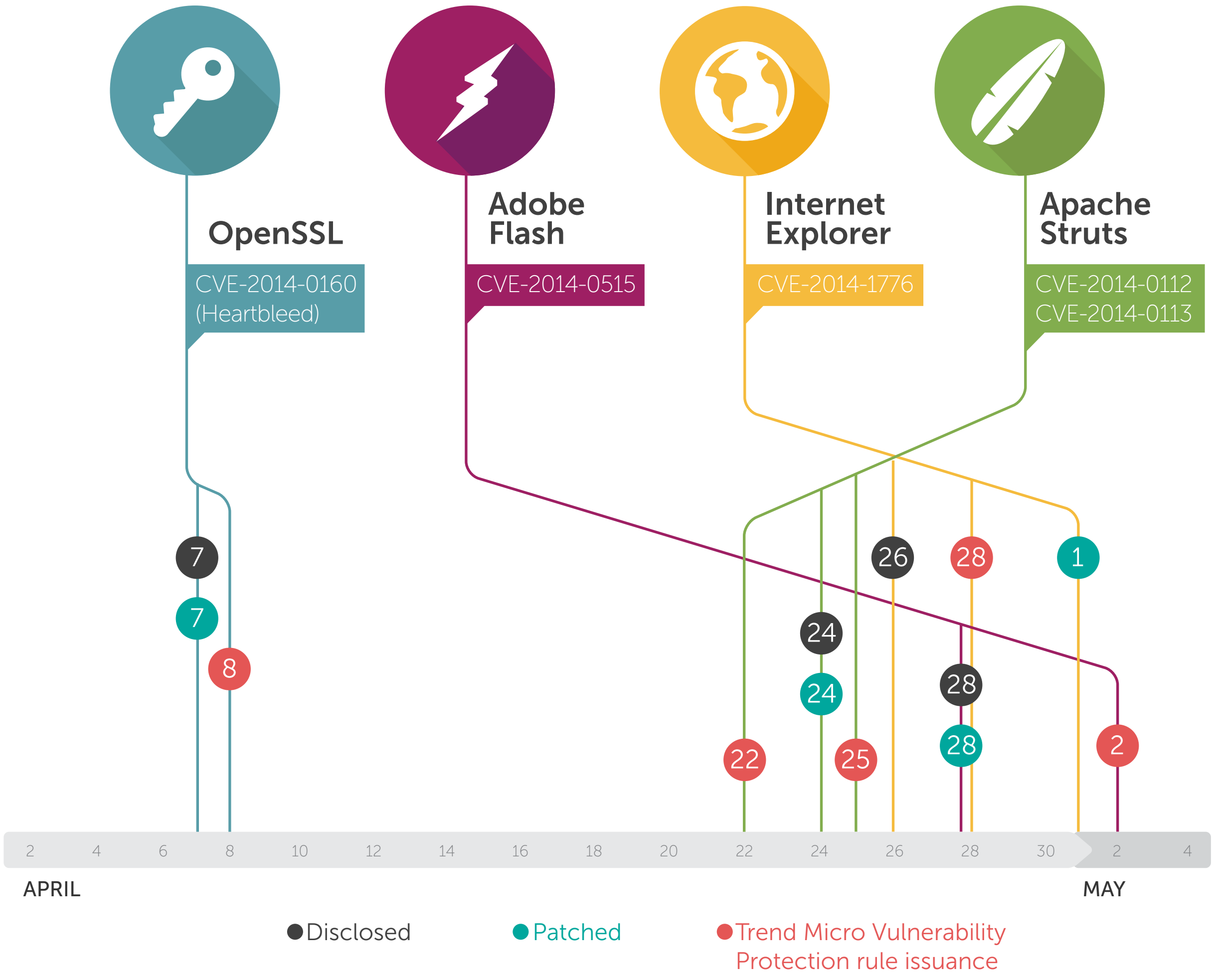
Heartbleed was not alone, however, as vulnerabilities in Windows® XP, which stopped receiving vendor support on April 8, were also seen this quarter. Computers still running the outdated OS stopped receiving patches since then, except for a zero-day vulnerability (CVE-2014-1776) discovered in Internet Explorer® versions 6 to 11.[6] This incident showed that the now-defunct OS still had vulnerabilities that could be exploited. Proof of this were the April, May, and June 2014 Patch Tuesday bulletins, which included patches for bugs in Windows Server® 2003 that also affected Windows XP.[7, 8, 9] As a result of the continued use of Windows XP even after Microsoft ceased supporting it in April, several organizations still suffered from DOWNAD/Conficker infections.[10]

Another zero-day vulnerability (CVE-2014-0515), this time in Adobe® Flash®, was also found in the latter part of April.[11] Adobe acknowledged that exploiting this bug on the Windows platform could allow remote attackers to take control of affected computers.

Apache Struts, an open source framework for developing Java™-based Web applications, was also found to be riddled with critical zero-day vulnerabilities.[12] Its developers released an advisory with details on two bugs (CVE-2014-0112 and CVE-2014-0113) that specifically affected versions 2.0.0 to 2.3.16.1 of the software.[13] This advisory urged developers to immediately upgrade to version 2.3.16.2 as a workaround.

On the mobile front, vulnerabilities in Android apps continued to pose serious security risks. Certain app components monitored this quarter had various security flaws that could leave user data at risk of being captured or of being used to launch attacks.[14] We are currently working closely with vendors and app developers to responsibly disclose these vulnerabilities.

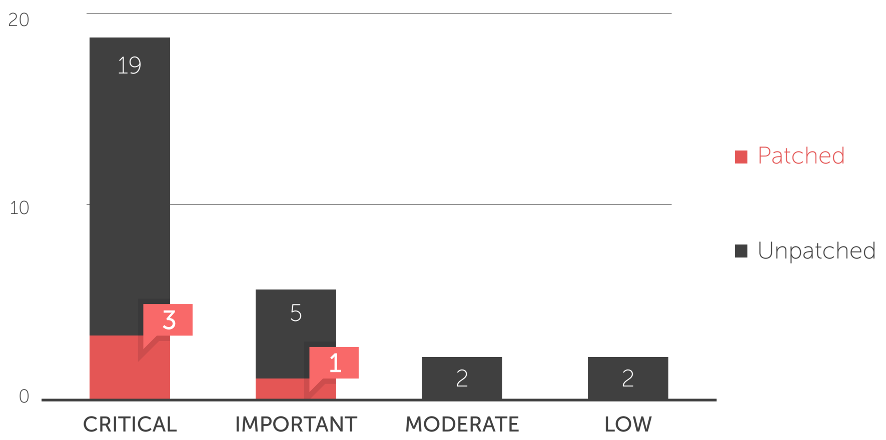
Timeline of Critical Vulnerabilities, 2Q 2014



NOTE: *One of the Trend Micro Vulnerability Protection rules that addresses the Internet Explorer vulnerability has been available since September 11, 2007.*

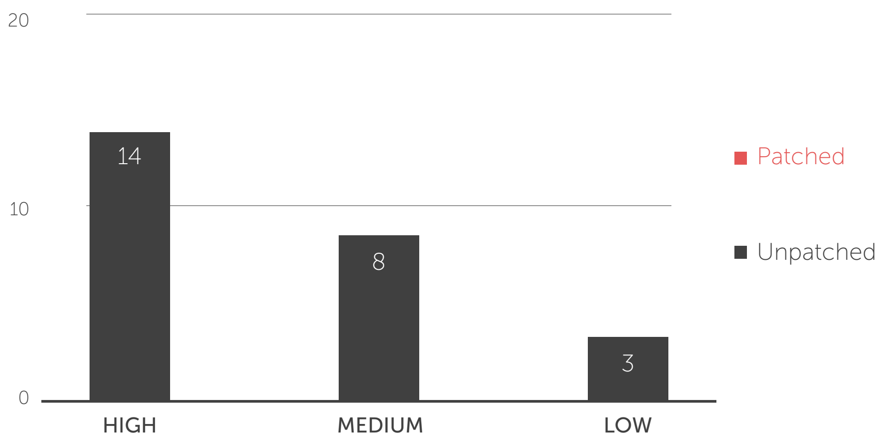
SOURCES:
http://heartbleed.com/
http://helpx.adobe.com/security/products/flash-player/apsb14-13.html
https://technet.microsoft.com/library/security/2963983
https://technet.microsoft.com/library/security/ms14-021
http://struts.apache.org/release/2.3.x/docs/s2-021.html

Windows XP Vulnerability Volume, 2Q 2014



NOTE: *The ratings in this table are based on the Microsoft Security Bulletin Severity Rating System, which can be found at http://technet.microsoft.com/en-us/security/gg309177.aspx.*

Java 6 Vulnerability Volume, 2Q 2014



NOTE: *The ratings in this table are based on the Common Vulnerability Scoring System (CVSS), which can be found at http://nvd.nist.gov/cvss.cfm.*

Three months after, Heartbleed continues to be a threat...

The Heartbleed issue caused several concerns about security to surface—how vulnerable users are and how easy it is to be a hacking victim. A lot people still have not learned their lesson, as a June 2014 scan by Errata Security showed that more than 300,000 servers were still vulnerable to the Heartbleed bug two months after its discovery.[15] It is still a big threat if developers have not recompiled all of their applications with vulnerable versions of OpenSSL. Deploying intrusion prevention system (IPS) solutions to mitigate the issue is, however, an appropriate quick step.

Reports have gone out that several organizations upgraded in panic from nonvulnerable to vulnerable versions. Though upgrading seems like a logical step toward security, organizations must remember two key things before patching. First, not all old software versions are vulnerable. And, second, they should always check software versions before jumping to upgrade them. Server-side administrators should review database configurations and service settings to limit upgrades to only the necessary.

In general, users should upgrade to the latest software versions and automate the download and installation of security patches for their OS, software, and browser plug-ins.

—Pawan Kinger
Director, Deep Security Labs

Severity of attacks escalated and organizations responded

> The severity of attacks against organizations escalated. Organizations responded differently, highlighting the importance of incident response plans and organization-wide security awareness.

The distributed denial-of-service (DDoS) attack on source code repository, Code Spaces, had the severest impact we have seen to date. It forced the company to go out of business.[16] The second quarter also saw DDoS attacks that targeted Rich Site Summary (RSS)/blog news reader, Feedly. The attack prevented its users from accessing their own information.[17] Attackers attempted to extort money from the service provider in exchange for normal operations. Evernote suffered the same fate but was able to recover.

Apart from damaging DDoS attacks, the second quarter also played witness to a number of data breaches. According to the ITRC, more than 400 data breach incidents have been reported as of July 15, 2014.[18, 19] These include the attack against online auction website, eBay, which put the personal details of its 145 million active buyers at risk.[20] As a result, the service provider asked its members to reset their passwords.[21]

Restaurant chain, P.F. Chang's, also suffered a major data breach that resulted in the theft of the credit card data of customers from across the United States.[22] An online notice in its corporate website announced its transition to the use of manual imprinting devices to process all subsequent credit and debit card payments as an added security measure.[23]

The data breaches and DDoS attacks recorded this quarter showed that an organization-wide strategy is required if companies wish to survive their aftermath. Organization-wide understanding and commitment to carrying out a strategic security plan is necessary. Otherwise, they may resort to highly impractical measures such as reverting to manual processing, as in P.F. Chang's case or, worse, to go out of business, as in Code Spaces's case.

Forming an incident response team that can spearhead employee awareness programs focusing on breach and DDoS attack prevention is advised. It is also a good practice to inform customers how their data is protected. And should an incident occur, customers must be informed of remediation and mitigation efforts as well as future plans so concerned organizations can prevent a recurrence. Those that subscribe to cloud services should consider keeping their data in several secure locations as backup. All users, meanwhile, should ensure that they do not use the same password across different accounts.

Reported Data Breach and DDoS Incidents, 2Q 2014

COMPANY	DATE DISCOVERED/ ATTACK OCCURRED	DECLARED CAUSE	ESTIMATED NUMBER OF AFFECTED	IMPACT OF DAMAGE	RESPONSE STRATEGY
DATA BREACHES					
eBay	Unknown	Small number of employee login credentials was compromised	145M active buyers	Theft of data such as customer names, encrypted passwords, email and home addresses, phone numbers, and dates of birth; significant effect on sales and earnings	Password change; communicated the breach via their official blog
P.F. Chang's	June 10, 2014	Security breach	33 branches	Theft of customers' credit card numbers	Return to use of manual credit card imprinting devices and addition of encryption-enabled terminals; posted a notification on their website
DDoS ATTACKS					
Code Spaces	June 17, 2014	Attacker control of its cloud control panel	Unknown	Data, offsite backup, and machine configuration deletion as well as company shutdown	Not applicable
Feedly	June 11–13, 2014	Website DDoS attack	12M users	User inability to access accounts and service disruption	Infrastructure changes; communicated the breach via their official blog
Evernote	June 10, 2014	Website DDoS attack	100M users	User inability to access accounts and service disruption	DDoS mitigation service use, which involved filtering out bogus packets; communicated the breach via Twitter and their official blog

SOURCES:
http://blog.ebay.com/ebay-inc-ask-ebay-users-change-passwords/
http://www.pfchangs.com/security/
http://blog.feedly.com/2014/06/11/denial-of-service-attack/
http://www.theregister.co.uk/2014/06/11/evernote_dos_attack/
http://www.codespaces.com/
http://www.forbes.com/sites/ryanmac/2014/07/16/ebay-ceo-sales-earnings-affected-by-cyberattack-body-blow-in-challenging-second-quarter/

The most-overlooked data breach effect...

Third parties often notify organizations and individuals alike that they have been breached, which tends to knock them off-kilter and to dynamically orchestrate an incident response plan—a short-term process that I consider ‘unorganized chaos.’ Initial breach response handling is paramount to maintain brand loyalty. Identifying lessons learned postbreach is also essential. The main outcome is to operate in more of an ‘organized chaos’ fashion. Business and life are chaotic and just being able to organize ‘chaos’ is critical.

The most-overlooked aspect of a breach is the downstream impact for years to come. As information assault continues on businesses, the data exfiltrated is coalesced and sold in unspeakable communities by people who do unimaginable things—all done at a company’s expense and for ludicrous sums of money. We have to remember that stolen data has no expiration date. It can and will be used in perpetuity. We should all rethink our security strategies as stewards of data and focus on becoming threat defense experts in our organizations.

Vendors must prioritize security, including incident response plans for breaches and DDoS attacks and organization-wide security awareness programs. Cloud service users must consider multiple but secure backup locations for business data.

—JD Sherry

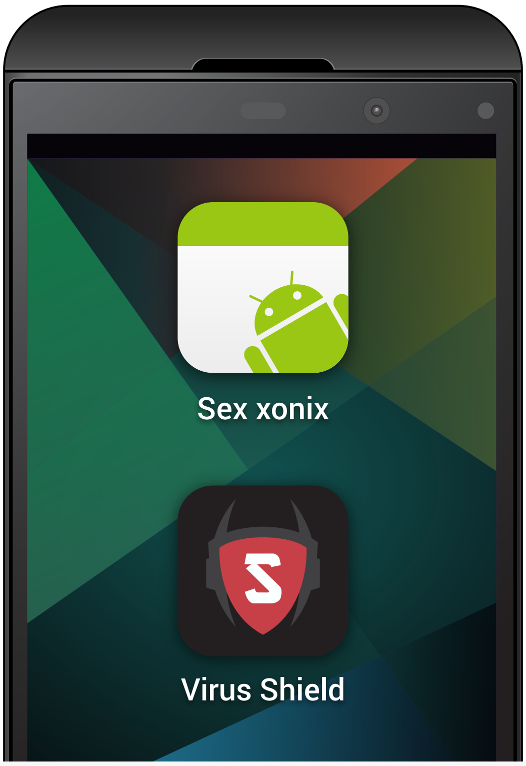
Vice President,
Technology and Solutions

Cybercriminals responded to online banking and mobile platform developments

> Cybercriminals responded to technological platform developments in online banking and mobility, which resulted in an increase in the number of new/improved malware.

Ransomware continued to spread this quarter after going through even more improvements. They went on to target the Android platform via ANDROIDOS_LOCKER.A, which puts its user interface (UI) on top of an unlocked screen and prohibits users from uninstalling it.[24] ANDROIDOS_LOCKER.HBT also showed how mobile ransomware picked up more tricks from computer malware—communicating with command-and-control (C&C) servers via Tor.[25, 26] Those affected were also asked to pay around US$30 to unlock their devices. Failure to pay the ransom could supposedly result in the destruction of all of the data on their mobile devices.

Although the number of ransomware-affected users decreased from around 11,000 at the end of last quarter to around 9,000 this quarter, new breeds with more advanced capabilities surfaced. Variants such as CryptoLocker with a Tor component, CryptoDefense, and CryptoWall were also spotted this quarter.[27]



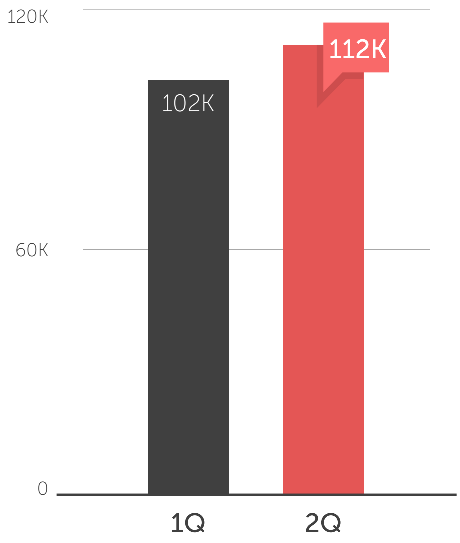
__TOP:__ ANDROIDOS_LOCKER.HBT poses as a fake app named "Sex xonix"; __BOTTOM:__ ANDROIDOS_FAKEAV.B disguised as "Virus Shield"

Fake antivirus also made a comeback in the form of a fake mobile app named "Virus Shield," which was previously available for download in Google Play™.[28, 29] The fake app detected as ANDROIDOS_FAKEAV.B was downloaded more than 10,000 times and even became a top paid app in a week's time.[30]

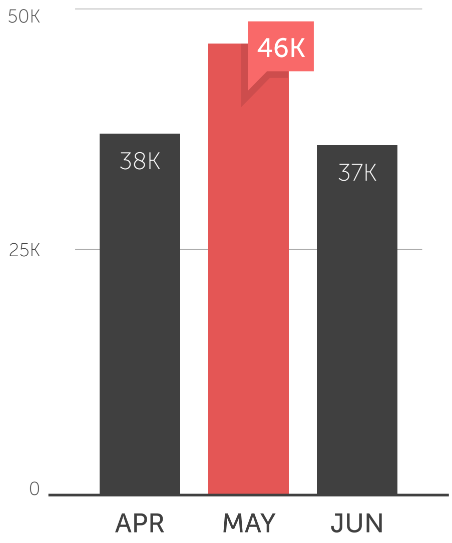
Japan also saw a significant growth in the number of online banking malware victims due to the rise in VAWTRAK detections in May.[31] Though not considered banking malware prior to this quarter, recent variants have expanded their capabilities to include stealing online banking credentials and credit card information.

Research on Operation Emmental also showed how computer and mobile threats seamlessly work together to wreak greater havoc over online bankers.[32, 33] The cybercriminals behind the operation target banks that use session tokens sent via Short Message Service (SMS) or two-factor authentication. Regional spam runs, nonpersistent malware, rogue Domain Name System (DNS) servers, phishing pages, Android malware, C&C servers, and real back-end servers all made up this complex operation.

Online Banking Malware Detection Volume Comparison, 1Q and 2Q 2014



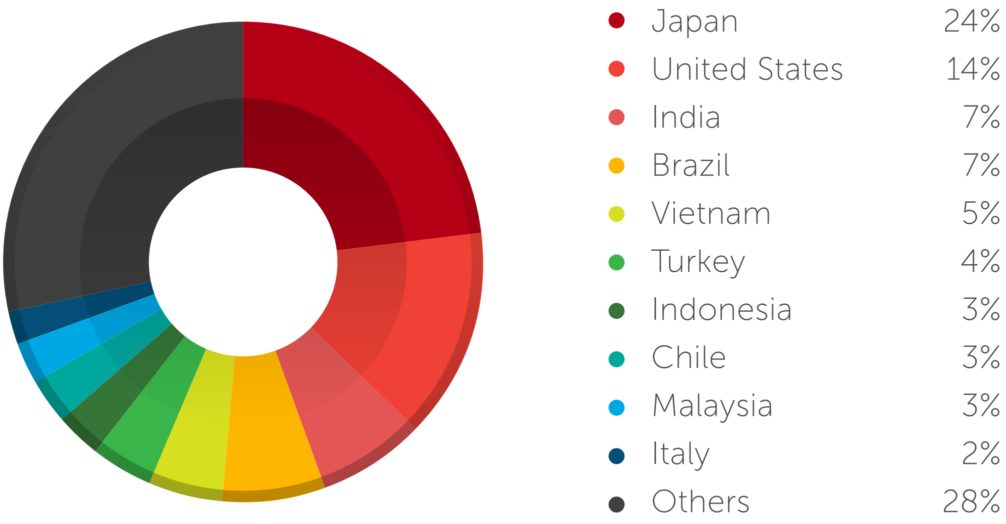
Online Banking Malware Detection Volume, 2Q 2014

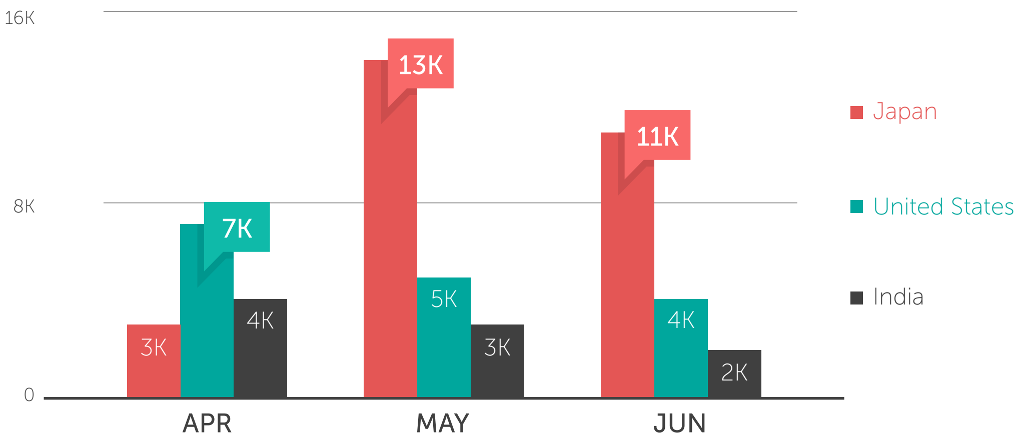


The number of online banking malware detections increased this quarter because of the rise in VAWTRAK cases in Japan.

NOTE: *The total volume of online banking malware refers to the number of unique infections per month.*

Countries Most Affected by Online Banking Malware, 2Q 2014





Japan rose to the top of the list of countries with the highest number of online banking malware infections this quarter due to VAWTRAK. Most of the countries cited last quarter remained in the list, apart from France, Mexico, and Australia, which were replaced by Indonesia, Chile, and Italy.

Collaboration with law enforcement agencies led to arrests worldwide

By working closely with several law enforcement agencies, we were able to directly and conclusively thwart various cybercriminal activities worldwide.

Disclosing our research findings to affected organizations in order to prevent financial losses due to cybercrime has proven effective.[34] This was evidenced by recognition from the Tokyo Metropolitan Police Department (MPD) in April for our findings on Citadel-related attacks against Japanese banks since June 2013.

We also provided information on Jam3s, whose real name is James Bayliss—a hacker who ran C&C servers related to SpyEye—to law enforcement agencies, which aided in his arrest in the United Kingdom in May.[35]

Just this June, the Federal Bureau of Investigation (FBI) announced that an international effort disrupted the activities of GameOver—a ZeuS/ZBOT variant capable of peer-to-peer (P2P) communication.[36] Trend Micro provided a cleanup tool for the FBI takedown effort, which contributed to the drop in the number of ZeuS/ZBOT-affected users this quarter. Data from the Smart Protection Network showed a 36% drop in number of affected users at the end of this quarter.

Meanwhile, some law enforcement efforts do take time. For instance, in the Esthost takedown back in 2011 by the FBI and the Estonian police, five of the six individuals involved are finally in the United States awaiting trial.[37] This just goes to show that putting cybercriminals to justice can take a while but eventually gets done.

Trend Micro works with law enforcement agencies...

The Forward-Looking Threat Research (FTR) Team—the dedicated e-crime unit of Trend Micro—handles all law enforcement investigation requests. Collaboration between FTR and law enforcement agencies is triggered either by an explicit request from a police unit or by crime-related FTR findings. We offer investigation support and share available threat intelligence with law enforcement agencies. We are the point of contact for national or commercial Community Emergency Response Team (CERT) and Computer Security Incident Response Team (CSIRT) collaborative efforts for Trend Micro.

We had several successful collaboration efforts in the past, the most recent of which led to a series of arrests related to the SpyEye banking Trojan. We shared information with contacts within the FBI and the National Crime Agency (NCA), which continued the investigation that ultimately led to a number of high-profile arrests.

Apart from cases that have already gone public, we are involved in a number of ongoing cases worldwide. We are always happy to work with any law enforcement agency, backed by Trend Micro threat intelligence and our cybercrime investigative expertise, because we believe that only through collaboration can we truly make the world a safer place for the exchange of digital information.

—Martin Rösler
Senior Director, Threat Research

User privacy issues resurfaced

Market forces, regulations, and courts worldwide are taking a concrete stand in defense of user privacy.

A year ago, Edward Snowden exposed the National Security Agency (NSA)'s widespread surveillance practices.[38] Data privacy advocates demanded a change in the law but the same practices remain intact. The Snowden revelations triggered discussions related to data stored in the cloud while greater awareness of cloud security threats resulted in several responses, including complaints from U.S. companies and loss of trust in some cloud service providers. These discussions still permeate today, as cloud service providers continue to fight to keep customer data out of the government's hands in an ongoing case in the United States.[39]

Long-standing concerns over the data organizations collect on individuals were manifested in the European decision on the "right to be forgotten" ruling on May 13, which allows users to ask Google to remove embarrassing online revelations from search results.[40] The ruling was considered a victory in Europe though recent discussions say it may contradict the right to freedom of expression declared in the United Nations (UN)'s Universal Declaration on Human Rights.[41]

In favor of digital privacy, in mid-June, the U.S. Supreme Court ruled that the police will need a warrant to search a person's mobile phone.[42] This landmark decision for and endorsement of privacy rights may affect the legal protection afforded to digital data in the future. Websites that record personal details may have access to certain information but only their owners have the right to use the information as they see fit.[43] Steps taken toward protecting one's own digital data are indeed a welcome change.

The role of Trend Micro in the privacy debate...

Day by day, questions and concerns surrounding privacy increase in importance. Nearly every person on the planet now is or should be concerned about online privacy. The coming age of the Internet of Everything (IoE)/Internet of Things (IoT) makes privacy failures all the greater by opening us up to more real-world consequences.

In this world of increasingly complex privacy and difficulty in protecting it, what is the role of a company like Trend Micro? It is to help reduce the complexity to make it easier to take advantage of all of the benefits the latest technology and services have to offer without having to surrender privacy.

It is our role as threat defense experts to act as a guide and resource to help people live their online lives as openly or as privately as they want, in safety.

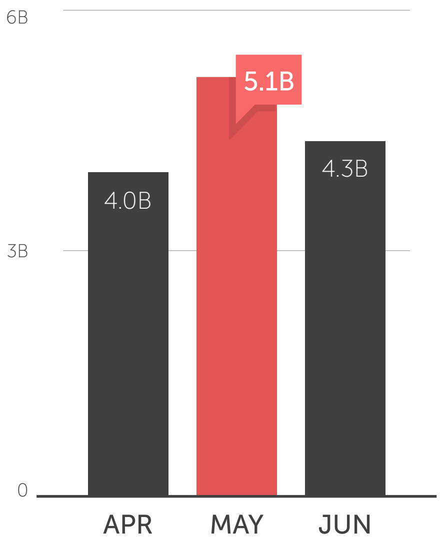
—Christopher Budd
Manager, Threat Marketing

Threat Landscape in Review

Malware, Spam, and Malicious Sites

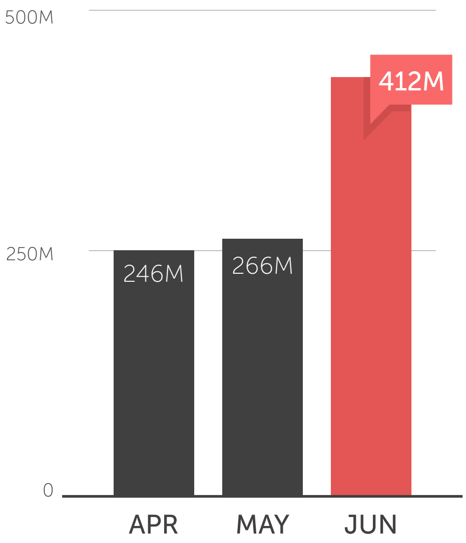
This quarter witnessed volume shifts across the various attack vectors we monitor via the Smart Protection Network. The nature of threats in both the consumer and enterprise segments changed, as evidenced by the decline in the number of DOWNAD/Conficker infections. Furthermore, the "demise" of Windows XP seemingly pushed attackers to take a different route in response.

Number of Spam-Sending IP Addresses the Trend Micro Smart Protection Network Blocked Access To, 2Q 2014



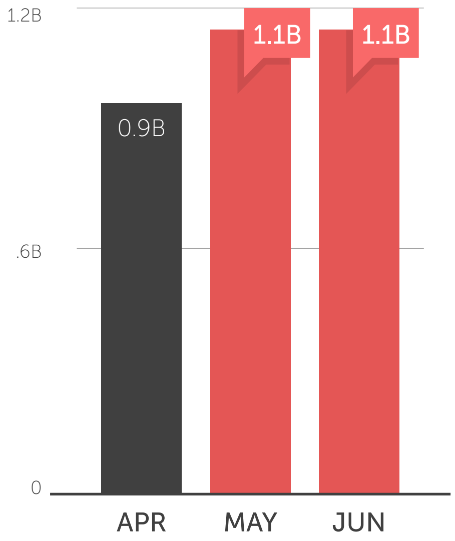
The number of spam-sending IP addresses we blocked access to this quarter neither drastically increased nor decreased compared with last quarter's 12.9 billion.

Number of Malicious Sites the Trend Micro Smart Protection Network Blocked Access To, 2Q 2014



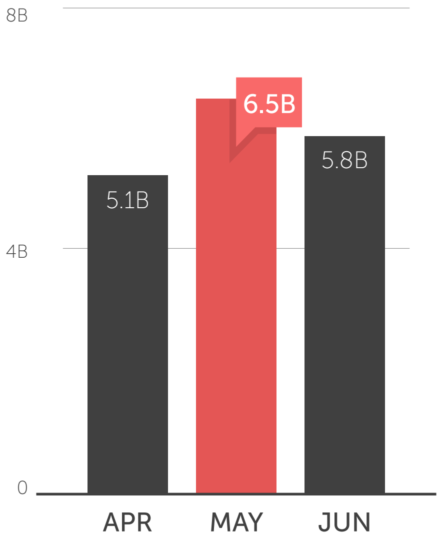
The number of malicious sites we blocked access to significantly increased in June. It is interesting to note that the top sites we blocked access to were adware related.

Number of Malicious Files Blocked by the Trend Micro Smart Protection Network, 2Q 2014



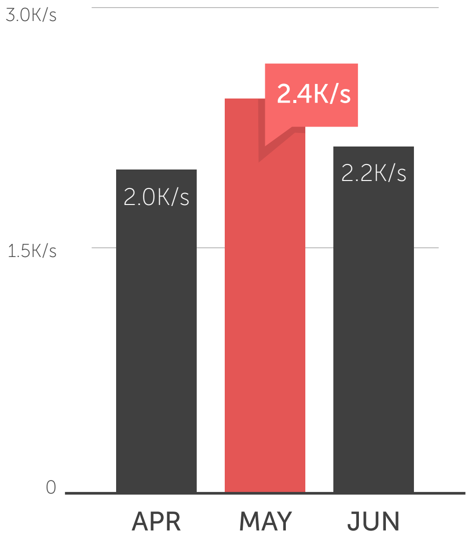
The number of malicious files we blocked doubled this quarter compared with the same quarter last year (1.7 billion).[44] The growing number of malware variants in general and the trend of using customized malware were hastened by the accessibility of malware toolkits in the cybercriminal underground.

Total Number of Threats Blocked by the Trend Micro Smart Protection Network, 2Q 2014



We blocked an average of 5.8 billion threats per month this quarter, indicating a slight increase from last quarter's 5.4 billion.

Trend Micro Smart Protection Network Overall Detection Rate, 2Q 2014



No drastic changes were seen in the number of threats we blocked per second from the previous quarter.

Top 3 Adware, 2Q 2014

NAME	VOLUME
ADW_INSTALCOR	234K
ADW_OPENCANDY	204K
ADW_DOWNWARE	107K

Top 3 Malware, 2Q 2014

NAME	VOLUME
WORM_DOWNAD.AD	35K
LNK_DUNIHI.SMIX	33K
JS_NEVAR.A	19K

Adware made up a large portion of the total number of threats (combined adware and malware) seen this quarter. ADW_OPENCANDY remained in the top 3 though its volume decreased compared with last quarter. These top adware have been around for years. Most adware are plug-ins that some developers bundle with free software. Developers earn money by recommending software or products to users through these installed adware.

WORM_DOWNAD continued to top the list of malware infectors this quarter. Although its volume declined due to the decreasing number of Windows XP users, infections continued to persist due in part to unsafe practices such as failing to update OSs.

NOTE: *The top malware do not include commonly found hacking tools such as key generators and product key viewers.*

Top 3 Malware by Segment, 2Q 2014

SEGMENT	2Q 2014	
	NAME	VOLUME
Enterprise	LNK_DUNIHI.SMIX	29K
	WORM_DOWNAD.AD	26K
	WORM_DOWNAD.FUF	5K
SMB	WORM_DOWNAD.AD	6K
	JS_CHECK.A	2K
	LNK_DUNIHI.SMIX	2K
Consumer	JS_NEVAR.A	18K
	JAVA_XPLOIT.GOQ	11K
	JS_REDIR.ED	10K

The enterprise segment was dominated by old threats such as those linked to USB media. The top consumer infectors, meanwhile, were tied to exploit kits. Finally, the small and medium-sized business (SMB) segment was plagued by a mix of old and fairly newer threats.

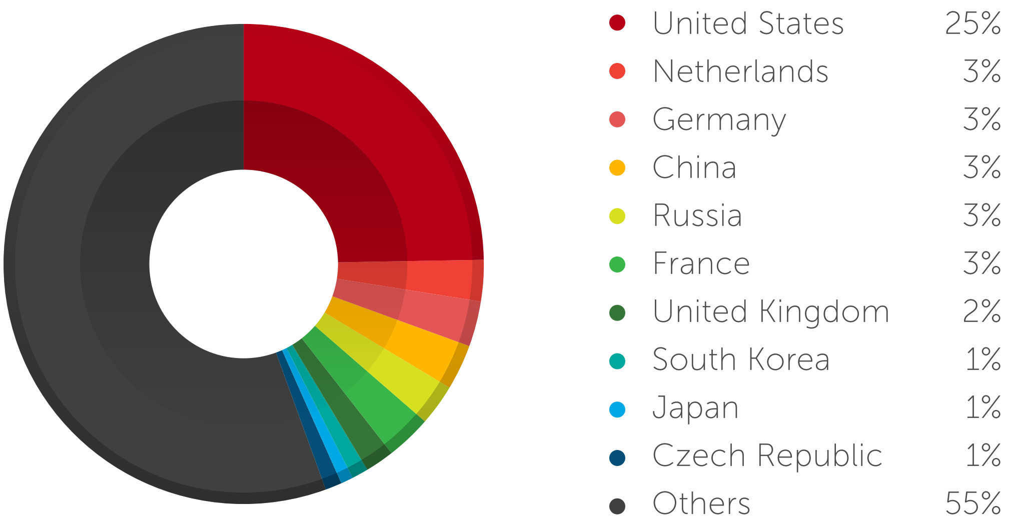
NOTE: *The top malware do not include commonly found hacking tools such as key generators and product key viewers.*

Top 10 Malicious Domains the Trend Micro Smart Protection Network Blocked Accessed To, 2Q 2014

DOMAIN	REASON FOR BLOCKING ACCESS TO
ads.alpha00001.com	Reported as a C&C server and redirects to enterfactory.com—a malicious website
www.ody.cc	Tied to suspicious scripts and sites that host BKDR_HPGN.B-CN
cnfg.toolbarservices.com	Detected as ADW_MONTIERA
storage.stgbssint.com	Detected as ADW_BUNDLED
cdn1.down.17173ie.com	Known for downloading malicious files
interyield.jmp9.com	Tied to malware attacks and other malicious activities
flyclick.biz	Tied to computer hijacking and other malicious activities
directxex.com	Known for downloading malicious files
sp-storage.spccint.com	Known for downloading malware
checkver.dsiteproducts.com	Detected as ADW_DOWNWARE

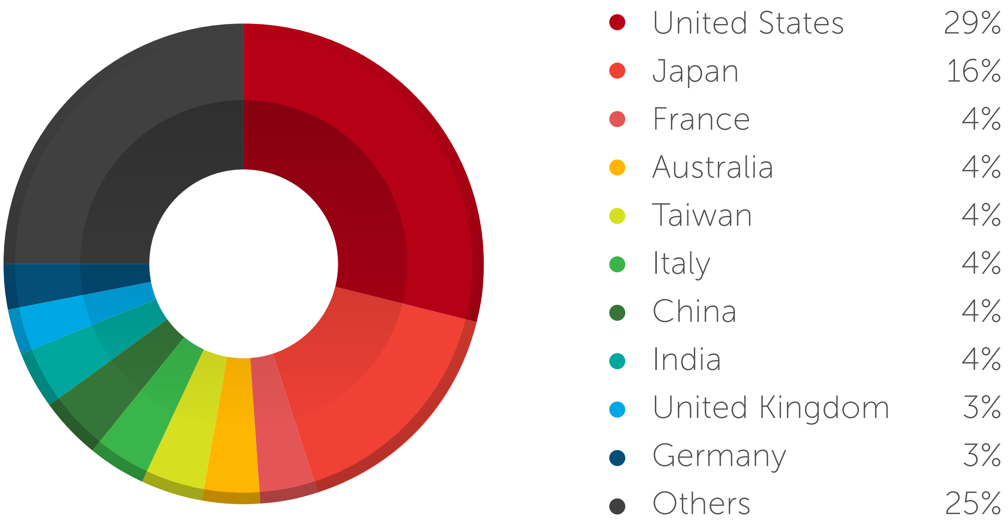
No drastic changes were seen in the number of users who accessed malicious domains from the previous quarter.

Top 10 Malicious URL Country Sources, 2Q 2014



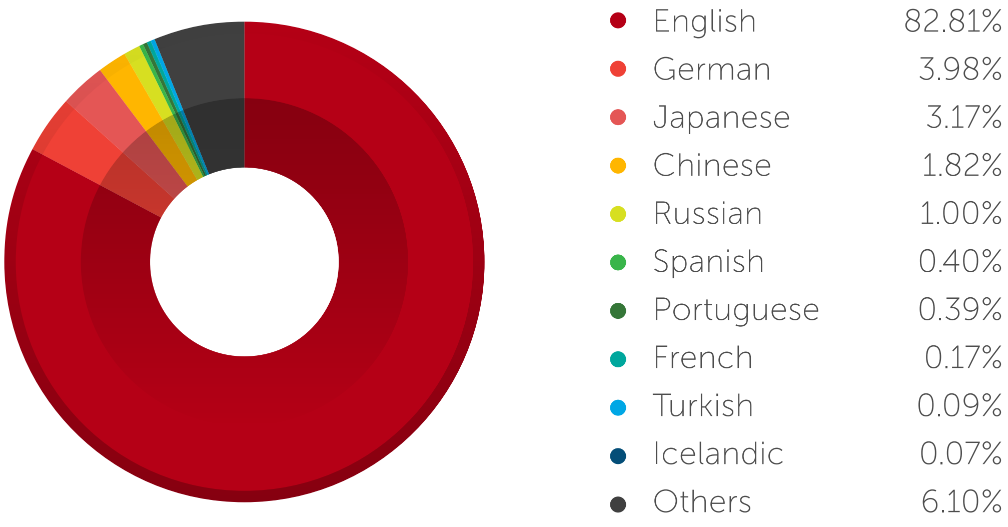
The United States's share of the malicious-URL-hosting pie reached 25% this quarter, showing a 3% increase from last quarter's 22%.

Countries with the Highest Number of Visits to Malicious Sites, 2Q 2014



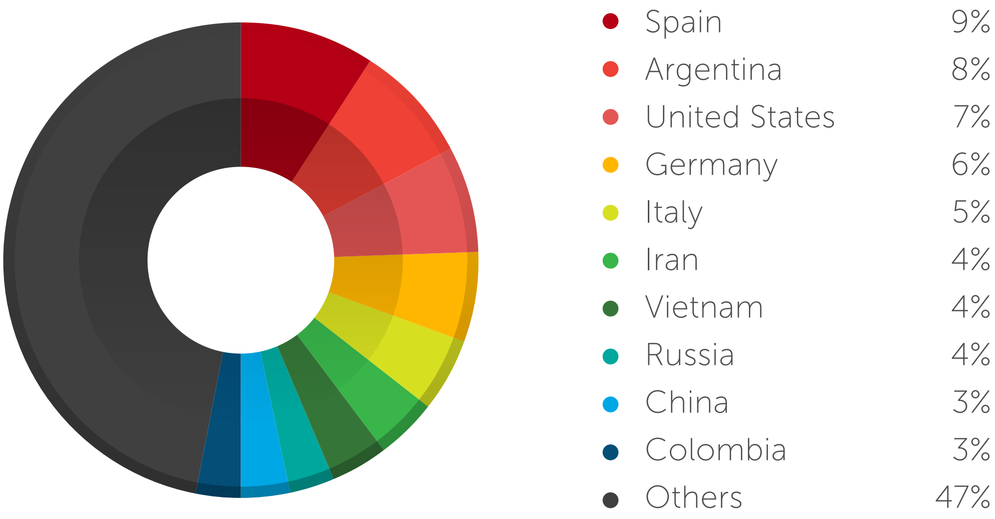
Italy and the United Kingdom joined the list of countries with the highest number of visits to malicious sites. Japan and the United States remained the top 2 countries, as in the previous quarter.

Most-Used Spam Languages, 2Q 2014



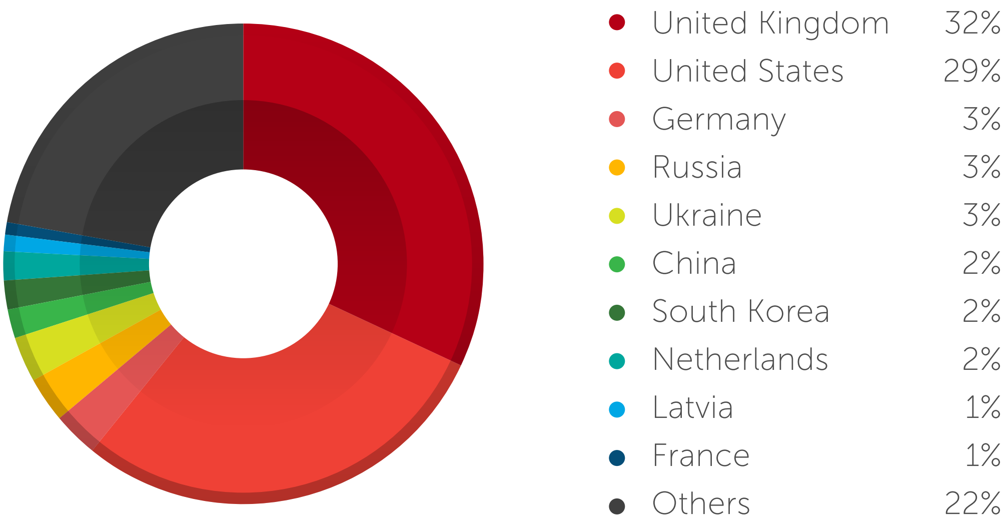
An apparent rise in the number of German spam was seen this quarter. English, however, retained the top spot.

Top Spam-Sending Countries, 2Q 2014



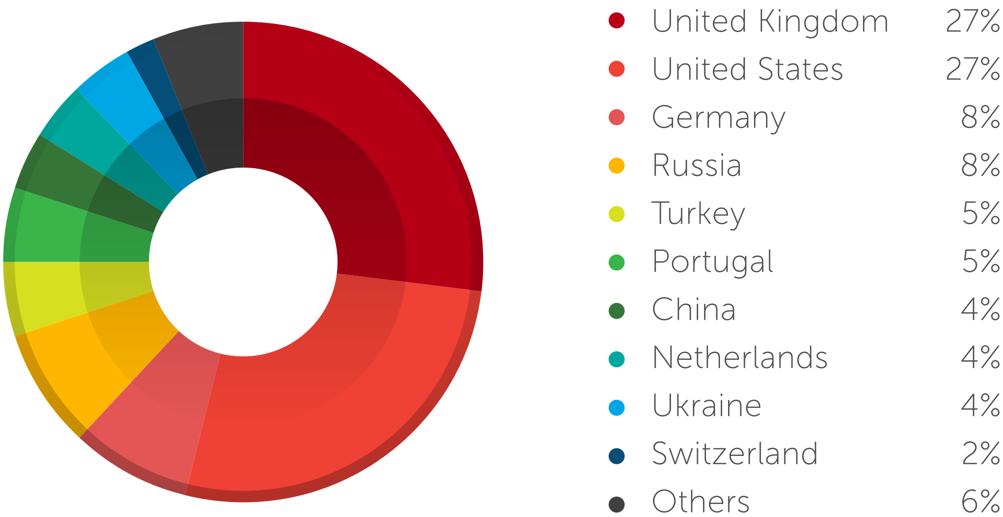
No significant changes were seen in the list of top spam-sending countries this quarter.

Countries with the Highest Number of Botnet C&C Servers, 2Q 2014



The United Kingdom continued to top the list of countries with the highest number of botnet C&C servers, as in the previous quarter.

Countries with the Highest Number of Botnet Connections, 2Q 2014

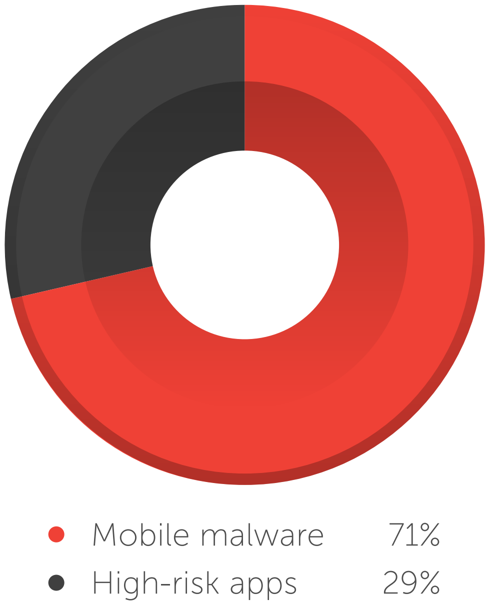


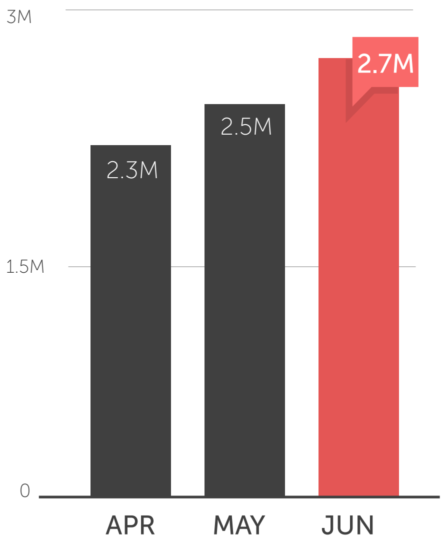
Users from the United Kingdom and the United States accounted for more than half of the network traffic that hit C&C servers from affected computers this quarter.

Mobile Threats

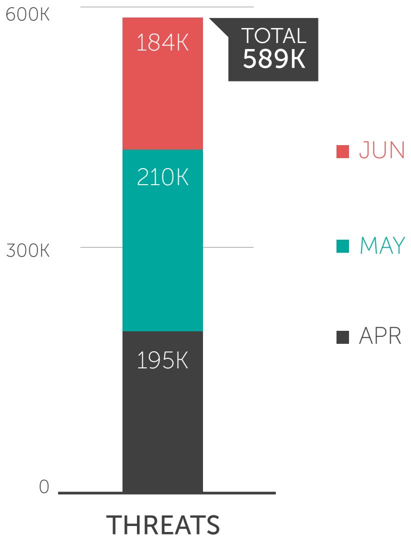
Mobile threats remained apparent, as evidenced by the constant increase in their number. High-risk apps such as adware also increased in volume.

Cumulative Android Threat Volume as of 2Q 2014





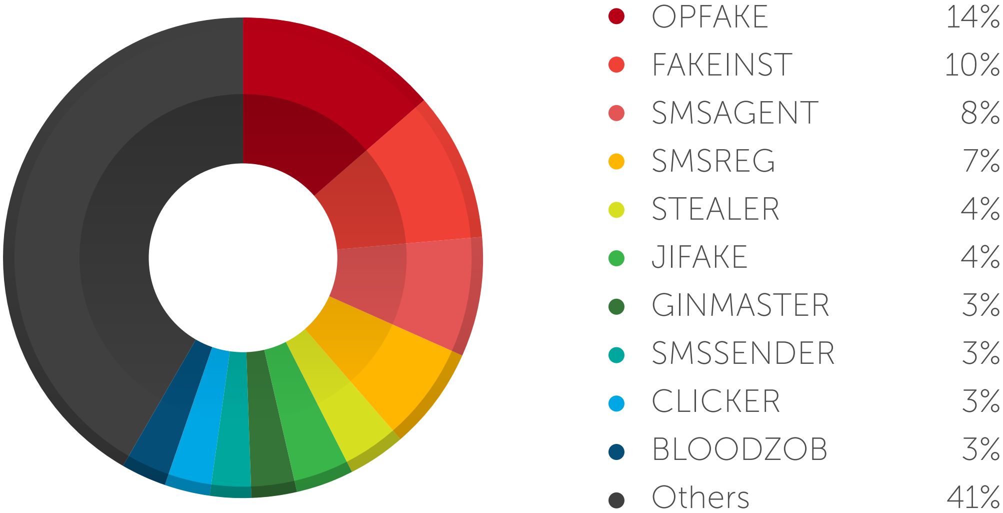
New Android Threat Additions per Month, 2Q 2014



Consistent with last quarter's numbers, the new mobile malware and high-risk app additions this quarter accounted for more than a fifth of the total number of Android threats.

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.*

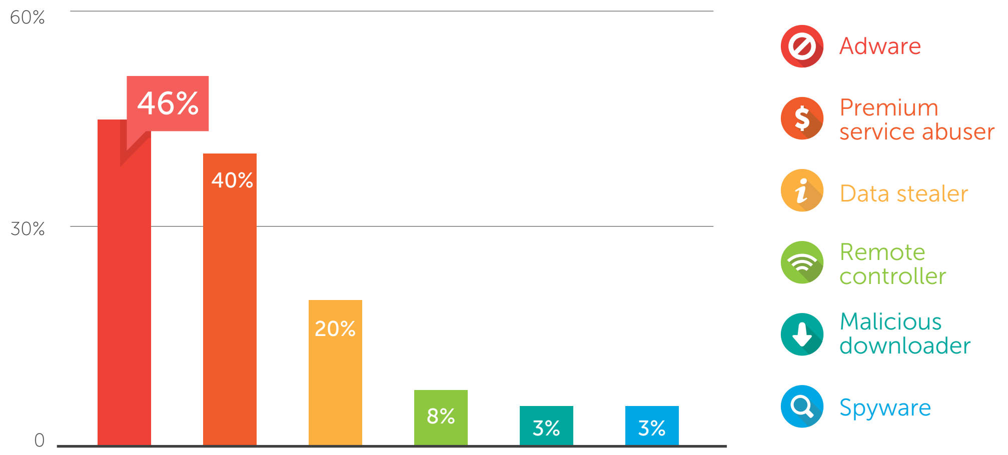
Top Android Malware Families, 2Q 2014



OPFAKE topped the list of Android malware families seen this quarter. FAKEINST rose to the second spot, possibly due to the rising number premium service abusers.

***NOTE:** Premium service abusers register victims to overpriced services while adware aggressively push ads and could collect personal information without victim consent.*

Top Android Threat Type Distribution, 2Q 2014



The share of adware remained the largest though it slightly decreased from last quarter. The shares of premium service abusers and data stealers increased as well. Spyware also figured as a top threat type in the mobile landscape.

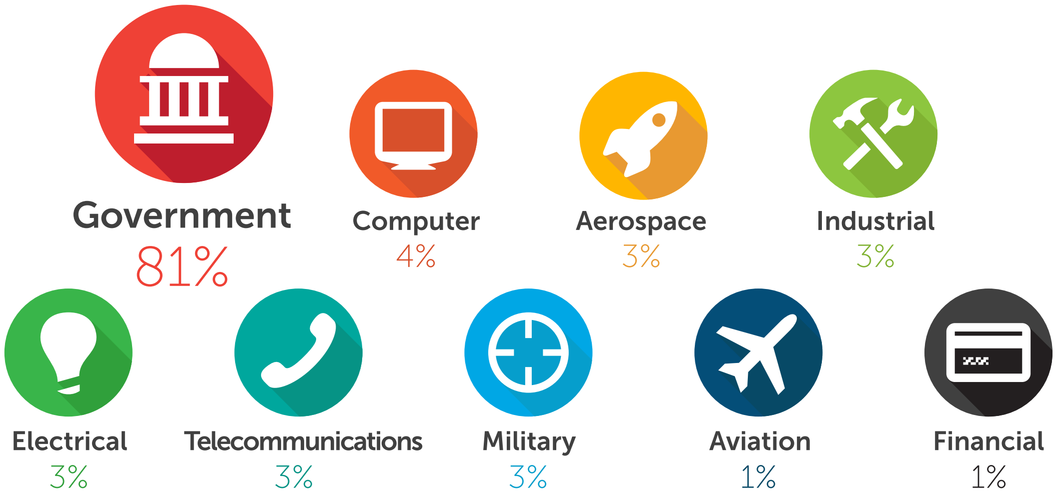
***NOTE:** Spyware track or monitor users' Global Positioning System (GPS) location, text messages, and calls then send this information to third parties. These are typically marketed as "spying tools" that users can install in the phone or tablet of anyone they wish to "spy on."*

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 April to June 2014. A mobile threat family may exhibit the behaviors of more than one threat type.

Targeted Attacks

The attacks seen this quarter primarily targeted government institutions via campaigns such as PLEAD and ANTIFULAI.[45, 46] We monitored both of these campaigns, which targeted various organizations in both the public and private sectors, particularly in Taiwan and Japan.

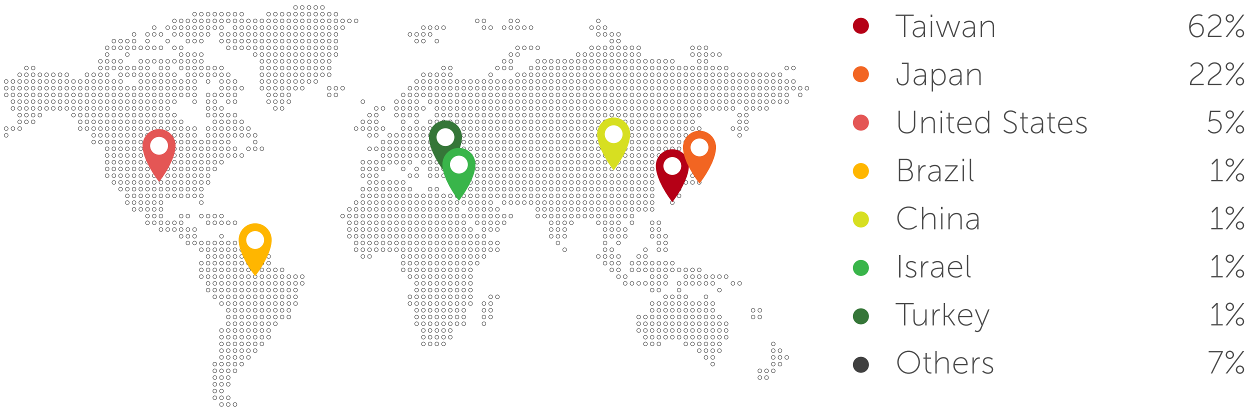
Targeted Attack Volume by Industry, 2Q 2014



The majority of the attacks continued to target government institutions this quarter.

NOTE: *This figure shows our findings on the targeted attacks we monitored this quarter.*

Targeted Attack Distribution by Country, 2Q 2014



Taiwan was the most targeted country this quarter, followed by Japan.

NOTE: *This map shows our findings on the targeted attacks we monitored this quarter.*

Notable Active Targeted Attack Campaigns, 2Q 2014

CAMPAIGN	MONTH DISCOVERED	TARGET	POINT OF ENTRY	REASON FOR BEING NOTABLE
PLEAD	May	Government and administrative agencies in Taiwan	Email	Use of the right-to-left override (RTLO) technique
ANTIFULAI	June	Government and various private sectors in Japan	Email	Exploited Ichitaro vulnerability
HAVEX	June	Industrial Control Systems (ICS) users primarily in Europe and in the United States	Phishing emails, watering hole attacks	Hacking of ICS-related sites to compromise legitimate applications

SOURCES:
http://blog.trendmicro.com/trendlabs-security-intelligence/plead-targeted-attacks-against-taiwanese-government-agencies-2/
http://blog.trendmicro.com/trendlabs-security-intelligence/antifulai-targeted-attack-exploits-ichitaro-vulnerability/
http://about-threats.trendmicro.com/us/webattack/139/HAVEX+Targets+Industrial+Control+Systems

The top concern with regard to targeted attacks…

Organizations' number 1 concern should be 'headline risk.' Targeted attacks dramatically increase reputational risk but there are two attack vectors of most concern.

First, watering-hole attacks are flourishing in the United States. A watering-hole attack is one wherein the corporate Web server is compromised and specific pages within its site attack visitors with tailor-made malware. These attacks are extremely effective against employees who utilize their websites as portals, which spread threats to customers and partners. This could have a tremendous reputational impact on the organizations' brands.

The second vector is 'island hopping.' Island-hopping attacks occur when attackers target an organization's network to get into its partners' and customers' networks. The lateral movement across trusted networked systems is extremely damaging to the victims' reputations and brands.

Attackers focus on the weakest link of the supply chain. The more reconnaissance attackers conduct on corporate supply chains, the more island-hopping attacks we will see.

—Tom Kellermann
Chief Cybersecurity Officer

Digital Life and IoE/IoT

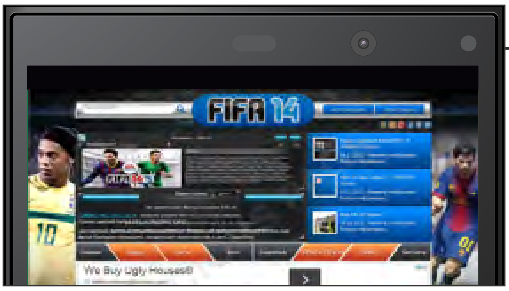
As the IoE/IoT phenomenon continues to unlock new possibilities for sharing and connecting with others, thus improving our way of life, those who benefit from it could also be vulnerable to attacks against it.

IoE/IoT devices connected to vulnerable wireless routers could allow any external user to access its firmware page and put users at risk if the routers are hacked.[47] Tampering with a vulnerable modem or router could also compromise any IoE/IoT device (e.g., smart meters or an entire smart hub) connected to it. Routers are a vital part of any Internet-connected network, as they are a main component in powering smart hubs—devices that connect all IoE/IoT devices to one another. Users should therefore keep them secure.

Apart from smart devices, Web-browsing activities also make up a huge part of people's digital lives. That is why vigilance when scouring for information or the mere act of going online is critical.

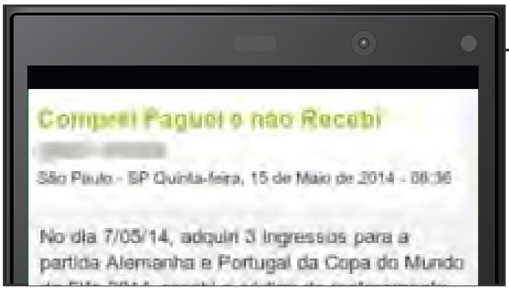
The 2014 FIFA World Cup held in Brazil was one of the most-sought-after sports events in recent history.[48] As such, users faced various threats, as it was one of the most widely used social engineering hooks this quarter, as evidenced by more than a billion Facebook comments and likes from over 200 million users and 300 million tweets.[49]

Recap of World-Cup-Related Threats, 2Q 2014



MAY 9

World-Cup-related searches led users to download a software key generator, which turned out to be a piece of adware.



Comprei Paguei e não Recebi

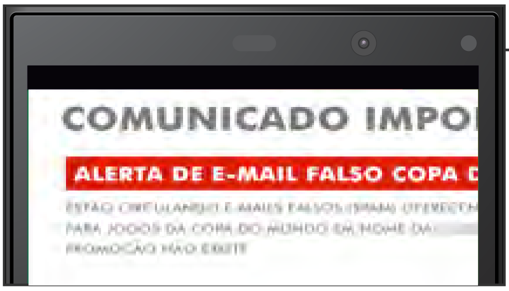
[redacted]

São Paulo - SP Quinta-feira, 15 de Maio de 2014 - 08:36

No dia 7/05/14, adquiri 3 ingressos para a partida Alemanha e Portugal da Copa do Mundo

MAY 20

Fake FIFA websites sold game tickets, causing victims to complain about paying the price even if they did not receive tickets.



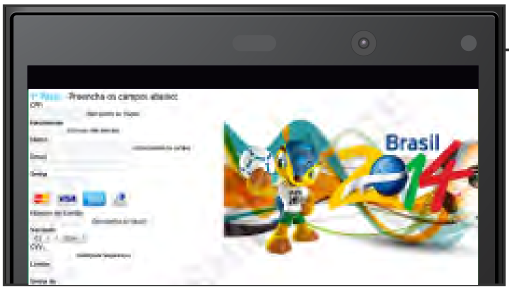
COMUNICADO IMPO

ALERTA DE E-MAIL FALSO COPA D

ESTÃO CIRCULANDO E-MAILS FALSOS (SPAM) OFERECEN
PARA JOGOS DA COPA DO MUNDO EM NOME DA [redacted]
PROMOÇÃO NÃO EXISTE

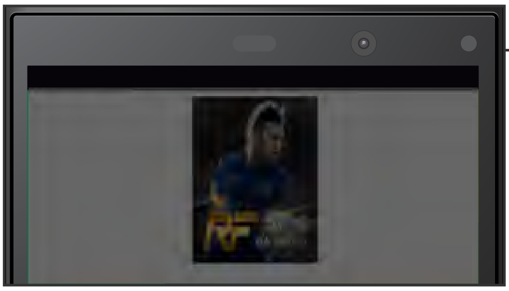
MAY 30

Spam claimed that the recipient was eligible to a raffle ticket for a chance to win World Cup tickets. This was a scam, of course.



JUN 9

Spam led to more phishing sites related to the World Cup



JUN 12

Fake World-Cup-related mobile apps spread on Google Play. ANDROIDOS_SMSSTEALER.HBT is another Android malware that took advantage of the World Cup fever. This malware family is notable for adding an SMS filter that blocks incoming text messages. Seventy-six domains were found upon analyzing its C&C servers, which were also used to host third-party app download websites.

SOURCES:

http://blog.trendmicro.com/trendlabs-security-intelligence/threats-get-a-kick-out-of-2014-fifa-world-cup-brazil-buzz/
http://blog.trendmicro.com/trendlabs-security-intelligence/brazilian-users-being-scammed-with-2014-fifa-world-cup-tickets/
http://blog.trendmicro.com/trendlabs-security-intelligence/home-court-advantage-banload-joins-fifa-world-cup/
http://blog.trendmicro.com/trendlabs-security-intelligence/phishing-sites-start-world-cup-campaign/
http://blog.trendmicro.com/trendlabs-security-intelligence/watch-out-for-fake-versions-of-world-cup-2014-apps/

The biggest IoE-/IoT-related event and the effect of radio-Internet convergence…

The biggest event this quarter was Google Glass's full commercial release, which was said to have sold out within hours. Even an adoption skeptic has to admit that's impressive for a technology that will be outdated in a few years. Add to that the much-talked-about iWatch from Apple's rumored release later this year and it's clear that 2015 will be the 'Year of the Connected,' if not quite yet the 'Year of the Infected.'

These technologies present new opportunities for attackers. The GPS on your wristband, for instance, won't simply track where you run daily, it will also reveal which ATMs you regularly use. Your heart rate monitor isn't only good for you at the gym, it's also good for someone to figure out how asleep you are at a given time. As consumer adoption increases, so will criminal adoption.

The cornerstone of IoE/IoT's success is communication. Radio and other wireless technologies are an integral part of this evolution. Unfortunately, many of the technical principles underlying legacy radio technologies that are being dragged in to power IoE/IoT were set in stone long before the commercial Web was a twinkle in Tim Berners-Lee's eye and were not designed with security in mind. Much like TCP/IP, they were rather designed for resilience.

We can fully expect criminal interest in this area to continue growing, as the manipulation or outright falsification of communication will have measurable real-world consequences because there are ill-gotten gains to be had and chaos to sow.

—Rik Ferguson

Vice President, Security Research

References

1. Noah Rayman. (July 3, 2014). *Time*. “Breaches of Your Personal Data Are Up 20%.” Last accessed July 16, 2014, http://time.com/2953428/data-breaches-identity-theft/.

2. Raimund Genes. (April 6, 2014). *TrendLabs Security Intelligence Blog*. “Advice for Enterprises in 2014: Protect Your Core Data.” Last accessed July 17, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/advice-for-enterprises-in-2014-protect-your-core-data/.

3. Pawan Kinger. (April 8, 2014). *TrendLabs Security Intelligence Blog*. “Skipping a Heartbeat: The Analysis of the Heartbleed OpenSSL Vulnerability.” Last accessed July 16, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/skipping-a-heartbeat-the-analysis-of-the-heartbleed-openssl-vulnerability/.

4. Maxim Goncharov. (April 10, 2014). *TrendLabs Security Intelligence Blog*. “Heartbleed Vulnerability Affects 5% of Select Top-Level Domains from Top 1M.” Last accessed July 16, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/heartbleed-vulnerability-affects-5-of-top-1-million-websites/.

5. Veo Zhang. (April 10, 2014). *TrendLabs Security Intelligence Blog*. “Heartbleed Bug—Mobile Apps Are Affected, Too.” Last accessed July 16, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/heartbleed-bug-mobile-apps-are-affected-too/.

6. Jonathan Leopando. (April 27, 2014). *TrendLabs Security Intelligence Blog*. “Internet Explorer Zero-Day Hits All Versions in Use.” Last accessed July 16, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/internet-explorer-zero-day-hits-all-versions-in-use/.

7. Abigail Pichel. (April 8, 2014). *TrendLabs Security Intelligence Blog*. “April 2014 Patch Tuesday Fixes Microsoft Word Zero-Day.” Last accessed July 16, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/april-2014-patch-tuesday-fixes-microsoft-word-zero-day/.

8. Abigail Pichel. (May 14, 2014). TrendLabs Security Intelligence Blog. “May 2014 Patch Tuesday Rolls Out 8 Bulletins.” Last accessed July 16, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/may-2014-patch-tuesday-rolls-out-8-bulletins/.

9. Bernadette Irinco. (June 10, 2014). *TrendLabs Security Intelligence Blog*. “June 2014 Patch Tuesday Resolves Critical Flaws in Internet Explorer, Microsoft Office.” Last accessed July 16, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/june-2014-patch-tuesday-resolves-critical-flaws-in-internet-explorer-microsoft-office/.

10. Maria Manly. (July 1, 2014). *TrendLabs Security Intelligence Blog*. “DOWNAD Tops Malware Spam Source in Q2 2014.” Last accessed July 16, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/downad-tops-malware-spam-source-in-q2-2014/.

11. Abigail Pichel. (April 28, 2014). *TrendLabs Security Intelligence Blog*. “Adobe Releases Patch for Flash Zero-Day Vulnerability.” Last accessed July 16, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/adobe-releases-patch-for-flash-zero-day-vulnerability/.

12. Pavithra Hanchagaiah. (April 28, 2014). *TrendLabs Security Intelligence Blog*. “Season of Zero-Days: Multiple Vulnerabilities in Apache Struts.” Last accessed July 16, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/season-of-zero-days-multiple-vulnerabilities-in-apache-struts/.

13. *Apache Struts 2 Documentation*. “S2-021.” Last accessed July 16, 2014, http://struts.apache.org/release/2.3.x/docs/s2-021.html.

14. Weichao Sun. (May 12, 2014). *TrendLabs Security Intelligence Blog*. “Android App Components Prone to Abuse.” Last accessed July 16, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/android-app-components-prone-to-abuse/.

15. Errata Security. (June 21, 2014). “300K Vulnerable to Heartbleed Two Months Later.” Last accessed July 23, 2014, http://blog.erratasec.com/2014/06/300k-vulnerable-to-heartbleed-two.html#.U8_Ds_mSySr.

16. Dan Goodin. (June 19, 2014). *Ars Technica*. “AWS Console Breach Leads to Demise of Service with “Proven” Backup Plan.” Last accessed July 16, 2014, http://arstechnica.com/security/2014/06/aws-console-breach-leads-to-demise-of-service-with-proven-backup-plan/.

17. Jay McGregor. (June 11, 2014). *Forbes*. “Feedly and Evernote Go Down as Attackers Demand Ransom.” Last accessed July 16, 2014, http://www.forbes.com/sites/jaymcgregor/2014/06/11/feedly-and-evernote-go-down-as-attackers-demand-ransom/.

18. Identity Theft Resource Center. (July 15, 2014). *ITRC*. “2014 Data Breach Category Summary.” Last accessed July 16, 2014, http://www.idtheftcenter.org/images/breach/ITRCBreachStatsReportSummary2014.pdf.

19. Identity Theft Resource Center. (July 15, 2014). *ITRC*. “2014 Breach List.” Last accessed July 16, 2014, http://www.idtheftcenter.org/images/breach/ITRC_Breach_Report_2014.pdf.

20. Rik Ferguson. (May 21, 2014). *Countermeasures*. “Oy Vey, eBay! Five Questions for You….” Last accessed July 16, 2014, http://countermeasures.trendmicro.eu/oy-vey-ebay-five-questions-for-you/.

21. eBay Inc. (May 21, 2014). eBay Inc. “eBay Inc. to Ask eBay Users to Change Passwords.” Last accessed July 16, 2014, http://www.ebayinc.com/in_the_news/story/ebay-inc-ask-ebay-users-change-passwords.

22. Narottam Medhora, Tanvi Mehta, and Ankit Ajmera. (June 10, 2014). *Reuters*. “Restaurant Chain P.F. Chang’s Investigating Possible Data Breach.” Last accessed July 16, 2014, http://www.reuters.com/article/2014/06/11/us-pfchang-dataprotection-idUSKBN0EM06C20140611.

23. P.F. Chang’s China Bistro Inc. (July 1, 2014). *P.F. Chang’s*. “Security Compromise Update.” Last accessed July 16, 2014, http://www.pfchangs.com/security/.

24. Abigail Pichel. (May 26, 2014). *TrendLabs Security Intelligence Blog*. “Ransomware Moves to Mobile.” Last accessed July 16, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-moves-to-mobile/.

25. Trend Micro Incorporated. (2014). *Threat Encyclopedia*. “ANDROIDOS_LOCKER.HBT.” Last accessed July 16, 2014, http://about-threats.trendmicro.com/us/malware/ANDROIDOS_LOCKER.HBT.

26. Weichao Sun. (June 7, 2014). *TrendLabs Security Intelligence Blog*. “Android Ransomware Uses Tor.” Last accessed July 16, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/android-ransomware-uses-tor/.

27. Maria Manly. (June 9, 2014). *TrendLabs Security Intelligence Blog*. “Social Engineering Watch: UPATRE Malware Abuses Dropbox Links.” Last accessed July 23, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/social-engineering-watch-upatre-malware-abuses-dropbox-links/.

28. Warren Tsai. (April 16, 2014). *Trend Micro Simply Security*. “FAKEAV in Google Play and How Trend Micro Mobile App Reputation Services Dynamic Analysis Helps Protect You.” Last accessed July 16, 2014, http://blog.trendmicro.com/fakeav-google-play-mobile-app-reputation-services/#.U8M4d5SSzTo.

29. Symphony Luo and Peter Yan. (2014). *Trend Micro Security Intelligence*. “Fake Apps: Feigning Legitimacy.” Last accessed July 17, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-fake-apps.pdf.

30. Trend Micro Incorporated. (2014). Threat Encyclopedia. “ANDROIDOS_FAKEAV.B.” Last accessed July 22, 2014, http://about-threats.trendmicro.com/us/malware/ANDROIDOS_FAKEAV.B.

31. Jonathan Leopando. (June 2, 2014). *TrendLabs Security Intelligence Blog*. “Banking Trojan Trend Hits Japan Hard.” Last accessed July 16, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/banking-trojan-trend-hits-japan-hard/.

32. David Sancho, Feike Hacquebord, and Rainer Link. (2014). *Trend Micro Security Intelligence*. “Finding Holes: Operation Emmental.” Last accessed July 23, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-finding-holes-operation-emmental.pdf.

33. David Sancho. (July 22, 2014). *TrendLabs Security Intelligence Blog*. “Finding Holes in Online Banking Security: Operation Emmental.” Last accessed July 23, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/finding-holes-operation-emmental/.

34. Trend Micro Incorporated. (April 29, 2014). *TrendLabs Security Intelligence Blog*. “The Challenge of Collaborating with Law Enforcement Agencies to Stop Cybercrime.” Last accessed July 16, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/the-challenge-of-collaborating-with-law-enforcement-agencies-to-stop-cybercrime/.

35. Trend Micro Incorporated. (May 22, 2014). *TrendLabs Security Intelligence Blog*. “SpyEye-Using Cybercriminal Arrested in Britain.” Last accessed July 16, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/spyeye-using-cybercriminal-arrested-in-britain/.

36. Lord Alfred Remorin. (June 2, 2014). *TrendLabs Security Intelligence Blog*. "GameOver: ZeuS with P2P Functionality Disrupted." Last accessed July 16, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/gameover-zeus-with-p2p-functionality-disrupted/.

37. Feike Hacquebord. (November 9, 2011). *TrendLabs Security Intelligence Blog*. "Esthost Taken Down—Biggest Cybercriminal Takedown in History." Last accessed July 26, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/esthost-taken-down-biggest-cybercriminal-takedown-in-history/.

38. Editor. (June 5, 2014). *KUOW.org*. "A Year After Snowden, U.S. Tech Losing Trust Overseas." Last accessed July 16, 2014, http://kuow.org/post/year-after-snowden-us-tech-losing-trust-overseas.

39. David Kravets. (July 15, 2014). *Ars Technica*. "Obama Administration Says the World's Servers Are Ours." Last accessed July 26, 2014, http://arstechnica.com/tech-policy/2014/07/obama-administration-says-the-worlds-servers-are-ours/.

40. Raimund Genes. (June 5, 2014). *TrendLabs Security Intelligence Blog*. "Privacy and the Right to Be Forgotten." Last accessed July 16, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/privacy-and-the-right-to-be-forgotten/.

41. Rich McCormick. (July 11, 2014). The Verge. "Google's Top Lawyer Says EU's 'Right to Be Forgotten' Restricts Freedom of Expression." Last accessed July 16, 2014, http://www.theverge.com/2014/7/11/5889133/google-top-lawyer-says-right-to-be-forgotten-restricts-rights.

42. Bill Mears. (June 25, 2014). *CNN*. "Supreme Court: Police Need Warrant to Search Cell Phones." Last accessed July 16, 2014, http://edition.cnn.com/2014/06/25/justice/supreme-court-cell-phones/.

43. Office of the Data Protection Commissioner. (2014). *Data Protection Commissioner*. "A Guide to Your Rights." Last accessed July 17, 2014, http://www.dataprotection.ie/docs/A-guide-to-your-rights-Plain-English-Version/858.htm.

44. Trend Micro Incorporated. (May 2013). Trend Micro Security Intelligence. "TrendLabs 2Q 2013 Security Roundup: Mobile Threats Go Full Throttle." Last accessed July 26, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-2q-2013-trendlabs-security-roundup.pdf.

45. Kervin Alintanahin. (May 23, 2014). *TrendLabs Security Intelligence Blog*. "PLEAD Targeted Attacks Against Taiwanese Government Agencies." Last accessed July 26, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/plead-targeted-attacks-against-taiwanese-government-agencies-2/.

46. Maersk Menrige. (June 4, 2014). *TrendLabs Security Intelligence Blog*. "ANTIFULAI Targeted Attack Exploits Ichitaro Vulnerability." Last accessed July 26, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/antifulai-targeted-attack-exploits-ichitaro-vulnerability/.

47. Ilja Lebedev. (May 20, 2014). *TrendLabs Security Intelligence Blog*. "When Networks Turn Hostile." Last accessed July 16, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/when-networks-turn-hostile/.

48. Ryan Certeza. (July 13, 2014). *TrendLabs Security Intelligence Blog*. "Being Secure in the Most-Connected World Cup Ever." Last accessed July 23, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/being-secure-in-the-most-connected-world-cup-ever/.

49. Prashant Pansare (July 15, 2014) *Diligent Media Corporation Ltd*. "This Is Why the FIFA World Cup 2014 Was the Biggest Social Media Event." Last accessed July 23, 2014, http://www.dnaindia.com/blogs/post-this-is-why-the-fifa-world-cup-2014-was-the-biggest-social-media-event-2002244.

Created by:

TrendLabs

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

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.