The Invisible Web Unmasked
Contents

1 | CYBERCRIME:
   Takedowns, Banking Trojans,
   Site Compromises, and
   Refined Malware Techniques Seen

6 | MOBILE:
   Mobile Malware and High-Risk Apps:
   1-Million Strong

10 | DIGITAL LIFE SECURITY ISSUES:
   On Privacy and Data Theft:
   A New “Identity Crisis”

12 | EXPLOITS AND VULNERABILITIES:
   Java Vulnerabilities Remain a Major Concern

13 | TARGETED ATTACKS:
   Sykipot Targets Aviation Data

15 | Appendix
Introduction

News about cybercrime circulated in recent months. The takedown of Liberty Reserve, an illegal digital currency system, and the recent seizure of the online black market, Silk Road, were among the many incidents this quarter that triggered greater public awareness of online threats.\(^1\) The arrest of the alleged Blackhole Exploit Kit creator in October also proved that cybercrime is indeed a business that thrives right under our noses.\(^2\)

Cybercriminals continued to refine their techniques this quarter. Online banking malware infections increased in several regions, including the United States and Japan. We also caught a glimpse of the massive scale of compromised sites. Our research on BKDR_FIDOBOT showed that the backdoor was used to attack more than 17,000 domains in a day. We also observed malware operation refinements like EXPIRO’s use of the Styx Exploit Kit and MEVADE malware’s use of The Onion Router (TOR) network.

On the mobile front, the number of malicious and high-risk Android™ apps surpassed the 1-million mark like we predicted. A significant portion of these dangerous apps were disguised as either fake or Trojanized versions of popular apps.

Internet Explorer® and Java security issues continued to put computers at risk, as a couple of zero-day exploits were discovered this quarter. Document exploits remained a staple in spear-phishing emails related to targeted attacks though we noted improvements in the Sykipot malware family, which now targets information related to civil aviation.
CYBERCRIME

Takedowns, Banking Trojans, Site Compromises, and Refined Malware Techniques Seen

Law enforcement agencies took home several wins, affecting the current threat landscape. The Liberty Reserve takedown caused cybercriminals to scramble for alternative currencies. They had to resort to other means like using Bitcoins to continue their operations. The infamous Silk Road takedown also showed the hidden but equally nefarious side of cybercrime, particularly the use of the Deep Web to hide illegal site networks. Lastly, the alleged Blackhole Exploit Kit author known as “Paunch” made headlines when he was arrested in early October. These positive developments in law enforcement spurred awareness of cybercriminal underground elements that most Internet users were not privy to.

Overall Trend Micro™ Smart Protection Network™ Numbers

We were able to protect Trend Micro customers from an average of 2,797 threats per second this quarter.
DOWNAD/Conficker remained the top malware this quarter. Adware packaged with fake software offers continued to victimize Internet users. Despite being the top malware though, the number of DOWNAD/Conficker infections decreased to 345,000 from last quarter’s 509,000, possibly due to number of users who upgraded OSs in light of the impending end of support for Windows® XP.

**Top Malware**

<table>
<thead>
<tr>
<th>Malware</th>
<th>Infections</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORM_DOWNAD.AD</td>
<td>345K</td>
</tr>
<tr>
<td>ADW_BPROTECT</td>
<td>246K</td>
</tr>
<tr>
<td>ADW_BHO</td>
<td>238K</td>
</tr>
</tbody>
</table>

DOWNAD/Conficker remained the top malware for three consecutive quarters while adware continued to trail behind.
### Top Malware by Segment

<table>
<thead>
<tr>
<th>Segment</th>
<th>Name</th>
<th>Volume</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENTERPRISE</td>
<td>WORM_DOWNAD.AD</td>
<td>205K</td>
</tr>
<tr>
<td></td>
<td>ADW_BPROTECT</td>
<td>28K</td>
</tr>
<tr>
<td></td>
<td>PE_SALITY.RL</td>
<td>17K</td>
</tr>
<tr>
<td>SMB</td>
<td>WORM_DOWNAD.AD</td>
<td>33K</td>
</tr>
<tr>
<td></td>
<td>HKTL_PASSVIEW</td>
<td>7K</td>
</tr>
<tr>
<td></td>
<td>TROJ_FAKEAV.BMC</td>
<td>5K</td>
</tr>
<tr>
<td>CONSUMER</td>
<td>ADW_BHO</td>
<td>158K</td>
</tr>
<tr>
<td></td>
<td>ADW_BPROTECT</td>
<td>138K</td>
</tr>
<tr>
<td></td>
<td>TROJ_FAKEAV.BMC</td>
<td>87K</td>
</tr>
</tbody>
</table>

Consumers likely download adware most because they were often packaged with fake free software. Enterprises and small and medium-sized businesses (SMBs), meanwhile, were most affected by DOWNAD/Conficker.

### Banking Trojan Volume Surge

The online banking malware volume surged this quarter. They spread across the globe and no longer concentrated on certain regions like Europe and the Americas. We continued to see this trend, with infection counts going beyond the 200,000 mark, the highest infection number since 2002.

**Online Banking Malware Infections**

Online banking malware accounted for more than 200,000 detections this quarter—the highest-recorded volume since 2002.
A large portion of online banking malware infections were due to ZeuS/ZBOT Trojans. ZeuS/ZBOT variants were, in fact, the most distributed malware by spam this quarter. New ZBOT variants emerged, specifically KINS malware, which came armed with anti-debugging and anti-analysis routines.

Citadel variants, meanwhile, continued to plague Japan, particularly targeting financial institutions and varied Webmail services like Yahoo!® Japan and Gmail™, among others.5

The United States and Brazil remained the most-affected countries by online banking malware. Japan, meanwhile, rose to the third from the fifth spot last quarter, largely due to the increase in Citadel malware infections.

Compromising Sites: A Norm?

Cybercriminals routinely use compromised sites to hide their tracks and host malware, spam templates, and redirection tools. Spambots like Stealrat heavily relied on techniques like using compromised sites to cloak malicious operations.6

Top Online Banking Victim Countries

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>SHARE</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>23%</td>
</tr>
<tr>
<td>Brazil</td>
<td>16%</td>
</tr>
<tr>
<td>Japan</td>
<td>12%</td>
</tr>
<tr>
<td>India</td>
<td>6%</td>
</tr>
<tr>
<td>Australia</td>
<td>3%</td>
</tr>
<tr>
<td>France</td>
<td>3%</td>
</tr>
<tr>
<td>Germany</td>
<td>2%</td>
</tr>
<tr>
<td>Vietnam</td>
<td>2%</td>
</tr>
<tr>
<td>Taiwan</td>
<td>2%</td>
</tr>
<tr>
<td>Mexico</td>
<td>2%</td>
</tr>
<tr>
<td>Others</td>
<td>29%</td>
</tr>
</tbody>
</table>

How Users End Up on Compromised Sites

* Spam data includes the backup email server’s URL, the sender’s name, the recipient’s address, and the email template.
We got a glimpse of the scale of site compromises by investigating BKDR_FIDOBOT. This backdoor brute-forced its way into sites that ran on either Joomla!™ or WordPress and was used to attack more than 17,000 domains in a single day. The majority of affected sites were either owned by individuals or small businesses and hosted in the United States.

**Refined Malware Techniques and Hidden Networks**

Other notable malware this quarter include EXPIRO. The malware first surfaced in 2010 and was known to infect files. Recent variants that emerged this quarter, however, stole FTP credentials. The EXPIRO variants used in attacks last July were also distributed using the Styx Exploit Kit.

In the latter part of August, we observed MEVADE malware download a TOR component to initiate widespread connections to specific sites. This was the reason behind reports of a growth in the number of TOR users. TOR allowed cybercriminals to more effectively hide their command-and-control (C&C) servers. It is also virtually impossible to take down a TOR-hidden service. MEVADE malware also spread alongside certain adware variants via a downloader disguised as an Adobe® Flash® Player update.

**When Popular Online Banking Crimeware Were Discovered**

![Graph showing the timeline of popular online banking crimeware from 2006 to 2013]

This quarter, we saw a resurgence of banking malware, which started making headlines with the introduction of the ZeuS toolkit way back in 2006.
MOBILE

Mobile Malware and High-Risk Apps: 1-Million Strong

Before 2013 ended, the number of malicious and high-risk apps targeting the Android platform reached the 1-million mark. Among these, 80% were malicious in nature, topped by premium service abusers. Premium service abusers are known to send unauthorized text messages to certain numbers and often register users to premium-rate services. This type of malicious app is especially popular in Russia, most likely due to the country’s lack of “standard” app stores.¹³

The remaining 20% were considered high-risk apps, including those that aggressively pushed ads to users, also known as “adware.” Adware infections eventually lead to device information theft.
Cross-Platform Threats Pose Mobile Security Risks

Beyond the dangers malicious apps posed, mobile devices were also hit by threats that transcended platforms. These include a fake WhatsApp email containing a link that, when clicked using a mobile device, may lead to a site that hosts a premium service abuser. This was not the first time that mobile devices were targeted by multi-platform threats. In this case though, the attackers opted to use spam as infection vector instead of relying on a more “direct” approach like blackhat search engine optimization (SEO) or social media abuse.

Another cross-platform issue was the rise of the number of phishing sites specifically designed for mobile devices. According to data we gathered from January to September this year, we noted a 53% increase in the number of phishing sites compared with the same period last year. This quarter, 42% of the sites spoofed banks and other financial institutions.
Vulnerabilities and Exploits
Compound Mobile Security Woes

The discovery of the “master key” vulnerability last quarter highlighted cybercriminals’ ability to find ways to “update” legitimate apps with malicious code to affect nearly every Android device. This quarter, we witnessed continued abuse of this vulnerability to churn out Trojanized versions of a well-known online banking app.  

The Black Hat cybersecurity conference last July additionally touched on other points pertaining to mobile security. A SIM card flaw that could allow attackers to obtain a digital key was, for instance, discovered. Also at the conference, researchers from the Georgia Institute of Technology showed off a proof-of-concept (POC) charger that could allow attackers to execute malicious commands on devices that ran on the latest iOS version.

Where Users Stumbled Upon Malicious and High-Risk Apps

While 27% of malicious and high-risk apps came from app stores, they were also seen in other sources like malicious sites. Note that the total only represents 42% of the overall number of malicious apps sourced from August 2010 to September 2013.
What Premium Service Abusers Do

Mobile devices are vulnerable to threats like information theft when infected by premium service abusers, which remained the top mobile threat type this quarter. Based on research covering the period, November 2012-May 2013, premium service abusers can affect devices in various ways.

- **DELETE DATA** can access your SD card data
  - 96%

- **MONITOR MESSAGES** can read your messages
  - 92%

- **SEND DEFAULT MESSAGES** can send out predefined messages
  - 86%

- **VIEW CONTACTS** can access your contact list
  - 48%

- **TRACK LOCATION** can track your location
  - 14%
DIGITAL LIFE

On Privacy and Data Theft: A New “Identity Crisis”

Recent events and threats surrounding social media and personal information paved the way for resurfacing issues on data security, also known as a new type of “identity crisis.” Internet users are still constantly being challenged by managing and preventing their personal information from falling into cybercriminals’ hands.

Among the numerous threats that aim to steal personal information, phishing scams made a notable impact this quarter due to a massive increase in Apple-related phishing sites. The spike was likely caused by the clamor for the latest Apple products and developments over the past few months, including rumors last May about the iOS 7 release. Another spike in the phishing site volume was seen last June and July when rumors about the iPhone 5c spread. Last September, we saw a spam run use the newly released iPhone models as lure to steal personally identifiable information (PII).19

The rise in Apple-related phishing pages continued even after the huge spike last May.
Mobile banking users were not spared from attacks that leveraged similar social engineering techniques. We found a phishing site that mimicked a well-known financial institution designed to gather crucial data like log-in credentials, email addresses, and even government-issued IDs.20

Security threats on social media persisted this quarter, most notably those that took advantage of users with rich digital lives. A “free followers” scam showed how cybercriminals made a quick buck by offering fake followers, “likes,” and retweets to interested buyers.21

Threats targeting social media were not limited to “free followers” scams this quarter. We also saw malware disguised as fake video player updates make the rounds on social networking sites. When installed, they hijacked users’ social media account credentials, specifically those for Facebook, Google+, and Twitter.22 This quarter was also plagued by a slew of fake Twitter accounts that lured followers to sites that supposedly hosted hacking tools for both Facebook and Twitter but instead led to survey scams.23

Despite these security setbacks, some positive developments pertaining to managing online accounts were introduced. These include the Touch ID fingerprint sensor on the iPhone 5s, a security tool meant to make it easier for owners to unlock their phones compared with using a PIN code.24 Though Apple’s effort to secure users’ online accounts was commendable, it must not be considered a cure-all because user behavior is still a crucial security factor.

Notable Social Engineering Lures Used

**SUMMER MOVIES**

- OBAMACARE
- WHATSAPP
- PLANTS vs. ZOMBIES
- ENDER’S GAME
- ROYAL BABY
- iPhone 5s and 5c
EXPLOITS AND VULNERABILITIES

Java Vulnerabilities Remain a Major Concern

After several zero-day incidents at the beginning of the year, Java vulnerabilities remained a crucial concern. This quarter, a Java 6 vulnerability exploit was included in the Neutrino Exploit Kit.\(^{25, 26}\) Because Oracle stopped supporting this version, all affected software will no longer receive security updates and fixes, including for the recently identified bug. Even worse, the Oracle announcement means that around 31 recently disclosed vulnerabilities will never be patched.

Just a week after the September Patch Tuesday, a zero-day Internet Explorer exploit that affected even the latest version was discovered.\(^{27}\) Microsoft immediately released a fix to address the issue though.

Old vulnerabilities remained a favorite cybercriminal target, as our research on Apache Struts showed.\(^{28}\) Our investigation revealed that the Chinese underground created automated tools to exploit bugs in older versions of Apache Struts, just three days after the flaws were made known to the public.

How Exploits Dodge Security

1. Crawl URL A
2. Check if IP address is in database
3. If IP address is not in database
4. Site loads
5. Crawl URL B
6. Check if IP address is in database
7. If IP address is in database
8. Site does not load

*Attackers keep a list of IP addresses they believe researchers use and block access from these.*
Targeted attack campaigns continued to go after various targets like governments, large organizations, and enterprises. Attackers typically aim to exfiltrate or steal data from targets. One such campaign that recently underwent some modifications was Sykipot.

The Sykipot campaign was first seen in 2007. It initially targeted industries like telecommunications, computer, government, and aerospace, among others but remains active to this day. We did observe recent changes to the campaign’s operations though, including using updated identifiers, drive-by exploits, and dynamic link library (DLL)/process injections. It now also targets civil aviation information.

While monitoring targeted attacks, we continued to see the use of old, patched vulnerabilities in spear-phishing attacks. One widely attacked vulnerability was the MSCOMCTL.OCX RCE Vulnerability, also known as “CVE-2012-0158,” which was addressed by Microsoft with MS12-027 as early as April last year.

Following the release of the latest Apache Struts version, meanwhile, we found automated tools that exploit vulnerabilities found in older versions of the software sold underground. We also saw some targeted attacks exploit the said bugs in Asia.

.PKZIP and .MIME files were the top file types threat actors used to attack their intended victims via spear phishing. Common file types like documents and spreadsheets were also used to gain entry to target networks.
Government agencies were the top attack targets this quarter, followed by telecommunications and IT/software companies. Enterprises should fortify their networks to avoid becoming a victim of targeted attacks.
Appendix

Top Spam Languages

1. English 89.39%
2. Chinese 2.49%
3. Japanese 1.88%
4. German 0.95%
5. Russian 0.70%
6. Portuguese 0.24%
7. Spanish 0.16%
8. French 0.08%
9. Icelandic 0.07%
10. Turkish 0.05%
Others 3.99%

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

Top Spam-Sending Countries

1. USA 9.16%
2. Argentina 6.71%
3. Italy 6.69%
4. Spain 6.45%
5. India 6.16%
6. Taiwan 4.31%
7. Colombia 4.26%
8. Peru 3.97%
9. Mexico 3.82%
10. Germany 3.27%
Others 45.20%

Consistent with the top spamming language, the USA sent out the most spam. Latin American countries like Argentina, Spain, Colombia, Mexico, and Peru remained part of the top 10.
Top Malicious Domains Blocked

<table>
<thead>
<tr>
<th>DOMAINS</th>
<th>REASONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ads.alpha00001.com</td>
<td>Hijacks well-known web browsers to redirect users to fake sites, including ad sites</td>
</tr>
<tr>
<td>trafficconverter.biz</td>
<td>Hosts and distributes worms, particularly DOWNAD/Conficker</td>
</tr>
<tr>
<td><a href="http://adsgangsta.com">http://adsgangsta.com</a></td>
<td>Related to exploit kit operations</td>
</tr>
<tr>
<td><a href="http://www.ody.cc">http://www.ody.cc</a></td>
<td>Related to sites hosting BKDR_HPGN.B-CN</td>
</tr>
<tr>
<td>az7t8.com</td>
<td>Involved in attacking high-traffic sites</td>
</tr>
<tr>
<td>ckstatic.com</td>
<td>Involved in attacking high-traffic sites</td>
</tr>
<tr>
<td>announce.opensharing.org</td>
<td>Hosted hacking software and used in peer-to-peer</td>
</tr>
<tr>
<td>promos.fling.com</td>
<td>Involved in a zombie network spread from an adult dating site.</td>
</tr>
<tr>
<td><a href="http://labambaka.com">http://labambaka.com</a></td>
<td>Hosts and distributes malware, related to spamming</td>
</tr>
<tr>
<td>international-spksz.ru</td>
<td>Hosts and distributes malware, related to spamming</td>
</tr>
</tbody>
</table>

The top malicious domains this quarter hosted sites that hijacked Web browsers to redirect users to fake ad sites. This most likely led to the increase in adware this quarter.

Number of Connections to Botnets per Month

- **JULY**: 12.7M connections
- **AUGUST**: 10.7M connections
- **SEPTEMBER**: 13.9M connections

The number of connections to botnets increased in July but dipped in August before rising again in September.
Malicious URL Country Sources

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>SHARE</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>24%</td>
</tr>
<tr>
<td>Netherlands</td>
<td>3%</td>
</tr>
<tr>
<td>China</td>
<td>3%</td>
</tr>
<tr>
<td>Germany</td>
<td>3%</td>
</tr>
<tr>
<td>France</td>
<td>3%</td>
</tr>
<tr>
<td>South Korea</td>
<td>2%</td>
</tr>
<tr>
<td>UK</td>
<td>2%</td>
</tr>
<tr>
<td>Russia</td>
<td>1%</td>
</tr>
<tr>
<td>Japan</td>
<td>1%</td>
</tr>
<tr>
<td>Canada</td>
<td>1%</td>
</tr>
<tr>
<td>Others</td>
<td>57%</td>
</tr>
</tbody>
</table>

Like last quarter, a significant share of the malicious URLs found this quarter were hosted in the United States.

Countries That Most Accessed Malicious URLs

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>SHARE</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>35%</td>
</tr>
<tr>
<td>Japan</td>
<td>14%</td>
</tr>
<tr>
<td>China</td>
<td>7%</td>
</tr>
<tr>
<td>India</td>
<td>4%</td>
</tr>
<tr>
<td>Taiwan</td>
<td>4%</td>
</tr>
<tr>
<td>South Korea</td>
<td>4%</td>
</tr>
<tr>
<td>Germany</td>
<td>3%</td>
</tr>
<tr>
<td>Australia</td>
<td>3%</td>
</tr>
<tr>
<td>Russia</td>
<td>2%</td>
</tr>
<tr>
<td>UK</td>
<td>2%</td>
</tr>
<tr>
<td>Others</td>
<td>22%</td>
</tr>
</tbody>
</table>

Most of the users that accessed malicious URLs were from the United States this quarter.
Countries with the Greatest Number of Botnet Connections

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>SHARE</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>25%</td>
</tr>
<tr>
<td>Malaysia</td>
<td>19%</td>
</tr>
<tr>
<td>Portugal</td>
<td>4%</td>
</tr>
<tr>
<td>Russia</td>
<td>4%</td>
</tr>
<tr>
<td>Canada</td>
<td>4%</td>
</tr>
<tr>
<td>South Korea</td>
<td>4%</td>
</tr>
<tr>
<td>Belgium</td>
<td>3%</td>
</tr>
<tr>
<td>Colombia</td>
<td>2%</td>
</tr>
<tr>
<td>Germany</td>
<td>2%</td>
</tr>
<tr>
<td>Netherlands</td>
<td>2%</td>
</tr>
<tr>
<td>Others</td>
<td>31%</td>
</tr>
</tbody>
</table>

The United States recorded the greatest number of connections to botnets this quarter. Malaysia slipped to second place, as the political tension subsided in the country.

Countries with the Highest Malicious Android App Download Volumes

- Ukraine: 13%
- Myanmar (Burma): 10%
- Libya: 9%
- Nigeria: 7%
- Vietnam: 5%
- Russia: 4%
- Argentina: 4%
- Antigua and Barbuda: 4%
- Canada: 3%
- India: 3%

Ukraine recorded the highest malicious app download volume, overtaking the UAE, which dropped out of the list. This could be attributed to the increased in popularity of smartphones in Eastern Europe. The mobile growth in Nigeria and Argentina could also be the reason for their inclusion. The ranking was based on the percentage of apps categorized as “malicious” over the total number of apps scanned per country. The ranking was, however, limited to countries with at least 10,000 scans.
This quarter, new entries like Kazakhstan, Uganda, and Ukraine topped the list of countries most at risk of privacy exposure. This could be partly due to the growing popularity of smartphones in the countries. The ranking was based on the percentage of apps categorized as “privacy risk inducers” over the total number of apps scanned per country. The ranking was, however, limited to countries with at least 10,000 scans.
References


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.