TREND MICRO™

TrendLabs 2012 Mobile Threat and Security Roundup

# Repeating History

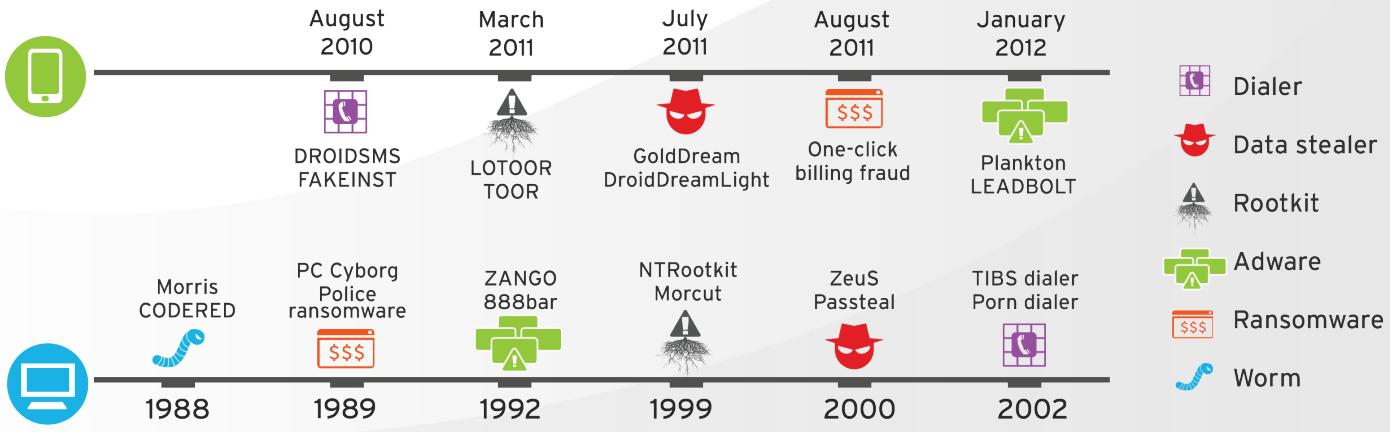
Android seems to be repeating history by way of Windows. The platform's growing dominance in the mobile landscape echoes that of Windows in the desktop and laptop space.[1] And much like Windows, Android's popularity is making it a prime target for cybercriminals and attackers, albeit at a much faster pace.

In 2012, we detected 350,000 malicious and high-risk Android app samples, showing a significant increase from the 1,000 samples seen in 2011. It took less than three years for malicious and high-risk Android apps to reach this number—a feat that took Windows malware 14 years.[2]

Just as Windows malware varied, so did Android malware—around 605 new malicious families were detected in 2012. Premium service abusers, which charge users for sending text messages to a premium-rate number, comprised the top mobile threat type, with transactions typically costing users US$9.99 a month.[3] And victims of mobile threats didn't just lose money, they also lost their privacy. The issue of data leakage continued to grow as more ad networks accessed and gathered personal information via aggressive adware.

Aggressive adware in mobile devices are now similar to the notorious spyware, adware, and click-fraud malware rampant in the early days of the PC malware era. They, like PC malware, generate profit by selling user data. PC malware took advantage of loopholes in legitimate ads and affiliate networks, while today's aggressive adware can cause data leakages that aren't always limited to malicious apps. Even popular and legitimate apps can disclose data.[4]

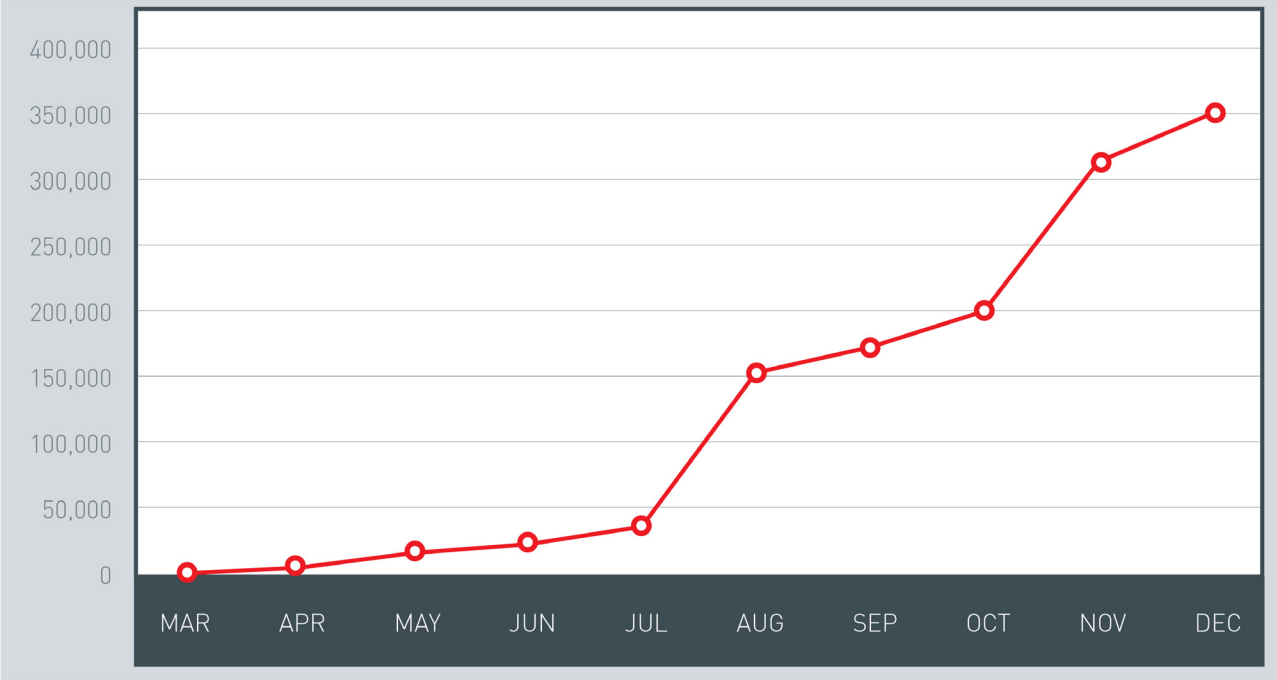
Android Versus PC Threat Type Timeline Comparison




We've seen the same kinds of threats in the early web threat days of PC malware appear in the Android malware landscape—all in roughly three years.

# The Mobile Threat Landscape

Android Threat Growth

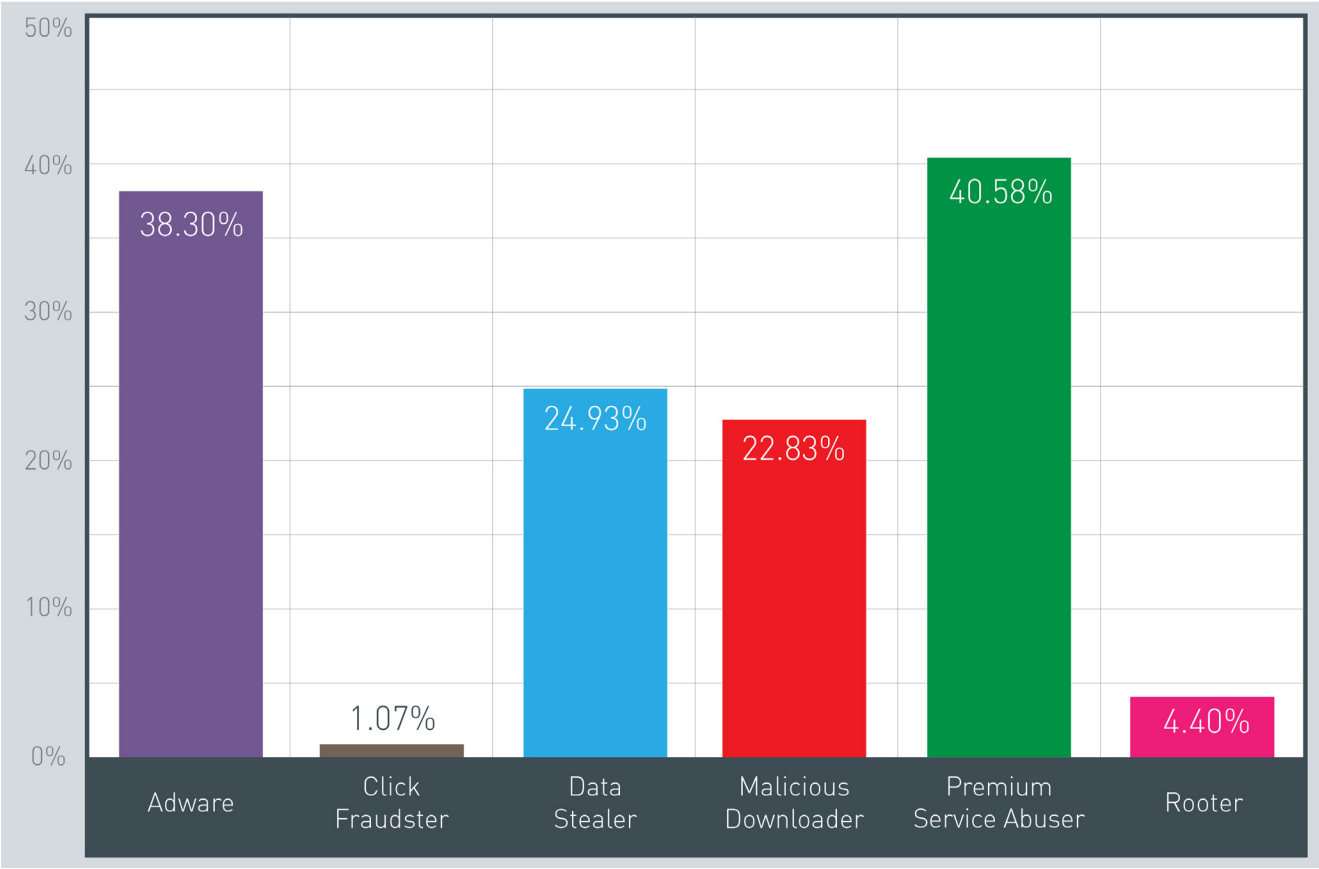



The increase in the number of detections in the latter part of 2012 was due to the rise of high-risk apps.

2012 saw an exponential increase in the number of detected Android malware, with 350,000 malicious samples by yearend. The number of detections spiked in the third quarter from 41,000 to 156,000 samples. The significant increase was due to the swell in aggressive adware.[5]

The growth of Android malware also indicates the speed by which cybercriminals are targeting multiple platforms. We released our "Annual Security Roundup: Evolved Threats in a 'Post-PC' World," which goes into more detail about the new post-PC threat environment.

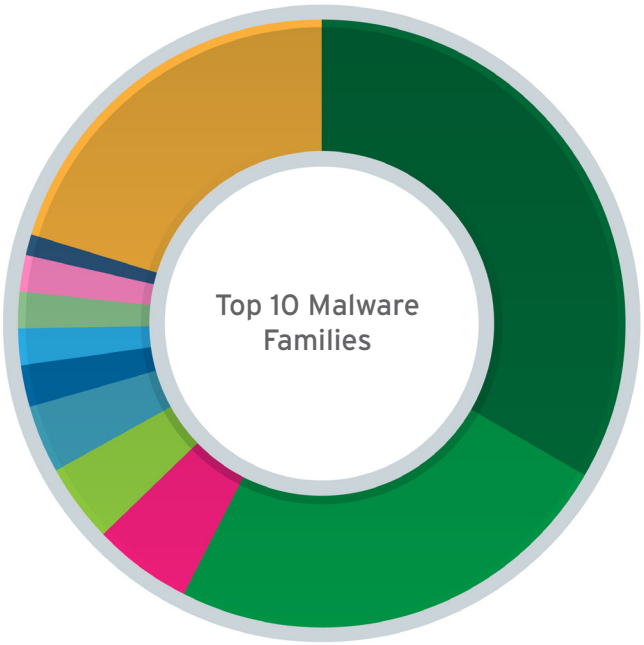
Distribution of Threat Types




Premium service abusers topped this year's list of most common malicious and high-risk Android app detections. They behave like the dialers of the desktop environment. Dialers call premium numbers and leave users with charges for calls to long-distance numbers or pay-per-call sites.

Cybercriminals may have favored premium service abusers because they are simpler to create and less risky to use compared with committing credit card fraud or distributing fake antivirus.

Premium service abusers also topped the list of most commonly seen Android malware in 2012. Often disguised as popular apps, they are designed to trick users into installing them. We spotted a rogue version of the game "Bad Piggies," which was actually a FAKEINST variant.[6] SMSBOXER variants spoof several best-selling Android apps, including "Angry Birds Space" and Instagram.[7] GAPPUSIN variants, meanwhile, download other malicious apps and steal information from infected devices.[8]



## Data Types Commonly Stolen

The information stolen by data stealers—one of the top threats this year—may be used by cybercriminals for malicious schemes. They can, for instance, take advantage of a user's contact list for SMS phishing or sell stolen information in the underground market. Some frequently stolen data include:

- Application Programming Interface (API) key—a value that authenticates service users
- Application ID
- Contact list
- International Mobile Station Equipment Identity (IMEI)—a number used to identify mobile devices
- International Mobile Subscriber Identity (IMSI)—a number used to identify subscribers in a network
- Location
- Network operator
- Phone ID and model
- Phone number
- Text messages

## Top 10 Countries with the Most Malicious Apps Downloaded


Nigeria was the country with the most malicious apps downloaded, followed by Peru and India. Other countries in the top 30 include New Zealand (17), Germany (24), and the U.S. (26).

The ranking was based on the percentage of apps rated as malicious over the total number of apps scanned per country. The ranking was limited to countries with at least 10,000 scans. The rating was based on the yearly analysis of real-time threat detection via Trend Micro™ Mobile Security Personal Edition.

# Notable Development in Mobile Malware

Mobile malware attacks showed increasing levels of sophistication. From traditional social engineering lures, cybercriminals developed new methods of victimizing users throughout the year. The introduction of new methods can lead to more complex attacks in the future.

Cybercriminals still favored social engineering. Rogue or Trojanized versions of popular apps like "Angry Birds Space" and Instagram were used to disguise premium service abusers.[9] Cybercriminals were quick to capitalize on new apps, too. As previously stated, fake versions of "Bad Piggies" appeared merely a month after the release of the legitimate version.[10] Cybercriminals sometimes met the demand for apps before legitimate vendors did. Fake Pinterest apps appeared in the market months before the official version came out. These fake apps were often hosted on Russian domains, with a domain for each fake app.

New attack methods were seen this year. In contrast to the typical routine of premium service abusers, a fake version of the GoWeather app logs in to a third-party app store to download paid apps and media without the user's knowledge.[11] A Trojanized security app was used together with the desktop threat, ZeuS, to steal Mobile Transaction Authentication Numbers (mTANs) from the text messages of online banking users. A photo app leveraged system exploits to allow remote attackers to gain administrator privileges on a device.

Threat actors are now expanding their targeted attacks to include mobile platforms. While monitoring a command-and-control (C&C) server connected to the Luckycat campaign, we discovered specific Android malware variants in the early stages of development.[12]

# Mobile Vulnerabilities

Software vulnerabilities have long been exploited by cybercriminals and attackers for their malicious schemes. For instance, zero-day vulnerabilities were exploited in attacks using the Blackhole Exploit Kit[13] and remote access Trojans (RATs).[14] But such vulnerabilities were no longer just limited to the desktop environment. Android vulnerabilities were also discovered in 2012, making affected devices possible new infection vectors. Patching mobile vulnerabilities may be difficult as some carriers or phone manufacturers are slow to release updates.[15] Older OS versions may not even receive updates—an issue similar to some Windows™ legacy systems.[16]

### Dialpad App Vulnerability

This vulnerability was found in the dialer app of certain smartphones. A vulnerable dialer app can directly execute Unstructured Supplementary Service Data (USSD) codes, including malicious ones, without prompting the user.[17] Cybercriminals can use this to remotely wipe data from a device.

### SMS Phishing Vulnerability

This vulnerability can allow a running app to send fake text messages to the user.[18] Attackers or cybercriminals can exploit this vulnerability to bypass user permissions. They can simply use fake text messages to solicit sensitive user information.

### Android Debug Bridge (ADB) Vulnerability

The ADB was created to allow developers to communicate with connected Android devices for debugging purposes. However, its implementation contained a vulnerability that can allow a malicious app to gain full control of a targeted app. Malicious apps can take advantage of this vulnerability to steal data and control the run-time behavior of its targeted app.

### Samsung Exynos Vulnerability

This vulnerability was found in a driver of certain Samsung devices. It allows any installed app to access the phone's memory.[19] Attackers can use this vulnerability to gain complete control of a device.

# Aggressive Mobile Adware and Other High-Risk Tools

App developers integrate advertising libraries to their apps to generate revenue. According to our research, over 90% of the free apps we found contained ad libraries—modules used by ad networks to push ads.

Though ad libraries are not inherently malicious, we found apps with ad libraries that try to gather data without explicitly notifying users. They also aggressively display ads, even via notifications. The aggressive display of ads is reminiscent of Windows adware, which have been plaguing desktops and laptops and annoying users with pop-up messages.

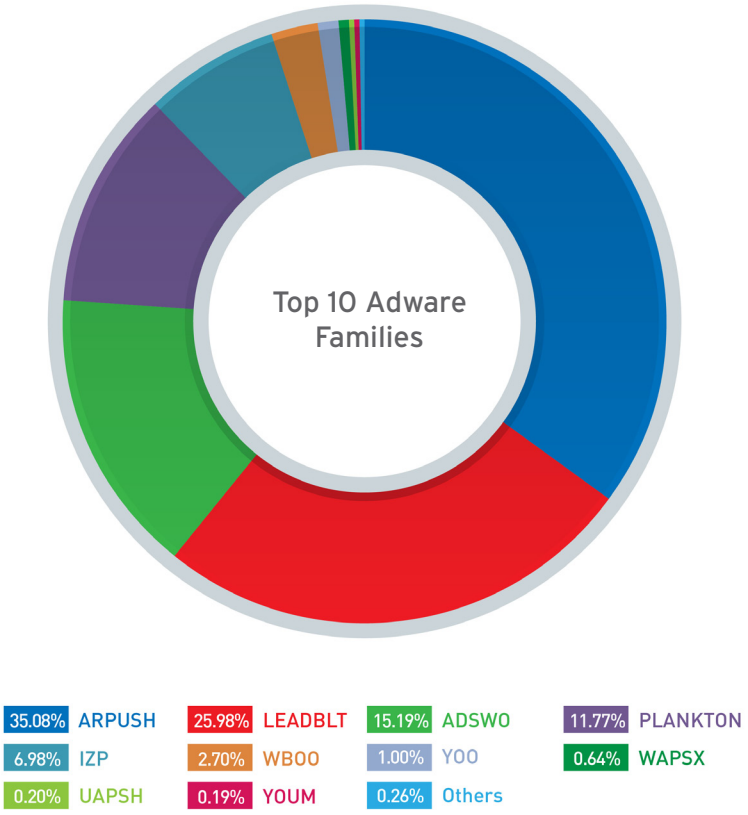
The prevalence of aggressive adware brought three major issues to light:

**Fraudulent text messages:** Ad networks sometimes send out ads in the form of fake text messages. This method tricks users to click ads.[20]

**User annoyance:** Some apps send out constant notifications or announcements. Not only does this annoy users, it also contributes to battery drainage.[21]

**Data leakage:** Ad libraries can collect sensitive data like GPS location, call logs, phone numbers, and device information.[22] One study found that some ad libraries even made personal information directly accessible to advertisers.[23] Ad libraries expanded the number of parties privy to private information, which can lead to misuse.

However, efforts have been made to remedy these issues. Some of the top mobile ad networks enforced compliance measures in line with Google's revised developer policy. Their new software developer kits (SDKs) had opt-in mechanisms, giving users the ability to either allow or forbid ad networks to collect data and display ads outside apps.




Aside from aggressive adware, other high-risk tools also became prominent this year. While not inherently malicious, these apps can be exploited by malicious individuals for their own gain. High-risk tools may be viewed as the mobile equivalent of PC grayware. They can track user data like device location, phone calls, and messages. One particular app, Spy Phone PRO+, gained notoriety because despite clearly stating its purpose, it was downloaded more than 100,000 times from Google Play.[24]

# Other Mobility Issues

Just as desktop and laptop users have concerns beyond malware, so do mobile users. Privacy is a concern for both platform users, given the amount of data sent online. Desktop and laptop users often worry about the speed and performance of their computers. Mobile users, meanwhile, are concerned with device battery consumption.

Early desktop users were rarely concerned with OS version updates as these often came several years in-between. Mobile users now face the task of regularly updating their devices as platform refreshes come in at a much faster rate.

### App Use and Privacy

App use has become the cornerstone for smartphone ownership. A Nielsen study showed that the number of apps U.S. smartphone users install increased from 32 in 2011 to 41 in 2012.[25] Research from Flurry revealed that the average amount of time spent on apps grew 35% in 2012.[26] But while apps continue to rise in popularity, users may not be aware that they can put personal data at risk.[27] Apps like "Angry Birds" and "Angry Birds Space" can access data like a phone's IMEI number and a user's location.

The issue of data access is made more difficult because each user has a different definition of privacy. What may seem invasive to one user may be viewed as routine by another. It is up to users to decide the how much information they are willing to disclose to their apps.

Top 10 Countries at Risk of Privacy Exposure


India topped the list, followed by Turkey and the Philippines. Other countries in the top 30 include Germany (15), Australia (16), and the U.K. (19).

The ranking was based on the percentage of apps rated as high-risk over the total number of apps scanned per country. The ranking was limited to countries with at least 10,000 scans. The rating was based on the yearly analysis of real-time threat detection via Trend Micro™ Mobile Security Personal Edition.

## Managing Battery Life

Privacy wasn't the only concern of users. A Trend Micro study found that battery drainage was the biggest smartphone concern of more than 60% of the respondents.[28] While users can tweak their device settings to lower power consumption, they fail to realize that app use also causes battery drainage.

A study by Purdue University and Microsoft stated that more energy is consumed by third-party ads in free apps than the apps themselves.[29] Recent findings from Trend Micro™ Longevity for Android™ app showed that 18% of the apps users downloaded rated "poor" in battery utilization.

### Top 10 Countries with the Most Battery-Draining Apps


The country with the most battery-draining apps is Thailand. Other countries in the list include Japan, Singapore, and the U.S.

The rating was based on yearly analysis of data collated via Trend Micro Longevity for Android. The ranking was limited to countries with at least 10,000 scans.

## Security by Mobile Platform

Performance and ease of use are not the only things now considered when buying a smartphone. Security has also become a major factor to consider, especially in the presence of mobile threats. In 2012, mobile OS vendors released platform refreshes with upgraded or new security and privacy features.

Apple has long taken an aggressive stance when it comes to securing its iOS platform. Its most recent version, iOS 6, gives users more control over their privacy. The new privacy settings let users decide which apps can access data like user location, contacts, photos, Bluetooth-shared files, Tweets, and Facebook posts. iOS 6 used Identifier for Advertisers (IFA) tracking technology, which allows users to switch off mobile tracking and be marked as unwilling participants in advertisers' data-gathering process. IFA only kept track of online habits, a marked difference from the previously used Unique Device Identifiers (UDIDs), which paired devices to users' personal information.

Jelly Bean 4.2, the latest version of the Android OS, offers users control over app access rights and access to files on a shared device. Jelly Bean had an improved setup that divided permissions into two categories—privacy and device access. It also came with real-time malicious app scanning that complemented Bouncer, a service that scans Google Play for potentially malicious apps.[30]

Windows 8 boasts of multiple layers of security, including three key security features—extended Information Rights Management (IRM) and automatic device encryption, real-time phishing filtering, and Kids Corner. Extended IRM and device encryption control the amount of access allowed to specific emails and documents hosted on a Windows server. Real-time phishing filtering uses Microsoft's SmartScreen URL reputation system to notify users every time they land on phishing sites. Kids Corner allows children access to only the apps and media content a parent selects.

# The Future of Android Malware

As the popularity of Android continues to grow, so will the number of threats its users face. The volume of malicious and high-risk Android apps will reach 1 million in 2013.[31] Aside from increasing in number, here are additional predictions about Android malware:

**New delivery methods:** Social networking apps now allow users to sync various social networking accounts. Malicious individuals will take advantage this feature to simultaneously post mobile malware links to different social networks.

QR codes will also be exploited by malicious individuals to spread Android malware.

**Combined mobile-desktop threats:** Android malware will also become part of attack chains involving desktop threats, particularly for attacks targeting online banking transactions.

**More devices (and more threats) in the workplace:** Bring your own device (BYOD) is fast becoming a norm for many organizations.[32] But rather than having uniform devices, users will opt to bring multiple devices that run on different platforms.[33] Cybercriminals and attackers will take advantage of the multiple devices and platforms at work to spread malware.

**More sophisticated malware:** Android malware will continue to evolve to avoid detection by security apps and bypass platform security measures. This evolution will come in the form of rootkits. Security researchers have published a proof-of-concept (POC) rootkit, which shows how rootkits can be used by malware authors to gain full control of a mobile device without being detected.[34]

**New targets:** More malware attacks will focus on new payment methods like near-field communications (NFC) to steal financial information.

# Protecting Your Mobile Devices

With the constant changes in the mobile threat landscape, smartphone owners should secure their devices. Here are some steps to protect devices against mobile threats:

- **Use your device's built-in security features.** Opt for phones that have security features and use them. Built-in security features like password, pattern, or PIN lock options prevent outsiders from accessing your data should your phone get misplaced or stolen.
- **Do research on apps before downloading them even from trusted sources.** Cybercriminals often disguise malware by spoofing popular apps. Familiarize yourself with details of popular apps (e.g., the name of the developer) to ensure that you download the legitimate version. It is advisable to download from reputable app stores like Google Play than third-party ones.
- **Read permissions before installing apps.** Malicious apps usually seek access to various kinds of data stored in a mobile device. Read permissions to check what type of actions an app will perform once installed. Be wary of apps that require more permissions than necessary (e.g., a calendar app that seeks access to your call logs).
- **Regularly check for software updates.** Software updates are usually released to address issues like vulnerabilities or improve software performance.
- **Invest in a security app.** Security apps can inform you if an app has malicious or suspicious behaviors. Some apps even protect data with features like remote wipe or privacy scanner.
- **Set BYOD policies at work.** Organizations should decide which employees will only be allowed to bring devices and what types of devices they will support. Set up procedures to take if a device is stolen, lost, or damaged.

## References


1 http://www.businesswire.com/news/home/20121101006891/en/Android-Marks-Fourth-Anniversary-Launch-75.0-Market
2 http://www.av-test.org
3 http://news.cnet.com/8301-27080_3-20048132-245.html
4 http://blog.trendmicro.com/trendlabs-security-intelligence/do-you-know-what-data-your-mobile-app-discloses/
5 http://about-threats.trendmicro.com/us/mobilehub/mobilereview/rpt_mothly_mobile_review_201209_the_growing_problem_of_mobile_adware.pdf
6 http://blog.trendmicro.com/trendlabs-security-intelligence/malicious-developers-released-rogue-bad-piggies-versions/
7 http://blog.trendmicro.com/trendlabs-security-intelligence/rogue-instagram-and-angry-birds-space-for-android-spotted/
8 http://blog.trendmicro.com/trendlabs-security-intelligence/1730-malicious-apps-still-available-on-popular-android-app-providers/
9 http://blog.trendmicro.com/trendlabs-security-intelligence/rogue-instagram-and-angry-birds-space-for-android-spotted/
10 http://blog.trendmicro.com/trendlabs-security-intelligence/malicious-developers-released-rogue-bad-piggies-versions/
11 http://blog.trendmicro.com/trendlabs-security-intelligence/android-malware-family-downloads-paid-media-and-apps/
12 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_adding-android-and-mac-osx-malware-to-the-apt-toolbox.pdf
13 http://blog.trendmicro.com/trendlabs-security-intelligence/java-zero-days-and-the-blackhole-exploit-kit/
14 http://blog.trendmicro.com/trendlabs-security-intelligence/new-ie-zero-day-exploit-leads-to-poisonivy/
15 http://blog.trendmicro.com/trendlabs-security-intelligence/dirty-ussds-and-the-android-update-problem/
16 http://windows.microsoft.com/en-US/windows/end-support-help
17 http://www.theregister.co.uk/2012/09/25/samsung_flaw/
18 http://www.theregister.co.uk/2012/11/08/android_vulnerability_in_adware/
19 http://blog.trendmicro.com/trendlabs-security-intelligence/exynos-based-android-devices-suffer-from-vulnerability/
20 http://blog.trendmicro.com/trendlabs-security-intelligence/164-unique-android-adware-still-online/
21 http://about-threats.trendmicro.com/us/mobilehub/mobilereview/rpt_mothly_mobile_review_201209_the_growing_problem_of_mobile_adware.pdf
22 http://about-threats.trendmicro.com/us/mobilehub/mobilereview/rpt-monthly-mobile-review-the-hidden-risk-behind-mobile-ad-networks-201212.pdf
23 http://www4.ncsu.edu/~mcgrace/WISEC12_ADRISK.pdf
24 http://blog.trendmicro.com/trendlabs-security-intelligence/17-bad-mobile-apps-still-up-700000-downloads-so-far/
25 http://blog.nielsen.com/nielsenwire/?p=31891
26 http://blog.flurry.com/bid/92105/Mobile-Apps-We-Interrupt-This-Broadcast
27 http://blog.trendmicro.com/trendlabs-security-intelligence/do-you-know-what-data-your-mobile-app-discloses/
28 http://fearlessweb.trendmicro.com/2012/misc/report-3rd-party-advertising-in-free-apps-drains-smartphone-battery-power/
29 http://research.microsoft.com/en-us/people/mzh/eurosys-2012.pdf
30 http://googlemobile.blogspot.com/2012/02/android-and-security.html
31 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/spotlight-articles/sp-trend-micro-predictions-for-2013-and-beyond.pdf
32 http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_forrester_measure-value-of-consumerization.pdf
33 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/spotlight-articles/sp-trend-micro-predictions-for-2013-and-beyond.pdf
34 http://www.reuters.com/article/2010/07/30/us-hackers-android-idUSTRE66T52020100730

## TREND MICRO INCORPORATED

Trend Micro Incorporated (TYO: 4704; TSE: 4704), 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 industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

TREND MICRO™

Securing Your Journey to the Cloud

## TRENDLABS℠

TrendLabs is a multinational research, development, and support center with an extensive regional presence committed to 24x7 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.

TrendLabs

Global Technical Support & R&D Center of TREND MICRO