SOPHOS

# When Malware Goes Mobile: Causes, Outcomes and Cures

By **Vanja Svajcer,** Principal Researcher, SophosLabs

Malicious software—commonly referred to as "malware"—mainly targets desktop PCs. But cybercriminals are increasingly setting their sights on smartphones and other mobile devices. In spite of preventative measures like Apple's walled garden and Google's Bouncer application for Android, malware impacts both iOS and Android platforms. This paper includes step-by-step, platform-specific policies and strategies you can employ to protect your data and keep mobile devices safe from the malware writers determined to break into them.

## The smartphone as emerging threat vector

With mobile subscriptions totaling 6 billion by the end of 2011,[1] one thing remains very clear. Mobile devices are rapidly replacing the personal computer at home and in the workplace. We rely on smartphones and tablets for everything Internet-related in our lives, from web surfing to ecommerce transactions to online banking.

Because of our increasing reliance on mobile devices, they represent an emerging threat vector ready to be exploited by cybercriminals. They are also open to new classes of attack. For example, criminals often use malicious mobile apps to send text messages to premium mobile phone numbers, racking up unauthorized charges.

We can expect the threat vector to increase exponentially as mobile devices are used more frequently to make payments. In August 2012, rival U.S. coffee chains Starbucks[2] and Dunkin Donuts[3] began accepting mobile payments via iOS and Android-enabled mobile devices. Starbucks' mobile payment solution makes use of digital wallets,[4] technology that allows businesses to accept secure mobile transactions and deliver offers, coupons, rewards, and receipts to customers' smartphones.

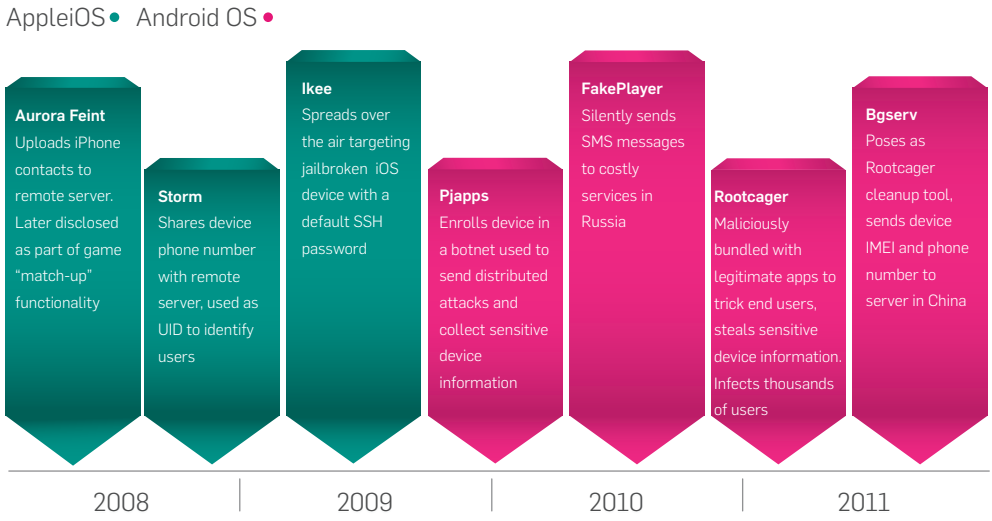
These announcements will undoubtedly accelerate the daily use of digital wallets and other forms of mobile payment. They will also act as a magnet for malicious malware writers.

## The business of cybercrime

We used to imagine malware coming from loosely knit groups of hackers walled up in non-descript offices, spending their days pinging websites in search of vulnerabilities to exploit. Today the purpose of nearly all malware is to make money for cybercriminals. Over the last 10 years the creation of malware has evolved into an organized international criminal enterprise.

1 Global Mobile Statistics 2012 Part A: Mobile Subscribers; Handset Market Share; Mobile Operators
http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#subscribers
2 Starbucks to Accept Square Mobile Payments
http://www.ign.com/articles/2012/08/08/starbucks-to-accept-square-mobile-payments
3 Doughnut App Arrives: Dunkin' Donuts Accepts Mobile Payments
http://www.latimes.com/business/technology/la-fi-tn-dunkin-donuts-app-20120816,0,5277462.story
4 Digital Wallets Are the Next Phase of the Payments Industry Transformation
http://www.forbes.com/sites/forrester/2012/08/02/the-digital-wallets-wars-are-the-next-phase-of-the-payments-industry-transformation/

## Mobile Malware Timeline




Data: "An Intense Look at the Mobile Computing Threat" presentation by Joshua Wright, SANS Institute/ Information Week/reference #92190

> "Bad guys go where the money is. Everywhere people have gone, bad guys have followed."[5]

In an August 2012 article in InfoWorld,[6] IT security writer Roger Grimes pointed out that cybercrime syndicates are recruiting amateur hackers and coders to sign on as full-time employees of their increasingly professional organizations. These criminal operations now have HR departments and project management teams. The goal of these multi-level, service-oriented syndicates is no longer political hacktivism or carrying out denial-of-service (DoS) attacks. Their mission is to steal money and intellectual property from individuals and businesses.

At the heart of these organizations are what Grimes called "malware mercenaries"—malware writers who work daily to turn out malware intended to bypass security measures, attack specific customers and achieve specific outcomes. And like the independent malware creators of the past, these criminal organizations continue to sell their malware on the open market in fierce bidding forums.

Currently cybercriminals are developing malware to specifically target mobile devices. There are two prominent ways the criminals use malware to make money from unsuspecting mobile device users: banking malware and premium-rate SMS fraud.

5 Your Smartphone: A New Frontier for Hackers
http://www.usatoday.com/tech/news/2011-08-07-smartphone-security-hackers_n.htm
6 IT's 9 Biggest Security Threats
http://www.infoworld.com/d/security/its-9-biggest-security-threats-200828

## Banking malware

Fraudsters have built a highly specialized industry around capturing authentication information used to access online financial institutions. Their attacks initially relied on simple key-logging software to capture your username and password. But evolving techniques have led to an advanced cat-and-mouse game between criminals and banks.

Malicious mobile software such as Spyeye and Zeus (aka, Spitmo and Zitmo) attack users that visit a website set up by malware writers, their sponsors, or their partners. If the user visiting the malicious site is using a Windows-based web browser, the site serves the Windows version of malware. If the user visits a malicious website from a mobile browser, the malware serves up mobile versions of Zeus or Spyeye.

In either case the website has the ability to identify the platform you're using to access that website. For users of the Android platform, the malicious website will serve an Android package (APK file). This app is designed to steal the mobile transaction authentication numbers (mTANs) associated with a banking transaction. MTANs are temporary passwords users receive from their banks via SMS message.

Zeus intercepts all incoming SMS messages and transmits them to either a website or phone number controlled by the attacker. Zeus also allows the attacker to control malware settings using HTTP requests or SMS messages. For example, by sending a specifically formatted SMS message, the attacker can change the destination number of forwarded SMS messages such as those from a bank. Zeus also targets devices running other mobile operating systems such as BlackBerry OS.

## Premium-rate SMS fraud

Rather than ask you for your credit card or attempt to withdraw money directly from your bank account, many mobile phone malware authors use premium-rate SMS services to make money.

Once installed, a malicious application disguised as a pirated app for your Android may come with a little something extra, a module that will start sending SMS messages to premium rate numbers at your expense.

For more information on premium-rate SMS fraud, download the whitepaper Exposing the Money Behind the Malware.

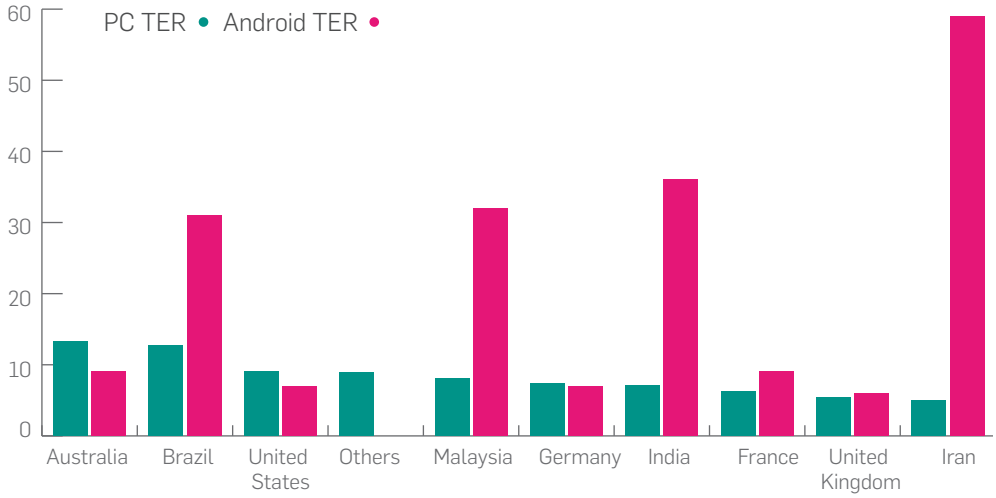
# Why iOS is safer than Android

Google's Android platform has become a larger target for mobile malware writers than Apple iOS. This could be a result of Android's popularity—with more than 1 million activations per day, Android smartphones command a 59% market share worldwide.[7] However, the relative vulnerability of Android vs. iOS comes down to the level of control the vendors have over products and the marketplace for development and distribution of apps.

Mobile malware writers know the best way to infect as many devices as possible is to attack central application markets. The cybercriminals plant applications that include hidden (obfuscated) malicious functionality in an attempt to avoid detection included in the vendor's application vetting process (e.g., Google Bouncer).

In 2011 alone, Google removed more than 100 malicious applications from its app store. Google discovered 50 applications infected by a single piece of malware known as Droid Dream, which had the capability to compromise personal data.[8] However, Google hasn't always acted in a timely manner to prevent infections. Users downloaded one harmful app more than 260,000 times before the company removed it from the app market.[9]

### Android Threat Exposure Rate




TER (threat exposure rate) is a measure of percentage of devices in a particular country that are reporting some kind of detection, typically but not always malware related. Increasingly, and as this chart suggests, the threat exposure rates for mobile devices are reaching parity with the threat exposure rates for personal computers.
Source: SophosLabs

7 A Top 10 List of Android Phones
http://www.baselinemag.com/business-intelligence/slideshows/A-Top-10-List-of-Android-Phones/
8 Aftermath of the Droid Dream Android Market Malware Attack
http://nakedsecurity.sophos.com/2011/03/03/droid-dream-android-market-malware-attack-aftermath/
9 Your Smartphone: A New Frontier for Hackers
http://www.usatoday.com/tech/news/2011-08-07-smartphone-security-hackers_n.htm

## Apple and iOS

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.

However, iOS isn't 100% invulnerable. Take the tale of Charlie Miller, a security researcher who deliberately created a suspicious application and submitted it to Apple. Apple initially approved the application, which uncovered a bug in iOS. As soon as Apple discovered that the application was suspicious, the company suspended Charlie's developer account for one year.[10]

## 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.

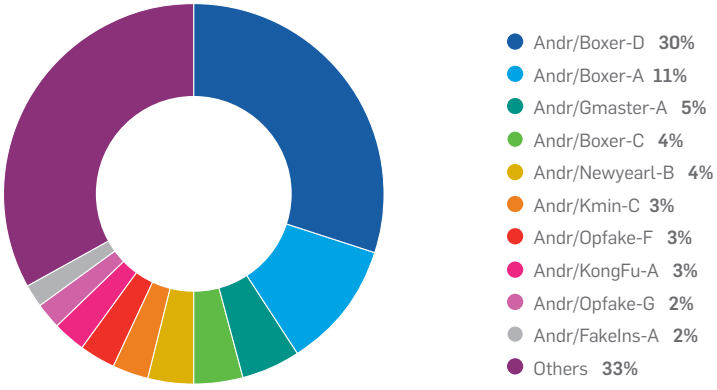
One alternative market for these "cracked" or "cloned" applications is Blackmart, and the apps cracked for that market are known as PJApps. Tools used to crack legitimate applications allow the mobile malware writers to repackage popular applications and add their own functionality. Repackaged apps will typically include some potentially unwanted pieces, such as advertising frameworks or malicious capabilities.

10 Apple Suspends Veteran Researcher From iOS Dev Program for Exploiting a Bug
http://www.eweek.com/c/a/Security/Apple-Suspends-Veteran-Researcher-from-iOS-Dev-Program-for-Exploiting-a-Bug-489867/

Another family of Android-specific malware reported to Sophos is known as DroidSheep, a tool used by hackers to listen to network traffic and gain access to online accounts of popular websites. Attackers running DroidSheep can impersonate victims' accounts and gain access to sites not using a secure connection. DroidSheep allows the attacker to sniff wireless network traffic and steal authentication tokens, which the attacker can then use to impersonate someone else. Popular sites such as Yahoo, Google, and Facebook support HTTPS connections, which a tool like DroidSheep cannot infiltrate.

The most prolific family of Android malware is known as Boxer. In April 2012, when the popular photo sharing application Instagram was released on the Android platform, mobile malware writers immediately took notice.[11] The malware creators copied the contents of the Instagram site and created a fake, malicious counterpart complete with rogue applications. Once installed, the app sends SMS messages to premium-rate services, concentrated mostly in Eastern European countries like Russia, Ukraine and Kazakhstan. In the process, cybercriminals earn a fast and tidy commission at the expense of users.

## Top Malware Families Discovered



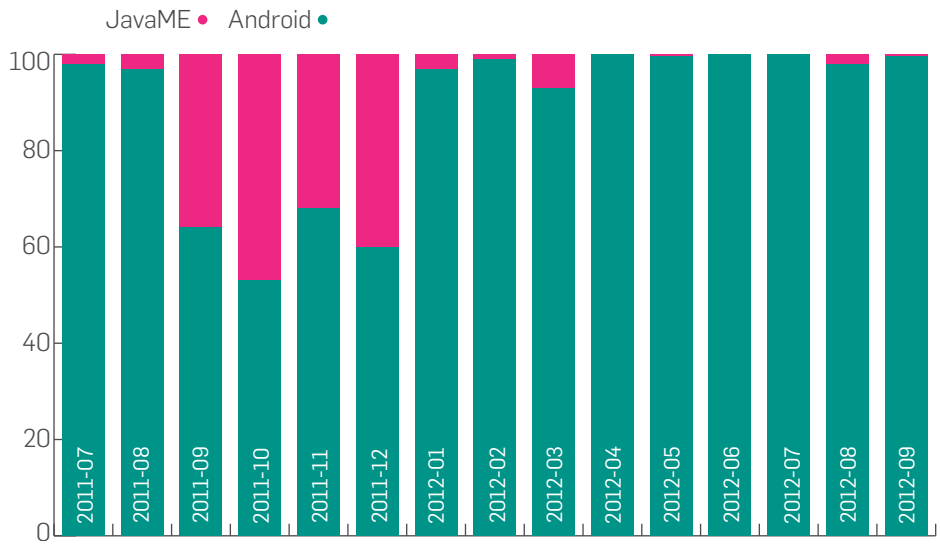

One third of all discovered Android samples belong to the Boxer family.
Source: SophosLabs

11 Fake Instagram App Slings SMS Trojan Onto Android Gear
http://www.theregister.co.uk/2012/04/19/instagram_android_sms_trojan/

# Mobile malware by the numbers

The prolific nature of threats—especially on the Android platform—continues to increase. In 2011 SophosLabs observed 81 times more Android malware than in 2010—an 8,000% leap. In 2012 SophosLabs has already seen 41 times more malware than in all of 2011—a growth rate of nearly 4,100%.

**Discovered Android vs JavaME Malware Samples**




By mid-2011 the number of discovered JavaME based samples nearly paralleled the number of Android samples. By mid-2012 the number of monthly discovered Android samples exceeded JavaME samples by several orders of magnitude.
Source: SophosLabs

# 10 tips to prevent mobile malware

Now that we've identified the causes and challenges associated with mobile malware, how do you prevent it? By taking back control of your devices and their applications.

Here are 10 tips for securing your mobile users and preventing mobile malware infections.[12]

## 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 than what it needs to do its job, you shouldn't install it.

12 10 Tips for Protecting Mobile Users
http://www.darkreading.com/security/perimeter-security/240006133/10-tips-for-protecting-mobile-users.html

### 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 bring-your-own-device (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 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

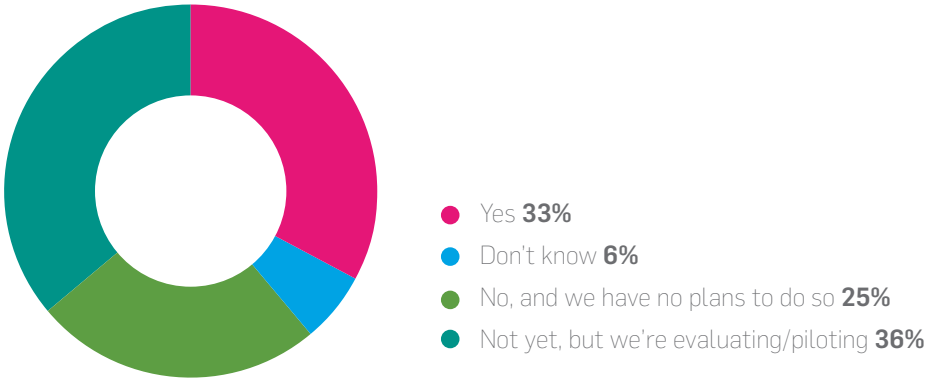
Mobile users want to store data they can access from any device, and they may use services without the approval of IT. Businesses should consider building a secure cloud-based storage service to accommodate users in a secure way.

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

Although malware exists for iOS and BlackBerry, 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.

### Use of Mobile Device Management Software to Enforce Security Policy

Does your organization use mobile device management software to set and enforce a single security policy across different types of devices?




Source: InformationWeek 2011 Strategic Security Survey of 1,084 business technology and security professionals, March 2011

# Sophos Mobile Control

## Mobile device management (MDM) for enhanced usability, better protection

**Sophos Mobile Control 2.5** gives you a wide range of tools to keep mobile devices from becoming a threat to your business. Your users are asking to use their own smartphones and tablets, so we're helping you say yes to BYOD. We've improved the usability of our solution and provide new features, giving you all the data you need at a glance.

### Get your users up and running faster

We let you use the groups you already have in Active Directory. For example, you can automatically assign newly registered devices in SMC and apply the appropriate policies to them. This helps you to get your users set up and ready to go to work in less time.

### Fewer clicks to get more done

As an administrator, you don't want managing mobile devices to take up too much of your time. We empower you to work faster with improved workflows and provide data on the inventory as pie charts, so you can see the current status at a glance.

### Know you're compliant and stay that way

As mobile technology constantly changes, you need to be sure that devices stay compliant. Our improved compliance check not only runs more tests, but allows you to decide how serious a compliance breach is. Set it to inform the user or apply the risk mitigation actions you see fit.

### Distribute and control apps and data

We now support iOS managed apps. So you can push apps—from the App Store or those developed in-house—right to your iOS users. You can securely remove managed apps and the data they contain, if your user leaves the company or the device becomes non-compliant.



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

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

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

Boston, USA | Oxford, UK


A Sophos Whitepaper 10.12v1.dNA

SOPHOS