TrendLabs℠ 2013 Annual Security Roundup

TREND MICRO™

Cashing in on Digital Information

An Onslaught of Online Banking Malware and Ransomware

Contents

Introduction

Good old-fashioned stick-'em-up bank heists have seemingly been pushed to the curb by digital heists in 2013. Cybercriminals who used sophisticated techniques to get hold of credit card numbers, bank accounts, and even personally identifiable information (PII) in a matter of minutes have taken the place of traditional thieves. Information is, after all, the new currency. And with it on hand, cybercriminals can hold victims at their mercy, which should make us all realize that we stand to lose more than we think.

We saw old threats "refined" throughout 2013. The number of online banking malware we detected, for one, increased as the year progressed, even in countries they did not previously target. October 2013 also proved troublesome for users, as the number of ransomware infections increased and as the malware took an even more crippling form—CryptoLocker. These and other refinements over the past year echoed what we predicted would happen—cybercriminals would improve existing tools instead of create new ones.[1]

On the mobile security front, we witnessed the mobile malware and high-risk app volume surpass the 1-million mark as early as September 2013.[2] The current volume has, in fact, reached roughly 1.4 million, with 1 million new malicious and high-risk apps found in 2013 alone.

Media coverage on targeted attacks may have decreased in 2013 but we continued to find campaigns worldwide. We found attacks target various countries, including Brazil, France, and Germany.

In the vulnerability space, Oracle's end of support for Java™ 6 led to the rise of even more problems, which highlighted risks involved with not upgrading or continuing to use unsupported software versions.[3]

Taken together, while assaults against personal data have already been occurring for quite some time, they did not reach public consciousness as much as they did in 2013. Going after personal information proved to be a resounding theme last year, highlighted by debates on Edward-Snowden-fueled revelations about state monitoring on citizens. 2013 may have, in fact, prompted everyone to ask one of the most important questions in today's "digital age"—How can we keep our information safe? For most, the answer can be one of two things—disclose less or find products that can help us protect ourselves.

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.*

CYBERCRIME AND THE CYBERCRIMINAL UNDERGROUND

Malware that went straight for victims' money not only rose in number; they also targeted users in more regions.

Money-Grabbing Malware Numbers Soared

2013 was a challenging year for users worldwide, as refined threats posed serious risks to their digital lives. Common tasks like making online banking transactions and engaging in other financial-related activities put their private information and wallets at great risk.

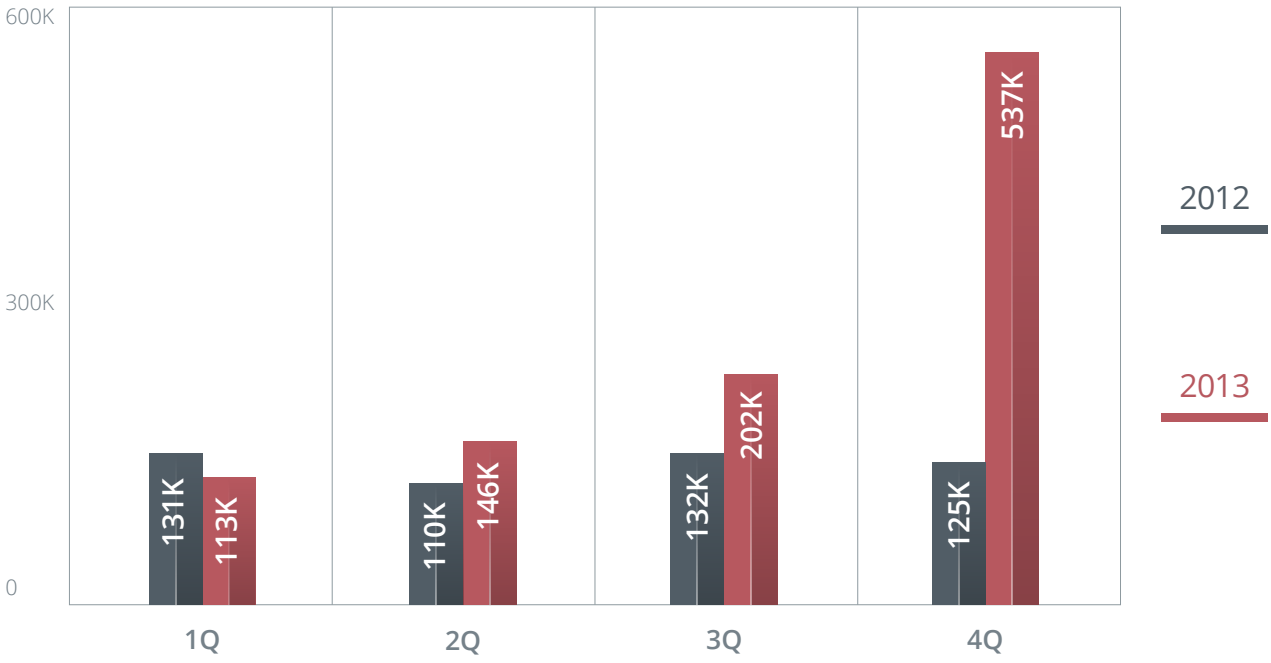
Online banking malware took center stage in terms of volume increase. Our number of online banking malware detections reached almost 1 million by the end of 2013. The United States and Japan remained most affected by online banking malware in the fourth quarter of 2013, with Brazil and Taiwan trailing close behind. The increase in the volume could be attributed to more online banking threat activities in Brazil and Japan.

In Brazil, we observed an increase in the use of .CPL files or malicious Control Panel items that were embedded in .RTF file spam attachments.[4] This trend started sometime in September 2013 and deviated from the typical online banking malware social engineering tactic of using .RAR or .ZIP files as attachment.

We also observed an increase in the number of ZBOT infections in Japan in the third and fourth quarters of 2013, which suggested a rise in cybercriminal activity either in the country or targeting Japanese users who weren't considered a big online banking malware target in previous years.

Malware refinements and the surge in the online banking malware volume led to a grave consequence for victims—actual monetary loss.[5, 6, 7, 8]

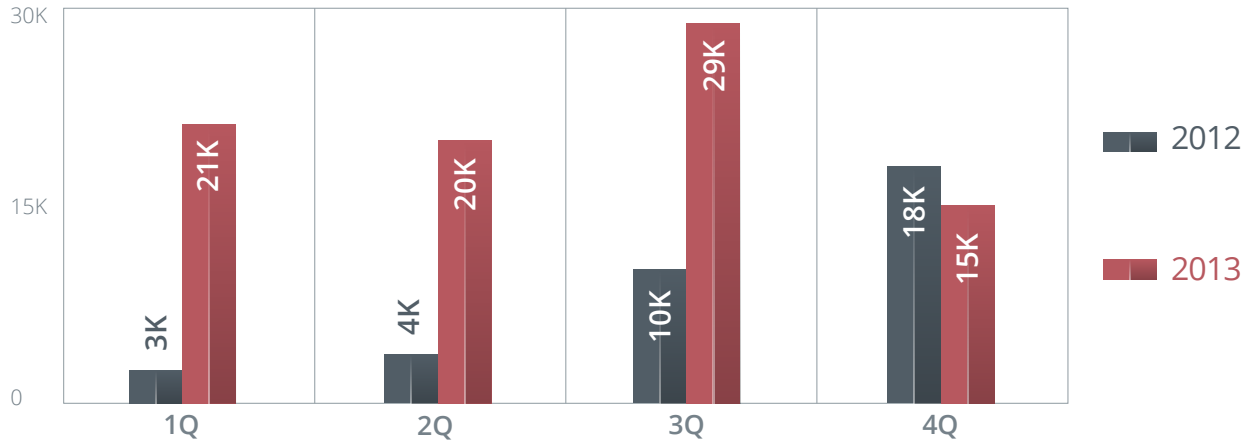
Total Online Banking Malware Volume, 2012 and 2013



The total number of online banking malware infections in 2013 doubled from 2012's around 500,000. This could be attributed to the spike in the number of online banking malware in Japan in the fourth quarter of 2013. A spike was also seen in Brazil during the holidays, when cybercriminals spread phishing emails and banking Trojans.

As a prime example of refinement, meanwhile, CryptoLocker's emergence last October as an improved version of ransomware showed how cybercriminals enhanced their tools rather than created new ones.[9] A spam campaign proved responsible for several infections, as we found emails carrying TROJ_UPATRE variants, known CryptoLocker carriers, as attachment.[10] CryptoLocker not only blocked user access to infected computers, it also forced them to buy a decryption tool for US$300 or with cryptocurrencies just to make the problem go away.

Quarterly Ransomware Volume, 2012 and 2013

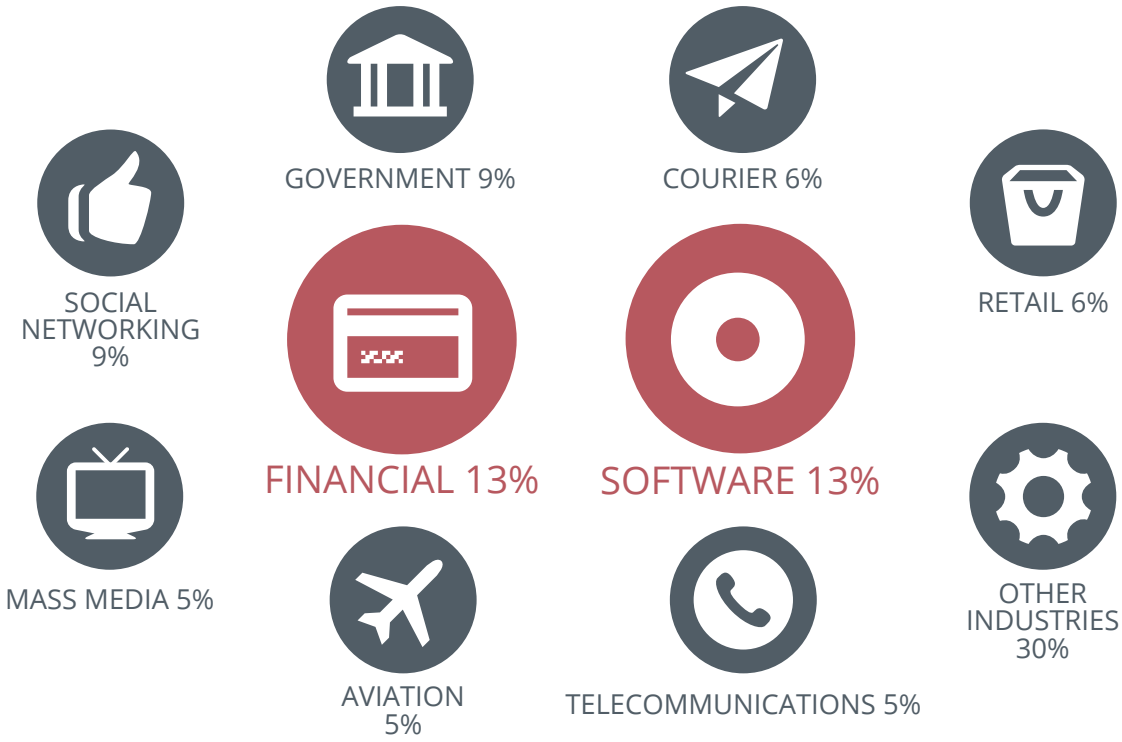


The total number of ransomware we detected in 2013 more than doubled compared with that in 2012. The volume was particularly high in the third quarter of 2013 (30,000) due to the rise in the number of CryptoLocker detections last October.

Cybercriminal efforts to stay under the radar were relentless.[11] Last October, we also documented their use of sites in the so-called "Deep Web" that guaranteed anonymous and untraceable access.[12] We analyzed how they used the network to exchange tools and tactics by closely examining existing marketplaces.

All of these, however, didn't translate to lack of security industry wins in 2013. The October arrest of the Blackhole Exploit Kit creator, Paunch, led to a notable decrease in the overall spam volume in November 2013, as shown by Smart Protection Network data.[13] This trend reflected the Blackhole Exploit Kit's demise.[14] By December, however, the overall spam volume started to gradually rise once more, as cybercriminals went after organizations in the financial and software industries.

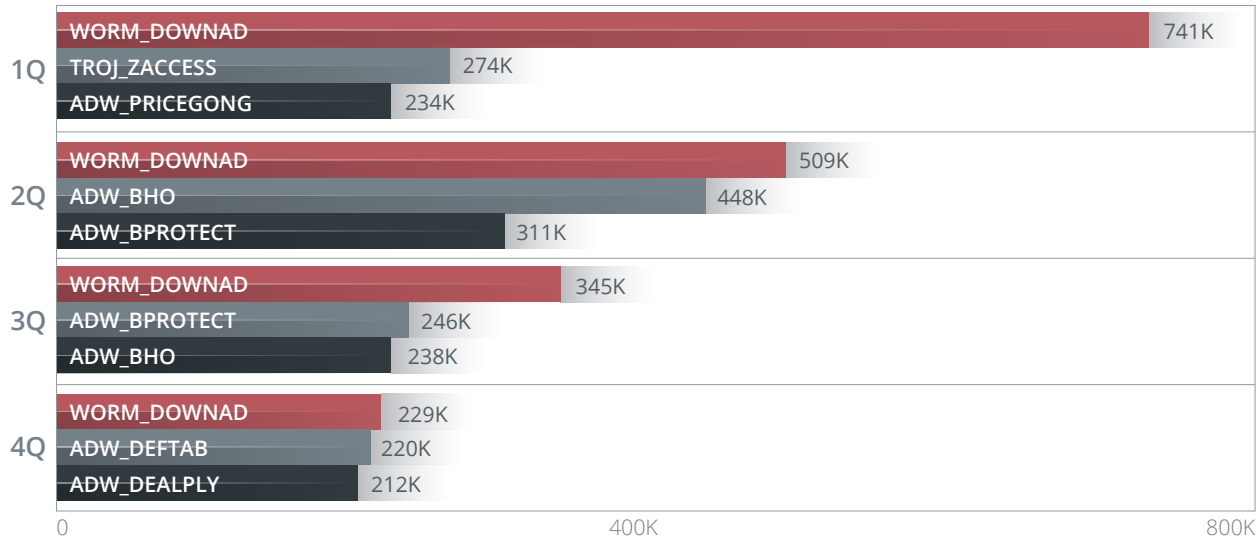
Top Industries Spoofed by Blackhole Exploit Kit Spam, 2013



Based on our tracking of Blackhole-Exploit-Kit-related spam campaigns, around 25% targeted banks and software companies.

As a not-so-surprising twist, the notorious DOWNAD/Conficker worm slowly lost momentum throughout 2013, as more and more users—individuals and organizations alike—shifted to newer Windows® versions. In fact, the 2013 overall Smart Protection Network numbers show that the DOWNAD/Conficker detection volume decreased from 741,000 in the first quarter to only 229,000 by the end of December. Despite the decline, DOWNAD/Conficker remained the top malware among enterprises and small and medium-sized businesses (SMBs) in 2013. Patching the vulnerability addressed by MS08-067 though prevents DOWNAD/Conficker infections. Vulnerability shielding via Trend Micro Deep Security also prevents the worm from spreading throughout a network.

Top 3 Malware, 2013



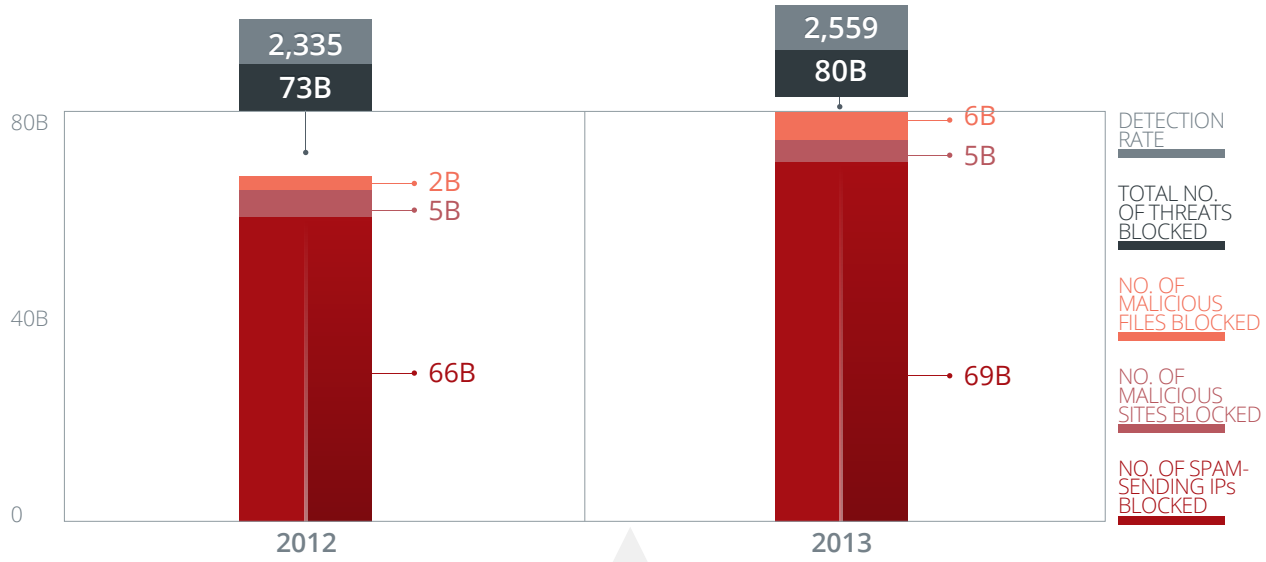
DOWNAD/Conficker remained the top malware in the fourth quarter of 2013 though the total volume significantly dropped from 741,000 in the first quarter.

Top 3 Malware by Segment, 2013

1Q		2Q		3Q		4Q	
ENTERPRISE							
WORM_DOWNAD	364K	WORM_DOWNAD	360K	WORM_DOWNAD	86K	WORM_DOWNAD	184K
PE_SALITY	81K	ADW_BPROTECT	53K	ADW_BPROTECT	33K	ADW_DEALPLY	44K
PE_VIRUX	34K	ADW_BHO	28K	ADW_TOOLBAR	21K	ADW_DEFTAB	43K
SMB							
WORM_DOWNAD	81K	WORM_DOWNAD	59K	WORM_DOWNAD	17K	WORM_DOWNAD	42K
PE_SALITY	17K	ADW_BPROTECT	9K	ADW_TOOLBAR	9K	ADW_DEFTAB	23K
TROJ_ZACCESS	14K	ADW_BHO	8K	ADW_BPROTECT	8K	HKTL_PASSVIEW	17K
CONSUMER							
TROJ_ZACCESS	163K	ADW_BHO	370K	ADW_BHO	158K	ADW_DEFTAB	89K
CRCK_KEYGEN	162K	ADW_BPROTECT	216K	ADW_BPROTECT	138K	ADW_OPENCANDY	60K
ADW_PRICEGONG	157K	BKDR_BIFROSE	208K	TROJ_FAKEAV	87K	ADW_BHO	54K

DOWNAD/Conficker malware plagued businesses until the last quarter of 2013 while consumers mostly fell prey to adware. This was not surprising because consumers were more likely to upgrade software than companies, which had to adhere to budget constraints and compliance issues.

Trend Micro Smart Protection Network Blocking Rates, 2012 and 2013



The total number of threats we blocked increased by 7 billion from 2012 to 2013. Our detection rate also rose, as we now block more than 2,500 threats per second.

Deep Web and Cybercriminal Underground Ware Prices, 2013

Crimeware prices varied, depending on where they were sold. Counterfeit Euro and U.S. banknotes were sold at significant prices. Fake documents were also considered precious commodities. Besides peddling stolen data, note that cybercriminals also offered services like Web development.
***Note:** "CUSD" stands for "counterfeit U.S. dollars"; "CEUR" stands for "counterfeit Euros"; "normalized cost" refers to "the average cost on sites in the Deep Web"*

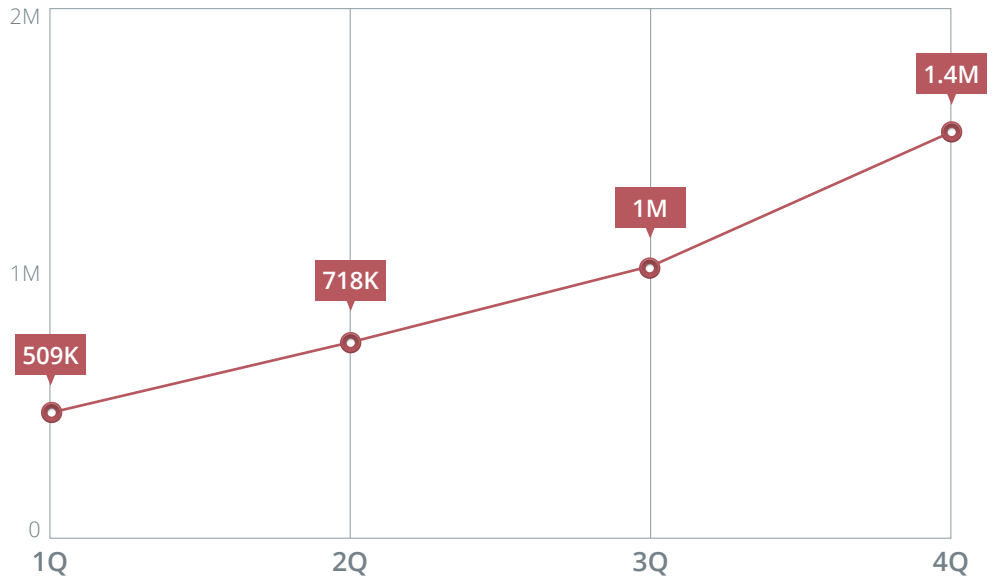
MOBILE

Mobile threats grew both in terms of volume and sophistication, made possible by the PC-to-mobile shift.

Bigger Number, Wider Reach

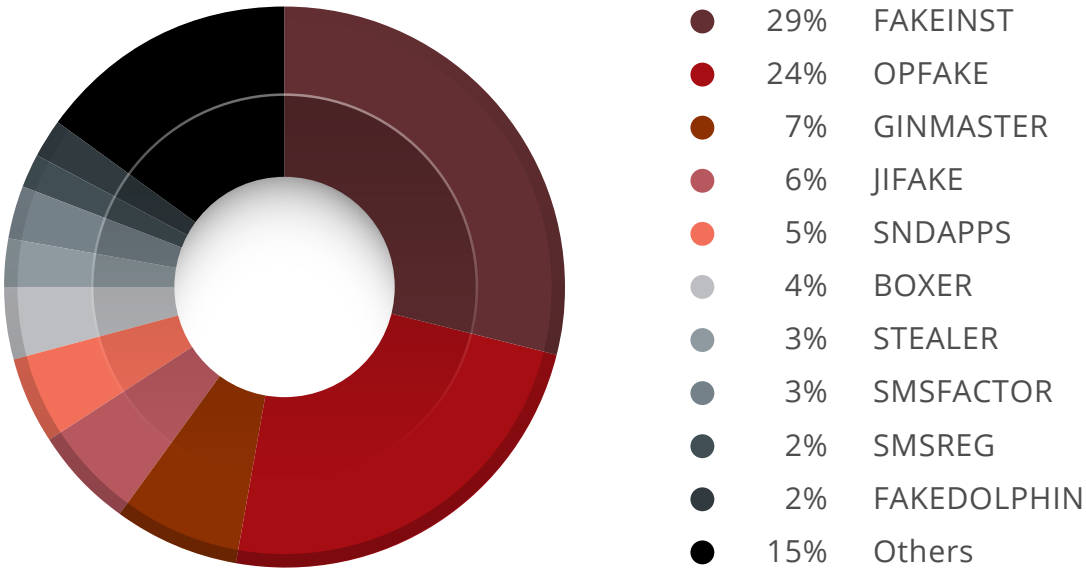
Android™ was and still is the most dominant mobile OS in the market today. In fact, Gartner believes that the number of Android users will surpass the 1-billion mark this year.[15] But along with its dominance last year came a large number of malicious and high-risk or potentially unwanted apps—almost 1.4 million—by the end of 2013 since the discovery of the first Android Trojan in 2010. This translated to 1 million new Android threats found in 2013 alone. Cybercriminals will continue to exploit the OS's dominance, as we predict the malicious and high-risk app volume to reach 3 million by the end of this year.[16]

Malicious and High-Risk Mobile App Growth, 2013



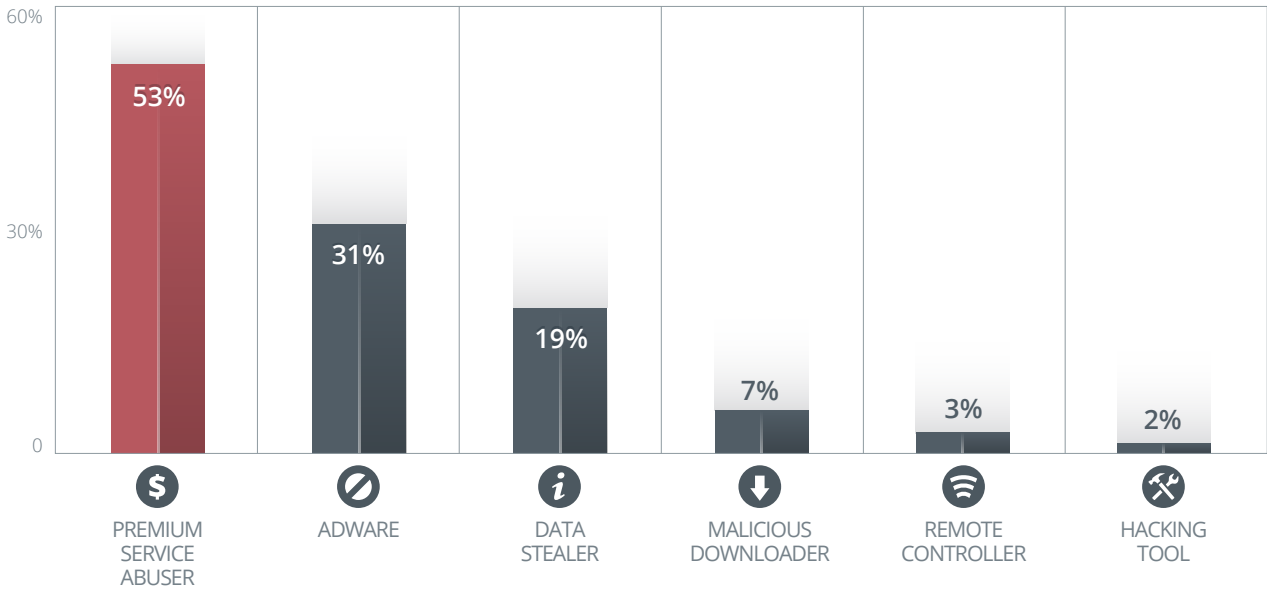
The number of mobile malware and high-risk apps more than doubled from 2012 to 2013. The number of malicious apps found in third-party and legitimate app stores also rose.
***Note:** High-risk or potentially unwanted apps are those that can compromise user experience because they display unwanted ads, create unnecessary shortcuts, or gather device information without user knowledge nor consent. Examples include aggressive adware.*

Top New Mobile Malware Family Additions, 2013



As usual, Trojanized versions of popular apps made up most of the additions to 2013's list of Android malware families.

Top Mobile Threat Types, 2013



Premium service abusers and adware remained the most common Android threats in 2013. Premium service abusers registered victims to overpriced services while adware aggressively pushed ads and could even collect personal information without victim consent.
***Note:** A mobile malware family may exhibit the behaviors of more than one threat type.*

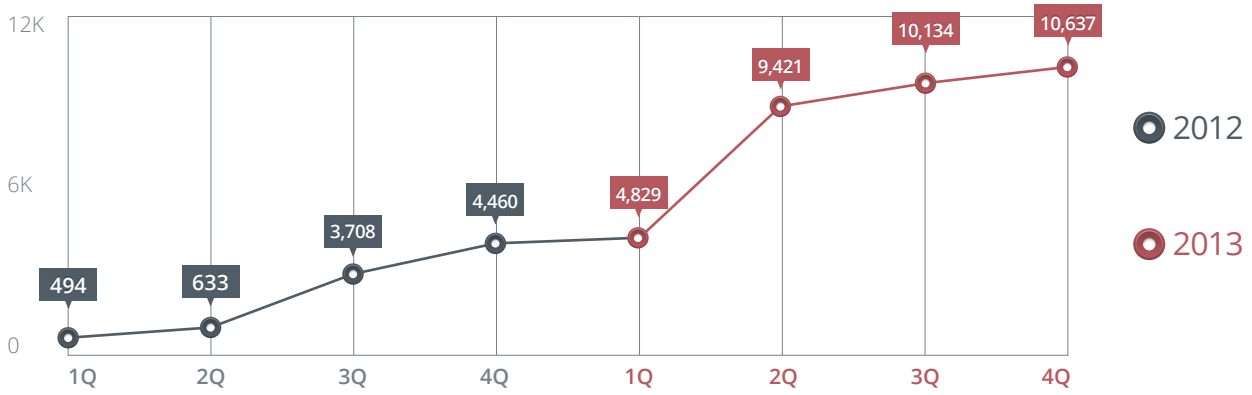
As we noted in the third quarter of 2013, while the majority of the malicious and high-risk apps found in the wild were hosted on malicious domains (80%), they also found their way to legitimate, including third-party, app stores (27%). We were, for instance, able to download some malicious apps from Google Play that pushed ads that led to fraudulent sites.[17] BlackBerry, in partnership with Trend Micro, also identified and blocked 2% of repackaged Android apps before they could be sold in BlackBerry World because these were flagged as either "malicious" or "high-risk" apps. Apple's App Store℠ was not spared as well, as security researchers created a proof-of-concept (PoC) app that slipped past the vendor's app approval process. They discovered that attackers could still effectively hide malicious behaviors that normally led to rejection during the standard review process just like what happened back in 2011.[18, 19] These incidents highlighted just how cybercriminals continuously improved their malicious mobile wares to get them onto even legitimate app stores.

How App Submission Works

This diagram shows how developers could submit their apps to both Google Play and Apple's App Store. Android apps require uploading a signed .APK file, market media, the necessary listing details, and copy before the .APK file can finally be activated and the app published. The App Store, meanwhile, requires developers to undergo a tedious approval process, as Apple implements an underlying security model to protect both user data and an app from being modified and distributed without its developer's knowledge.

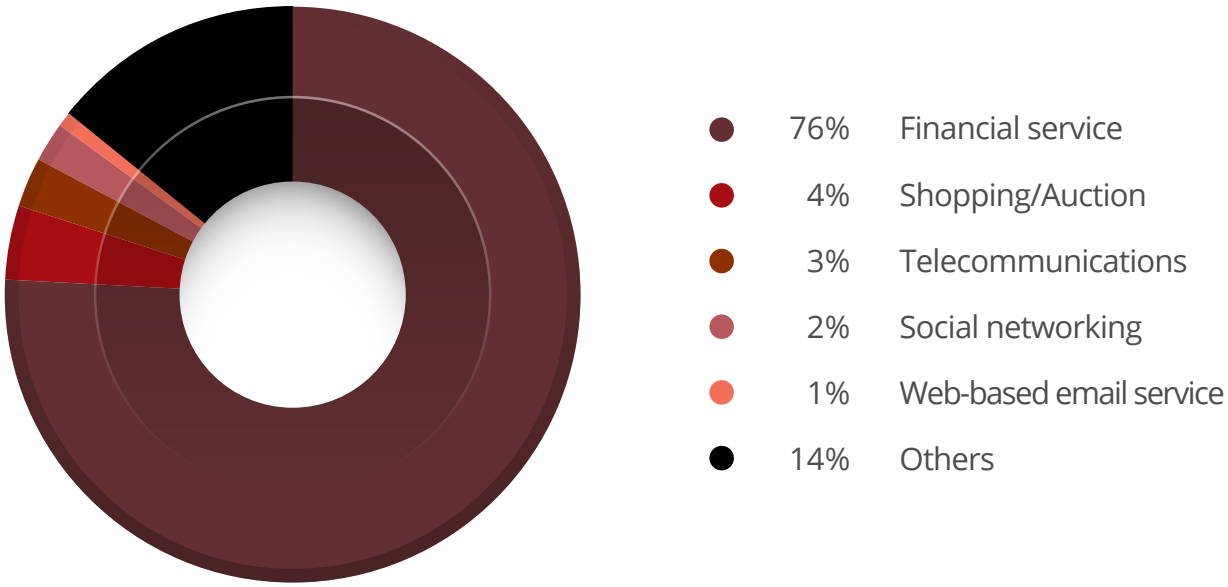
Apart from malicious and high-risk apps, Web threats like phishing continued to spread to mobile devices.[20] In 2013, the total number of mobile phishing sites, though still not comparable to those seen in the PC space, rose by 38% from 2012. Unlike traditional phishing sites seen on computers, mobile phishing sites were specially crafted to steal information from users who browsed the Web and engaged in various online activities via their smartphones or any other type of mobile device.[21]

Mobile Phishing Site Volume Growth, 2012 and 2013



Although the increases were not consistent, the cumulative number of mobile phishing sites continuously rose throughout 2012 and 2013. We particularly saw a huge spike in the second quarter of 2013 due to a rise in the spoofed PayPal site volume.

Top Mobile Phishing Targets, 2013

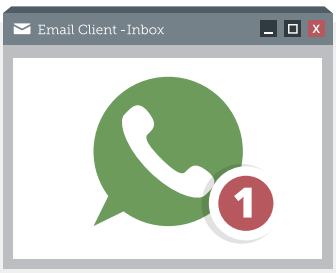


Financial sites remained the most favored phishing target even in the mobile space in 2013, particularly in the second quarter. PayPal was the most abused company when it came to phishing scams.

Spam also figured as a mobile threat vector, as evidenced by a WhatsApp scam we saw last September.[22] That said, mobile threats definitely grew not just in terms of volume but also in terms of sophistication, especially with regard to infection vector. They used spam and delivered different types of malware, depending on a victim's OS.

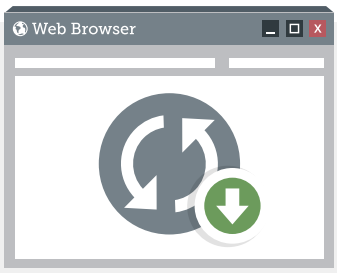
WhatsApp Scam Infection Chain

1



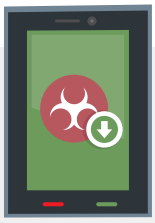
Fake WhatsApp voice mail arrives via email

2



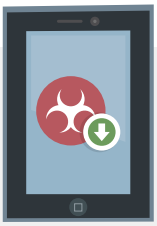
Clicking the image with the word "Play" leads the victim to a malicious site, which prompts the download of a mobile version of a fake app

3A



On an Android device, clicking "Play" opens a fake browser, which is actually a piece of malware; the browser triggers the sending of text messages to certain phone numbers and convinces the victim to download another malicious app

3B

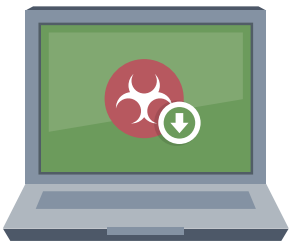


On an iOS device, clicking "Play" leads the victim to a site that downloads a malicious app; jailbroken devices are at greater risk though, as iOS devices can only download apps from the App Store by default

This scam highlighted how some cybercriminals have "gone mobile." The attack primarily focused on mobile devices, as all others were included just as an afterthought.

Banking threats also made waves in the mobile space by introducing a compromise to two-factor authentication methods.[23] The Perkele crimeware toolkit was specifically designed to affect mobile apps and could be used for man-in-the-middle (MitM) attacks. PERKEL malware, created with Perkele, intercepted mobile banking authentication messages.[24] In the second quarter of 2013, FAKEBANK malware went after mobile banking users' account information, call logs, and text messages in the guise of a legitimate banking app.[25]

How MitM Attacks Work



1 Malware infects a victim's computer

2 Victim visits a monitored online banking site

3 PC malware prompts the victim to scan a QR code; when scanned, QR code downloads another malware

4 PC malware initiates a banking transaction; SMS containing authentication code is sent to the mobile device

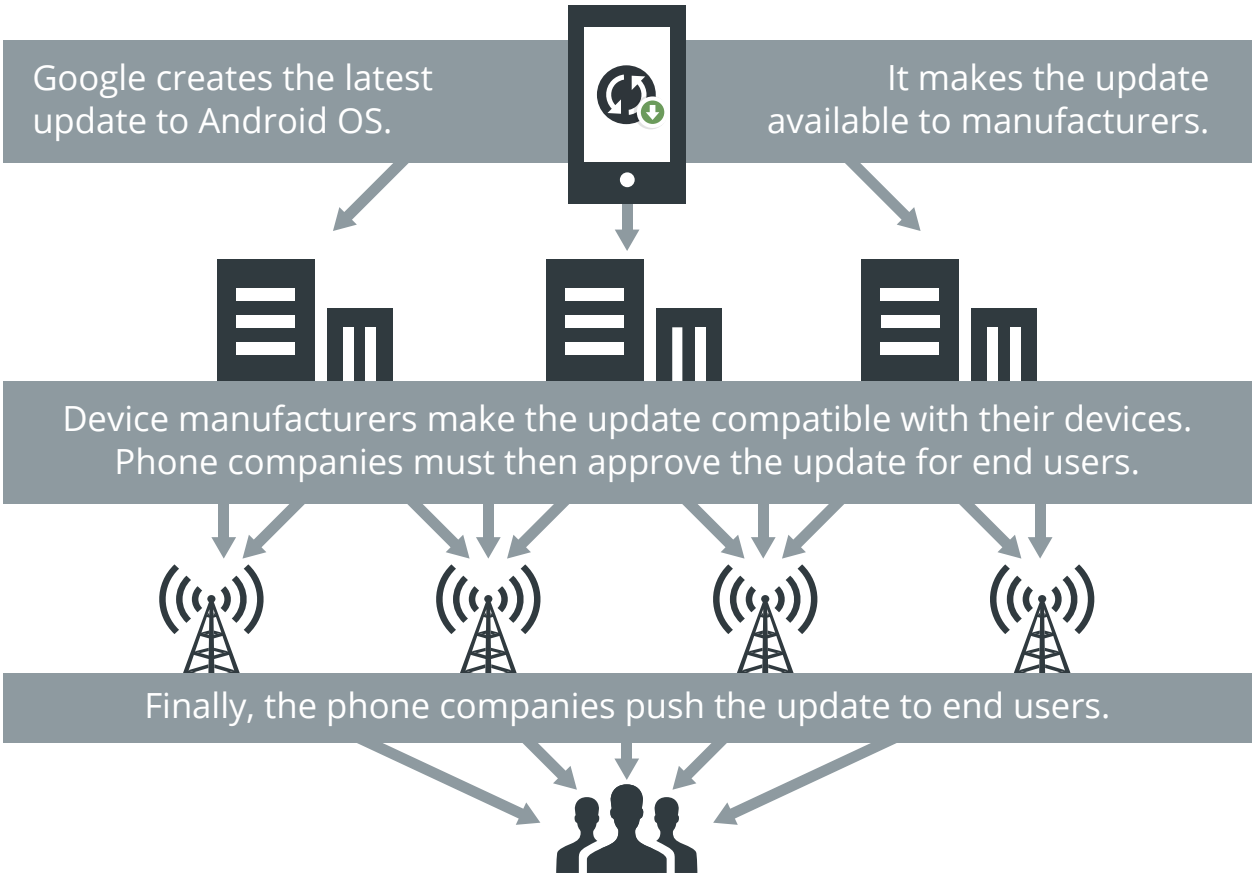
5 Mobile malware intercepts SMS containing the one-time passcode; attacker's server receives the code

6 PC malware receives code and completes transaction

Successful MitM attacks typically gave attackers access to banking information. In MitM attacks, attackers got their hands on all kinds of communication routed from a smartphone to an online banking site and vice versa.
Note: *The steps in this diagram were based on an incident involving PERKEL malware.*

Several mobile vulnerabilities made headlines in 2013.[26] Security flaws in SIM cards and mobile OSs were unraveled, top-billed by the Android "master key" vulnerability found last July, which allowed installed apps to be turned malicious without user consent nor knowledge.[27] OBAD malware also exploited a critical vulnerability in Android.[28] Patching vulnerabilities remained a concern, especially for most Android users, given the complex process security updates had to go through before they reached users. Then again, no OS remained safe, as an iOS 6 security flaw was also found, which could grant complete access to an iPhone® or iPad® running the said platform.

How the Android Update Process Works



Android's complicated update process could be one reason why devices remained vulnerable to various threats.

TARGETED ATTACK CAMPAIGNS AND CYBER ATTACKS

Targeted attacks showed no signs of abating though they no longer gained as much attention.

Targeted Attack Trends

Attackers continued to hone their techniques in 2013 and focused on gaining access to government information. We saw targeted attacks in different parts of the globe. Old vulnerabilities alongside new ones were heavily used. The CVE-2012-0158 vulnerability, for instance, was exploited via a specially crafted .DOC or .RTF file that affected Microsoft™ Office® 2003, 2007, and 2010 users worldwide because though the bug has been patched, not everyone updated their software.[29] A zero-day exploit for Internet Explorer® was also used in a watering hole attack targeting the U.S. Department of Labor site last May.[30] Our investigation revealed that visitors of the compromised site were redirected several times before they ended up with BKDR_POISON-infected computers.[31]

Given the potential data loss that can result from becoming a target, protecting infrastructure is more crucial than ever.

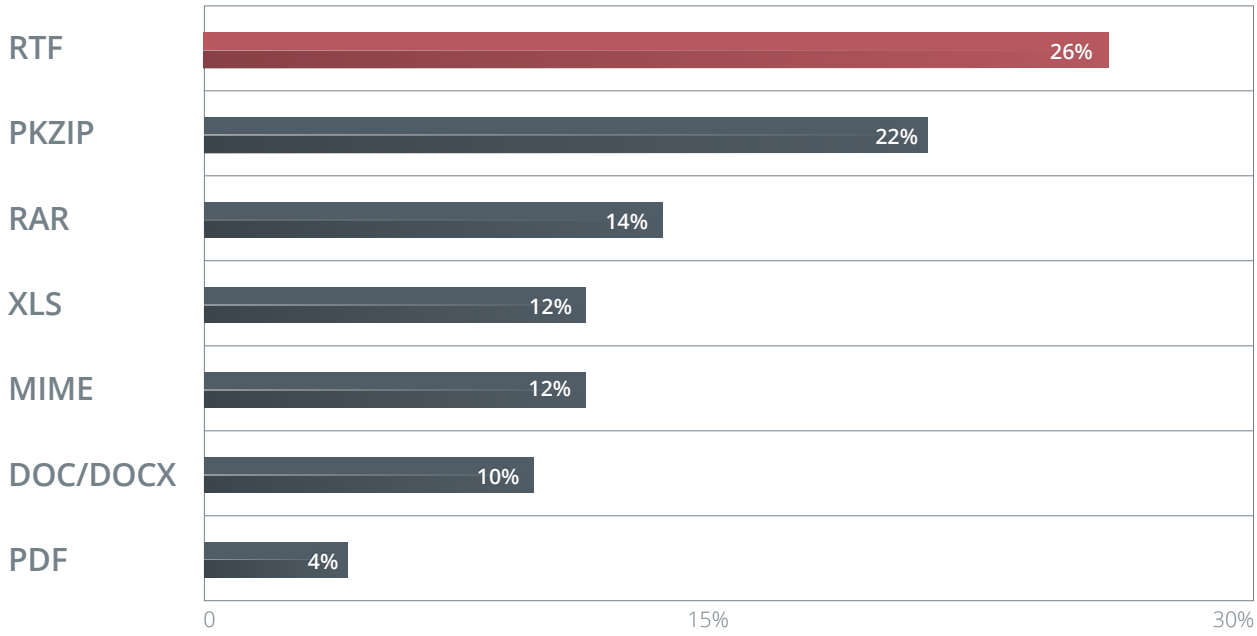
Industry Targets, 2013

Government sites suffered most from targeted attacks in 2013.
Note: *This chart shows our findings on the targeted attacks we monitored throughout 2013.*

Countries Most Affected by Targeted Attacks, 2013

Targeted attackers did not discriminate among countries in 2013. Countries in Asia, particularly Japan and Taiwan, were, however, hit the hardest.
Note: *This chart shows our findings on the targeted attacks we monitored throughout 2013.*

File Types Used as Spear-Phishing Email Attachments for Targeted Attacks, 2013



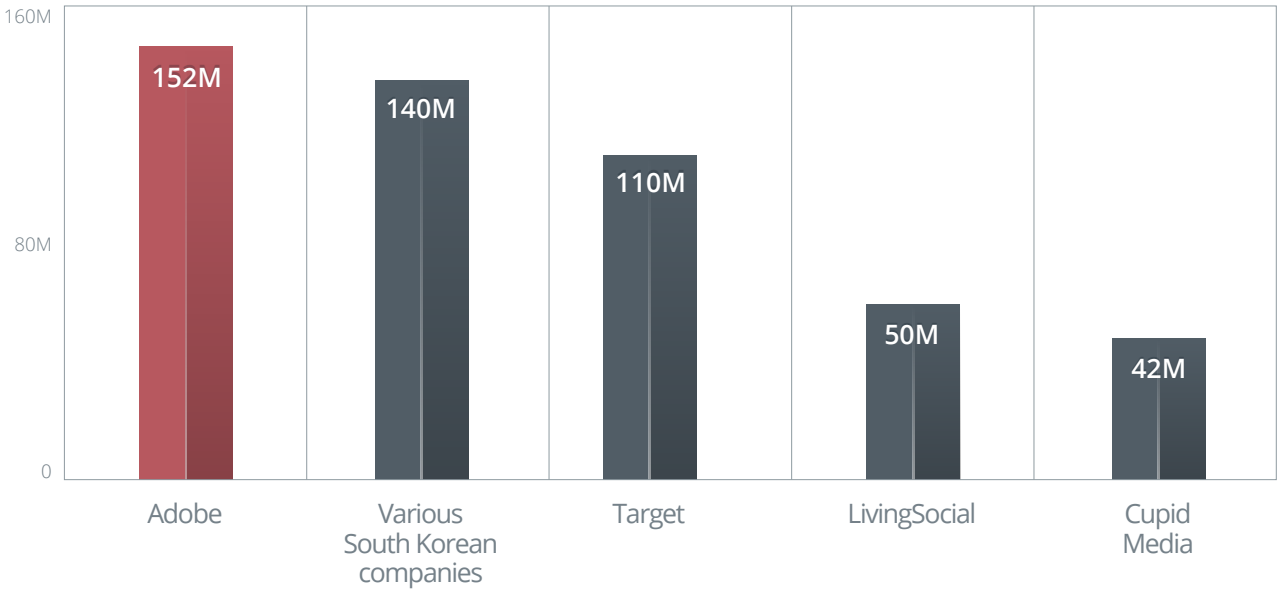
.RTF files were most used in targeted attacks, closely followed by .PKZIP files. This could be attributed to the fact that .RTF files allowed for multiplatform exchange of documentation and that most security software don't scan compressed files like those with the .PKZIP extension name.
Note: *This chart shows our findings on the targeted attacks we monitored throughout 2013.*

Throughout 2013, we saw varied targeted attack campaigns, each with a unique technique. The Safe campaign, for instance, used spear-phishing emails to exploit the Microsoft Office vulnerability, CVE-2012-0158.[32] Attackers used nearly 12,000 unique IP addresses spread across more than 100 countries that were connected to only two sets of command-and-control (C&C) infrastructure. The EvilGrab campaign, meanwhile, showcased attackers' ability to adapt to their targets, as they mostly targeted organizations in the Asia-Pacific region. Their routines were also customized, as when they went after Tencent QQ data.[33] Additional research showed that 89% of EvilGrab's activity targeted government organizations.[34]

Data Breaches Grew in Number

Data breaches were also fairly common in 2013, as several high-profile targets were revealed. Evernote, for instance, suffered a breach last March, which prompted it to reset the passwords of its 50 million users.[35] Around the same number of users were victimized by the LivingSocial breach later in May.[36] In addition, the Identity Theft Resource Center (ITRC) reported that the health care industry suffered a total of 267 data breaches, which accounted for the loss of more than 4 million records.[37]

Data Breach Incidents with the Highest Number of Stolen Records, 2013



Adobe suffered most from data breaches though 2013 showed that no company, regardless of size, is safe from cyber attacks.

Cyber Attacks Affected Real-World Operations

Earlier last March, the MBR Wiper attack strongly hit South Korea and paralyzed several major banking and media companies, which left many of the country's citizens unable to withdraw money from ATMs and news broadcasting crews cut off from their resources.[38] Another destructive attack against South Korea occurred on June 25, which raised the country's cybersecurity alarm from level 1 to 3, as this affected different government and news sites.[39] These examples showed how a digital attack could have destructive real-world implications.

EXPLOITS AND VULNERABILITIES

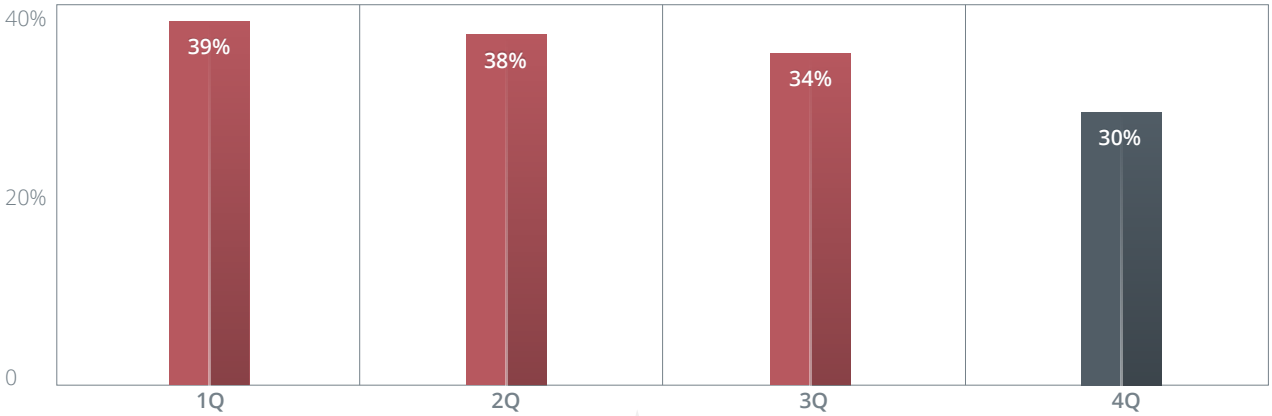
Java exploits highlighted the known problem of using old, unsupported software versions.

The Problem with Being Unpatchable

Attackers didn't need to seek out new vulnerabilities in 2013, as some computers either remained unpatched or ran software versions that were no longer supported. We saw this most when attackers continuously targeted Java 6, which 76% of organizations still ran, even after Oracle withdrew support for the software. It didn't help that Java vulnerabilities accounted for 91% of the total number of Web-based attacks in 2013.[40]

Attackers also exploited other low-hanging fruits apart from Java. Windows XP was among the affected OSs, as evidenced by 45 Microsoft security bulletins released between July 2012 and July 2013.[41] And because Microsoft will no longer support Windows XP security-wise starting this April, around 30% of the world's PCs, which currently run the OS, will become even more vulnerable to attacks.[42] This will also pose a serious problem for banks, as more than 95% of ATMs in the United States still run Windows XP.[43]

Windows XP User Base Decline, 2013



The Windows XP share of the Microsoft OS pie steadily declined throughout 2013, most likely due to the looming end of support for the software this coming April. The end of support means users should become more vigilant against threats, especially exploits for unpatched or unpatchable vulnerabilities. They should, in fact, consider upgrading their OS or at least using security software.
Source: *NetMarketshare.com*

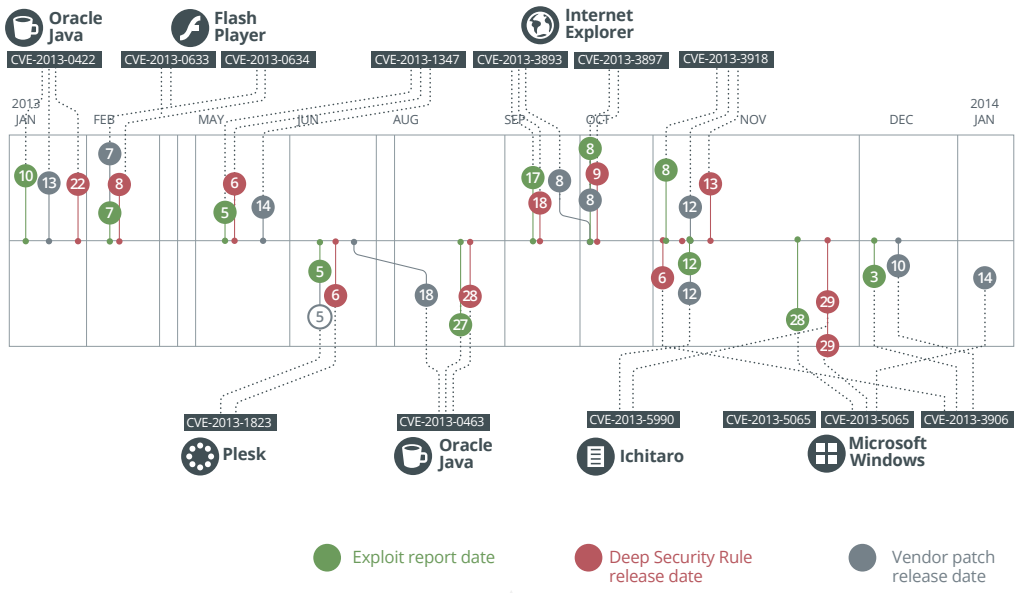
Last February, Adobe® Flash® and Adobe Reader® were also hit by spam attacks bearing malicious .SWF and .PDF file attachments.[44, 45]

Server-side vulnerabilities like that on Ruby on Rails™ seen last May also allowed attackers to turn affected servers into malicious Internet Relay Chat (IRC) bots.[46] The Plesk zero-day exploit spotted last June also allowed attackers to gain control over Web servers. The theft of the source code of Web application development platform, ColdFusion, last October further gave cybercriminals an upper hand with regard to getting past secure IT operations. These incidents brought to light how important maintaining secure Web servers and patching computers were, especially in an enterprise setting.[47]

Windows had its fair share of 2013 exploit attacks. CVE-2013-5065, which was seen last November, for instance, allowed attackers to gain complete control of affected computers via elevated access privileges. The same vulnerability was also exploited via a malicious .PDF file to deliver a backdoor to affected computers as part of targeted attack campaigns.[48] This vulnerability, however, has since been patched.

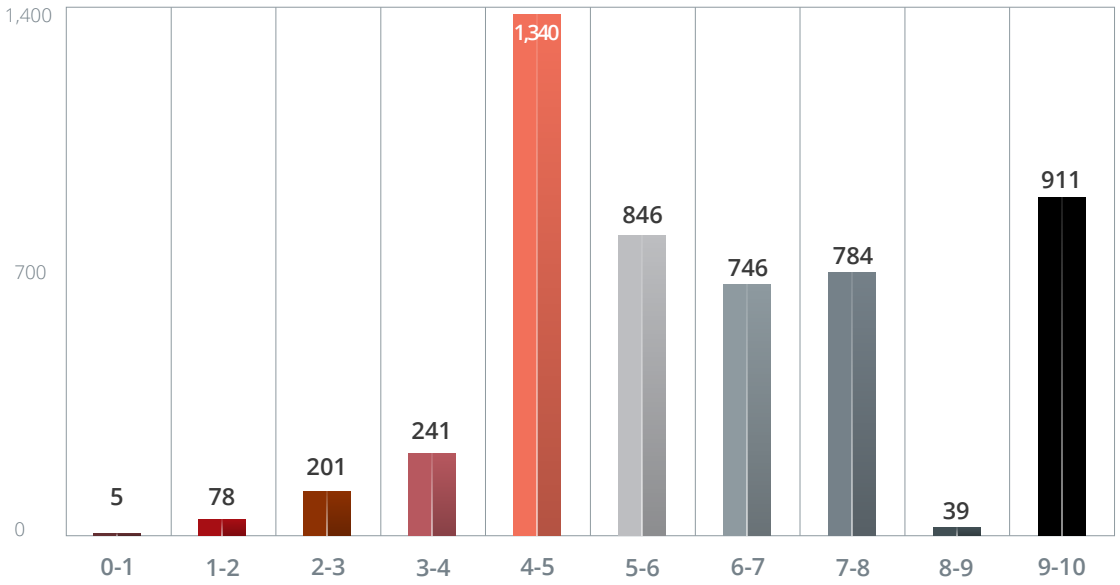
2013 also showed that old but reliable exploits still worked because users either refused or failed to patch or upgrade their software for various reasons. This behavior made it easy for attackers to do their jobs in 2013; users in 2014 will surely suffer the same fate if this practice lives on.

Timeline of Zero-Day Attacks, 2013



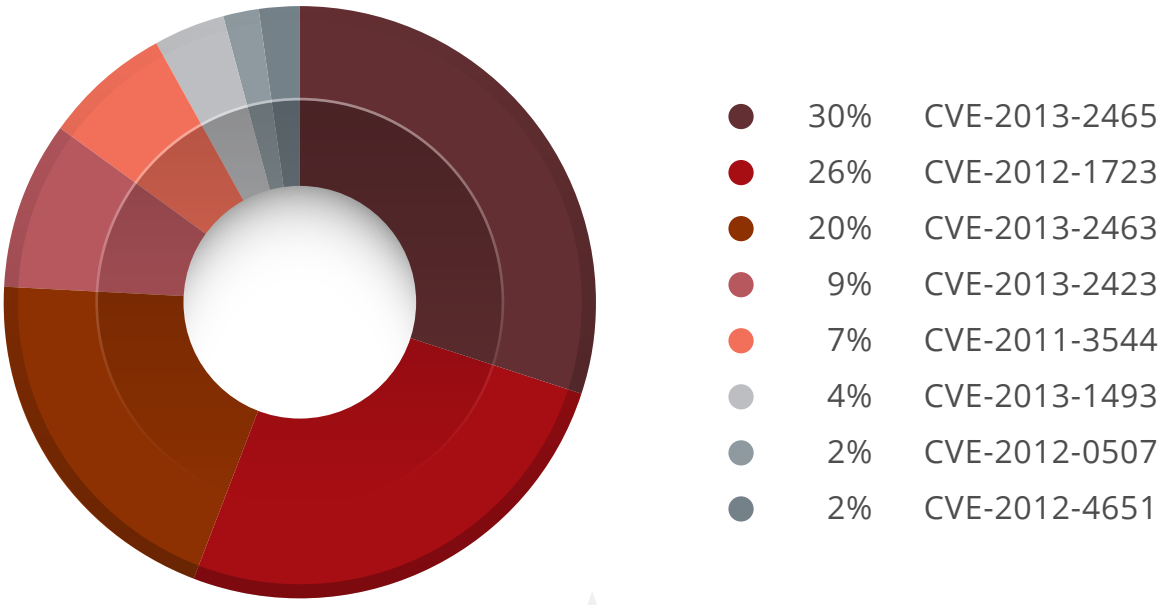
"Retired" software or those that no longer received support from their vendors were ripe exploit targets in 2013, as users of Plesk software older than Parallels Plesk Panel 9.5 and Java 6 learned. We were, however, able to issue Deep Security rules for Microsoft Windows and Internet Explorer exploits even before patches for these were released.

CVE Vulnerability Severity Ratings, 2013



Based on ratings set in CVEdetails.com, 62% of the vulnerabilities disclosed in 2013 were of "medium" (4.0-6.9) severity while almost 30% were of "high" (7.0-10.0) severity. The numbers closely compare with those cited in 2012. This means that users should remain vigilant when it comes to updating their software, upgrading to the latest versions, and, in cases of unpatched vulnerabilities, using security software.
Source: CVEdetails.com

Most Exploited Java Browser-Based Vulnerabilities



This chart shows the most exploited Java 6 and 7 browser-based vulnerabilities in 2013 according to our Browser Exploit Prevention System data. The data show that cybercriminals exploited almost an equal number of new and year-old vulnerabilities.
***Note:** The numbers were based only on a month's worth of exploit attempts or attacks against certain Java vulnerabilities we monitored in 2013.*

DIGITAL LIFE SECURITY ISSUES

Although digital life and privacy threats, especially concerning social media, "personal cloud," and online account use, remained constant, the discovery and eventual ebb of state-sponsored monitoring into mainstream awareness may pose further risks to user data.

Social Engineering + Social Media = Business as Usual

"Old" and income-generating cybercriminal tricks remained a major concern among users when it came to keeping personal information safe. But the emergence of news surrounding the amount of data the National Security Agency (NSA) gathered added another layer of concern for those unaware of how their information was gathered and used.[49] Despite recent events, however, 2013 was "business as usual" for cybercriminals who used social media as "standard" means to deliver threats.

As in years past, social engineering remained the most effective cybercriminal tool to get victims to either click a malicious link or download malware, and inadvertently disclose sensitive data. In 2013, the launch of much-awaited gadgets like the PlayStation 4® and Xbox® One, widely celebrated occasions like Halloween, and natural disasters like Typhoon Haiyan proved top social engineering lures.

Top Social Engineering Lures, 2013

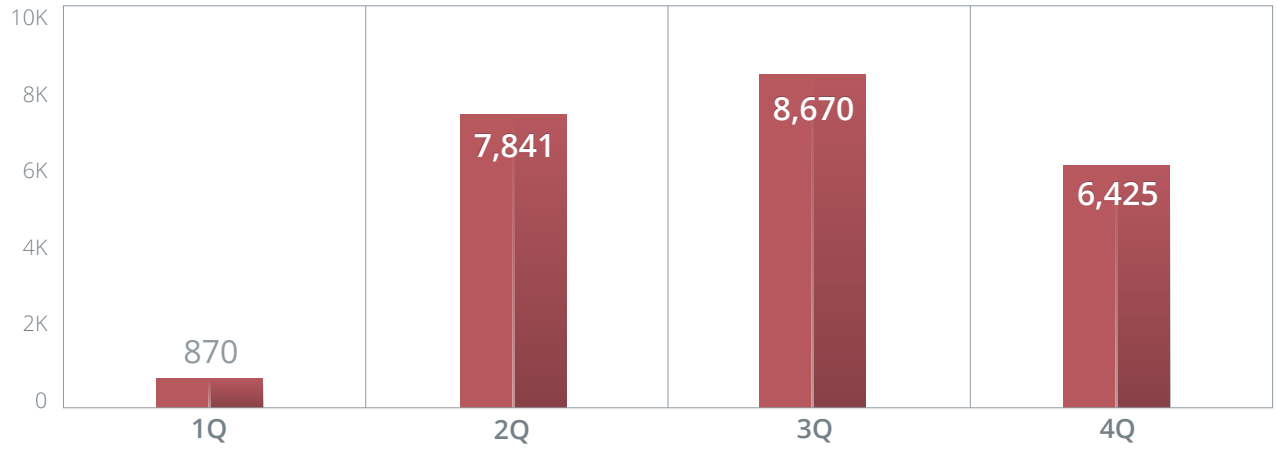
As usual, cybercriminals used the most-talked-about issues, events, movies, gadgets, and natural disasters to lure as many victims as possible to their specially crafted traps.

Various social media platforms continued to be littered with threats. We saw an endless slew of Facebook scams; even its messaging app was not spared.[50, 51, 52, 53] We also found malicious Twitter accounts that offered a variety of hacking tools last October, after the site went through a major account hack earlier in April.[54, 55]

Pinterest did not suffer major attacks apart from one case wherein a Blackhole Exploit Kit spam run used its name. Fraudsters began spreading fake online video streaming sites on Tumblr last year.[56, 57] The 2013 social media threat spotlight shone most brightly on Instagram though, as the number of fake accounts and "free-follower" scams on the site continuously rose throughout the year.[58, 59]

Amid the social media buzz, phishing still proved a lucrative means to earn a living for the bad guys, as those who lost their Apple IDs could attest to.[60]

Apple-Related Phishing Page Volume Growth, 2013



We noted an increase in the number of phishing sites targeting Apple IDs in 2013. Some attacks asked not only for victims' Apple IDs but also for their billing addresses and other personal and financial information.

Users should realize that revealing too much information on sites can make their personal information ripe for cybercriminal picking. Data remained valuable commodities in the cybercriminal underground; the bad guys even had their own business model.[61] "Fullz" or a collection of crucial information beyond names, addresses, and credit card numbers typically stolen from unsuspecting users continued to be sold in underground forums.

Threats to our digital lives, the recent revelations about government spying on private citizens, and the ongoing public distrust beg the question, "Is privacy in today's digital age really dead?"

Appendix

Quarterly Online Banking Malware Detections by Country, 2013

1Q	
COUNTRY	SHARE
USA	33%
Brazil	10%
Australia	5%
Taiwan	5%
Canada	4%
Japan	3%
India	3%
France	3%
Philippines	3%
Germany	2%
OTHERS	29%

2Q	
COUNTRY	SHARE
USA	28%
Brazil	22%
Australia	5%
France	5%
Japan	4%
Taiwan	4%
Vietnam	3%
India	2%
Germany	2%
Canada	2%
OTHERS	23%

3Q	
COUNTRY	SHARE
USA	23%
Brazil	16%
Japan	12%
India	6%
Australia	3%
France	3%
Germany	2%
Vietnam	2%
Taiwan	2%
Mexico	2%
OTHERS	29%

4Q	
COUNTRY	SHARE
USA	22%
Japan	19%
Brazil	12%
Taiwan	6%
France	5%
Germany	3%
India	3%
Canada	2%
Australia	2%
Italy	2%
OTHERS	24%

The number of ZBOT infections in Japan rose in the last two quarters of 2013, which suggested a rise in cybercriminal activity either in Japan or targeting Japanese users who weren't considered a big online banking malware target in previous years.

Countries with the Highest Number of Botnet C&C Servers, 2013

1Q	
COUNTRY	**SHARE**
USA	36%
Australia	11%
South Korea	6%
China	6%
Germany	3%
United Kingdom	3%
Brazil	2%
Italy	2%
Taiwan	2%
Chile	2%
OTHERS	27%

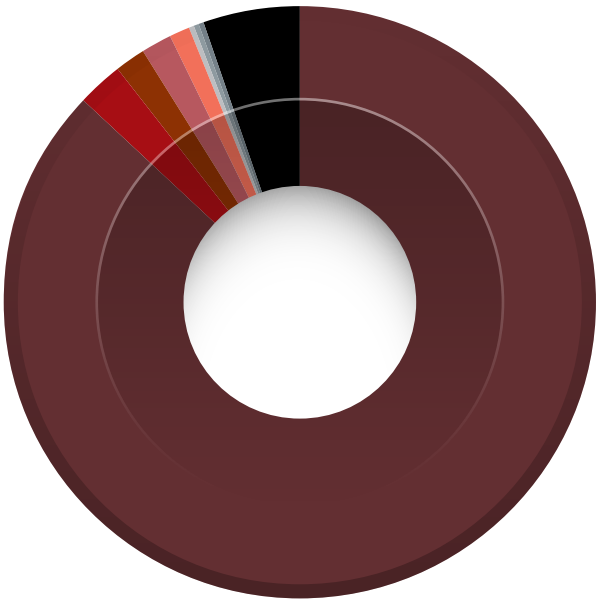
2Q	
COUNTRY	**SHARE**
USA	24%
Australia	5%
South Korea	3%
China	3%
Germany	3%
Taiwan	2%
France	2%
United Kingdom	2%
Brazil	1%
Canada	1%
OTHERS	54%

3Q	
COUNTRY	**SHARE**
USA	14%
Ukraine	7%
Russia	3%
Germany	3%
China	2%
Taiwan	2%
Australia	2%
South Korea	2%
United Kingdom	2%
Netherlands	1%
OTHERS	62%

4Q	
COUNTRY	**SHARE**
United Kingdom	17%
USA	15%
Ukraine	4%
Germany	3%
Netherlands	3%
Russia	3%
China	2%
Australia	1%
South Korea	1%
India	1%
OTHERS	50%

While the United States topped the banking victims' list in most of 2013, our data show that online banking malware infections are spreading worldwide. As in the third quarter of 2013, infections have been moving away the usual targets, the Americas, to Europe.

Top Spam Languages, 2013



87.14%	English
2.36%	Chinese
1.84%	Japanese
1.48%	German
1.20%	Russian
0.28%	Portuguese
0.21%	Spanish
0.12%	Icelandic
0.10%	Italian
0.10%	French
5.17%	Others

English remained spammers' most preferred language because it is most used worldwide.

Top Spam-Sending Countries, 2013

10%	USA
6%	Spain
6%	India
5%	Argentina
5%	Italy
4%	Taiwan
4%	Colombia
4%	China
4%	Peru
3%	Mexico
49%	Others

Consistent with the top spamming language, the United States sent out the most spam. Latin American countries like Argentina, Spain, Colombia, Mexico, and Peru remained part of the top 10.

Top Malicious Domains Blocked, 2013

DOMAIN BLOCKED	REASON FOR BLOCKING
trafficconverter.biz	Has a record for hosting and distributing worms
ads.alpha00001.com	Is a malicious browser hijacker that affects Mozilla Firefox, Chrome, Internet Explorer, and other PC browsers; redirects victims to fake sites by modifying default browser, Domain Name System (DNS), and HOSTS file settings
ody.cc	Has links to suspicious scripts and sites that host BKDR_HPGN.B-CN
adsgangsta.com	Has ties to malware attacks
pu.plugrush.com	Has ties to the Blackhole Exploit Kit spam campaigns
promos.fling.com	Downloads malware
ws-cloud.snap.do	Is known for involvement in malicious activities
embed.redtube.com	Is known for involvement in malicious activities
trafficholder.com	Has ties to child exploitation sites
indirs-locmocz.ws	Is known for involvement in malicious activities

Most of the domains we blocked user access to had ties to malicious activities, which included serving malware.

Malicious URL Country Sources, 2013

COUNTRY	SHARE
USA	24%
Netherlands	4%
Germany	3%
China	3%
Japan	3%
South Korea	2%
France	2%
Russia	2%
United Kingdom	1%
Canada	1%
OTHERS	55%

A significant share of the malicious URLs we blocked access to were hosted in the United States.

Countries That Accessed Malicious URLs Most, 2013

COUNTRY	SHARE
USA	29%
Japan	15%
China	7%
India	5%
Taiwan	5%
South Korea	4%
Russia	3%
Australia	3%
Germany	3%
Italy	2%
OTHERS	24%

Most of the users that accessed malicious URLs were from the United States.

Countries with the Highest Malicious Android App Volumes, 2013

Belarus	10%
Bulgaria	5%
Vietnam	5%
Argentina	5%
Russia	4%
Ukraine	4%
Canada	2%
India	2%
France	2%
Italy	2%

Belarus topped the list of countries with the highest malicious Android app volume. This could be due in part to the smartphone penetration growth in the country.[62]
Note: *The ranking was based on the percentage of apps categorized as "malicious" over the total number of apps scanned per country. The ranking was, however, limited to countries with at least 10,000 scans.*

Countries Most at Risk of Privacy Exposure Due to App Use, 2013

Uganda	17%
Saudi Arabia	17%
Bulgaria	11%
India	9%
Argentina	8%
Ukraine	8%
Canada	6%
Indonesia	6%
Italy	6%
Singapore	6%

Uganda topped the list of countries most at risk of privacy exposure. It consistently made the list in most of 2013.
Note: *The ranking was based on the percentage of apps categorized as "privacy risk inducers" over the total number of apps scanned per country. The ranking was, however, limited to countries with at least 10,000 scans.*

References

1. Trend Micro Incorporated. (2012). "Security Threats to Business, the Digital Lifestyle, and the Cloud: Trend Micro Predictions for 2013 and Beyond." Last accessed January 18, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/spotlight-articles/sp-trend-micro-predictions-for-2013-and-beyond.pdf.
2. Trend Micro Incorporated. (September 2013). *Threat Encyclopedia.* "Malicious and High-Risk Android Apps Hit 1 Million: Where Do We Go from Here?" Last accessed January 18, 2014, http://about-threats.trendmicro.com/us/mobile/monthly-mobile-review/2013-10-malicious-and-high-risk-android-apps-hit-1-million.
3. Trend Micro Incorporated. (2013). "TrendLabs 3Q 2013 Security Roundup: The Invisible Web Unmasked." Last accessed January 18, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-trendlabs-3q-2013-security-roundup.pdf.
4. Jeffrey Bernardino. (December 17, 2013). *TrendLabs Security Intelligence Blog.* "Control Panel Files Used as Malicious Attachments." Last accessed January 23, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/control-panel-files-used-as-malicious-attachments/.
5. Brian Krebs. (August 7, 2013). *Krebs on Security.* "$1.5 Million Cyberheist Ruins Escrow Firm." Last accessed January 29, 2014, http://krebsonsecurity.com/2013/08/1-5-million-cyberheist-ruins-escrow-firm/.
6. Brian Krebs. (May 23, 2013). *Krebs on Security.* "NC Fuel Distributor Hit by $800,000 Cyberheist." Last accessed January 29, 2014, http://krebsonsecurity.com/2013/05/nc-fuel-distributor-hit-by-800000-cyberheist/.
7. Brian Krebs. (April 30, 2013). *Krebs on Security.* "Wash. Hospital Hit by $1.03 Million Cyberheist." Last accessed January 29, 2014, http://krebsonsecurity.com/2013/04/wash-hospital-hit-by-1-03-million-cyberheist/.
8. John E. Dunn. (October 23, 2013). *Computerworld.* "UK SME Left £70,000 in the Red After Lightning-Fast Phishing Attack." Last accessed January 29, 2014, http://news.idg.no/cw/art.cfm?id=F0176E45-E7DE-BA82-31C5C4AE4C5B7FB7.
9. Joselito Dela Cruz. (October 11, 2013). *TrendLabs Security Intelligence Blog.* "Threat Refinement Ensues with CryptoLocker, SHOTODOR Backdoor." Last accessed January 18, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/threat-refinement-ensues-with-crypto-locker-shotodor-backdoor/.
10. Kervin Alintahanin. (October 21, 2013). *TrendLabs Security Intelligence Blog.* "CryptoLocker: Its Spam and ZeuS/ZBOT Connection." Last accessed January 23, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/cryptolocker-its-spam-and-zeuszbot-connection/.
11. Vincenzo Ciancaglini. (November 8, 2013). *TrendLabs Security Intelligence Blog.* "The Boys Are Back in Town: Deep Web Marketplaces Back Online." Last accessed January 18, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/the-boys-are-back-in-town-deep-web-marketplaces-back-online/.
12. Robert McArdle. (October 4, 2013). *TrendLabs Security Intelligence Blog.* "Cybercrime in the Deep Web." Last accessed January 18, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/cybercrime-in-the-deepweb/.
13. Jonathan Leopando. (October 21, 2013). *TrendLabs Security Intelligence Blog.* "Blackhole Arrests—How Has the Underground Reacted?" Last accessed January 18, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/blackhole-arrests-how-has-the-underground-reacted/.
14. Merianne Polintan. (January 7, 2014). *TrendLabs Security Intelligence Blog.* "A Year of Spam: The Notable Trends of 2013." Last accessed January 31, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/a-year-of-spam-the-notable-trends-of-2013/.
15. Gartner, Inc. (January 7, 2014). *Newsroom.* "Gartner Says Worldwide Traditional PC, Tablet, Ultramobile, and Mobile Phone Shipments on Pace to Grow 7.6 Percent in 2014." Last accessed January 23, 2014, http://www.gartner.com/newsroom/id/2645115.
16. Trend Micro Incorporated. (2013). *Threat Encyclopedia.* "Blurring Boundaries: Trend Micro Security Predictions for 2014 and Beyond." Last accessed January 31, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-trend-micro-security-predictions-for-2014-and-beyond.pdf.
17. Symphony Luo. (December 20, 2013). *TrendLabs Security Intelligence Blog.* "1,730 Malicious Apps Still Available on Popular Android App Providers." Last accessed January 23, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/1730-malicious-apps-still-available-on-popular-android-app-providers/.
18. Weichao Sun. (May 14, 2013). *TrendLabs Security Intelligence Blog.* "Mobile Ads Pushed by Android Ads Lead to Scam Sites." Last accessed January 29, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/mobile-ads-pushed-by-android-apps-lead-to-scam-sites/.
19. Peter Yan. (September 13, 2013). *TrendLabs Security Intelligence Blog.* "Spam Leads to Multiplatform Mobile Threat." Last accessed January 19, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/spam-leads-to-multi-platform-mobile-threat/.

20. Andy Greenberg. (November 7, 2011). *Forbes*. "iPhone Security Bug Lets Innocent-Looking Apps Go Bad." Last accessed January 24, 2014, http://www.forbes.com/sites/andygreenberg/2011/11/07/iphone-security-bug-lets-innocent-looking-apps-go-bad/.

21. Trend Micro Incorporated. (February 2013). *Threat Encyclopedia*. "Mobile Phishing: A Problem on the Horizon." Last accessed January 28, 2014, http://about-threats.trendmicro.com/us/mobilehub/mobilereview/rpt-monthly-mobile-review-201302-mobile-phishing-a-problem-on-the-horizon.pdf.

22. Jakob Nielsen. (April 10, 2012). *NN/g Nielsen Norman Group*. "Mobile Site Vs. Full Site." Last accessed January 31, 2014, http://www.nngroup.com/articles/mobile-site-vs-full-site/.

23. Stuart Dredge. (August 19, 2013). *The Guardian*. "iOS Malware Can Sneak Through Apple's Approval Process, Researchers Show." Last accessed January 19, 2014, http://www.theguardian.com/technology/appsblog/2013/aug/19/ios-malware-apple-iphone-ipad-jekyll.

24. Trend Micro Incorporated. (2013). *Threat Encyclopedia*. "A Look at Mobile Banking Threats." Last accessed January 19, 2014, http://about-threats.trendmicro.com/us/mobile/monthly-mobile-review/2013-08-mobile-banking-threats.

25. Trend Micro Incorporated. (2013). *Threat Encyclopedia*. "ANDROIDOS_FAKEBANK.A." Last accessed January 19, 2014, http://about-threats.trendmicro.com/us/malware/ANDROIDOS_FAKEBANK.A.

26. Trend Micro Incorporated. (2013). *Threat Encyclopedia*. "Emerging Vulnerabilities: Glitches Go Mobile." Last accessed January 19, 2014, http://about-threats.trendmicro.com/RelatedThreats.aspx?language=au&name=Emerging+Vulnerabilities%3A+Glitches+Go+Mobile.

27. Jonathan Leopando. (July 10, 2013). *TrendLabs Security Intelligence Blog*. "Android Vulnerability Affects 99% of Devices—Trend Micro Users Protected." Last accessed January 19, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-solution-for-vulnerability-affecting-nearly-all-android-devices/.

28. Leo Zhang. (July 13, 2013). *TrendLabs Security Intelligence Blog*. "Cybercriminals Improve Android Malware Stealth Routines with OBAD." Last accessed January 19, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/cybercriminals-improve-android-malware-stealth-routines-with-obad/.

29. The MITRE Corporation. (2013). *CVE*. "CVE-2012-0158." Last accessed January 19, 2014, http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0158.

30. Gelo Abendan. (May 14, 2013). *TrendLabs Security Intelligence Blog*. "May 2013 Patch Tuesday Includes Critical IE 8 Zero-Day Issue." Last accessed January 23, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/may-2013-patch-tuesday-includes-critical-ie-8-zero-day-issue/.

31. Trend Micro Incorporated. (2013). *Threat Encyclopedia*. "BKDR_POISON." Last accessed January 30, 2014, http://about-threats.trendmicro.com/Search.aspx?language=au&p=BKDR_POISON.

32. Kyle Wilhoit. (May 17, 2013). *TrendLabs Security Intelligence Blog*. "Hiding in Plain Sight: A New Targeted Attack Campaign." Last accessed January 19, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/hiding-in-plain-sight-a-new-apt-campaign/.

33. Jayronn Christian Bucu. (September 18, 2013). *TrendLabs Security Intelligence Blog*. "EvilGrab Malware Family Used in Targeted Attacks in Asia." Last accessed January 19, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/evilgrab-malware-family-used-in-targeted-attacks-in-asia/.

34. Trend Micro Incorporated. (2013). *Threat Encyclopedia*. "2Q Report on Targeted Attack Campaigns." Last accessed January 19, 2014, http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/2q-report-on-targeted-attack-campaigns.pdf.

35. Reuters. (March 3, 2013). *NBC News*. "Evernote Resets 50 Million Passwords After Hackers Access User Data." Last accessed January 19, 2014, http://www.nbcnews.com/technology/evernote-resets-50-million-passwords-after-hackers-access-user-data-1C8659106.

36. Katie W. Johnson. (March 3, 2013). Bloomberg BNA. "LivingSocial Reveals Cyber Attack, Notifies 50 Million, Says No Credit Data Breached." Last accessed January 19, 2014, http://www.bna.com/livingsocial-reveals-cyberattack-n17179873787/.

37. The Identity Theft Resource Center. (2013). "Identity Theft Resource Center; 2013 Data Breach Category Summary." Last accessed January 19, 2014, http://www.idtheftcenter.org/images/breach/2013/BreachStatsReportSummary2013.pdf.

38. Marco Dela Vega. (June 25, 2013). *TrendLabs Security Intelligence Blog*. "Compromised Auto-Update Mechanism Affects South Korean Users." Last accessed January 19, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/compromised-auto-update-mechanism-affects-south-korean-users/.

39. Christopher Budd. (April 2, 2013). *TrendLabs Security Intelligence Blog*. "Three Lessons from the South Korea MBR Wiper Attacks." http://blog.trendmicro.com/trendlabs-security-intelligence/three-lessons-from-the-south-korea-mbr-wiper-attacks/.

40. Cisco Inc. (2014) "Cisco 2014 Annual Security Report." Last accessed January 19, 2014, https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

41. Mark Hachman. (August 16, 2013). *PCWorld*. "Zero Day Forever—Move Away from Windows XP, Now." Last accessed January 24, 2014, http://www.pcworld.com/article/2046839/zero-day-forever-move-away-from-windows-xp-now.html.

42. David Murphy. (January 11, 2014). *PCMag*. "When Windows XP Dies, so Does Its 'Microsoft Security Essentials.'" Last accessed January 19, 2014, http://www.pcmag.com/article2/0,2817,2429423,00.asp.

43. Fox News Network LLC. (January 17, 2014). *FoxNews.com*. "World's ATMs Still Running Windows XP--and Wildly Out of Date." Last accessed January 19, 2014, http://www.foxnews.com/tech/2014/01/17/atms-running-windows-xp-and-wildly-out-date/.

44. Pavithra Hanchagaiah. (February 8, 2013). *TrendLabs Security Intelligence Blog*. "Zero-Day Vulnerabilities Found in Adobe Flash Player." Last accessed January 19, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/zero-day-vulnerability-hits-adobe-reader/.

45. Trend Micro Incorporated. (February 13, 2013). *TrendLabs Security Intelligence Blog*. "Zero-Day Vulnerability Hits Adobe Reader." Last accessed January 19, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/zero-day-vulnerabilities-found-in-adobe-flash-player/.

46. Gelo Abendan. (May 30, 2013). *TrendLabs Security Intelligence Blog*. "Trend Micro Deep Security Guards Users from Ruby on Rails Exploit." Last accessed January 19, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-deep-security-guards-users-from-ruby-on-rails-exploit/.

47. Sooraj K.S. (June 6, 2013). *TrendLabs Security Intelligence Blog*. "Plesk Zero-Day Exploit Results in Compromised Web Server." Last accessed January 19, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/plesk-zero-day-exploit-results-in-compromised-webserver/.

48. Jayronn Christian Bucu. (December 2, 2013). *TrendLabs Security Intelligence Blog*. "Windows XP/Server 2003 Zero-Day Payload Uses Multiple Anti-Analysis Techniques." Last accessed January 19, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/windows-xpserver-2003-zero-day-payload-uses-multiple-anti-analysis-techniques/.

49. Zack Whittaker. (January 17, 2014). *ZDNet*. "Obama Unveils NSA Reforms: 'Keep Calm and Carry on Spying.'" Last accessed January 24, 2014, http://www.zdnet.com/obama-unveils-nsa-reforms-keep-calm-and-carry-on-spying-7000025303/.

50. Paul Pajares and Gelo Abendan. (October 1, 2013). *TrendLabs Security Intelligence Blog*. "Fake Facebook Mobile Page Steals Credit Card Details." Last accessed January 19, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/fake-facebook-mobile-page-steals-credit-card-details.

51. Karla Agregado. (April 10, 2013). *TrendLabs Security Intelligence Blog*. "New Approach to the Old 'Facebook Profile Viewer' Ruse." Last accessed January 19, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/new-approach-to-the-old-facebook-profile-viewer-ruse/.

52. Anthony Joe Melgarejo. (March 31, 2013). *TrendLabs Security Intelligence Blog*. "Malware Phishes with Fake Facebook Security Check Page." Last accessed January 19, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/malware-phishes-with-fake-facebook-security-check-page.

53. Anthony Joe Melgarejo. (May 2, 2013). *TrendLabs Security Intelligence Blog*. "Backdoor Leads to Facebook and Multiprotocol Instant-Messaging Worm." Last accessed January 19, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/backdoor-leads-to-facebook-and-multi-protocol-instant-messaging-worm/.

54. Jonathan Leopando. (October 10, 2013). *TrendLabs Security Intelligence Blog*. "Twitter Still Being Used by Shady Hackers." Last accessed January 19, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/twitter-still-being-used-by-shady-hackers/.

55. Christopher Budd. (April 23, 2013). *TrendLabs Security Intelligence Blog*. "Another Social Media Day, Another Twitter Hack." Last accessed January 19, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/another-day-another-twitter-hack/.

56. Paul Pajares. (July 8, 2013). *TrendLabs Security Intelligence Blog*. "Man of Steel, Fast and Furious 6 Among Online Fraudsters' Most Used Lures." Last accessed January 19, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/man-of-steel-fast-and-furious-6-among-online-fraudsters-most-used-lures/.

57. Gelo Abendan. (May 2, 2013). *TrendLabs Security Intelligence Blog*. "Fake Iron-Man 3 Streaming Sites Sprout on Social Media." Last accessed January 19, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/fake-iron-man-3-streaming-sites-sprout-on-social-media/.

58. Karla Agregado. (June 25, 2013). *TrendLabs Security Intelligence Blog*. "Scam Sites Now Selling Instagram Followers." Last accessed January 19, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/scam-sites-now-selling-instagram-followers/.

59. Karla Agregado. (May 16, 2013). *TrendLabs Security Intelligence Blog*. "Get Free Followers! on Instagram? Get Free Malware, Survey Scams Instead." Last accessed January 19, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/get-free-followers-on-instagram-get-free-malware-survey-scams-instead/.

60. Paul Pajares. (October 1, 2013). *TrendLabs Security Intelligence Blog*. "Apple Spikes as Phishing Target." Last accessed January 19, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/apple-spikes-as-phishing-target/.

61. Kyle Wilhoit. (January 16, 2013). *TrendLabs Security Intelligence Blog*. "What Would Scammers Want with My Information?" Last accessed January 19, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/what-would-scammers-want-with-my-information/.

62. Telecom.paper BV. (January 21, 2014). *Telecompaper*. "MTS Belarus Smartphone Penetration Jumps to 25%." Last accessed January 29, 2014, http://www.telecompaper.com/news/mts-belarus-smartphone-penetration-jumps-to-25--991402.

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.

Trend Micro Incorporated, a global leader in security software and solutions, strives to make the world safe for exchanging digital information. For more information, visit www.trendmicro.com.

TREND MICRO™

Securing Your Journey to the Cloud