SOPHOS

Security made simple.

# Sophos Mobile Security Threat Report

*Launched at Mobile World Congress, 2014*

By Vanja Svajcer, Principal Researcher, SophosLabs

# Contents

## 10 years of malware for mobile devices

**2004**

**Cabir**
First worm affecting Symbian Series 60 phones. Spreads from phone to phone by using Bluetooth OBEX push protocol.

**2009**

**Ikee and Duh**
Worms affecting jailbroken iPhones using Cydia app distribution system due to a hardcoded password in sshd.

**2010**

**FakePlayer**
First malware for Android makes money by sending SMS messages to premium line numbers in Russia.

**2011**

**DroidDream**
First large attack to Google Play market. Over 50 apps containing a root exploit published to Android Market.

**2012**

**Zitmo**
Popular Windows bot and banking malware Zeus improved with its Android component designed to steal banking mTANs.

**2013**

1000 new Android malware samples discovered every day

**Masterkey**
A vulnerability in Android discovered exploiting certificate validation in Android which allows malware to disguise as a legitimate app.

**2014**

2000 new Android malware samples discovered every day

**DownAPK**
Windows based malware uses Android debugging bridge to install fake banking app to Android devices connected to the infected PC.

## Introduction

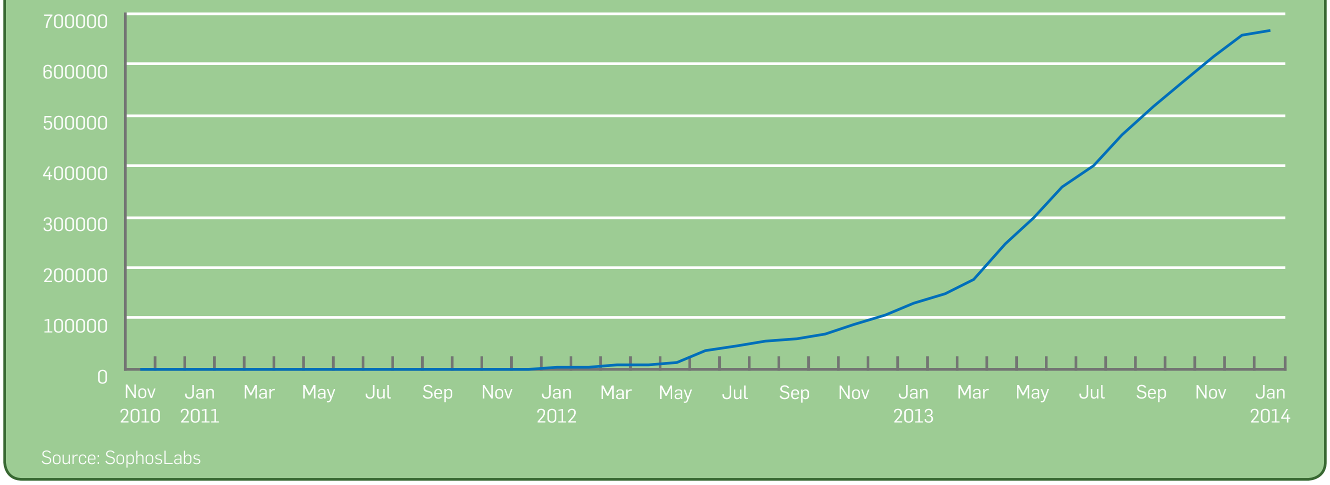
It's been 10 years since the arrival of the first mobile malware in 2004, but it is only within the past few years that it has become a true threat to end users. Indeed, the rapid growth in smartphone and tablet usage over the past two years has led to the inevitable rise in targeting of these devices by cybercriminals. The exponential growth in Android devices—and the buoyant and largely unregulated Android app market—produced a sharp rise in malware targeting that platform.

To date SophosLabs has seen well over 650,000 individual pieces of malware for Android—a tiny fraction of the number of pieces of malware out there for the traditional PC, but a growing threat. Android malware has grown quickly in a short space of time and looks set to keep growing apace with our use of mobile devices.

## Huge Growth in Smartphones and Tablets

With mobile subscriptions worldwide totalling approximately 7 billion by the end of 2013, it is clear that mobile devices are rapidly replacing the personal computer at home and in the workplace. We now rely on smartphones and tablets for everything Internet-related in our lives, from web surfing to e-commerce transactions and online banking. Therefore, in the space of little more than a year or so, we have gone from talking about them as an emerging threat vector, to one which is already being consistently exploited by cybercriminals. They have rapidly become a potential treasure trove of personal data for the cyber criminal and also represent an easy way to get to end users, through social engineering techniques such as fake antivirus, which trick users into paying to get rid of non-existent malware.

**Fig. 1 Cumulative Android Malware Samples through January 2014**



Source: SophosLabs

The graphic in figure 2 shows mobile and desktop threat exposure (TER), measured as the percentage of PCs and mobile devices that experienced a malware attack, whether successful or failed, over a period of three months. The graph only shows malware attempts on devices protected by Sophos, but it's revealing that, while the majority of malware is still found on the desktop, in some countries, mobile malware is becoming a big phenomenon.

The Russian Federation is a special case, in that Russian cybercriminals are particularly active around mobile and much mobile malware is therefore targeted at Russian users. In particular, Russian cybercriminals are very active around SMS-based senders charging premium rates. Families like Boxer (see the top 10 Android malware families graph in figure 3) have been around for several years and yet still make up 25% of all Android malware seen to date.

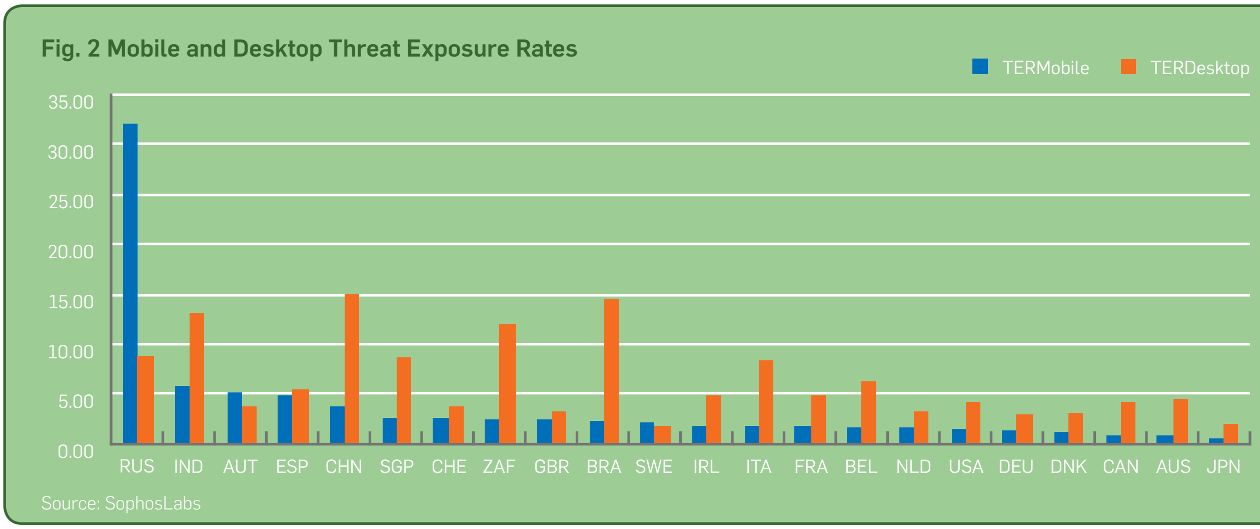
India, Austria, Spain and China also have a high TER when it comes to mobile (see figure 2).

## Android vs. iOS

Mobile malware writers know the best way to infect as many devices as possible is to attack central app markets. Therefore, today the most likely way that malware will find its way onto a mobile device is through downloading a malicious app that hasn't been sufficiently vetted. The cybercriminals plant applications that include hidden (obfuscated) malicious functionality in an attempt to avoid detection included in the vendor's application vetting process.

Inevitably, Google's Android platform has become a much greater target for mobile malware writers than Apple iOS because, unlike Apple, it does not employ a walled garden policy with regard to apps. It's also significant that Android has a large proportion of the mobile market—up to 79% in 2013, according to Strategy Analytics.[1]

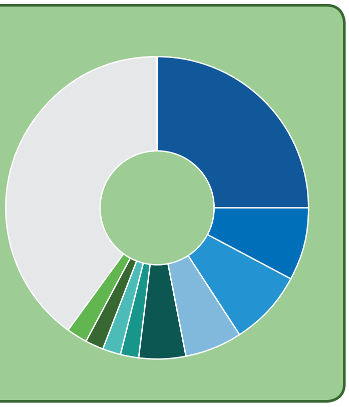
**Fig. 2 Mobile and Desktop Threat Exposure Rates**



Source: SophosLabs

**Fig. 3 Top 10 Android malware families discovered**

| | | | | | |
|---|---|---|---|---|---|
| ● Andr/Boxer-D | 25% | ● Andr/FakeIns-D | 5% | ● Andr/Wkload-A | 2% |
| ● Andr/Opfake-C | 8% | ● Andr/SMSSend-J | 2% | ○ Other | 40% |
| ● Andr/FakeIns-B | 8% | ● Andr/Opfake-H | 2% | | |
| ● Andr/MTK-C | 6% | ● Andr/Spy-L | 2% | | |



Note: Percentages rounded to nearest whole percent
Source: SophosLabs

[1] Engadget, http://www.engadget.com/2014/01/29/strategy-analytics-2013-smartphone-share/

### Apple

Apple's walled garden App Store—where applications are fully vetted before being made available to customers—has prevented widespread malware infection of iOS users. As a centralized point of distribution, the App Store provides users with confidence that the apps they download have been tested and validated by Apple.

Evidence of malicious malware showing up in the App Store is anecdotal at best, as Apple does not typically volunteer such information. However, it's safe to assume that since Apple does not make APIs available to developers, the iOS operating system has fewer vulnerabilities, even if it's not 100% invulnerable.

### Google and Android

Like Apple, Google provides a centralized market for mobile applications called Google Play. However, that is offset by the Android's ability to install apps from third-party sources. Some are well-known and reputable such as Amazon. Others are not, and originate from malware hotspots in Russia and China. The criminal developers deconstruct and decompile popular apps like Angry Birds, and publish malicious versions and make them available for free.

## Types of Attack: How a Hacker Profits

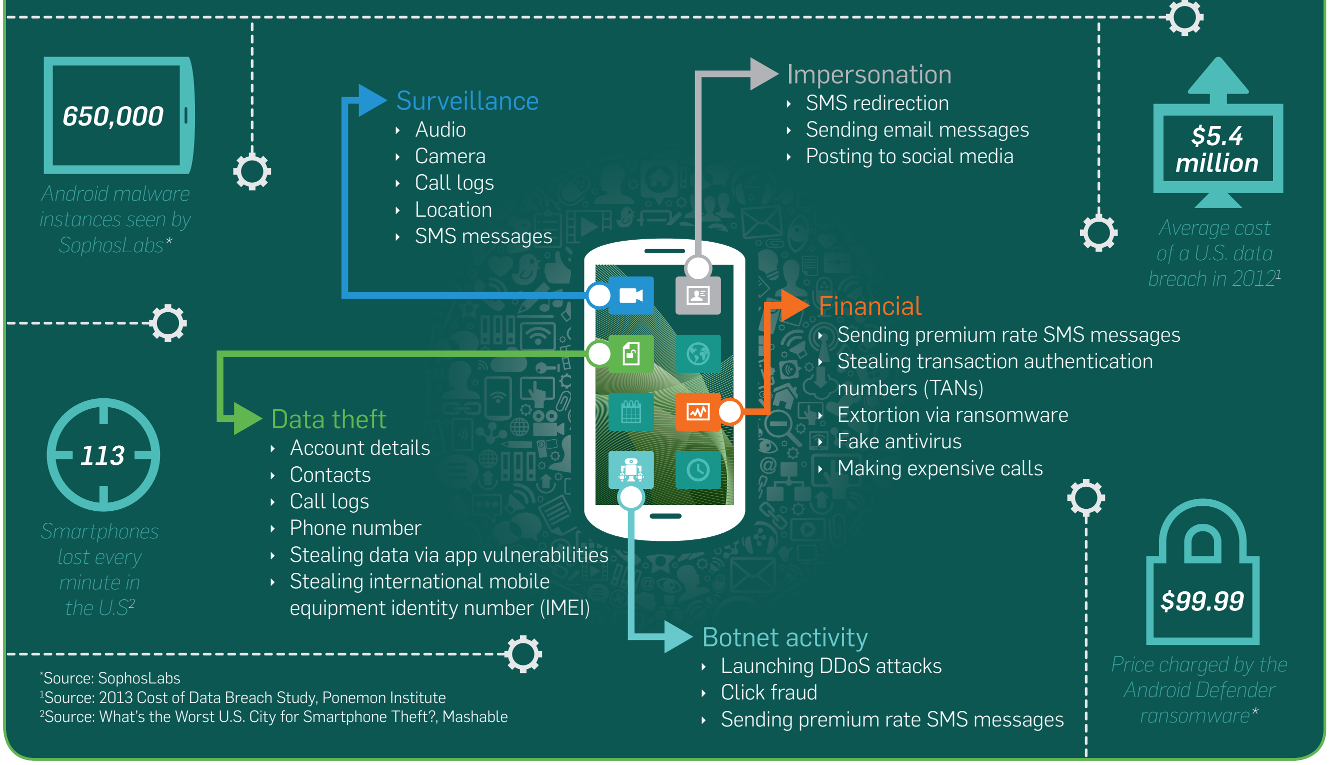
The infographic Anatomy of a Hacked Mobile Device (figure 4) shows the many different ways that a hacker can profit from a compromised mobile device. Some of these, such as ransomware, fake AV, botnet activity and data theft, have migrated from the traditional PC.

However, because of the nature of mobile devices, they are also open to new types of attack. For example, cybercriminals saw the value early on of using malicious mobile apps to send text messages to premium mobile phone numbers, racking up unauthorized charges. And, their very portability obviously makes them vulnerable to being physically lost and the potential data loss as a result if the device is not encrypted or properly secured.

Today, the evolution of mobile banking poses a potentially even greater risk for users. Because today's powerful mobile devices make it easy for users to conduct financial transactions on the move, they're already being actively targeted by malware designed to steal data and money. Therefore, protecting your smartphone from malware and keyloggers has to be a basic principle of secure mobile banking.

**Fig. 4 Anatomy of a Hacked Mobile Device: How a hacker can profit from your smartphone**

Your Android smartphone may look innocent. But when compromised by malware, it can illegally watch and impersonate you, participate in dangerous botnet activities, capture your personal data, and even steal your money.



**650,000**

*Android malware instances seen by SophosLabs**

Surveillance
- Audio
- Camera
- Call logs
- Location
- SMS messages

Impersonation
- SMS redirection
- Sending email messages
- Posting to social media

**$5.4 million**

*Average cost of a U.S. data breach in 2012*[1]

Financial
- Sending premium rate SMS messages
- Stealing transaction authentication numbers (TANs)
- Extortion via ransomware
- Fake antivirus
- Making expensive calls

**113**

*Smartphones lost every minute in the U.S*[2]

Data theft
- Account details
- Contacts
- Call logs
- Phone number
- Stealing data via app vulnerabilities
- Stealing international mobile equipment identity number (IMEI)

Botnet activity
- Launching DDoS attacks
- Click fraud
- Sending premium rate SMS messages

**$99.99**

*Price charged by the Android Defender ransomware**

*Source: SophosLabs
[1] Source: 2013 Cost of Data Breach Study, Ponemon Institute
[2] Source: What's the Worst U.S. City for Smartphone Theft?, Mashable

## Android Malware – Mutating and Getting Smarter

Since we first detected Android malware in August 2010, we have recorded well over 300 malware families and more than 650,000 individual pieces of Android malware. The Android malware ecosystem is in many ways following the paths first established years ago by Windows malware.

Recently, we have seen great innovation in how Android malware seeks to avoid and counter detection methods. Ginmaster is a case in point. First discovered in China in August 2011, this Trojanized program is injected into many legitimate apps that are also distributed through third-party markets.

In 2012, Ginmaster began resisting detection by obfuscating class names, encrypting URLs and C&C instructions, and moving toward the polymorphism techniques that have become commonplace in Windows malware. In 2013, Ginmaster's developers implemented far more complex and subtle obfuscation and encryption, making this malware harder to detect or reverse engineer. Meanwhile, with each quarter since early 2012, we have seen a steady growth in detections of Ginmaster, reaching nearly 7500 samples by the end of January 2014.

### New Android botnets

In late 2013, reports surfaced of a large-scale botnet controlling Android devices in much the same way botnets have controlled PCs. This botnet, which Sophos detects as Andr/GGSmart-A, thus far seems limited to China. It uses centralized command and control to instruct all of the mobile devices it has infected; for example, to send premium SMS messages that will be charged to the device owner. Unlike typical Android attacks, it can change and control premium SMS numbers, content, and even affiliate schemes across its entire large network. This makes it better organized, and potentially more dangerous, than much of the Android malware we've seen before.

### Ransomware comes to Android

Ransomware has a long history—the first versions were detected 25 years ago. For those unfamiliar with it, ransomware makes your files or device inaccessible, and then demands a payment to free them. In June 2013, Sophos researcher Rowland Yu discovered a ransomware attack against Android devices. Called Android Defender, this hybrid fake antivirus/ransomware app demands a $99.99 payment to restore access to your Android device.

Upon starting, Android Defender uses a variety of social engineering tactics and an unusually professional look and feel to repeatedly seek device administrator privileges. If given those privileges, it can restrict access to all other applications, making it impossible to make calls, change settings, kill tasks, uninstall apps, or even perform a factory reset. It presents a warning message about infection that is visible on screen, no matter what a user is doing. It can even disable Back/Home buttons and launch on reboot to resist removal. About the only thing it doesn't do is encrypt your content or personal data.

### Bank account theft, delivered via smartphone

In September 2013, we detected a new form of banking malware that combines conventional browser attacks against Windows with social engineering designed to compromise Android devices and complete the theft via smartphone. SophosLabs detects this malware as Andr/Spy-ABN—and although we are encountering relatively low levels of this malware, it has already targeted French, Dutch and Indian financial institutions.

Like its predecessor Zeus, Andr/Spy-ABN begins on the Windows side, injecting code into Internet Explorer to intercept user information before it's encrypted and forwarded to financial institutions. It also captures browser personal certificates and cookies. Once authenticated, users are told that their bank now requires the use of a new smartphone app as an anti-fraud measure (how ironic). The user is asked for his/her phone number and model, and an SMS is sent, linking to a download of the malicious app. If this isn't bad enough, the injected code even blocks users from accessing their accounts until the smartphone malware has been installed and provides an activation code.

Some financial organizations now require malware protection to be in place before customers can register for online banking. Encrypting all data on a mobile device, and securing that device with a PIN creates an additional barrier in case the device is lost or stolen.

The second challenge is around user authentication of the mobile banking application, the weak link in what was otherwise a very convenient service. User passwords are easy to guess, and continuously sophisticated and targeted phishing attacks tricked users into giving up their usernames/passwords and the keys to the kingdom and their financial assets.

Most financial organizations today require multi-factor authentication via security tokens and other mechanisms. For twofactor authentication (2FA), it is not only what you know (i.e., a password), but also what you possess (i.e., a token) that are necessary to access sensitive information, adding a significant layer of security. This carries some cost in convenience, but is worth it at the end.

### PUAs: Growing as app writers aggressively seek to monetize

Although not malware, potentially unwanted applications (PUA) are thriving on Android, as you can see from the cumulative graph showing PUA growth (figure 5). PUAs are Android apps that may not strictly qualify as malware, but may nevertheless introduce security or other risks.

Many users may carelessly install apps that link to aggressive advertising networks, can track their devices and locations, and may even capture contact data. These apps make money simply by serving pornographic or other inappropriate advertising up to users.

Companies may wish to eliminate third-party apps due to the information they expose, or because they may have a duty of care to protect employees from inappropriate content and a potentially hostile work environment.

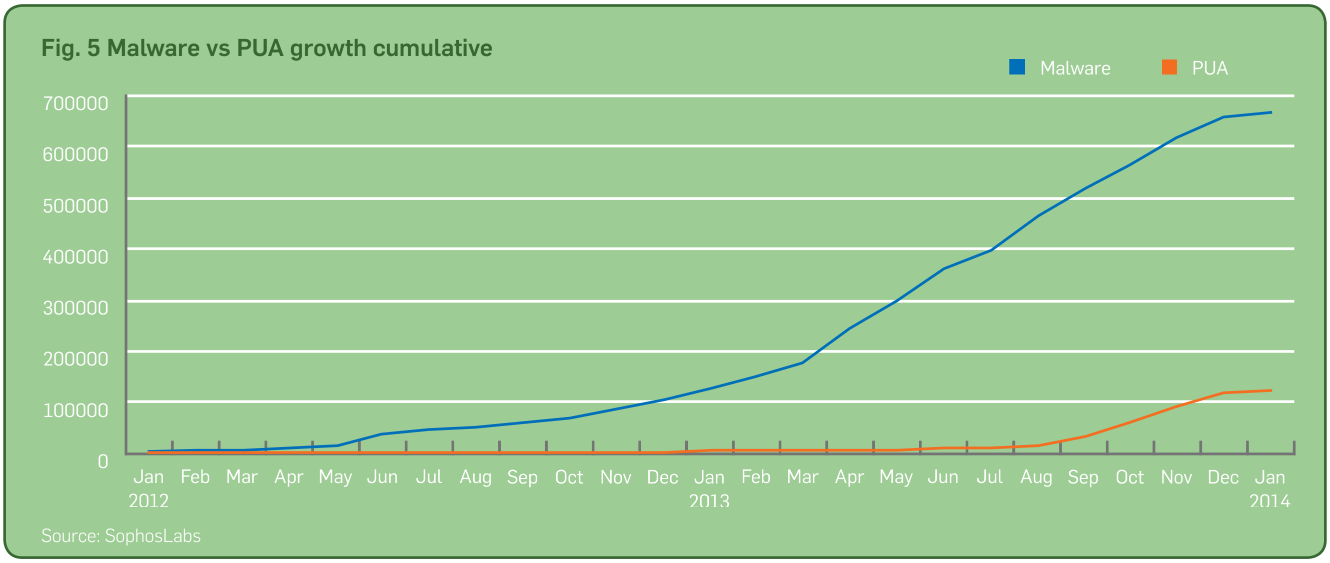
### Securing Android

Google has taken some significant steps to further secure the Android platform recently. First, Android 4.3 eliminated the feature where Android application packet (APK) files would be automatically downloaded from third-party sources when the default Android browser app was used. This was a natural security hole for drive-by download attacks introduced by Android design.

Second, Google has tightened its Developer's Agreement, especially as it relates to PUAs, which aren't unmistakably malware but which behave in ways far more intrusive than most users desire.

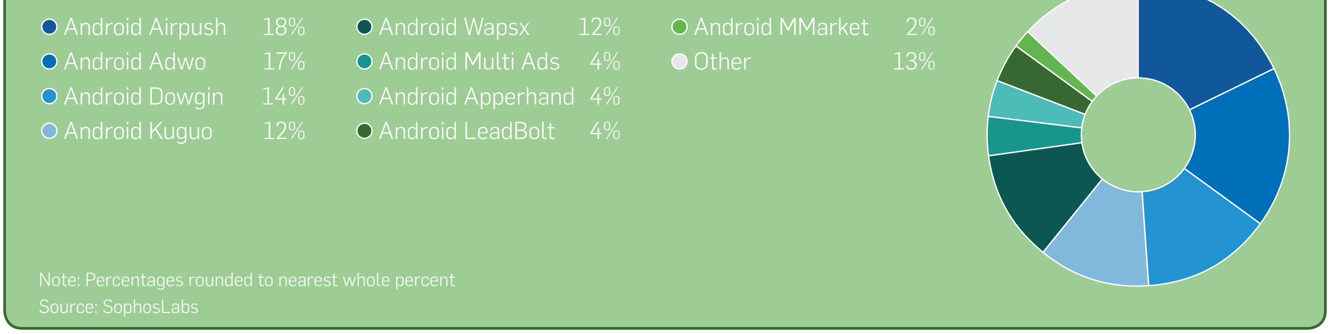
Google has identified several app and ad framework behaviors that will no longer be permitted. For example, developers can no longer place third-party advertising and links on the home screen, change the browser home page, or use the system notification area for purposes unrelated to their useful functionality.

**Fig. 5 Malware vs PUA growth cumulative**



Source: SophosLabs

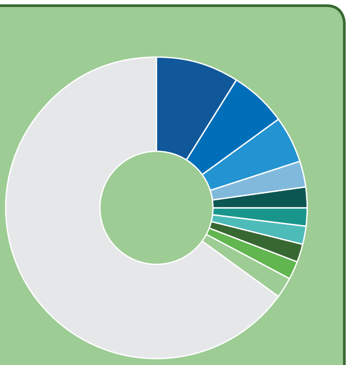
**Fig. 6 Top Android PUAs discovered**



Note: Percentages rounded to nearest whole percent
Source: SophosLabs

**Fig. 7 Most Widespread Android Malware Detections, October 2013**

While no single Android malware family is currently dominant, today's most widely detected Android malware is Andr/BBridge-A. This Trojan uses a privilege escalation exploit to install additional malicious apps on your device. Andr/BBridge-A has demonstrated real staying power—it was second on our list of Android infections way back in June 2012.



| | | | | | |
|---|---|---|---|---|---|
| ● Andr/BBridge-A | 9% | ● Andr/Adop-A | 2% | ● Andr/SmsSend-BE | 2% |
| ● Andr/Fakeins-V | 6% | ● Andr/Boxer-D | 2% | ○ Andr/MTK-B | 2% |
| ● Andr/Generic-S | 5% | ● Andr/SmsSend-BY | 2% | ● Other | 65% |
| ● Andr/Qdplugin-A | 3% | ● Andr/DroidRt-A | 2% | | |

Note: Percentages rounded to nearest whole percent
Source: SophosLabs

## Mobile Malware in 2014: What to Expect

### 1. Android malware, increasingly complex, seeks out new targets

In 2013 SophosLabs saw exponential growth in Android malware, not only in terms of the number of unique families and samples, but also the number of devices affected globally. While we expect that new security features in the Android platform will make a positive change in infection rates over time, their adoption will be slow, leaving most users exposed to simple social engineering attacks.

Cybercriminals will continue to explore new avenues for Android malware monetization. Although their options on this platform are more limited than Windows, mobile devices are an attractive launching pad for attacks aimed at social networks and cloud platforms. Mitigate this risk by enforcing a BYOD policy that prevents side-loading of mobile apps from unknown sources and mandates anti-malware protection.

### 2. Personal data danger from mobile apps and social networks

Mobile security in general will continue to be a hot topic in 2014. The continuing adoption of emerging apps for personal and business communication widens the attack surface, particularly for social engineering scams and data exfiltration attempts. Your address book and your social connections graph is a treasure for cyber-crooks of all sorts, so be mindful of whom you entrust to access it and why. Mobile and web applications control for business users will help mitigate this risk.

### 3. Additional security needs to be built in to remove burden from user

Mobile devices are increasingly being used for banking and other online transactions. Since it is in the interests of both financial organizations and end users alike to increase this everyday use, it seems likely that additional security layers will need to be built into mobile devices to remove the security burden from the end user and provide a truly secure experience.

## 10 Tips to Prevent Mobile Malware

Users can take some fairly simple steps to protect their mobile devices. The following 10 tips are aimed at organizations needing to secure their mobile users and prevent mobile malware infections on company or BYOD devices. Equally, many of these tips apply to everyday consumers, who should also protect their personal devices.

### 1. Inform users about mobile risks

A mobile device is a computer and should be protected like one. Users must recognize that applications or games could be malicious, and always consider the source. A good rule of thumb: if an app is asking for more information than what it needs to do its job, you shouldn't install it.

### 2. Consider the security of over-the-air networks used to access company data

Generally speaking, over-the-air (i.e., Wi-Fi) networks are insecure. For example, if a user is accessing corporate data using a free Wi-Fi connection at an airport, the data may be exposed to malicious users sniffing the wireless traffic on the same access point. Companies must develop acceptable use policies, provide VPN technology, and require that users connect through these secure tunnels.

### 3. Establish and enforce BYOD policies

BYOD should be a win-win for users and companies, but it can result in additional risk. Ask yourself: How do I control a user-owned and managed device that requires access to my corporate network? Employees are often the best defense against the theft of sensitive data. Employees using their own mobile devices must follow policies that keep the business compliant with regulatory requirements.

### 4. Prevent jailbreaking

Jailbreaking is the process of removing the security limitations imposed by the operating system vendor. To "jailbreak" or to "root" means to gain full access to the operating system and features. This also means breaking the security model and allowing all apps, including malicious ones, to access the data owned by other applications. In brief, you never want to have root-enabled or jailbroken devices in your company.

### 5. Keep device operating systems up to date

This sounds easier than it actually is. In the Android ecosystem, updates can be blocked a number of ways: by Google (which updates the operating system); by the handset manufacturer (which may decide to release updates only for the latest models); or by the mobile provider (which may not increase bandwidth on their network to support updates). Without the ability to update your Android OS, your device is vulnerable to potential exploits. Research mobile providers and handset manufacturers to know which ones apply updates and which don't.

### 6. Encrypt your devices

The risk of losing a device is still higher than the risk of malware infection. Protecting your devices by fully encrypting the device makes it incredibly difficult for someone to break in and steal the data. Setting a strong password for the device, as well as for the SIM card, is a must.

### 7. Mobile security policies should fit into your overall security framework

IT needs to strike a balance between user freedom and the manageability of the IT environment. If a device does not comply with security policies, it should not be allowed to connect to the corporate network and access corporate data. IT departments need to communicate which devices are allowed. And you should enforce your security policy by using mobile device management tools.

### 8. Install apps from trusted sources; consider building an enterprise app store

You should only permit the installation of apps from trusted sources, such as Google Play and Apple App Store. However, companies should also consider building enterprise application stores to distribute corporate custom apps and sanctioned consumer apps. Your chosen security vendor can help set up an app store and advise which applications are safe.

### 9. Provide cloud-sharing alternatives

Mobile users want to store data they can access from any device, and they may use services without the approval of IT. Businesses should consider building a secure cloud-based storage service to accommodate users in a secure way.

### 10. Encourage users to install anti-malware on their devices

Although malware exists for iOS, BlackBerry and platforms supporting Java Micro Edition, those operating system interfaces don't support anti-malware. However, the risk of infection is highest for Android, where security software is already available. Make sure all your Android devices are protected by anti-malware software.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK | Boston, USA

SOPHOS