TrendLabs℠ 1Q 2014 Security Roundup

TREND MICRO™

Cybercrime Hits the Unexpected

Bitcoin- and PoS-System-Related Attacks Trouble Users

Distributed by:

ITU

It gives me immense pleasure to share this report, developed by Trend Micro and distributed by ITU based on our fruitful partnership. This report is part of ITU's overall support to its 193 Member States within the framework of the Global Cybersecurity Agenda. This is clear result of our partnership with Private Sector in our effort to tackle this growing Global phenomenon.

These efforts are aimed at equipping Member States with information on the latest cybersecurity threats and corresponding counter-measures, and eventually contribute to the creation of a safe and secure cyberspace for consumers, businesses and youth everywhere.

This Trend Micro quarterly report underlines the existing and emerging malicious cyber activities observed during the first quarter of 2014. Some highlights of this report:

- Cybercriminals are continuing to innovate and create new ways to commit digital crimes. Crypto-currency exchanges and wallets are being compromised for the purpose of theft. In addition, online banking malware are being enhanced with new technologies to exact the maximum damage.
- With the exponential growth in the mobile industry, cyber-criminals are increasingly targeting mobile devices. There is a proliferation of maliciously tampered and re-packaged apps that circumvent the security firewalls in mobile devices.
- We are also witnessing cases of attacks directly aimed at organizations that rely on specific Point of Sales (Pos) systems features. It is clear that reliance on antivirus software alone is no longer adequate to combat cyber-threats. A customized strategy that improves detection, analysis and response is needed to minimize risk and impact from targeted attacks.
- Several attacks on Internet of Everything (IoE) devices have been noted. The underlying causes are inadequate or flawed design and security practices rather than code-level vulnerabilities. Manufacturers need to integrate security practices into the development lifecycle instead of adding them on as an afterthought.

I believe the information presented in this report gives a clear perspective on the current cybersecurity landscape. I am confident that it will be a valuable source of information for Member States and will assist them in our common effort to foster awareness and strengthen global cybersecurity.

Dr. Hamadoun I. Touré
ITU Secretary-General

TREND MICRO | TrendLabs 1Q 2014 Security Roundup

Contents

Introduction

At the end of 2013, we realized that digital heists pushed stick-'em-up bank heists to the curb.[1] While this holds true amid large data breach incidents and rampant cybercrime, the first quarter of 2014 also showed that today's cybercriminals are aiming at previously nontargeted entities to carry out malicious deeds. Proof of these include the US$480-million digital heist Bitcoin exchange, MtGox, suffered from and recent attacks against large retailers via point-of-sale (PoS) terminals.[2, 3] These high-profile crimes targeted unexpected information sources even if attackers went after the same thing—money, used the same techniques despite more strategic planning, and were motivated by greed.

In this era of electronic transactions, nothing screams "crime" like a massive data breach, whether carried out by individual attackers or sophisticated cybercriminal gangs. Instead of going only after individuals, cybercriminals went after unusual targets like PoS terminals in retail chains.[4]

This quarter's biggest stories featured well-orchestrated schemes and large sums of money lost to enterprising cybercriminals. Online banking malware, for instance, exhibited new behaviors though the core tactics cybercriminals used to spread them stayed the same. Bitcoins and related attacks gained prominence as a financial instrument and a threat. The mobile threat landscape did not undergo drastic changes this quarter though it has been dubbed "more mature" with the emergence of more Android™ bugs. The retailer data breaches we saw in recent months highlighted the need for customized defense strategies.

Cybercriminal tactics this quarter taught us that no matter how advanced a defense strategy is, malicious actors will always go in for the kill to gain immediate profit, no matter how unusual the target appears.

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.*

TREND MICRO | TrendLabs 1Q 2014 Security Roundup

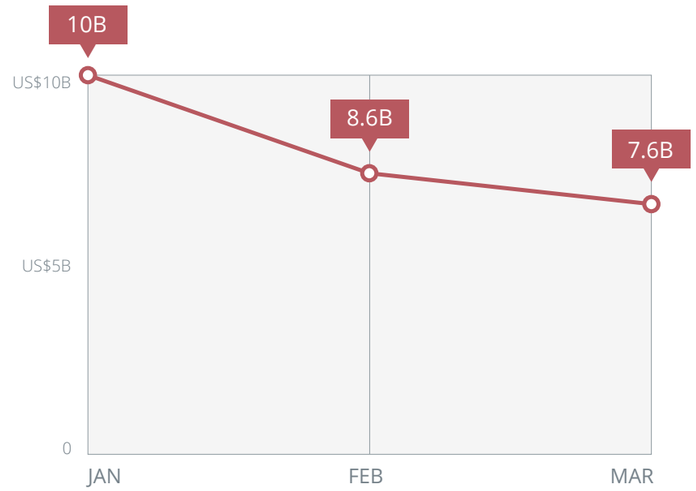
CYBERCRIME AND THE CYBERCRIMINAL UNDERGROUND

Bitcoin Matured as a Currency and Attracted More Cybercriminals

The nature of the Bitcoin technology and network has drastically changed over time. As such, related threats have also evolved. In the past, attackers compromised systems and used them to mine for the valuable digital currency; today, Bitcoin exchanges and wallets are targeted for theft. This March, for instance, BitCrypt, an addition to the ransomware scene, stole various cryptocurrency wallets, including Bitcoin wallets.[5]

We also saw several Bitcoin exchanges worldwide suffer after being robbed, including MtGox, Flexcoin, new Silk Road, and Poloniex, among others.[6, 7, 8, 9] This does not mean Bitcoin mining is no longer profitable though. If done right, Bitcoin mining—a process that manages Bitcoin transactions and creates new ones—can be a lucrative investment, as a Bitcoin's average weekly price can still reach as much as US$945 on the largest exchange.[10]

Value of Bitcoins in Circulation



Source: https://blockchain.info

With roughly 12 million Bitcoins in existence at the start of this year, the total value of Bitcoins rose to as high as US$10 billion. However, due to the MtGox heist this February, its value has been fluctuating between US$6 billion and US$8 billion this quarter, with the lowest value this March. Despite the drop in value and fluctuating exchange rates, however, Bitcoin users who purchased the cryptocurrency in the first quarter of 2013 still gained more than a tenfold increase on their investment today.

Bitcoin-Mining and -Wallet-Stealing Malware

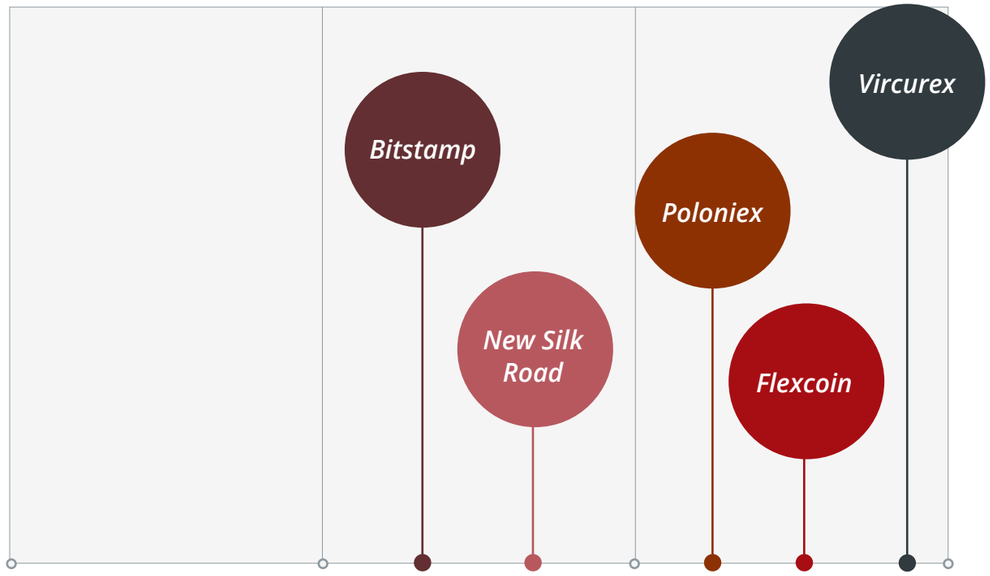
DETECTION NAME	ROUTINE	DATE FIRST SEEN
BKDR_BTMINE	Mines Bitcoins by downloading miners	September 2011
KELIHOS	Looks for and steals *wallet.dat* files	April 2013
SHIZ	Monitors Bitcoin-related processes for stealing purposes	November 2013
COINMINE (DevilRobber)	Copies all of the contents of *wallet.dat* and sends them to File Transfer Protocol (FTP) servers	December 2013
FAREIT/TEPFER (Pony)	Looks for and steals *wallet.dat, .wallet,* and *electrum.dat* files **NOTE:** FAREIT is a known downloader of CRIBIT/BitCrypt, which steals Bitcoin and other cryptocurrency wallets.	March 2014
KAGECOIN	Mines for Bitcoins on Android devices	March 2014

This quarter, we saw many Bitcoin-wallet-stealing malware, apart from miners.

After a few years of functioning as a currency, Bitcoin also proved to be an efficient means to get into illicit transactions. In the latter part of 2013, the creators of the notorious CryptoLocker malware shifted their monetization tactics to Bitcoin as a mode of payment for files or systems held for ransom.[11]

Despite its developers' intention of introducing the Bitcoin as an innovative online payment means, its use also proved efficient for money laundering and illegal product purchasing, including cybercriminal tools like BlackOS from underground markets.[12] Bitcoin use, after all, is a highly convenient system for anonymous purchasing since it can circulate online without being tied to any bank account.

Timeline of Known Bitcoin Attacks, 1Q 2014



Sources: Bitstamp, Vircurex, Poloniex, Flexcoin, and new Silk Road

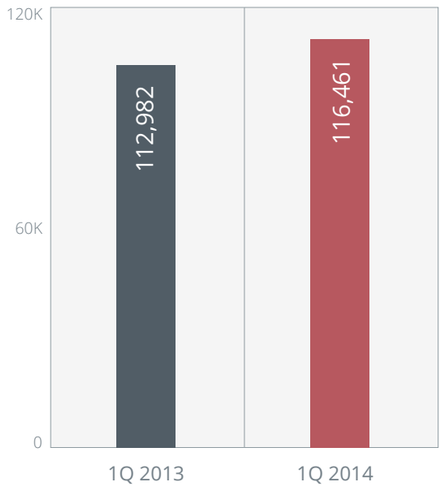
This quarter, several Bitcoin exchanges admitted to suffering attacks and breaches, resulting in the loss of Bitcoins in some instances or, worse, in the bankruptcy and shutdown of affected exchanges.

Online Banking Malware Showed New Behaviors but Familiar Core Tactics

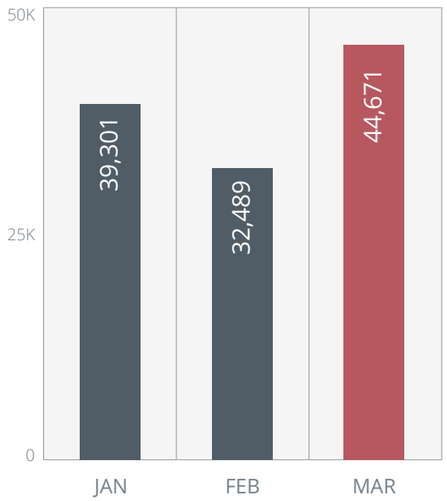
Online banking malware exhibited a variety of notable behaviors this quarter. In January, for instance, we found ZeuS/ZBOT samples that targeted 64-bit systems. Their routines include preventing the execution of various anti-malware analysis tools and sporting a Tor component that hid communications with command-and-control (C&C) servers.[13]

That same month, a BANLOAD variant used a different infection approach—checking for security plug-ins before executing malicious routines.[14] Control Panel (CPL) malware and a unique "timed" ZeuS/ZBOT downloader further proved that no two online banking malware were the same when it came to technique.[15, 16]

Online Banking Malware Volume Comparison, 1Q 2013 and 1Q 2014



Online Banking Malware Volume, January–March 2014



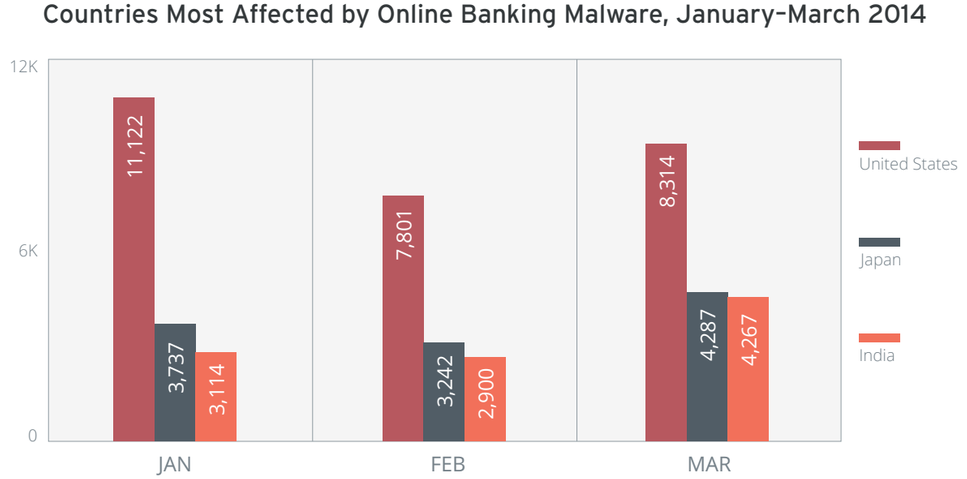
The number of online banking malware detections this quarter reached roughly 116,000, showing a slow but steady increase from 113,000 detections in the first quarter of 2013.

Countries Most Affected by Online Banking Malware

COUNTRY	SHARE
United States	23%
Japan	10%
India	9%
Brazil	7%
Turkey	4%
France	3%
Malaysia	3%
Mexico	3%
Vietnam	3%
Australia	3%
Others	32%

The United States was most hit by online-banking-malware-related attacks as usual. India slowly rose to the top 3 due to a spike in the number of online bankers in the country, which could be attributed to a vastly improved banking industry.[17] The mobile banking transaction volume grew along with the number of online money transfers–a top-ranking secondary means of making inward remittances in India.[18, 19]

Countries Most Affected by Online Banking Malware, January–March 2014



The United States, Japan, and India maintained their rankings throughout the quarter when it came to online banking malware detection.

Ransomware Continued to Go Regional

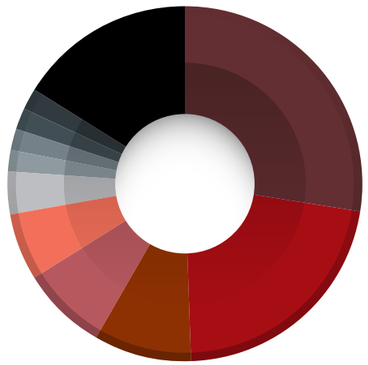
CryptoLocker's emergence in October 2013 was a prime example showing how cybercriminals refined their techniques and enhanced existing tools instead of creating new ones. Based on past monitoring of CryptoLocker, the malware continued to pose a unique challenge for security researchers this quarter. Armed with sophisticated social engineering tactics, encryption technology, and a countdown timer, victims were better scared and thus pressured to pay up.

This quarter, already-widespread ransomware went through even more advancements after cybercriminals seemed to have figured out their global "appeal." Scaring people into submission proved effective no matter where the victims resided. Case in point: In February, a CryptoLocker-like ransomware variant victimized users in Hungary and Turkey.[20] We've seen this happen before with the Police Trojan, which specifically targeted users in Italy, Spain, France, and the United Kingdom.[21] The current trend shows just how much history can repeat itself.

More than targeting specific countries, ransomware also came with other malicious behaviors, including Bitcoin theft, with the entry of BitCrypt. This ransomware-cum-cryptocurrency-stealer obtained funds from various cryptocurrency wallets, including Bitcoin wallets.

The ransomware volume was particularly high in the third quarter of 2013 due to a rise in CryptoLocker detections. This quarter, the United States topped the list of most affected countries, accounting for almost 30% of the total, followed by Japan and India. Feedback from the Trend Micro Smart Protection Network also showed that 40% of the BitCrypt (detected as CRIBIT) victims were based in the United States.

Countries Most Affected by Ransomware



United States	28%
Japan	22%
India	9%
Turkey	8%
Australia	5%
Germany	4%
France	2%
United Kingdom	2%
Canada	2%
Italy	2%
Others	16%

The countries that were most affected by ransomware in 2013 did not drastically change this year though a slight decrease in volume was seen.

The Dark Side of Tor Was Revealed

Tor's main purpose as a worldwide network of servers is to foster online privacy tool research and development (R&D). The cloak of anonymity Tor provides, however, also made it an attractive platform for cybercriminals' malicious schemes, as it is also easy to access and use. The Deep Web, which has often been associated with Tor in the past, is being abused by cybercriminals because of its ability to bypass search engine crawlers, allowing them to remain anonymous.[22]

We saw Tor particularly abused in March when CRIGENT used Windows® PowerShell® to spread through scripts before downloading two well-known online anonymity tools, one of which involved the Tor network.[23] The previously mentioned 64-bit ZeuS/ZBOT variant also took advantage of Tor to hide communications with C&C servers.

The fact that the Tor client is easy to set up allowed cybercriminals to carry out complex behaviors without deploying additional configuration files. The hidden services that Tor provides could also attract cybercriminals to abuse it even more in the coming months.

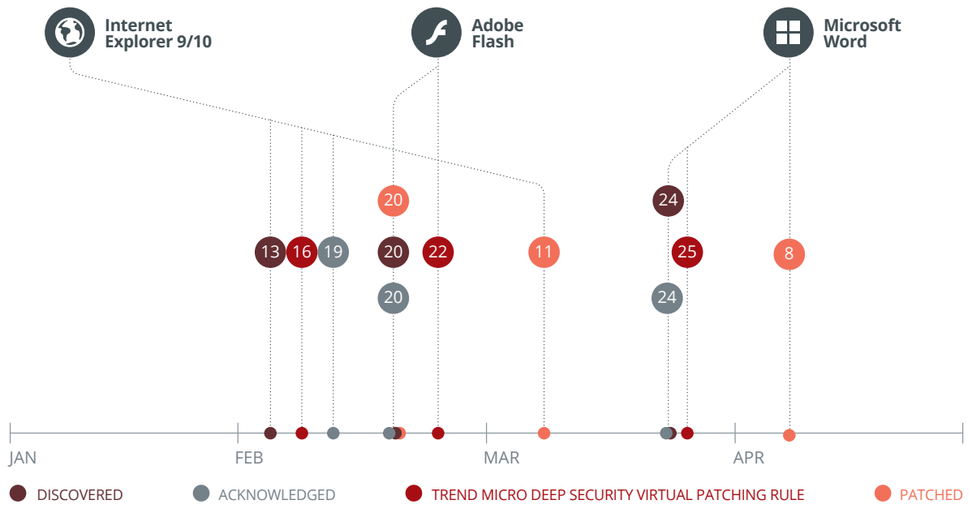
Zero-Day Exploits and Windows XP End of Support Highlighted Risks Unpatched Bugs Posed

Various zero-day exploits were found this quarter for a mix of browser, browser plug-in, and other software vulnerabilities. Microsoft™ Office® 2010 proved to be a viable target, as evidenced by the vendor's security bulletin for March, which included a patch for a zero-day vulnerability in Microsoft Word®.[24]

Earlier in February, another favorite target, Adobe® Flash®, was exploited to spread PlugX, a remote access tool known for its stealth mechanisms.[25] Microsoft Security Advisory 2934088, also released that month, alerted versions 9 and 10 users to an Internet Explorer® zero-day exploit used in targeted attacks.[26] This was a particularly grave issue for Microsoft, as it affected most Windows versions, except Windows 8.1 and Windows XP, which carried Internet Explorer versions 11 and 8, respectively.

Zero-day exploits like those used in the Internet Explorer 9 and 10 attacks were significant because they could evade mitigation techniques such as address space layout randomization (ASLR) and Data Execution Prevention (DEP). The ability to evade these mitigation techniques proved effective in recent attacks, which gave us reason to believe that cybercriminals will try to make their exploits increasingly platform agnostic in the future.

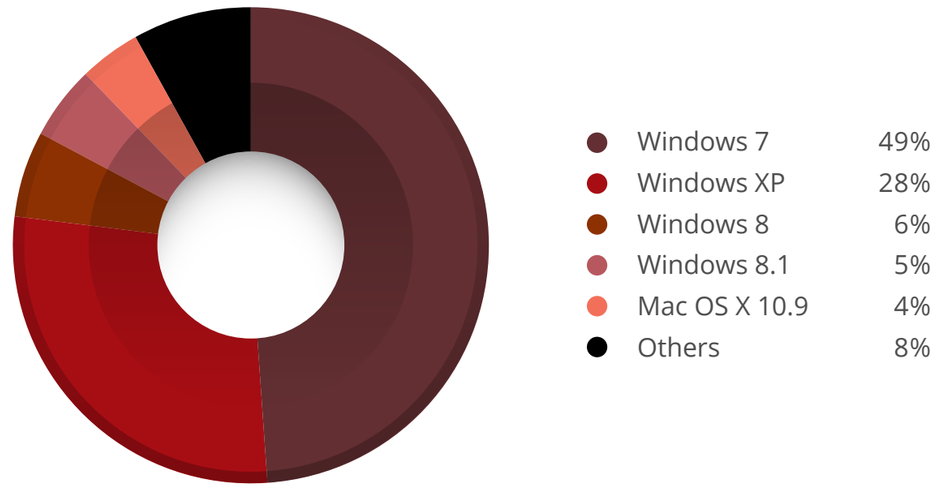
Timeline of Zero-Day Exploits, 1Q 2014



We were able to provide protection to Trend Micro Deep Security and OfficeScan™ with Intrusion Defense Firewall (IDF) plug-in users for two of the three major zero-day exploits seen this quarter even before vendors released patches.

Although the zero-day exploits found this quarter did not affect Windows XP, that does not mean its users are spared.[27] In fact, the end of support for Windows XP as of April 8, 2014 could make systems even more prone to attacks.[28] It does not help that versions of Internet Explorer higher than 8 are not compatible with the platform, which means Windows XP users will get left behind with older and vulnerable versions of the browser. They can, of course, use alternative browsers to escape threats that target Internet Explorer though simply switching may not be 100% foolproof against attacks that target other possibly vulnerable browsers. Security software will still be able to protect the outdated platform but newly discovered vulnerabilities will no longer be fixed and be left wide open forever for attackers to exploit.[29]

OS Market Shares, March 2014



Source: Netmarketshare.com

As of March 2014, Windows XP remains a major player in the desktop OS market with an almost 30% share.
NOTE: *The numbers from Netmarketshare.com tend to vary so the figures above show the possible worst-case scenario for Windows XP.*

Expert Insights

Cybercriminals continued to find new avenues to commit digital crime and evade countermeasures applied against their creations. Online banking malware continued to thrive with the emergence and/or modification of new malware families, each with different targets and varying anti-detection techniques. Online banking malware distribution methods were also continuously refined to infect systems only in certain countries/regions. They also came armed with tools to make sure the systems they're infecting are preferred targets. Some could even detect systems' IP addresses and keyboard layouts to ensure these are located in specific target countries/regions.

Since law enforcement activities against online theft are slowly being ramped up, cybercriminals are starting to add more layers to ensure anonymity in order to protect their identities and avoid getting arrested. Using Tor as a C&C channel allowed them a little more anonymity and gave them some degree of additional resilience against security software detection and takedown.

Cybercriminals' interest in Bitcoin, meanwhile, revolved around the fact that it shows the most promise and greatest adoption, presenting itself as a prime target for mining or theft. Finally, CryptoLocker made waves because of its ability to encrypt stored files, resulting in actual loss of not just documents but also the money victims hand out to "file-nappers."

Martin Rösler
Senior Director, Threat Research

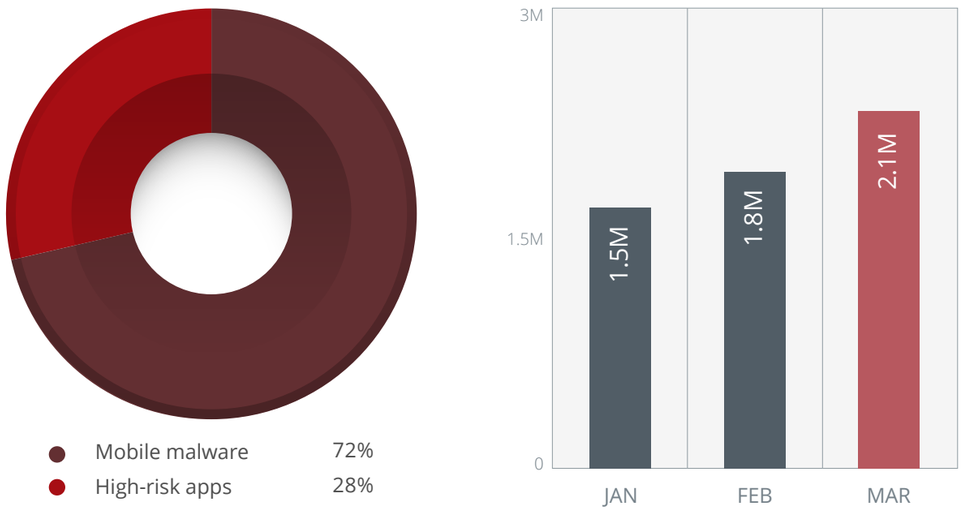
MOBILE THREAT LANDSCAPE

App Repackaging, Growing Underground Economy, and Toolkit Availability Pushed Mobile Malware and High-Risk App Count to 2 Million

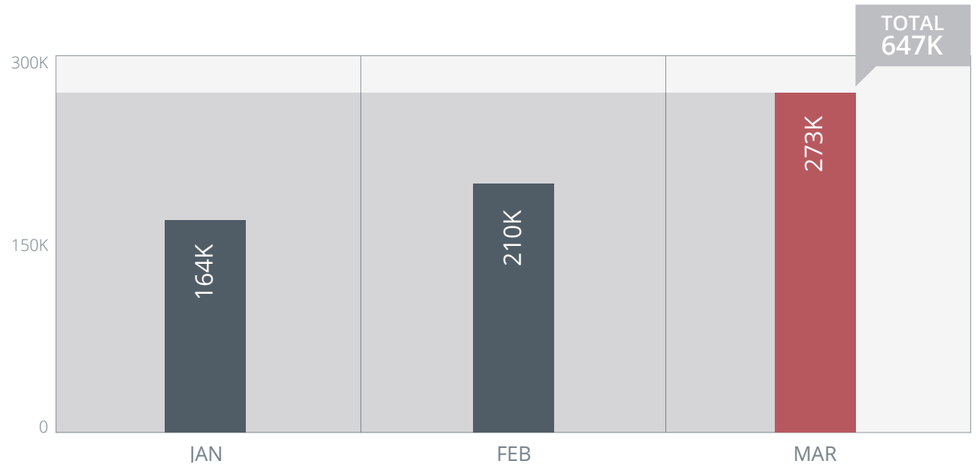
Growing at an even faster pace than last year, the number of mobile malware and high-risk apps hit 2 million this quarter. One reason for the volume growth could be the growing demand for malicious tools and services that can be used to create and distribute mobile malware underground.[30] One such tool, DENDROID—a remote administration tool—made it convenient to Trojanize legitimate mobile apps for US$300.[31, 32]

The proliferation of repackaged apps—those that have been maliciously tampered with to get past Android devices' security features and usually came armed with data-stealing and premium service abuse capabilities—also contributed to the huge spike in mobile malware and high-risk app volume growth. Great examples of this malicious app type were Trojanized versions of the once-famous app, Flappy Bird (detected as FAKEINST variants), which spread throughout third-party app stores this quarter.[33] These could even be a reason why OPFAKE/FAKEINST variants—our detection for repackaged apps—stayed at the top of the mobile malware list this quarter.

Android Cumulative Threat Volume



Monthly Mobile Malware and High-Risk App Volume



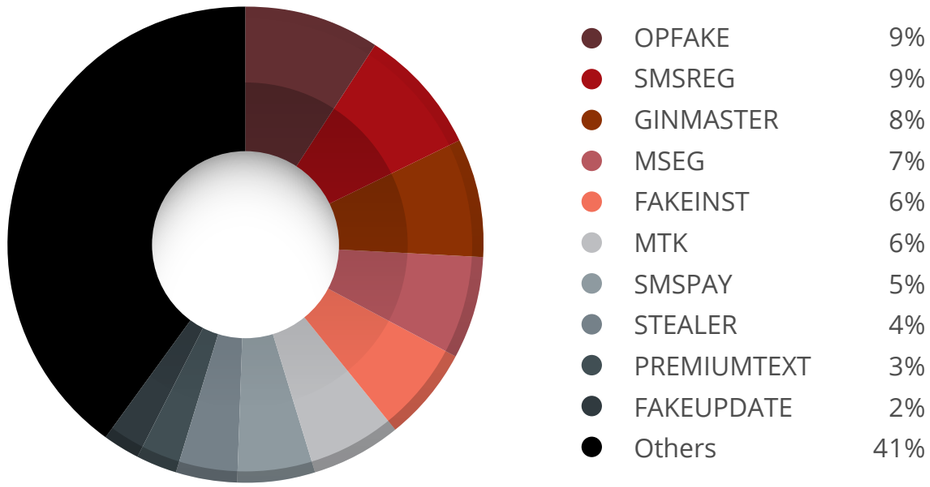
The newly detected mobile malware and high-risk apps found this quarter accounted for almost a third of the total number of Android threats.
NOTE: *High-risk or potentially unwanted apps are those that can compromise user experience because they display unwanted ads, create unnecessary shortcuts, or gather device information without user knowledge or consent. Examples include aggressive adware.*

Adware Toppled Premium Service Abusers in Terms of Volume

Premium service abusers—the most common Android threat type in 2013—no longer topped the Android threat list this quarter.[34] Adware surpassed premium service abusers in terms of volume possibly due to a recent announcement made by major carriers on dropping premium-text-service-billing rates after acknowledging that these could end up in cybercriminals' hands.[35]

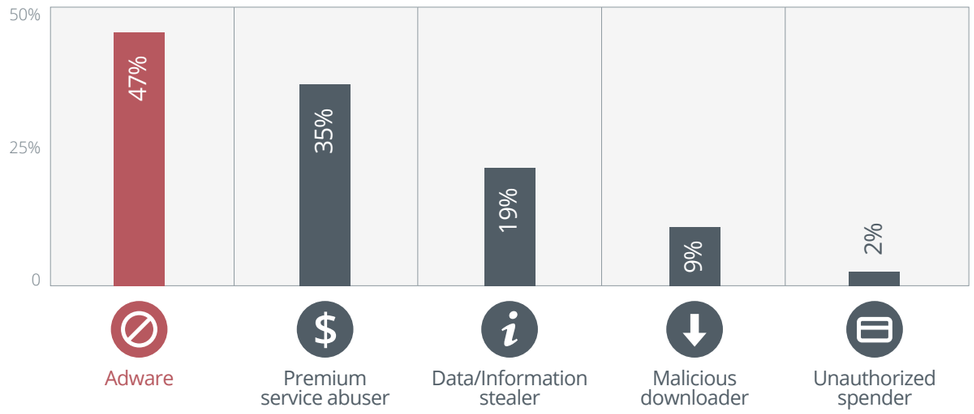
Viewing premium service abusers as less "profitable" attack tools, therefore, cybercriminals set their sights on spreading adware instead to victimize more users.

Top Android Malware Families



The top malware families at the end of 2013 continued their reign this quarter.
NOTE: *Premium service abusers register victims to overpriced services while adware aggressively push ads and can even collect personal information without victim consent.*

Top Android Threat Type Distribution



Adware toppled premium service abusers in terms of mobile threat distribution. The other threat types showed slightly decreased numbers from last year.
NOTE: *The distribution numbers were based on the top 20 mobile malware and adware families that comprised 88% of the total number of mobile threats detected by the Trend Micro Mobile App Reputation Technology from January to March this year. A mobile threat family may exhibit the behaviors of more than one threat type.*

More Bugs Showed a More Mature Mobile Threat Landscape

Another sign that today's mobile threat landscape has matured was a spike in the number of vulnerabilities found in the Android platform. This spelled out even more risks for the millions of Android device users. In March, we analyzed an Android bug that affected versions 4.0 and above, which could be used to trap devices in an endless cycle of reboots, rendering them unusable.[36] That same month, we saw a vulnerability that put at least 10,000 apps at risk of leaking user data by bypassing certain customized device permissions.[37]

iOS had its share of vulnerabilities this quarter, too, highlighted by the "goto fail" Secure Sockets Layer (SSL) security problem in version 7 discovered in February.[38] Apple immediately released security update iOS 7.0.6 to patch the flaw, which could inadvertently lead to eavesdropping and session hijacking when a vulnerable device is connected to a shared network.

Threats Migrated from Computers to Mobile Devices with Varying Results

Bitcoin-mining malware exhibited new abilities and routines this quarter.[39] They have started targeting mobile devices with the emergence of a malware family we detect as ANDROIDOS_KAGECOIN.HBT, which installed cryptocurrency miners into infected devices. These allowed cybercriminals to use infected mobile devices' computing resources to mine for Bitcoins, Litecoins, and Dogecoins. Infection resulted in shorter battery life, which could ultimately lead to a shorter device lifespan.[40]

Other examples of such threats were TORBOT and DENDROID. ANDROIDOS_TORBOT.A was the first mobile malware variant that used Tor to access remote servers so their users can maintain a certain degree of anonymity.[41] Once connected, it could make phone calls and intercept and send text messages to specific numbers. ANDROIDOS_DENDROID.HBT, meanwhile, which was sold underground as a crimeware, exhibited routines reminiscent of typical computer malware, including the ability to intercept text messages, record calls, and take photos without a device user's consent.

Expert Insights

It has been 10 years since the first piece of proof-of-concept (PoC) mobile malware (SYMBOS_CABIR) appeared in the wild.[42] However, with the exponential growth in the mobile device volume in recent years, it is not surprising to see the number of mobile malware outpace the computer threat growth. Today, technical methods to victimize computer users like Tor use and cryptocurrency mining are also being used to plague mobile device users. More and more cybercriminals are shifting targets, riding the popularity and widespread use of mobile devices, apart from the fact that they are not as protected as computers. We are bound to see more vulnerabilities in mobile platforms, especially Android, because of its huge user base. But that does not mean users have to suffer.

Using reliable mobile security software and adhering to best practices will help. Though it is hard to ensure that all apps available for download are malware free, downloading only from official app stores can dramatically lessen your device's chances of getting infected. Carefully going through the list of permissions an app requests when installed is critical. If it asks for access to services or information that it does not really require to fulfill its intended purpose, it is better not to install it.[43] And should an app be proven vulnerable, best not to install it until the bug is fixed.

Kenny Ye
Mobile Threat Researcher

TARGETED ATTACK CAMPAIGNS AND CYBER ATTACKS

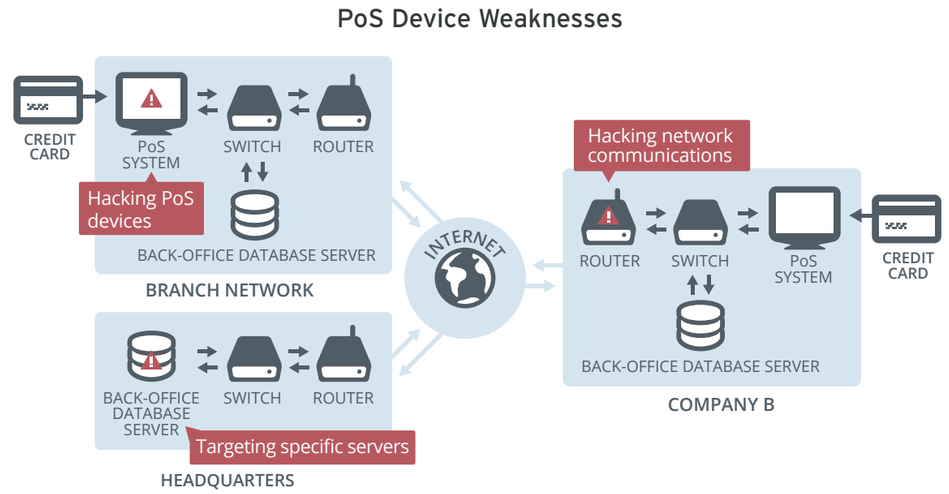
PoS System Breaches Stressed the Importance of Customized Defense Strategies

We saw how the large-scale retail and hospitality industry breaches impacted users in the United States this quarter. Millions of customers were put at immediate risk when their personal information was sold for credit card fraud, as was the case in the said breaches.[44, 45]

However, incidents were not limited to the United States, as payment card information from users in South Korea was also stolen via PoS terminals this quarter.[46]

Throughout the first three months of this year, we saw how unusual attack targets—PoS terminals—and oft-overlooked tools with regard to security proved attack worthy. Used in the retail and hospitality industries to accept payments and provide operational information in accounting, sales tracking, and inventory management, PoS systems help cut costs and provide productivity gains. PoS systems could have a dramatic effect on any retail or hospitality business with the benefits they bring. As such, PoS system owners need to consider security especially as cybercriminals will continue to find ways to compromise devices in their ever-evolving quest to obtain money.

How do hackers infiltrate PoS devices? A report we wrote on PoS system breaches revealed that these had multiple points of weakness that could allow hackers to steal data.[47] We mapped out the most possible scenarios by which large-scale breaches could occur, which included hacking PoS devices, hacking network communications, and targeting specific servers.



When targeting specific servers, attackers could go after an update mechanism that would allow them to deploy malware to connected PoS devices in order to steal customer information. In recent months, we identified several PoS malware families that could scrape and send credit card information to attackers. ALINA or Trackr, for instance, scanned systems' memory to check if their contents match regular expressions, which indicate the presence of card information that could be stolen. Other destructive PoS malware include FYSNA, which is known for using the Tor network, and vSkimmer or HESETOX, which uploaded stolen data to C&C servers.

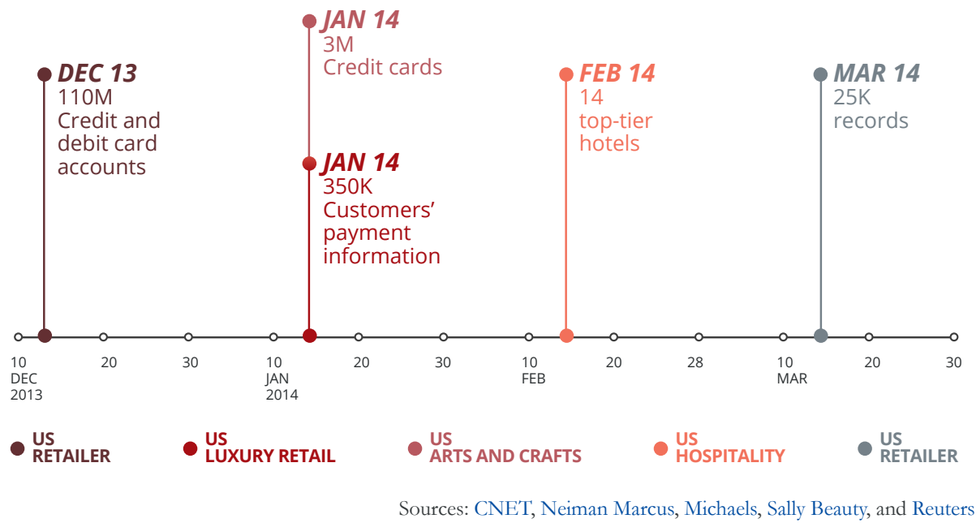
PoS Malware

DETECTION NAME	ROUTINE	DATE FIRST SEEN
ALINA (Trackr)	Scans systems' memory to check if their contents match regular expressions, which indicate the presence of card information that could be stolen	May 2010
DEXTR	Shares folder containing stolen data via the KaZaA network	February 2011
HESETOX (vSkimmer)	Uploads stolen data to C&C servers	January 2012
POCARDL	Steals information like user's directory name and credit and/or debit card data	October 2012
FYSNA	Uses the Tor network	December 2013
DECBAL	Steals data and sends it via HTTP POST to a remote site	January 2014

We have been detecting PoS malware since 2010. Since then, their routines have continuously improved to more effectively and anonymously steal financial information.

The previously mentioned risks associated with PoS device use all highlight why companies, especially those that accepts card payments should consider implementing a customized defense strategy—one that specifically fits their network and how they create, use, and process card information. It did not help either that we saw seven times more PoS malware in the first quarter of 2014 compared with the whole 2013.

Timeline of High-Profile Breaches



Sources: CNET, Neiman Marcus, Michaels, Sally Beauty, and Reuters

This quarter, different companies admitted to suffering from breaches via their PoS systems, which led to the theft of personal information of as many as 110 million users in one case.

Reflection Attacks Succeeded Despite Having Known Solutions in Place

Hackers abused weaknesses in the Network Time Protocol (NTP)—a system used to synchronize computer clocks to launch distributed denial-of-service (DDoS) attacks this January.[48] Because NTP servers are known for being highly susceptible to flooding and are generally public facing, vulnerable ones succumbed to attacks, as these often accepted connections from anyone. This incident gave way to continued and widespread DDoS runs of unprecedented scale. Since then, reflection attacks have become "commonplace," affecting all industries. But all was not lost, as IT administrators could reconfigure running services or upgrade their servers as mitigation.[49]

The Siesta Campaign and the Continued Proliferation of Targeted Attacks

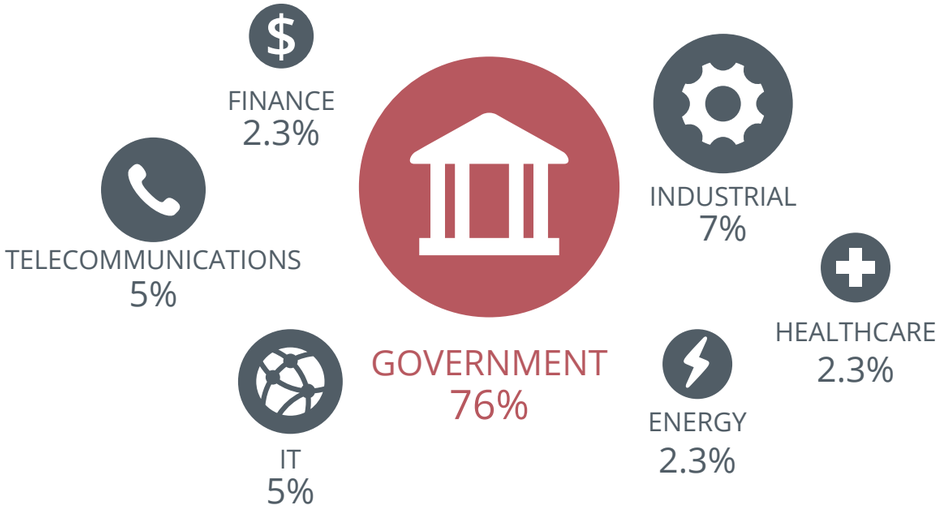
Targeted attacks continued to plague enterprises worldwide, as evidenced by the Siesta Campaign, which was uncovered this March. Aptly named, the campaign accepted one of two encrypted commands, "Sleep" and "Download: <download URL>," as it targeted several institutions in a wide range of industries.[50] Emails were sent from spoofed email addresses of personnel within certain organizations.

The Siesta campaign's targets include a wide range of industries, including consumer goods and services, energy, finance, healthcare, media and telecommunications, public administration, security and defense, and transport and traffic.

Targeted Attack Volume by Country/Region

Taiwan and Japan saw the most number of targeted attacks this quarter.
NOTE: *This chart shows our findings on the targeted attacks we monitored throughout the first quarter of 2014.*

Targeted Attack Volume by Industry



Governmental institutions were still the most preferred targets this quarter.
NOTE: *This chart shows our findings on the targeted attacks we monitored throughout the first quarter of 2014.*

Expert Insights

2014 kicked off with similar telemetry as seen in much of 2013. The trajectory remained fairly consistent, as we looked deep into the threat landscape in the first quarter of 2014. DDoS and PoS malware attacks dominated the headlines. Organizations continued to struggle with attacks that were targeted in nature, which could be directly aimed at the energy, financial, healthcare, and retail industries or critical infrastructure. It came down to a simple equation—high-value targets that promised massive payouts were compromised with the least amount of effort as possible. Granted, high-value targets had better defenses than most so efforts had to be well-funded and -orchestrated. However, this did not stop attackers from also picking on organizations that might not have robust processes. This often meant they lacked sufficient breach detection and notification systems to alert them of attack behaviors and suspect communications after they have circumvented traditional perimeter defenses. Contextual threat intelligence also proved lacking in many cases. Most people in the information and communication technology (ICT) community need to take the mindset that we have already been compromised. Breach response and remediation will enable organizations to carry on with business operations and not be shell-shocked and even shut down when an incident occurs.

We also saw targeted attacks directly aimed at organizations that relied on specific PoS system functionality and malware packages crafted to evade traditional anti-malware technologies. Combinations of spear-phishing emails to deliver malicious payloads were also seen to coerce users to click malicious links to nefarious sites that harbored malware. This approach remained the tip of the spear and the origin of most targeted attacks. Today, organizations are learning that relying on antivirus software alone is no longer sufficient. More transparency is needed across networks to analyze entire attack life cycles.

DDoS attacks continued to plague enterprises big and small. Disruptions are getting larger and many organizations are advancing their posture against these but we continued to see DDoS attacks as a staple weapon in many cyber attacks. This quarter, we saw an increase in DDoS attacks targeting NTP vulnerabilities to shut down unpatched servers. Traditional and virtual servers alike were affected and it is important to look at augmenting technologies like virtual patching or vulnerability shielding to aid patching efforts. This reduces the amount of time needed for remediation by laying down an effective compensating control until an organization can fully execute its patch management life cycle. This is especially effective for most known vulnerabilities and has tremendously helped organizations to reduce risks and do more with less. Organizations' staff will love you for it and it will significantly reduce your risk profile without crushing productivity.

It is still apparent that many organizations continue to struggle with keeping up with patch management processes and implementing traditional best practices. Over the past several years, staff sizes have shrunk and so have IT and security budgets. This combination has put organizations at a significant disadvantage and they have been struggling to keep pace.

With the damaging attacks seen this quarter, real-world cases showed that existing security controls need to evolve and security practitioners need to reassess IT security strategies to address targeted attacks. The customized nature of targeted attacks has changed the threat landscape. There is no silver bullet; instead, a customized defense strategy that improves detection, analysis, adaptation, and response is necessary to minimize risks and the impact of targeted attacks.

JD Sherry
Vice President, Technology and Solutions

DIGITAL LIFE AND THE INTERNET OF EVERYTHING

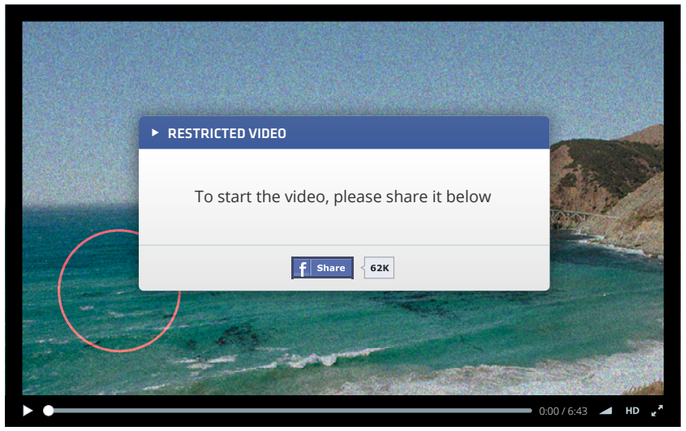
Even "Ephemeral" Apps Were Vulnerable

"Ephemeral" apps—new-generation apps that cater to users' desire to anonymously share content, send off-the-record messages, and share media—took the app ecosystem by storm last year as part of ongoing efforts to protect user privacy. Snapchat, one such app, however, unfortunately and ironically did the opposite this quarter. Attackers abused its application programming interface (API) that led to the leakage of its database containing the information of more than 4.6 million of its users.[51] The Snapchat team issued an update to provide users additional security to prevent future attempts to again abuse the app's API.[52] While the update may have comforted affected users, Snapchat's API abuse was nonetheless alarming, as it raised even more concerns about trusting apps, even those that promised privacy and anonymity.

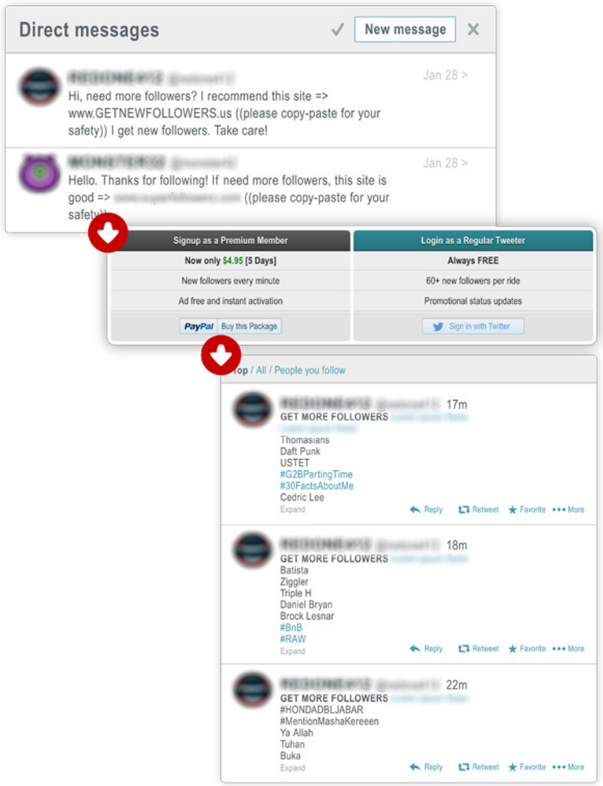
Search for Missing Flight MH370 and Other Social Engineering Techniques Used to Lure Victims In

Encountering malicious links on Twitter and other social media is not unusual.[53] We have seen one-too-many threats target social media users this quarter, ranging from "get free followers" scams to phishing attacks though the search for the missing flight MH370 took the cake. Cybercriminals took advantage of the hype to lure users to watch fake videos on Facebook, again proving that riding on reports of tragedies and disasters is still an effective ruse.[54]

Malicious site with embedded "video" related to the missing flight MH370



Twitter "free followers" scam direct message samples



This quarter, "get free followers" scams on Twitter sank to a new low, as cybercriminals resorted to spreading them even via direct messages. Links to phishing sites embedded in tweets also ran rampant.

Most-Used Social Engineering Lures

FLAPPY BIRD SEARCH FOR MH370 WHATSAPP **FREE FOLLOWERS ON INSTAGRAM** GRAND THEFT AUTO V

Cybercriminals continued to use the most-talked-about issues, events, movies, gadgets, and natural disasters to lure as many victims as possible to their specially crafted traps.

Another effective social engineering lure this quarter had to do with the supposed release of much-anticipated software. Cybercriminals, for instance, took advantage of the popularity of Grand Theft Auto V by spreading emails that boasted of the game's PC beta version.[55] Though proving to be a highly simplistic scam, as evidenced by the email's poor grammar and unofficial look, anticipation for the release of a PC version was still enough for excited gamers to fall for the ruse.

WhatsApp users were also duped into thinking the app had a PC version.[56] Like the Grand Theft Auto V beta scam, however, a WhatsApp PC version did not exist and victims instead ended up with banking-malware-infected systems for their trouble.

More Flaws Found in New IoE Devices

Several devices in the Internet of Everything (IoE) market underwent scrutiny, as security researchers exposed gaping system holes.

The technology-heavy Model S sedan by Tesla Motors, for instance, gained its fair share of media attention for setting a new standard for premium performance and integrating full mobile connectivity—a feature that may also leave the car vulnerable to hacking.[57] "Smart" Internet-connected TV sets like the Philips Smart TV were also analyzed by researchers who found that the vendor hardcoded the default password for Miracast into the firmware of some of its 2013 models.[58]

This meant that anyone could remotely access the TV within a certain range.

The IoE trend should constantly teach users that anything and everything that can go online can be hacked. Apart from cars and TV sets, smart lights also proved susceptible to hacking after a security researcher injected a malicious script that issued a blackout command through its router.[59] Security camera recorders were also hacked, not just to annoy users but for profit. Even DVRs could be hacked to record videos from security cameras, as an instructor at the SANS Technology Institute proved earlier this year.[60]

Expert Insights

While attacks on "smart" or "connected" devices are still not commonplace, we believe cybercriminals are already probing the possibilities for malfeasance offered by the new world of connected and often-unsecured devices. Once a killer app surfaces, attackers will be armed and ready to exploit them, just as they did when the Android platform succeeded. We have already seen real-world attacks on DVRs attached to security-monitoring cameras. Attackers attempted to use these to mine Bitcoins and the incident did not rely on randomly infecting devices, as the malware in question was deliberately encoded to run on ARM processors even though these were low-powered and were really not up to the task required of heavy-duty cryptography.

We have also seen several attacks that aimed to compromise home routers, as these offered a particularly well-placed vantage point for man-in-the-middle (MiTM) attacks against smart devices and negated the need to infect individual devices by directly placing threats in the data stream.

Recent PoC attacks against smart home-lighting solutions, electric car management systems, and smart TVs were also seen. Unfortunately, the majority of these bank on poor design or security practices by manufacturers rather than any code-level vulnerabilities in underlying OSs or interfaces.

It is disheartening to know that in rushing products to market, security is still so often an afterthought for vendors in the emerging IoE space. We should all keep in mind what Bill Gates said in his celebrated "Trustworthy Computing" memo to "Microsoft & Subsidiaries" 12 years ago:

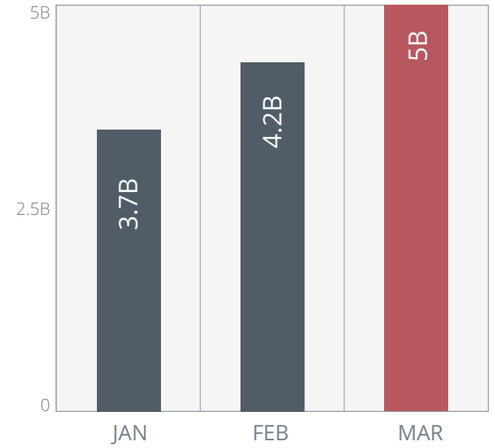
> *"Going forward, we must develop technologies and policies that help businesses better manage ever larger networks of PCs, servers, and other intelligent devices, knowing that their critical business systems are safe from harm. Systems will have to become self-managing and inherently resilient. We need to prepare now for the kind of software that will make this happen."*

This has never been more true and relevant than now.

Rik Ferguson
Vice President, Security Research

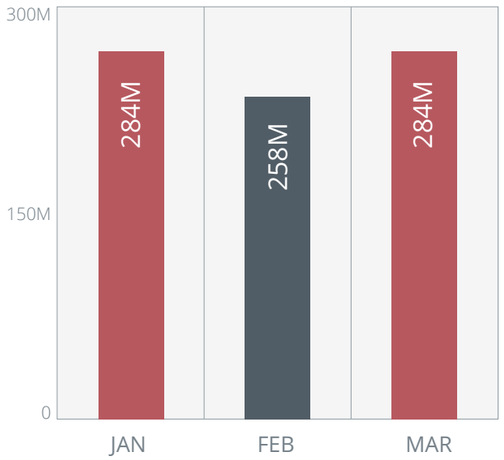
Appendix

Number of Spam-Sending IP Addresses Blocked by the Trend Micro Smart Protection Network



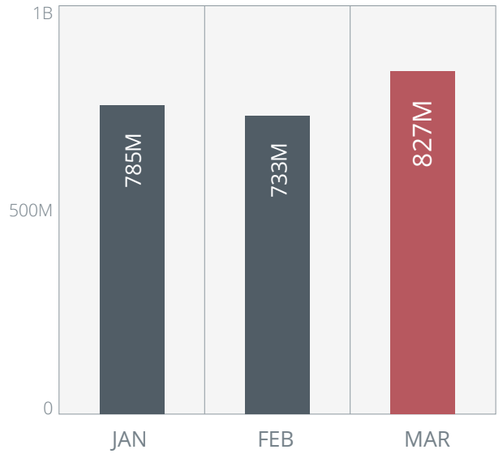
The number of spam-sending IP addresses the Trend Micro Smart Protection Network blocked did not change much from the end of last year.

Number of Malicious Sites the Trend Micro Smart Protection Network Blocked Access To



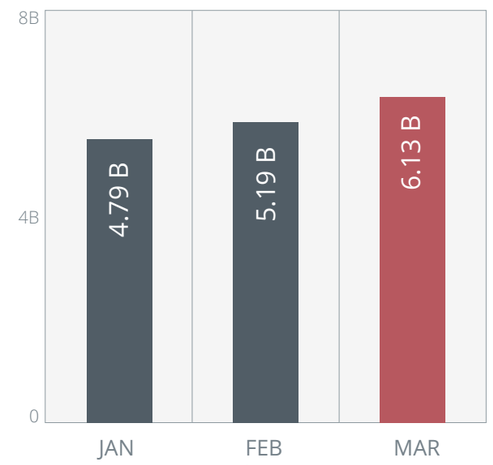
The number of malicious sites the Trend Micro Smart Protection Network blocked access to did not change much from the end of last year as well. This February, however, the number slightly declined.

Number of Malicious Files Blocked by the Trend Micro Smart Protection Network



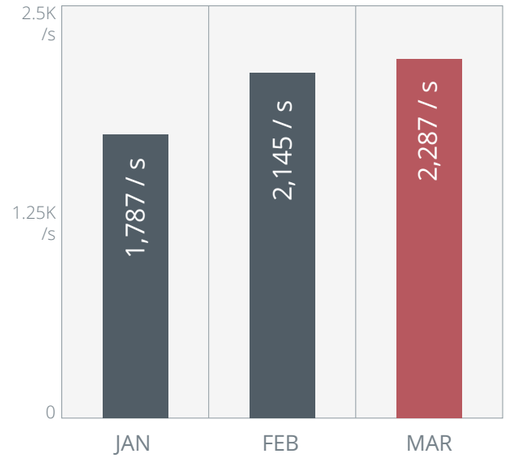
The number of malicious files blocked by the Trend Micro Smart Protection Network slightly increased compared with the previous quarter.

Total Number of Threats Blocked by the Trend Micro Smart Protection Network



The Trend Micro Smart Protection Network blocked 2 billion less threats this January compared with December 2013. The total number of threats blocked, however, steadily increased from 2013 to 2014.

Trend Micro Smart Protection Network Overall Detection Rate



No drastic changes were seen in the number of threats the Trend Micro Smart Protection Network blocked per second from the previous quarter.

Top 3 Malware

DETECTION NAME	VOLUME
ADW_NEXTLIVE	487K
ADW_OPENCANDY	394K
ADW_SENSAVE	390K

The top 3 malware this quarter were all adware, the total number of which increased from last quarter.

Top 3 Malware by Segment

SEGMENT	DETECTION NAME	VOLUME
Enterprise	WORM_DOWNAD.AD	69K
	ADW_OPENCANDY	25K
	ADW_NEXTLIVE	25K
SMB	WORM_DOWNAD.AD	28K
	ADW_SENSAVE	12K
	ADW_MONTIERA	12K
Consumer	ADW_NEXTLIVE	266K
	ADW_OPENCANDY	240K
	ADW_SENSAVE	234K

The number of malware targeting enterprises and small and medium-sized businesses (SMBs) decreased compared with the previous quarter. The number of malware targeting consumers, meanwhile, notably increased. Conficker/DOWNAD remained a threat to enterprises, most likely due to a large number of systems still running Windows XP, which is vulnerable to the threat.

Top 10 Malicious Domains the Trend Micro Smart Protection Network Blocked Accessed To

DOMAIN	REASON FOR BLOCKING ACCESS TO
ads.alpha00001.com	Reported as a C&C server and redirected users to enterfactory.com, another malicious site
ody.cc	Tied to suspicious scripts and sites that hosted BKDR_HPGN.B-CN
optproweb.info	Tied to a malicious file
interyield.jmp9.com	Known for spamming activities related to adware
sp-storage.spccint.com	Known for downloading malicious files
adsgangsta.com	Tied to malware attacks and had malicious records
fistristy.com	Known for downloading malware
advconversion.com	Known for spamming activities
namnamtech.com	Known for downloading malware
extremlymtorrents.com	Tied to spam URLs and parked sites

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

Top 10 Malicious URL Country Sources

COUNTRY	SHARE
United States	22%
France	3%
Netherlands	3%
Japan	3%
Germany	2%
China	2%
South Korea	2%
United Kingdom	2%
Russia	2%
Canada	1%
Others	58%

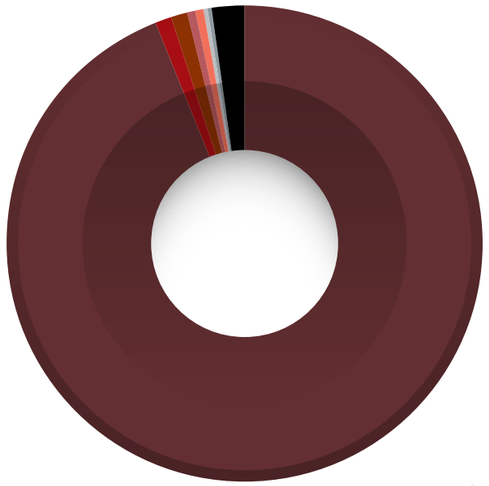
Almost all of the countries from which users who accessed malicious links came last quarter are still part of the list above.

Countries with the Most Number of Users Who Accessed Malicious Links

COUNTRY	SHARE
United States	34%
Japan	17%
Taiwan	4%
China	4%
France	3%
Australia	3%
Germany	3%
India	3%
South Korea	3%
Russia	3%
Others	23%

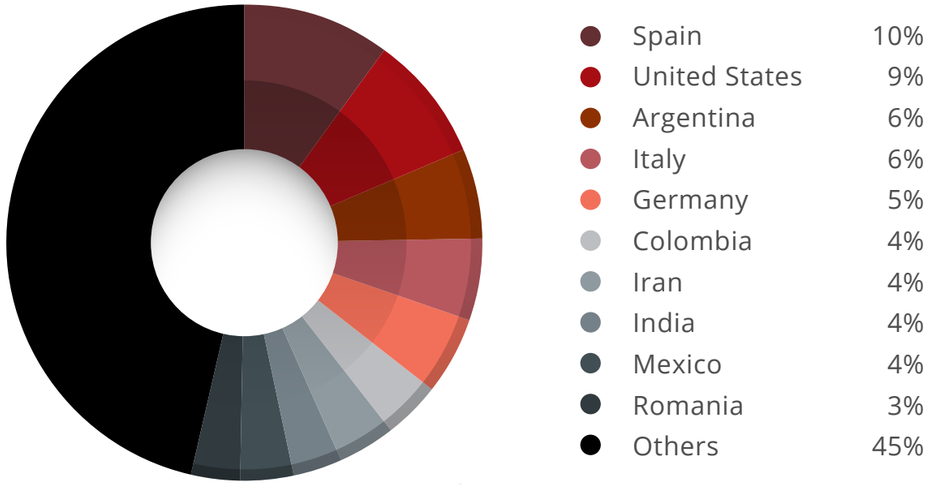
United States had the most number of users who accessed malicious links this quarter.

Most-Used Spam Languages



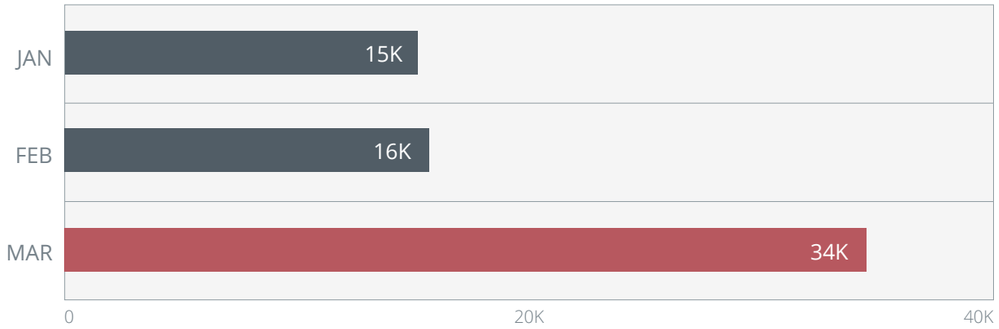
No significant changes to the most-used spam languages were seen this quarter.

Top Spam-Sending Countries



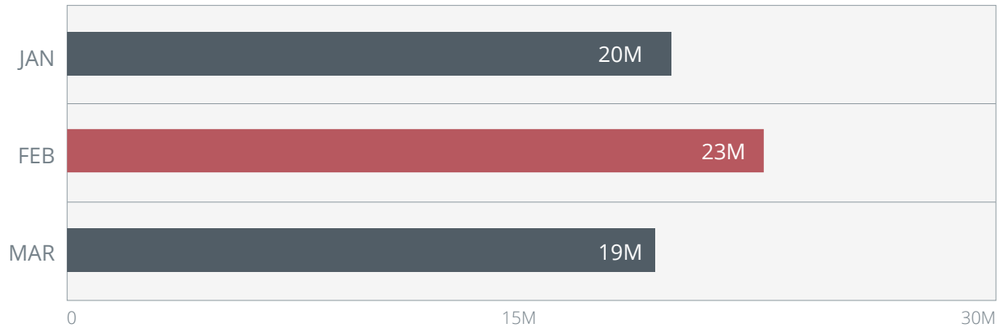
No significant changes were seen in the list of top spam-sending countries this quarter.

Number of Botnet C&C Servers Detected per Month



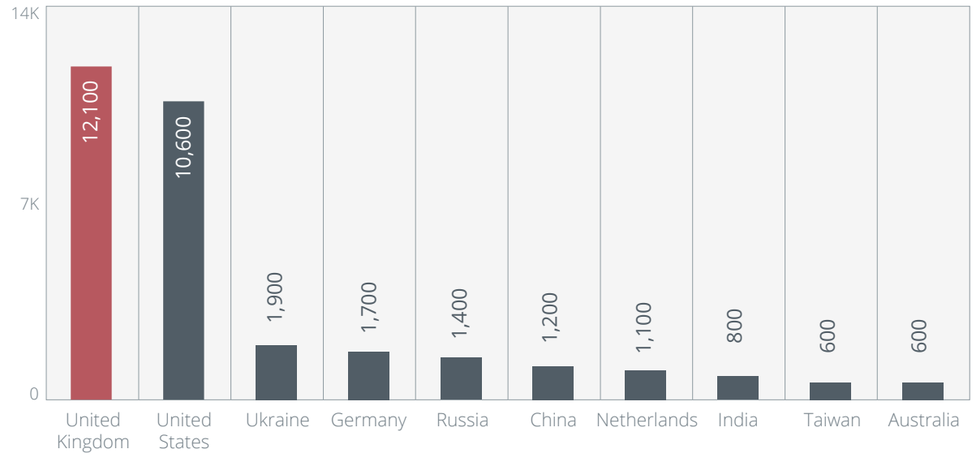
The number of botnet C&C servers seen grew in the first quarter compared with previous quarters, largely due to the growth seen this March. Levels for the rest of the quarter were consistent with previous months.

Number of Botnet Connections Detected per Month



The number of botnet connections detected per month decreased compared with last quarter.

Countries with the Most Number of Botnet C&C Servers



South Korea dropped off the list of countries with the most number of C&C servers this quarter.

References

[1] Trend Micro Incorporated. (2013). "Cashing in on Digital Information: An Onslaught of Online Banking Malware and Ransomware." Last accessed April 14, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-cashing-in-on-digital-information.pdf.

[2] Carter Dougherty and Grace Huang. *Bloomberg*. (March 1, 2014). "MtGox Seeks Bankruptcy After $480 Million Bitcoin Loss." Last accessed April 15, 2014, http://www.bloomberg.com/news/2014-02-28/mt-gox-exchange-files-for-bankruptcy.html.

[3] Trend Micro Incorporated. (2014). "Point-of-Sale System Breaches: Threats to the Retail and Hospitality Industries." Last accessed April 16, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-pos-system-breaches.pdf.

[4] Hadley Malcolm. (January 10, 2014). *USA Today News*. "Target: Data Stolen from Up to 70 Million Customers." Last accessed April 15, 2014, http://www.usatoday.com/story/money/business/2014/01/10/target-customers-data-breach/4404467/.

[5] Rhena Inocencio. (March 24, 2014). *TrendLabs Security Intelligence Blog*. "Ransomware and Bitcoin Theft Combine in BitCrypt." Last accessed April 15, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-and-bitcoin-theft-combine-in-bitcrypt/.

[6] Russell Brandom. (February 26, 2014). *The Verge*. "Who Stole $400 Million from MtGox?" Last accessed April 15, 2014, http://www.theverge.com/2014/2/26/5450206/who-stole-400-million-from-mt-gox.

[7] Flexcoin. (March 3, 2014). "Flexcoin Is Shutting Down." Last accessed April 28, 2014, http://flexcoin.com/.

[8] Cyrus Farivar. (February 14, 2014). *Ars Technica*. "New Silk Road Hit with $2.6-Million Heist Due to Known Bitcoin Flaw." Last accessed April 28, 2014, http://arstechnica.com/security/2014/02/new-silk-road-hit-with-2-6-million-heist-due-to-known-bitcoin-flaw/.

[9] Simple Machines. (2014). *Bitcoin Forum*. "BTC Stolen from Poloniex." Last accessed April 28, 2014, https://bitcointalk.org/index.php?topic=499580.

[10] Anthony Volastro. (January 23, 2014). *CNBC*. "CNBC Explains: How to Mine Bitcoins on Your Own." Last accessed April 15, 2014, http://www.cnbc.com/id/101332124.

[11] Trend Micro Incorporated. (November 27, 2013) *Trend Micro Simply Security Blog*. "CryptoLocker Evolves with New Monetization Schemes." Last accessed April 22, 2014, http://blog.trendmicro.com/cryptolocker-evolves-new-monetization-schemes/.

[12] Trend Micro Incorporated. (March 19, 2014). *TrendLabs Security Intelligence Blog*. "New BlackOS Software Package Sold in Underground Forums." Last accessed April 15, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/new-blackos-software-package-sold-in-underground-forums/.

[13] Anthony Joe Melgarejo. (January 7, 2014). *TrendLabs Security Intelligence Blog*. "64-bit ZBOT Leverages Tor, Improves Evasion Techniques." Last accessed April 15, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/64-bit-zbot-leverages-tor-improves-evasion-techniques/.

[14] Mark Joseph Manahan. (January 16, 2014). *TrendLabs Security Intelligence Blog*. "BANLOAD Limits Targets via Security Plug-In." Last accessed April 15, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/banload-limits-targets-via-security-plugin/.

[15] Fernando Mercês. (January 27, 2014). *TrendLabs Security Intelligence Blog*. "A Look into CPL Malware." Last accessed April 15, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/a-look-into-cpl-malware/.

[16] Rika Joi Gregorio. (February 28, 2014). *TrendLabs Security Intelligence Blog*. "ZeuS Downloader Runs in January, Crashes Rest of the Year." Last accessed April 15, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/zeus-downloader-runs-in-january-crashes-rest-of-the-year/.

[17] Dr. N. Jamaludddin. (November 2013). "E-Banking: Challenges and Opportunities in India." Last accessed April 24, 2014, http://www.wbiworldconpro.com/uploads/melbourne-conference-2013-november/banking/1384600741_607-Jamal.pdf.

[18] Somasroy Chakraborty. (April 12, 2013). *Business Standard*. "Mobile Banking Transactions Double, Payments Rise Threefold." Last accessed April 24, 2014, http://www.business-standard.com/article/finance/mobile-banking-transactions-double-payments-rise-threefold-113041100353_1.html.

[19] Greater Pacific. (March 2013). *Greater Pacific Capital*. "The Indian Diaspora: A Unique Untapped Global Asset for India." Last accessed April 24, 2014, http://greaterpacificcapital.com/march-2013/.

[20] Ilja Lebedev. (February 21, 2014). *TrendLabs Security Intelligence Blog*. "Ransomware 'Goes Local' in Europe." Last accessed April 15, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-goes-local-in-europe/.

[21] David Sancho and Feike Hacquebord. (2012). "The 'Police Trojan': An In-Depth Analysis." Last accessed April 15, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_police_trojan.pdf.

[22] Vincenzo Ciancaglini. (November 8, 2013). *TrendLabs Security Intelligence Blog*. "The Boys Are Back in Town: Deep Web Marketplaces Back Online." Last accessed April 22, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/the-boys-are-back-in-town-deep-web-marketplaces-back-online/.

[23] Alvin John Nieto. (March 27, 2014). *TrendLabs Security Intelligence Blog*. "Word and Excel Files Infected Using Windows PowerShell." Last accessed April 15, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/word-and-excel-files-infected-using-windows-powershell/.

[24] Abigail Pichel. (March 25, 2014). *TrendLabs Security Intelligence Blog*. "Microsoft Word Zero-Day Spotted in the Wild." Last accessed April 15, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/microsoft-word-zero-day-spotted-in-the-wild/.

[25] Pavithra Hanchagaia. (February 23, 2014). *TrendLabs Security Intelligence Blog*. "New Adobe Flash Player Zero-Day Exploit Leads to PlugX." Last accessed April 15, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-flash-player-zero-day-exploit-leads-to-plugx/.

[26] Jonathan Leopando. (February 14, 2014). *TrendLabs Security Intelligence Blog*. "New IE Zero-Day Targets IE9 and IE10." Last accessed April 15, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/new-ie-zero-day-targets-ie9-and-ie10/.

[27] Pawan Kinger. (March 31, 2014). *TrendLabs Security Intelligence Blog*. "Managing Windows XP's Risks in a Post-Support World." Last accessed April 15, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/managing-windows-xps-risks-in-a-post-support-world/.

[28] Trend Micro Incorporated. (March 2013). *Threat Encyclopedia*. "Managing Your Legacy Operating Systems: What Will Life Be Like After Windows XP?" Last accessed April 22, 2014, http://about-

TREND MICRO | TrendLabs 1Q 2014 Security Roundup

threats.trendmicro.com/ent-primers/#managing_your_legacy_systems.

[29] David Sancho. (April 7, 2014). *TrendLabs Security Intelligence Blog*. "Windows XP Support Ending—Now What?" Last accessed April 15, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/windows-xp-support-ending-now-what/.

[30] Lion Gu. (2014). "The Mobile Cybercriminal Underground Market in China." Last accessed April 17, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-mobile-cybercriminal-underground-market-in-china.pdf.

[31] Trend Micro Incorporated. (2014). *Threat Encyclopedia*. "ANDROIDOS_DENDROID.HBT." Last accessed April 16, 2014, http://about-threats.trendmicro.com/us/malware/ANDROIDOS_DENDROID.HBT.

[32] Abigail Pichel. (March 26, 2014). *TrendLabs Security Intelligence Blog*. "Mobile Malware and High-Risk Apps Reach 2M Mark, Go for 'Firsts.'" Last accessed April 15, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/mobile-malware-and-high-risk-apps-reach-2m-mark-go-for-firsts/.

[33] Veo Zhang. (February 18, 2014). *TrendLabs Security Intelligence Blog*. "Flappy Bird and Third-Party App Stores." Last accessed April 15, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/flappy-bird-and-third-party-app-stores/.

[34] Trend Micro Incorporated. (November 11, 2013). *TrendLabs Security Intelligence Blog*. "3Q Security Roundup: The Invisible Web, 1 Million Mobile Malware Highlight Quarter." Last accessed April 15, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/3q-security-roundup-the-invisible-web-1-million-mobile-malware-highlight-quarter/.

[35] Ina Fried. (November 13, 2014). *All Things D*. "AT&T, Sprint, T-Mobile, Verizon Dropping Most Premium Text Service Billing in Effort to Combat Fraud." Last accessed April 15, 2014, http://allthingsd.com/20131121/att-sprint-t-mobile-verizon-all-dropping-most-premium-text-service-billing-in-effort-to-combat-fraud/.

[36] Veo Zhang. (March 23, 2014). *TrendLabs Security Intelligence Blog*. "New Android Bug Causes 'Bricked' Devices." Last accessed April 15, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/new-android-bug-causes-bricked-devices/.

[37] Weichao Sun. (March 20, 2014). *TrendLabs Security Intelligence Blog*. "Android Custom Permissions Leak User Data." Last accessed April 15, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/android-custom-permissions-leak-user-data/.

[38] Apple Inc. (2013). *Apple*. "About the Security Content of iOS 7.0.6." Last accessed April 15, 2014, http://support.apple.com/kb/HT6147.

[39] Trend Micro Incorporated. (2013). *Threat Encyclopedia*. "Cybercriminals Unleash Bitcoin-Mining Malware." Last accessed April 15, 2014, http://about-threats.trendmicro.com/us/webattack/93/Cybercriminals+Unleash+BitcoinMining+Malware.

[40] Veo Zhang. (March 25, 2014). *TrendLabs Security Intelligence Blog*. "Mobile Malware Mines Dogecoins and Litecoins for Bitcoin Payout." Last accessed April 15, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/mobile-malware-mines-dogecoins-and-litecoins-for-bitcoin-payout/.

[41] Trend Micro Incorporated. (2014). *Threat Encyclopedia*. "ANDROIDOS_TORBOT.A." Last accessed April 16, 2014, http://about-threats.trendmicro.com/us/malware/ANDROIDOS_TORBOT.A.

[42] Trend Micro Incorporated. (2014). *Threat Encyclopedia*. "Mobile Malware: 10 Terrible Years." Last accessed April 23, 2014, http://about-threats.trendmicro.com/us/mobile/monthly-mobile-review/2014-03-mobile-malware-10-terrible-years.

TREND MICRO | TrendLabs 1Q 2014 Security Roundup

[43] Trend Micro Incorporated. (2014). *Threat Encyclopedia*. "12 Most Abused Android Permissions." Last accessed April 23, 2014, http://about-threats.trendmicro.com/us/library/image-gallery/12-most-abused-android-app-permissions.

[44] Gregory Wallace. (March 5, 2014). *CNN Money*. "Timeline: Retail Cyber Attacks Hit Millions." Last accessed April 15, 2014, http://money.cnn.com/2014/02/11/news/companies/retail-breach-timeline/.

[45] David Sancho. (February 16, 2014). *TrendLabs Security Intelligence Blog*. "Hitting the Data Jackpot." Last accessed April 15, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/hitting-the-data-jackpot/.

[46] Thomson Reuters. (April 10, 2014). *Reuters*. "Hackers Steal South Korean Credit Card Data to Aid Forgeries." Last accessed April 17, 2014, http://www.reuters.com/article/2014/04/11/us-korea-cybercrime-idUSBREA3A09820140411.

[47] Trend Micro Incorporated. (2014). "Point-of-Sale System Breaches: Threats to the Retail and Hospitality Industries." Last accessed April 17, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-pos-system-breaches.pdf.

[48] Ben April. (January 21, 2014). *TrendLabs Security Intelligence Blog*. "A Free Solution for DDoS Reflection Attacks: A Decade in Waiting." Last accessed April 15, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/a-free-solution-for-ddos-reflection-attacks-a-decade-in-waiting/.

[49] Network Working Group. (2000). "Network Ingress Filtering: Defeating Denial-of-Service Attacks Which Employ IP Source Address Spoofing." Last accessed April 15, 2014, http://tools.ietf.org/html/bcp38.

[50] Maharlito Aquino. (March 6, 2014). *TrendLabs Security Intelligence Blog*. "The Siesta Campaign: A New Targeted Attack Awakens." Last accessed April 15, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/the-siesta-campaign-a-new-targeted-attack-awakens/.

[51] Nicole Perlroth and Jenna Wortham. (January 2, 2014). *New York Times*. "Snapchat Breach Exposes Weak Security." Last accessed April 15, 2014, http://bits.blogs.nytimes.com/2014/01/02/snapchat-breach-exposes-weak-security/.

[52] Team Snapchat. (January 9, 2014). *Snapchat Blog*. "Find Friends Improvements." Last accessed April 15, 2014, http://blog.snapchat.com/post/72768002320/find-friends-improvements.

[53] Paul Pajares. (January 30, 2014). *TrendLabs Security Intelligence Blog*. "Does the Twitter Follower Scam Actually Work?" Last accessed April 15, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/does-the-twitter-follower-scam-actually-work/.

[54] Rika Joi Gregorio. (March 17, 2014). *TrendLabs Security Intelligence Blog*. "Malaysia Airlines Flight 370 News Used to Spread Online Threats." Last accessed April 15, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/malaysia-airlines-flight-370-news-used-to-spread-online-threats/.

[55] Michael Casayuran. (March 14, 2014). *TrendLabs Security Intelligence Blog*. "Grand Theft Auto V PC Beta Test Lures Victims." Last accessed April 15, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/grand-theft-auto-v-pc-beta-test-lures-victims/.

[56] Michael Casayuran. (February 25, 2014). *TrendLabs Security Intelligence Blog*. "WhatsApp Desktop Client Doesn't Exist, Used in Spam Attack Anyway." Last accessed April 15, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/whatsapp-desktop-client-doesnt-exist-used-in-spam-attack-anyway/.

[57] Nitesh Dhanjani. (March 28, 2014). "Cursory Evaluation of the Tesla Model S: We Can't Protect

Our Cars Like We Protect Our Workstation." Last accessed April 15, 2014, http://www.dhanjani.com/blog/2014/03/curosry-evaluation-of-the-tesla-model-s-we-cant-protect-our-cars-like-we-protect-our-workstations.html.

[58] Richard Chirgwin. (April 2, 2014). *The Register*. "SmartTV, Dumb Vuln: Philips Hardcodes Miracast Passwords." Last accessed April 15, 2014, http://www.theregister.co.uk/2014/04/02/smarttv_dumb_vuln_philips_hardcodes_miracast_passwords/.

[59] Sal Cangeloso. (August 15, 2013). *Extreme Tech*. "Philips Hue LED Smart Lights Hacked, Home Blacked Out by Security Researcher." Last accessed April 15, 2014, http://www.extremetech.com/electronics/163972-philips-hue-led-smart-lights-hacked-whole-homes-blacked-out-by-security-researcher.

[60] Robert McMillan. (April 1, 2014). *Wired*. "Hackers Turn Security Camera DVRs into Worst Bitcoin Miners Ever." Last accessed April 15, 2014, http://www.wired.com/2014/04/hikvision/.

Created by:

TrendLabs

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