

Android: Today's biggest target

Featuring research by [SophosLabs](#)

Over 100 million Android phones shipped in the second quarter of 2012 alone.³² In the U.S., a September 2012 survey of smartphone users gave Android a whopping 52.2% market share.³³ Targets this large are difficult for malware authors to resist. And they aren't resisting—attacks against Android are increasing rapidly. In these pages, we'll share some examples, and offer some perspective. We'll ask: How serious are these attacks? Are they likely to widen or worsen? And what reasonable steps should IT organizations and individuals take to protect themselves?



Unsophisticated, but profitable: Fake software, unauthorized SMS messages


Today, the most common business model for Android malware attacks is to install fake apps that secretly send expensive messages to premium rate SMS services. Recent examples have included phony versions of Angry Birds Space, Instagram, and fake Android antivirus products.³⁴ In May 2012, UK's mobile phone industry regulator discovered that 1,391 UK Android users had been stung by one of these scams. The regulator fined the firm that operated the payment system involved, halted fund transfers, and demanded refunds for those who'd already paid. However, UK users represented only about 10% of this malware's apparent victims—it has been seen in at least 18 countries.

Currently, one family of Android malware, Andr/Boxer, accounts for the largest number of Android malware samples we see, roughly one third of the total. Linked to .ru domains hosted in the Ukraine,

Andr/Boxer presents messages in Russian and has disproportionately attacked Eastern European Android users who visit sites where they've been promised photos of attractive women.

When they arrive at these sites, users see a webpage that is carefully crafted to entice them to download and install a malicious app. For example, the user might be prompted (in Russian) to install a fake update for products such as Opera or Skype. Or, in some cases, a fake antivirus scan is run, reports false infections, and recommends the installation of a fake antivirus program. Once installed, the new app begins sending expensive SMS messages. Many of these Trojans install with what Android calls the INSTALL_PACKAGES permission. That means they can download and install additional malware in the future.


Learn more about mobile device management

 Free tool: Mobile Security for Android

 Mobile Security Toolkit

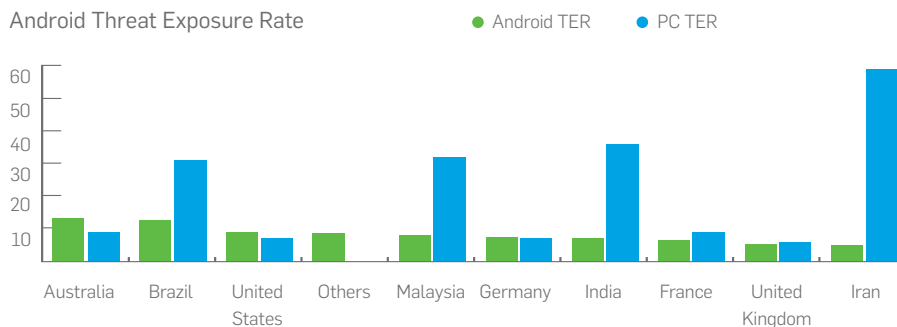
 Mobile Device Management Buyers Guide

 When Malware Goes Mobile

 Vanja Svajcer of SophosLabs explains Android malware

Android threats accelerate

In Australia and the U.S., Sophos is now reporting Android threat exposure rates exceeding those of PCs.



Threat exposure rate (TER): Measured as the percentage of PCs and Android devices that experienced a malware attack, whether successful or failed, over a three month period.

Source: SophosLabs

Joining the botnet

Until recently, most fake software attacks we've seen on Android have been relatively unsophisticated. For example, some use primitive polymorphic methods that involve randomizing images, thereby changing checksums to avoid detection. Leading security companies learned how to defeat this tactic many years ago.

But the attackers are making headway. For example, consider the malware-infected editions of Angry Birds Space we saw in April 2012 (Andr/KongFu-L). Again, available only through unofficial Android app markets, these Trojans play like the real game. But they also use a software trick known as the GingerBreak exploit to gain root access, install malicious code, and communicate with a remote website to download and install additional malware. This allows these Trojans to avoid detection and removal, while recruiting the device into a global botnet.

Capturing your messages and your bank account

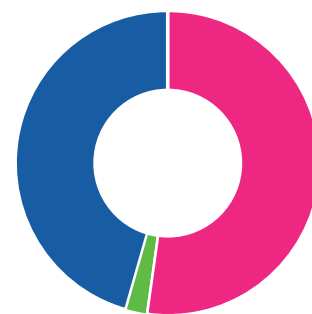
We have also begun to see Android malware that eavesdrops on incoming SMS messages and forwards them to another SMS number or server. This sort of data leakage represents a significant risk, both to individuals and to organizations.

The potential exists for attacks like these to target Internet banking services that send mobile transaction authentication numbers via SMS. Many banks send authentication codes to your phone via SMS each time you do an online transaction. This means that just stealing a login password is no longer enough for criminals to raid your account. But malware on your phone, such as the Zeus-based Andr/Zitmo (and similar versions targeting BlackBerry) are capable of intercepting those SMS messages.

Consider the following hypothetical scenario. Through a conventional phishing attack, a victim gives criminals sufficient information to allow them to sign in to your mobile banking account and also port your phone number (this has happened). They can now log in to your online bank account while also receiving an SMS containing the second-factor authentication token needed to complete a transaction.

Through the use of a malicious Android app that harvests SMS messages in real time and in concert with a social engineering attack, attackers open a brief window of opportunity to steal this token and use it before you can stop them.

Naked Security Survey
Is smartphone SMS/TXT spam a problem for you?



● Yes	43.78%
● It was, but I downloaded an app and it is sorted now	2.36%
● No—I rarely/never received an SMS text spam on my phone	45.29%

Based on 552 votes
Source: Naked Security

PUAs: Not quite malware, but still risky

It's worth mentioning the widespread presence of potentially unwanted applications (PUA). PUAs are Android apps that may not strictly qualify as malware, but may nevertheless introduce security or other risks.

First, many users have installed apps that link to aggressive advertising networks, can track their devices and locations, and may even capture contact data. These apps earn their profits simply by serving pornographic advertising. Many companies may wish to eliminate them 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.

Second, some sophisticated Android users have chosen to install Andr/DrSheep-A on their own devices. Similar to the well-known desktop tool Firesheep, Andr/DrSheep-A can sniff wireless traffic and intercept unencrypted cookies from sites like Facebook and Twitter. The legitimate use for this tool is to test your own network. However, it is often used to impersonate nearby users without their knowledge. We currently find Andr/DrSheep-A on 2.6% of the Android devices protected by Sophos Mobile Security. Corporate IT departments are unlikely to countenance the installation, let alone the use, of such tools.

If you "root" your device, it means you enable software to acquire full Android administrator privileges. The name comes from the administrator account, known as "root" on UNIX-like operating systems such as Android. Rooting is popular because it allows you greater control over your device—notably to remove unwanted software add-ons included by your service provider, and to replace them with alternatives of your own choosing.

Rooting bypasses the built-in Android security model that limits each app's access to data from other apps. It's easier for malware to gain full privileges on rooted devices, and to avoid detection and removal. For the IT organization supporting BYOD network access, rooted Android devices increase risk.

Mitigating the risks while they're still manageable

In most business environments, the risks from Android are modest at this point. But those risks are growing. Even as Google makes improvements that secure the platform against more obvious threats, new threats emerge. For example, some security experts have recently expressed concern about risks from new near field communications (NFC) features intended to allow advanced Android devices to function like credit cards.

Even today, Android malware can place a company's future at risk by exposing strategic information or stealing passwords. With this in mind, IT organizations should secure their Android devices against malware, data loss, and other threats. We recommend the following steps to bring down the level of risk. Remember, none of these tips are foolproof or sufficient in isolation. But in most environments, they will go a long way.

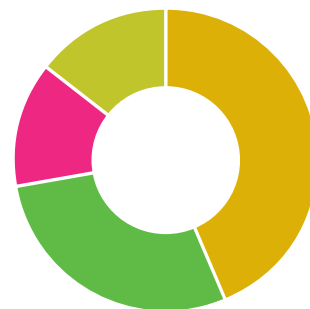
- ▶ Extend your IT security and acceptable use policies to Android devices, if you haven't done so already.
- ▶ Refuse access to rooted Android devices.
- ▶ Consider full device encryption to protect against data loss, and provide for remote wipe of lost or stolen devices. If you choose to encrypt, make sure your solution can also encrypt optional SD cards that may contain sensitive data, even if those SD cards are formatted differently.
- ▶ Where possible, establish automated processes for updating Android devices to reflect security fixes. Keep your Android devices up to date with the security patches provided by the manufacturer and by the vendors of any additional software you've installed.
- ▶ Consider restricting Android devices to apps from Google's official Play Store. Malware has turned up in the Play Store, but much less frequently than in many of the other unregulated, unofficial app markets, notably those in Eastern Europe and Asia.

- ▶ When you authorize app stores, limit users to apps with a positive history and a strong rating.
- ▶ Avoid social engineering attacks, and help your colleagues avoid them. This means carefully checking the permissions that an app requests when it's installed. For example, if you can't think of a specific credible reason why an app wants to send SMS messages, don't let it. And pause for a moment to consider whether you still want to install it.³⁵
- ▶ Finally, consider using an anti-malware and mobile device management solution on your Android devices. We recommend Sophos Mobile Control. But whatever solution you choose, get it from a company that has extensive experience with both antivirus and broader security challenges. Why? First, because attack techniques are beginning to migrate to Android from other platforms. Your solution provider should already know how to handle these. Second, because attacks are emerging and mutating more rapidly. Your provider should have the 24/7 global infrastructure to identify threats, and the cloud-based infrastructure to respond immediately. Third, and most importantly, because today's complex infrastructures require an integrated mobile security response that goes beyond antivirus alone to encompass multiple issues, ranging from networking to encryption.

Naked Security Survey

What is the most important consideration when you install an app on your Android device?

● Reputation of developer	43.78%
● Popularity of application	28.65%
● Cost of app	13.24%
● Download location	14.32%



Based on 370 respondents

Source: Naked Security

