SOPHOS
Security made simple.

Not Just for PCs Anymore: The Rise of Mobile Malware

Protect your mobile devices from malicious attacks

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

Mobile malware is not new. Worms first attacked Symbian Series 60 mobile phones as far back as 2004. Today, however, mobile malware is far more widespread, and far more dangerous—especially since smartphones and tablets are now widely used for critical business tasks. This whitepaper will take a close look at the fast-moving threat of mobile malware: how and why it's arisen, what forms it takes, where it stands, where it's headed, and what you can do about it.

Android, BYOD and mobile malware

Fifty-nine percent of IT and security professionals surveyed by the Ponemon Institute recently said mobile devices are increasing the prevalence of malware infections within their organizations.[1] This is no shock: the extraordinary growth of mobile platforms has made them an irresistible target. The only surprise would have been if these devices had escaped attack.

Years ago, PC malware exploded when Windows achieved dominance. Something similar is occurring with mobile. As the mobile marketplace has grown and evolved, the Android platform has become dominant. Worldwide, 70% of new smartphones now run Android, with iOS running a distant second. (Microsoft's Windows Phone 8 platform offers promise, but hasn't yet achieved significant market penetration.)

The Android platform's openness has made it attractive to users, device manufacturers, carriers, app developers—and to malware creators. That's where they're focused, and it's where you need to focus, too.

We'll take a closer look at the specific challenges of Android platform security in a moment. But first, it's worth mentioning one more issue organizations face in protecting mobile devices and users. In BYOD arrangements, mobile devices are often owned by users, who act as de facto administrators. Users typically decide which apps to run, and where to get them.

Wider smartphone and tablet usage is often correlated with a loss of organizational control. And that, in turn, can compromise security in multiple ways. This is why some organizations are pursuing choose your own device (CYOD) approaches, where users get to pick their devices from a list the company is prepared to support, will continue to own, and plans to centrally administer. Of course, CYOD isn't always an option, and many organizations have chosen to accept the tradeoffs associated with full BYOD.

Mobile malware risks

Organizations evaluating mobile malware risks should assess each of the ways it can damage them, including the following.

Productivity losses. Some forms of malware inconvenience users through aggressive advertising, prevent mobile devices from working properly, and increase support costs.

Direct costs. Some forms of malware and potentially unwanted applications (PUAs) have direct costs by utilizing paid mobile services such as SMS, with or without the user's awareness or understanding.

Security, privacy, and compliance risks. Mobile malware can compromise corporate and customer data, systems, and assets that must be protected—placing the organization at competitive, reputational and legal risk.

Some mobile malware and PUAs merely annoy and frustrate. Yet as a whole, mobile malware and PUAs represent a significant and growing problem.

1. *Global Study on Mobility Risks*, Ponemon Institute, February 2012, websense.com/assets/reports/websense-mobility-risks-ponemon-report.pdf

Android-specific threats

Like Windows for PCs in the 1990s, Android has quickly become the heart of a thriving ecosystem of hardware, software and services. As with Windows, there are few barriers to participation in this ecosystem. And, as with Windows, the platform has gained market leadership faster than it has implemented strong security.

The Android marketplace is huge and diverse. It encompasses a wide range of hardware and OS versions, making support far more complex for everyone from IT to carriers and manufacturers.

As of mid-2013, there were over 700,000 Android apps. In contrast to iOS, which delivers all apps through a single Apple store, Android users can get apps from multiple sources. They can use the official Google Play app store; or competitive app markets of varying reliability—including many in China, today's fastest-growing source of Android malware.

Seeking to avoid payment, some users retrieve apps from pirate sites and wind up installing apps that have been cracked and repackaged with malware. *Forbes* recently reported that one-third of Android developers claim to have lost at least $10,000 to piracy.[2]

These problems are aggravated by limitations of the Android platform. For instance, Android's permission system isn't finely grained enough for good security, and it's too complex for users to make good decisions about what to allow or block. As an example, few apps should be permitted to send or receive SMS messages. However, many Android games use SMS to handle add-on subscriptions to new game levels, making it difficult for users to be confident about which requests are legitimate.

While Google screens apps more carefully than it once did, it's still easy to add new apps to Google Play, and Google's control over the behavior of those apps is quite loose. The fake Zitmo-D certificate app remained on Google Play for months, and potentially unwanted Android Apperhand apps containing aggressive advertising frameworks are often found there. What's more, it's easy to decompile Android apps, add dangerous functionality, and repackage them as completely new apps.

How serious have these problems become? Sophos has identified more than 350,000 variants of Android malware, and another 230,000 variants of PUAs. We're currently adding detections for approximately 2,000 new Android samples every day, divided approximately equally between these two categories. In the following two sections, we will discuss both of them in detail.

2. *Software Pirates Plague Android Developers*, Brian Caulfield, *Forbes*, Sept. 9, 2011, http://www.forbes.com/sites/briancaulfield/2011/09/09/software-pirates-plague-android-marketplace/

Android Malware Samples

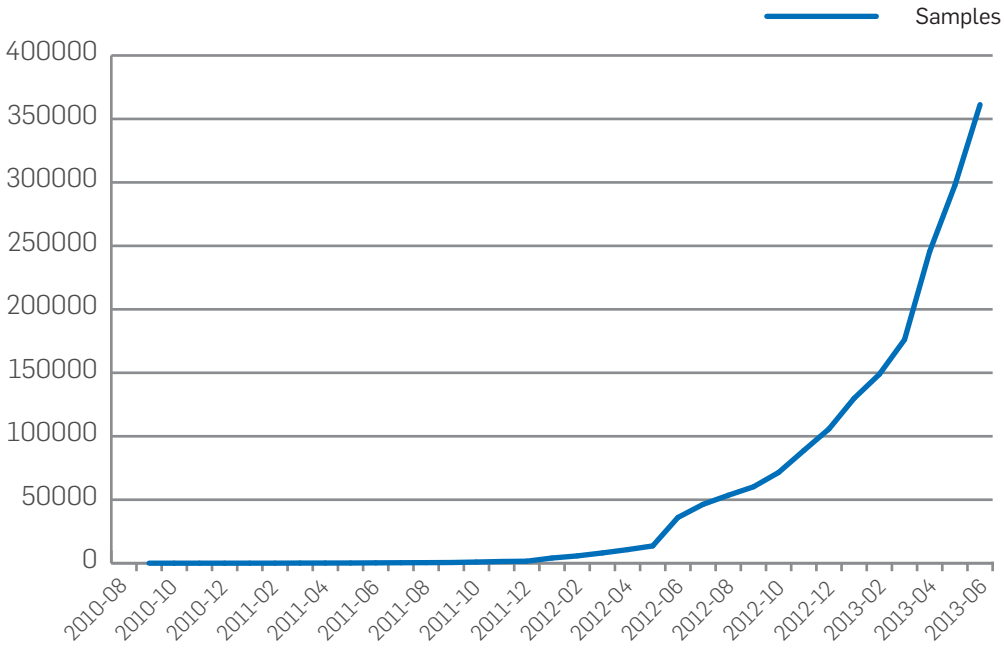

Figure 1. Cumulative number of Android malware variants detected by Sophos though June 2013.

Android PUA Samples

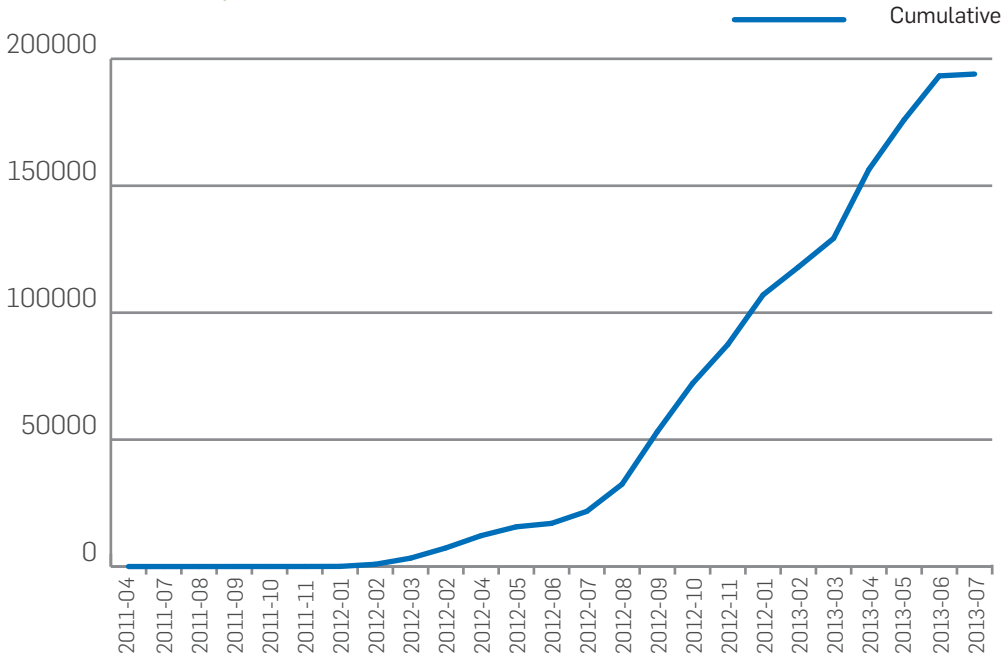

Figure 2. Cumulative number of Android PUA variants detected by Sophos through July 2013. Note: the July 2013 figure represents only the first week of the month.

Most common types of Android malware

Sophos currently encounters five primary types of Android malware: information stealers, SMS senders, pay-per-click/pay-per-install, phishing apps, and privilege escalation exploits. In this section, we'll discuss and provide examples of each.

Information stealers

What if your company's secret plans were being forwarded to malicious strangers? What if your most personal messages were? They might be, if you communicate via SMS text message and your Android device hosts an information stealing Trojan. Malware such as the Andr/SMSRep-B Trojan register a broadcast receiver that intercepts every SMS message you receive. The Trojan then codes the text messages through the industry-standard JSON scheme used by legitimate web services, and forwards them to a malicious web server using standard HTTP POST requests.

More recently, BadNews captured detailed phone information from several million Android users. BadNews introduced some distressing innovations. This Trojan infected devices through apps retrieved from the official Google Play store, not some dangerous third-party site. Second, the malware functionality was delayed. Users received an ad framework that had done nothing to flag it as dangerous, and hence passed Google's vetting process. Once installed, the framework later began sending premium-rate SMS malware to infected devices.

BadNews uses a pay-per-install (PPI) approach, renting its own infrastructure to affiliates who wish to install their own software. One affiliated software package that it later installed—whether intentionally or not—proved to be malicious. BadNews highlights the need for users to install protection that can be quickly updated to halt safe apps that go rogue.

SMS senders

One of the easiest ways to steal money from Android users is to coax their devices into sending messages to premium-rate SMS services. Consider, for example, Andr/AdSMS, which first appeared in China in 2011 and continues to bedevil users today. Andr/AdSMS has been integrated into malicious, "cracked" versions of multiple apps, including iCalendar, iMine and iMatch. It sends paid messages to different numbers depending on the app.

Users are silently subscribed to these services, so they find themselves paying for unwanted messages repeatedly. Since users often don't scrutinize their mobile bills closely, it may take them some time to even notice the charges, much less successfully remove the app and halt the messages.

Pay-per-click/Pay-per-install

Mobile advertising is a significant way for attackers to generate revenue. Traffic sent to affiliated partner sites from Android malicious apps offer the attackers financial incentives. App distributors also pay attackers based on how many times per-install apps are installed on compromised Android devices.

Andr/GMaster and Andr/MTK, each distributed in China, are representative of this type of app. These Trojan families set up a large mobile botnet via malicious code hidden in affected apps. The botnet's controllers employ it to generate millions of installations and advertising

traffic to legitimate developers and advertising services—thereby gaining indirect income from these third parties.

Phishing malware

With millions of people using their Android devices for banking, accessing those online accounts has become the holy grail for malware authors. Attackers quickly learned how to capture usernames and passwords by abusing available permissions and locating data left accessible on the device. And they have become even more sophisticated.

Consider Zitmo, which uses a mobile component of the notorious Zeus server-side toolkit that first attacked Windows PCs. When Android users inadvertently visit a site captured by malware authors, sponsors, or partners, that site serves up a malicious Android package file (APK).

Once installed, this app uses built-in Android mechanisms for capturing incoming SMS messages to steal the mobile transaction authentication numbers (mTANs) associated with a banking transaction. (mTANs are temporary passwords users receive from their banks, and represent an additional level of security beyond standard username/password authentication.)

Zitmo forwards mTANs to a website or phone number controlled by the attacker. Once the attackers have captured an mTAN along with standard authentication credentials, they can potentially make financial transactions in the user's name.

Privilege escalation exploits

Malware authors have discovered ways to exploit the Android platform to gain unwarranted privileges, access resources that should be off-limits, and perform unauthorized actions. In 2011, an early Android privilege escalation exploit, DroidDream, found its way into more than 50 apps on Google Play, and compromised over 200,000 devices in days.

More recently, the sophisticated GinMaster Trojan has spread throughout app markets in China, embedded into thousands of legitimate games, ringtones and other apps. GinMaster is complex: it's among the first Android malware to resist detection through polymorphism, seeking to appear different on every device. It also incorporates a malicious service capable of rooting devices, grabbing full privileges, capturing and forwarding confidential data, and installing new apps without any user involvement. We believe it's an unmistakable harbinger of even more powerful and dangerous Android malware on the way.

Android PUAs

Some apps aren't quite malware, but may degrade the user's experience or privacy in ways that make them undesirable to most users and organizations. We call these PUAs. For example, these apps might aggressively bombard users with advertising, spy on users' activities in unacceptable ways, or display inappropriate content that can place employers at risk of harassment claims.

Since these apps may offer capabilities that certain users may consider worth the trade-off, security companies can't simply call them malware. Nevertheless, many users and organizations want ways to block or remove them—especially since they're often installed without the user's full awareness, and can be difficult to remove.

While PUAs have existed for years on Windows, the distinction between malware and PUAs on mobile devices can seem even fuzzier. At Sophos, we've done advanced work to help our customers make useful distinctions and limit apps that are truly unwanted. We define an app as a PUA if it has one or more of the following characteristics:

- Can compromise a device's security by jailbreaking or rooting it
- Can remotely monitor a user or device without the user's knowledge (excluding apps advertised as providing genuine device administration capabilities)
- Was cracked or repackaged to evade payment to the app's developer
- Uses third-party services in ways that violate their terms or conditions
- Has been compiled from open source but changed to deliver ads
- Focuses primarily on ad packages and/or aggressive ad delivery methods

Avoiding mobile malware: The user's perspective

If you use an Android device, preventing mobile malware infection and avoiding PUAs begins with educating yourself. Here are seven easy-to-understand principles of self-protection. Use them consistently, and you can substantially reduce your risk.

1. If it sounds too good to be true, it probably is. Simple, right? If you expect a free lunch, it's you who might get eaten alive. Don't click on ads that sound too good to be true as you don't know what might be lurking behind it.

2. Use common sense when it comes to permissions. For example, if an app requests extended access to your contacts or other personal items, it should explain why. Don't hesitate to refuse access if you're not fully convinced.

3. Third party app stores carry the greatest risk. Google Play isn't perfect: malware-infected apps and PUAs evade its filters. But many third-party app stores are far riskier. Definitely avoid free file-sharing sites offering free versions of apps that normally require payment. Many of these apps have been cracked and infected.

4. Use consumer reviews as guidance. Multiple negative reviews or warnings about app misbehavior deserve to be taken seriously.

5. Protect your data, protect your phone. Consider using encryption to scramble data stored on your device or on cloud-based storage services. That way, if your data (or your phone itself) is lost or stolen, confidential or personal information never falls into the wrong hands.

6. Display your costs. Some carriers provide Android device settings that inform you whenever you're spending money. This can help you identify apps that are using paid services such as premium SMS without your knowledge or permission. Organizations whose carriers don't provide this capability can use Sophos Mobile Security's Privacy Advisor, which identifies apps that are using permissions that could result in SMS-related costs.

7. Get reliable protection. You wouldn't think of running a Windows PC without protection against malware, and you shouldn't run your Android device without it either. To help you protect yourself, we provide Sophos Mobile Security. It can scan both new and already-installed apps on your device and on all storage devices, without impacting performance or

battery life. It can identify and remove both malware and PUAs, protect you from visiting malicious web pages, and query the cloud to reflect up-to-the-minute threat intelligence. And, for users who run it on a standalone basis without managing it centrally through Sophos Mobile Control, it's entirely free.

Avoiding mobile malware: The organization's perspective

The preceding guidance is specifically for individual users. If you are responsible for securing an organization, you need a broader perspective and different guidelines. This section offers practical advice on where to start and what steps to take to secure your organization and protect your business.

Deploying tools that are both reliable and manageable

The rapid growth and evolution of Android malware means that every Android device should run reputable anti-malware protection. As we've just discussed, our Sophos Mobile Security delivers reliable, up-to-date protection to individual consumers. For organizations, however, that is a bare minimum solution. Since users typically administer their own mobile devices, they can remove it as easily as they've installed it—leaving you both vulnerable.

One way to overcome this problem is by using Sophos Mobile Control's mobile device management (MDM) features to require that Sophos Mobile Security remains installed on the user's device. You can gain far more control and flexibility, however, by licensing and running Sophos Mobile Security as a fully managed app that can be configured and tracked through the Sophos Mobile Control console.

Implement holistic, layered protection

When it comes to mobile devices—as with other clients and networks—organizations have multiple vulnerabilities. They need solutions that work together to provide holistic, layered protection. Consider Sophos Mobile Security as an example of what layered protection should include.

Malware/PUA scanning

Mobile security solutions should include both on-demand and scheduled scanning. They should be capable of both scanning apps as you install them and afterwards; and on your device and on removal storage devices. They should flag apps and PUAs that either pose a potential threat or are unsuitable for business networks. And, since threats change quickly (and even supposedly safe apps can change behavior) they should draw on the latest threat intelligence.

Loss/theft protection

A complete mobile security solution should be capable of remotely locking or wiping any lost or stolen Android device that has access to your business networks. It should allow you to send a variety of commands from predefined phone numbers by text message, including commands that make the device ring loudly so it can be found, and then displays a message

to the finder. It should offer tracking technology to increase your chances of recovering a device, and it should send you a message if the device's SIM card has been changed.

Spam protection

Complete mobile security protection should include spam filtering for both text messages and calls, with the ability to block and log malicious phone numbers, calls with a hidden caller ID, and text messages with potential malicious URLs.

USSD protection

USSDs are special codes used for a variety of functions. In many countries, they perform tasks like checking the amount of credit users have left on your phone. Attackers have found ways to capture USSD codes and use that information to exploit Android devices or perform unauthorized factory resets—as in the case of a high-profile recent attack on Samsung Galaxy S2 and S3 phones running TouchWiz.[3] A complete mobile security solution should protect against USSD attacks by checking USSD codes against up-to-date threat data, blocking codes as needed, scanning outbound numbers to ensure that your device is not transmitting USSD codes to a known malicious location, and warning users before executing any task that utilizes a USSD code.

Web filtering

Since malicious and compromised web pages are a key vector for malware and PUA infection, a complete mobile security solution should prevent users from visiting them.

App control

If your users and IT arrangements will permit it, consider restricting the installation of apps to those known to be safe. If this is a possibility, make sure your mobile security software will permit it.

Privacy protection

Without plain-English help and guidance, users are at the mercy of their apps. A complete mobile solution should provide the privacy help their apps don't typically provide. For example, it should tell users which apps are accessing their personal data, and which are capable of generating costs (by, for example, using premium-rate SMS services).

Consider manageability, flexibility, growth and cost

In evaluating mobile security solutions, check out the administration toolset: is it unified, intuitive, and easy? Then, check out the licensing arrangements: are you required to pay per device, or can you pay per user—and protect yourself against cost increases as users bring new tablets or other devices onto your network?

3. *How to Tell If Your Samsung Phone is Vulnerable to Today's USSD Hack*, Alex Dobie, *Android Central*, 9/25/12, www.androidcentral.com/ussd-test

Complement technical solutions with user education

As IT professionals have learned through hard experience, even the best technology can't solve security problems all by themselves. You need to involve users. That means educating them, and educating busy users takes time. As we all know, they don't take all your advice to heart the first time: they need to be coaxed, cajoled and reminded. Above all, they need to understand why your security precautions are in their best interest, and how you can work together to protect their personal data, as well as the organization's.

User education is hard work. But one part of it is easy—knowing what to tell them. For that, you can start with the principles outlined in the preceding section.

The problem is real, and so is the solution

Mobile malware has emerged as a real and significant problem. Addressing it is no longer optional. As with other IT security risks, technology isn't a silver bullet, but it is a key component of a holistic solution that also incorporates people and process. Sophos is exceptionally well qualified to help you implement such a solution—and we're at your service whenever you're ready to start.

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

7.13.GH.wpna.simple