Cybercrime Hits the Unexpected
Bitcoin- and PoS-System-Related Attacks Trouble Users
Contents

1 | Cybercrime and the Cybercriminal Underground

10 | Mobile Threat Landscape

15 | Targeted Attack Campaigns and Cyber Attacks

21 | Digital Life and the Internet of Everything

25 | Appendix
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.

\(\text{NOTE: All mentions of “detections” within the text refer to instances when threats were found on users’ computers and subsequently blocked by any Trend Micro security software. Unless otherwise stated, the figures featured in this report came from data gathered by the Trend Micro™ Smart Protection Network™ cloud security infrastructure, which uses a combination of in-the-cloud technologies and client-based techniques to support on-premise products and hosted services.}\)
CYBERCRIME AND THE CYBERCRIMINAL UNDERGROUND

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

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

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

*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.¹⁰
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. Bitcoin use, after all, is a highly convenient system for anonymous purchasing since it can circulate online without being tied to any bank account.

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.

Timeline of Known Bitcoin Attacks, 1Q 2014

Sources: Bitstamp, Vircurex, Poloniex, Flexcoin, and new Silk Road
TREND MICRO | TrendLabs 1Q 2014 Security Roundup

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. That same month, a BANLOAD variant used a different infection approach—checking for security plug-ins before executing malicious routines. 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.

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

<table>
<thead>
<tr>
<th></th>
<th>1Q 2013</th>
<th>1Q 2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>JAN</td>
<td>112,982</td>
<td>116,461</td>
</tr>
<tr>
<td>FEB</td>
<td>39,301</td>
<td>32,489</td>
</tr>
<tr>
<td>MAR</td>
<td>44,671</td>
<td></td>
</tr>
</tbody>
</table>

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

Although the zero-day exploits found this quarter did not affect Windows XP, that does not mean its users are spared. In fact, the end of support for Windows XP as of April 8, 2014 could make systems even more prone to attacks. 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.

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.
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
TREND MICRO | TrendLabs 1Q 2014 Security Roundup

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. One such tool, DENDROID—a remote administration tool—made it convenient to Trojanize legitimate mobile apps for US$300.

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. 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](image)

<table>
<thead>
<tr>
<th>Mobile malware</th>
<th>High-risk apps</th>
</tr>
</thead>
<tbody>
<tr>
<td>72%</td>
<td>28%</td>
</tr>
</tbody>
</table>
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. 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.

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

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. 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.

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. 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. 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.

Other examples of such threats were TORBOT and DENDROID. ANDROIDOS_TORBOTA was the first mobile malware variant that used Tor to access remote servers so their users can maintain a certain degree of anonymity. 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.\(^4\) 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.\(^4\) 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. 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.

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. 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.

PoS Device Weaknesses

![Diagram of PoS device weaknesses](image-url)
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

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

*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 accept 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
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. 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.

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. 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.
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 Country/Region**

Taiwan 61%
Japan 26%
Israel 2.6%
Asia/Pacific 2.6%
Spain 2.6%
Venezuela 2.6%
United States 2.6%

**Targeted Attack Volume by Industry**

- **Finance:** 2.3%
- **Government:** 76%
- **It:** 5%
- **Telecommunications:** 5%
- **Industrial:** 7%
- **Energy:** 2.3%
- **Healthcare:** 2.3%

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.
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. The Snapchat team issued an update to provide users additional security to prevent future attempts to again abuse the app’s API. 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. 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.
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

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. 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. 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. “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.
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. 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.

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

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

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

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

<table>
<thead>
<tr>
<th>SEGMENT</th>
<th>DETECTION NAME</th>
<th>VOLUME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise</td>
<td>WORM_DOWNAD.AD</td>
<td>69K</td>
</tr>
<tr>
<td>Enterprise</td>
<td>ADW_OPENCANDY</td>
<td>25K</td>
</tr>
<tr>
<td>Enterprise</td>
<td>ADW_NEXTLIVE</td>
<td>25K</td>
</tr>
<tr>
<td>SMB</td>
<td>WORM_DOWNAD.AD</td>
<td>28K</td>
</tr>
<tr>
<td>SMB</td>
<td>ADW_SENSAVE</td>
<td>12K</td>
</tr>
<tr>
<td>SMB</td>
<td>ADW_MONTIERA</td>
<td>12K</td>
</tr>
<tr>
<td>Consumer</td>
<td>ADW_NEXTLIVE</td>
<td>266K</td>
</tr>
<tr>
<td>Consumer</td>
<td>ADW_OPENCANDY</td>
<td>240K</td>
</tr>
<tr>
<td>Consumer</td>
<td>ADW_SENSAVE</td>
<td>234K</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>DOMAIN</th>
<th>REASON FOR BLOCKING ACCESS TO</th>
</tr>
</thead>
<tbody>
<tr>
<td>ads.alpha00001.com</td>
<td>Reported as a C&amp;C server and redirected users to enterfactory.com, another malicious site</td>
</tr>
<tr>
<td>ody.cc</td>
<td>Tied to suspicious scripts and sites that hosted BKDR_HPGN.B-CN</td>
</tr>
<tr>
<td>optproweb.info</td>
<td>Tied to a malicious file</td>
</tr>
<tr>
<td>interyield JMP9.COM</td>
<td>Known for spamming activities related to adware</td>
</tr>
<tr>
<td>sp-storage.spccint.com</td>
<td>Known for downloading malicious files</td>
</tr>
<tr>
<td>adsgangsta.com</td>
<td>Tied to malware attacks and had malicious records</td>
</tr>
<tr>
<td>fistristy.com</td>
<td>Known for downloading malware</td>
</tr>
<tr>
<td>advconversion.com</td>
<td>Known for spamming activities</td>
</tr>
<tr>
<td>namnamtech.com</td>
<td>Known for downloading malware</td>
</tr>
<tr>
<td>extremlym torrents.com</td>
<td>Tied to spam URLs and parked sites</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>SHARE</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>22%</td>
</tr>
<tr>
<td>France</td>
<td>3%</td>
</tr>
<tr>
<td>Netherlands</td>
<td>3%</td>
</tr>
<tr>
<td>Japan</td>
<td>3%</td>
</tr>
<tr>
<td>Germany</td>
<td>2%</td>
</tr>
<tr>
<td>China</td>
<td>2%</td>
</tr>
<tr>
<td>South Korea</td>
<td>2%</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>2%</td>
</tr>
<tr>
<td>Russia</td>
<td>2%</td>
</tr>
<tr>
<td>Canada</td>
<td>1%</td>
</tr>
<tr>
<td>Others</td>
<td>58%</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>SHARE</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>34%</td>
</tr>
<tr>
<td>Japan</td>
<td>17%</td>
</tr>
<tr>
<td>Taiwan</td>
<td>4%</td>
</tr>
<tr>
<td>China</td>
<td>4%</td>
</tr>
<tr>
<td>France</td>
<td>3%</td>
</tr>
<tr>
<td>Australia</td>
<td>3%</td>
</tr>
<tr>
<td>Germany</td>
<td>3%</td>
</tr>
<tr>
<td>India</td>
<td>3%</td>
</tr>
<tr>
<td>South Korea</td>
<td>3%</td>
</tr>
<tr>
<td>Russia</td>
<td>3%</td>
</tr>
<tr>
<td>Others</td>
<td>23%</td>
</tr>
</tbody>
</table>

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

Most-Used Spam Languages

- English: 93.98%
- German: 1.13%
- Japanese: 1.11%
- Chinese: 0.65%
- Russian: 0.58%
- Portuguese: 0.12%
- Spanish: 0.11%
- Icelandic: 0.06%
- French: 0.06%
- Turkish: 0.04%
- Others: 2.16%

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

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

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


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.