TrendLabs 3Q 2012 SECURITY ROUNDPUP

Android Under Siege: Popularity Comes at a Price
Smartphones are to the early 21st century what the PC was to the late 20th century—a universal tool valued for its productivity and fun factor but hated for the problems it can bring. Since smartphones are handheld computers that communicate, the threats they face are both similar and different from the PC challenges many of us are familiar with. Like the PC, many of today’s mobile malware prey upon the unwary. However, the nature of the mobile malware threat is, in some ways, very different.

Malware targeting Google’s Android platform increased nearly sixfold in the third quarter of 2012. What had been around 30,000 malicious and potentially dangerous or high-risk Android apps in June increased to almost 175,000 between July and September. This report will examine what led to the increase and what it means for users and developers alike.

We’ve seen nearly 175,000 malicious and high-risk Android apps to date and we’re still counting!
Also in this report:

- Dangerous zero-day exploits targeting Java and Internet Explorer (IE) were found. The IE vulnerability was used in an advanced persistent threat (APT) campaign.
- ZeroAccess malware, sometimes found on peer-to-peer (P2P) sharing sites, were the top infector in the computing public this quarter. The old DOWNAD/Conficker worm came a close second.
- PayPal attracted the most phishermen while Linkedin topped the list of chosen Blackhole Exploit Kit targets.
- See that spam? It likely arrived via Saudi Arabia (or India).
- Corporations and governments were still viable APT targets. Lurid and Nitro APT campaign improvements were also noted.
- Social media threats and privacy concerns lived on.

Trend Micro TrendLabs™ continuously monitors the threat landscape to raise security awareness and come up with proactive solutions for home users and organizations alike.

All of the figures contained in this report are based on Trend Micro™ Smart Protection Network™ data unless otherwise stated. The Smart Protection Network cloud security infrastructure rapidly and accurately identifies new threats, delivering global threat intelligence to secure data wherever it resides.
The number of malicious Android apps continued to increase. We also saw a significant rise in the number of aggressive mobile adware. Though most adware are designed to collect user information, a fine line exists between collecting data for simple advertising and violating one's privacy. Because they normally collect user information for legitimate purposes, they can serve as an effective means to gather more data than some would want to give out.


As predicted...

Smartphone and tablet platforms, especially Android, will suffer more cybercriminal attacks.
**Malicious Android Application Package Files**
- Still in the early stages of development\(^2\)
- Developed by the Luckycat APT campaign attackers
- Can execute commands sent from a remote command-and-control (C&C) server and collect device information


**Aggressive Mobile Adware**
- Known for aggressively displaying ads on affected devices to generate profit for app developers
- Tend to gather personal information without the users’ explicit knowledge or consent
- Significantly contributed to the rise in the number of malicious and high-risk Android apps led by variants that used legitimate ad networks to push malicious ads\(^3\)
- Some variants of which even pushed ads via notifications\(^4\)


The Obama vs Romney Android app, which served potentially unwanted ads, was downloaded as many as 1,000 times from Google Play alone.


“While it has been predicted that APT attackers will likely develop the capacity to attack targets via mobile devices, our discovery indicates that the development of such a capability is something they are pursuing.”


“At the end of the day... all mobile apps are essentially web clients; therefore, they are as unsecure as a browser and that’s how you should treat them.”

- David Sancho, senior threat researcher

Fake versions of legitimate Android apps are the most prevalent type of Android malware. This quarter, data stealers like Solar Charge and premium service abusers like Live Wallpapers in China or fake versions of best-selling apps that spread in Russia further raised concerns about the open nature of the Android ecosystem.

Note that the numbers in this chart are for all time and not just for this quarter.
Most mobile adware are simply a business model used to pay for an app offered for free or at low costs to users. But we also identified several adware that pose serious privacy-related threats. Apps that access your call history without informing you via an end-user license agreement (EULA) or their user interface (UI) constitute malicious behavior from a security perspective and are detected.

Ad networks present a unique challenge though. They connect advertisers to app developers that want to host ads for a fee. Unfortunately, the in-app libraries that ad networks provide sometimes gather more information than developers declare. While in some instances this oversight is unintentional, failure to alert users of data-gathering behavior introduces privacy risks.

App developers can either choose to closely examine ad libraries and ask their ad network to modify their code or rely on another ad network. We believe that the value of information stolen from users far outweighs the cost of due diligence on the side of developers and the ad networks that support them.

Even worse, we've now seen evidence of mobile apps being developed as targeted attack tools. Attackers are no longer just limiting their sights to computers as points of entry into target networks. Android's popularity has definitely not gone unnoticed. The fact that only 20% of Android device owners use a security app does not help. Using a solution that warns you of the potential problems certain apps can cause is one way to protect your data from thieving hands. In the end, you are responsible for the data you keep in your mobile device. Understand the permissions apps seek before giving them access to information that you may not even want to share.

5 http://fearlessweb.trendmicro.com/2012/misc/only-20-of-android-mobile-device-users-have-a-security-app-installed/
After more than six months, zero-day exploits again reared their ugly heads this quarter, proving they haven’t gone out of style. Aided by lack of discipline regarding patching for users and the difficulty of doing so for system administrators, exploits continued to wreak havoc. In 2011, we saw 1,822 critical vulnerabilities, which put a lot of organizations and company data at risk. Before the year ends, a new OS will come into the picture, which can be another venue for abuse.

While some reports have gone on to say that the zero-day exploit for CVE-2012-4681 may be used in targeted attacks, our analysis showed that this may not be the case... Targeted attacks are known for staying under the radar to successfully operate. The domains/IP addresses in this attack say the attackers have no intention of staying hidden.

— Manuel Gatbunton, threat response engineer

While some reports have gone on to say that the zero-day exploit for CVE-2012-4681 may be used in targeted attacks, our analysis showed that this may not be the case. Targeted attacks are known for staying under the radar to successfully operate. The domains/IP addresses in this attack say the attackers have no intention of staying hidden.

— Manuel Gatbunton, threat response engineer

Note that the numbers in this chart only show the volume of declared OS/software vulnerabilities.

Based on data available from http://cve.mitre.org/

Top 10 Vendors of Applications with the Most Number of Reported Vulnerabilities

- Apple
- Moodle
- Google
- Oracle
- Mozilla
- Cisco
- IBM
- Ffmpeg
- Adobe
- Microsoft

CVE-2012-4681

- A Java vulnerability exploited by a malicious .JAR/.class file, which allowed remote attackers to execute commands on vulnerable systems
- The zero-day exploit for which runs on all versions of IE, Mozilla Firefox, Opera, Google Chrome, and Safari
- The exploit for which also runs on Macs

CVE-2012-4969

- A vulnerability in IE versions 6 to 9
- The zero-day exploit for which loads malicious .SWF and .HTML files that download and execute PoisonIvy and PlugX variants
- A fix tool as well as an out-of-band security patch for which was released to ensure protection for affected users

Apple disclosed vulnerabilities in applications like Safari, iTunes, and iChat. Though it disclosed more product vulnerabilities than any other vendor, the data in the following chart does not include how severe the vulnerabilities reported were. In fact, despite the gap between the number of recorded vulnerabilities for Apple and Microsoft and the former’s increasing market share, the latter did suffer blows from the recently reported zero-day exploit attacks.
ZeroAccess malware, which have the ability to patch system files, rose in rank from third place in the second quarter to first place this quarter.\textsuperscript{12} We recorded more than 900,000 ZeroAccess malware detections to date. Backed by improvements to already-sophisticated cybercrime tools like the Blackhole Exploit Kit, more and more security risks are set to come into play.


\textit{As predicted...}

New threat actors will use sophisticated cybercrime tools to achieve their own ends.
ZeroAccess Malware

- May be hosted on P2P sharing sites, putting throngs of download aficionados at risk
- Has a new infection technique that patches system files with its variants
- Loads a malicious .DLL file along with the Adobe Flash Player installer, allowing the silent execution of the malware when Adobe Flash Player runs
- Accesses C&C servers to download other malicious components and monitor users’ activities

Blackhole Exploit Kit 2.0

- The development of which may have been triggered by the success of the slew of Blackhole Exploit Kit spam runs
- Announced in underground forums and via Pastebin posts in September
- Believed to be undergoing beta testing using a different URL format as one of the improvements to evade detection

Top 10 Blackhole Exploit Kit Targets

- Note that the numbers in this chart refer to the number of times each entity was used in a Blackhole Exploit Kit attack.

"The unusual combination (i.e., using Blackhole Exploit Kit 1.0 attack URLs and removing the plugindetect function in scripts) indicates that the authors of Blackhole Exploit Kit 2.0 may still be beta-testing specific features before fully releasing it into the wild."

- Jon Oliver, software architecture director

Blackhole Exploit Kits are web pages designed to try and exploit several vulnerabilities on a visitor’s computer. Once any of the exploits runs, the page serves up the end payload, usually a malware.
According to SpamRankings.net, the FESTI botnet uses SaudiNet for spamming activities, making Saudi Arabia, a newcomer, the top spam-sending country this quarter. Though Saudi Arabia was the top spam-sending country, that doesn’t mean the spammers live in it. They may just be taking advantage of the fact that Saudi Arabia-hosted IP addresses will not raise red flags as those of countries normally associated with cybercriminal activities as well as the likelihood that more botnets that send out spam exist in the country.

16 [http://www.spamrankings.net/about/newandnews.php/](http://www.spamrankings.net/about/newandnews.php/)
 Users end up on malicious sites by clicking links embedded in spam or ads displayed on the sites they visit.

<table>
<thead>
<tr>
<th>Malicious URL Blocked</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>trafficconverter.biz:80/antispyware/loadadv.exe</td>
<td>Distributes malware, particularly DOWNAD variants</td>
</tr>
<tr>
<td>trafficconverter.biz:80/</td>
<td>Distributes malware, particularly DOWNAD variants</td>
</tr>
<tr>
<td><a href="http://www.funad.co.kr:80/dynamic/adv/sb/searchnq_popu.html">www.funad.co.kr:80/dynamic/adv/sb/searchnq_popu.html</a></td>
<td>Poses security risks for compromised systems and/or networks</td>
</tr>
<tr>
<td>deepspacer.com:80/y2x8ms42fge0otk4yjhmzwwu4ztu5y2e4mtfjngewztqxnjmyodczfdxmxma==</td>
<td>Hosts malicious URLs, the registrant of which is a known spammer</td>
</tr>
<tr>
<td>tags.expo9.exponential.com:80/tags/burstmediacom/audienceeselectuk/tags.js</td>
<td>Engages in the distribution of malicious software</td>
</tr>
<tr>
<td><a href="http://www.trafficholder.com:80/in/in.php">www.trafficholder.com:80/in/in.php</a></td>
<td>Traffic site known for distributing malware</td>
</tr>
<tr>
<td>mattfoll.eu.interia.pl:80/logos.gif</td>
<td>Distributes Trojans</td>
</tr>
<tr>
<td><a href="http://www.luckytime.co.kr:80/item_data.php">www.luckytime.co.kr:80/item_data.php</a></td>
<td>Hosts malware</td>
</tr>
<tr>
<td>96.43.128.194:80/click.php</td>
<td>Distributes Trojans</td>
</tr>
<tr>
<td>am10.ru:80/code.php</td>
<td>Hosts adware and pop-ups that redirect to phishing sites</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Malicious Domain Blocked</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>trafficconverter.biz</td>
<td>Distributes malware, particularly DOWNAD variants</td>
</tr>
<tr>
<td><a href="http://www.funad.co.kr">www.funad.co.kr</a></td>
<td>Poses security risks for compromised systems and/or networks</td>
</tr>
<tr>
<td>deepspacer.com</td>
<td>Hosts malicious URLs, the registrant of which is a known spammer</td>
</tr>
<tr>
<td>tags.expo9.exponential.com</td>
<td>Engages in the distribution of malicious software</td>
</tr>
<tr>
<td>embed.redtube.com</td>
<td>Distributes malware and Trojans through videos</td>
</tr>
<tr>
<td>dl.baixaki.com.br</td>
<td>Distributes malware</td>
</tr>
<tr>
<td><a href="http://www.trafficholder.com">www.trafficholder.com</a></td>
<td>Traffic site known for distributing malware</td>
</tr>
<tr>
<td>oscex-en.url.trendmicro.co</td>
<td>Mistaken for the Trend Micro OfficeScan security suite site address</td>
</tr>
<tr>
<td>mattfoll.eu.interia.pl</td>
<td>Distributes Trojans</td>
</tr>
<tr>
<td><a href="http://www.luckytime.co.kr">www.luckytime.co.kr</a></td>
<td>Hosts malware</td>
</tr>
</tbody>
</table>
APTs upped the ante with the addition of malicious Android application package (APK) files, the file format used to distribute and install application software and middleware in Android OSs, as possible attack tools. Attackers, particularly those behind the Luckycat campaign, are adapting to the evolving threat landscape by developing malicious APK files as additions to their existing toolkits. Campaigns like Lurid and Nitro underwent operational changes, apart from using zero-day instead of older and more widely available exploits for attacks this quarter.


As predicted...

More hacker groups will pose a bigger threat to organizations that protect highly sensitive data.
**Enfal Malware**

- Infected 874 computers in 33 countries after prominently figuring in Lurid campaign attacks\(^{18}\)
- Known for communicating with specific servers that give potential attackers access to and even full control over infected systems
- Have been used in targeted attacks against government departments in Vietnam, Russia, and Mongolia as far back as 2006\(^{19}\)


**PlugX**

- A remote access Trojan (RAT) associated with Poisonivy malware, which are commonly used in targeted attacks\(^{20}\)
- Reportedly targets government organizations in various parts of Asia
- Arrives as an attachment to spear-phishing emails\(^{21}\)
- Exploits CVE-2010-3333, which was abused by a few APT campaigns like Luckycat and Taidoor\(^{22}\)


**Nitro Campaign**

- Used the Java zero-day exploit to enter target networks
- Attacks related to which continued even after the campaign’s exposure in 2011\(^{23}\)
- Proof that APT attackers also use zero-day exploits though not as often as more readily available ones to get into target networks


“Campaigns like Nitro don’t ‘come back,’ because they don’t go away. The Nitro attackers continued to be active after their activities were documented in 2011.”

— Nart Villeneuve, senior threat researcher


**Target Sector Distribution**

Most APT campaigns target organizations in the corporate/government sector because these handle more sensitive data than any other kind of organization\(^{24}\)

Despite the fact that billions of people use various social media sites, related privacy issues remain. We found that only 50% of Facebook users check their privacy settings every 2–3 months. They aren't likely to change their settings that often though. And so survey scams live on because the payoff—getting tons of personal data from users—is something the bad guys can’t pass up on.  


As predicted...

The new generation of young social networkers is more likely to reveal personal data to other parties such as in social networking sites.
**Tumblr Survey Scams**

- Trick users into giving out personal information via the fake TumViewer web app
- Also come in the guise of work-from-home job posts for those in search of additional income


**Fake WhatsApp for Facebook**

- Seen circulating via Facebook notifications and posts touting pages contacts liked
- When associated links are clicked, lead users to a page that requires them to give the fake app certain permissions


---

### The information you share can often answer security questions. What information do people share most?

- **63%** birthday
- **61%** school
- **51%** family members
- **48%** hometown
- **44%** favorite TV shows
- **38%** favorite musicians
- **33%** favorite books
- **26%** vacation plans
- **23%** pets' names

---

"Familiarize yourself with both the privacy settings and the security policies of any social and professional networking site you use. If you’re not happy with them, stop using the sites."

- Rik Ferguson, director of security research and communications


---

**TOP 5 SOCIAL ENGINEERING LURES**

---

"iPhone5 World Of Warcraft Obama London Olympics 2012"
TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers’ and partners’ needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com.

TRENDBLASSM

TrendLabs is a multinational research, development, and support center with an extensive regional presence committed to 24 x 7 threat surveillance, attack prevention, and timely and seamless solutions delivery. With more than 1,000 threat experts and support engineers deployed round-the-clock in labs located around the globe, TrendLabs enables Trend Micro to continuously monitor the threat landscape across the globe; deliver real-time data to detect, to preempt, and to eliminate threats; research on and analyze technologies to combat new threats; respond in real time to targeted threats; and help customers worldwide minimize damage, reduce costs, and ensure business continuity.

©2012 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.