the Availability Digest

www.availabilitydigest.com

The Malware Threat to Android

September 2012

Can smart phones be infected by malware? You bet! Furthermore, studies by many security firms show that Android is the primary mobile target of hackers. Why is this, and what can you as an Android smartphone user do to protect yourself?

It is true that smartphone malware attacks are much rarer than are such attacks on PCs, but smartphones are a lot newer. The troublesome fact is that these attacks are increasing at an alarming rate, not only in terms of actual device infections but in terms of malware versions:

- Sophos found that newly discovered malware versions increased 41 times from 2011 to 2012.
- Juniper Networks reported that malware samples increased 472% between July and November, 2011.
- McAfee stated that threats increased by over 1,200% in the first quarter of 2012 to 7,000 from 600.
- Security vendors reported 8 million new attacks in the first quarter of 2012.
- According to Kaspersky Lab, mobile attacks increased 600% between 2010 and 2011. 65% of these were against Android

Why Android?

The majority of malware versions and attacks have been against Android mobile devices. This is not surprising as Android has become the world's leading smartphone platform. As of the beginning of 2012, Android had a 59% share of the worldwide smartphone market. As of the third quarter, there were 500 million Android devices in use, and 1.3 million were being added every day.

Android is based on Linux and designed primarily for touchscreen mobile devices such as smartphones and tablets. Developed by Google, Android is available as open-source under the Apache license. Smartphone manufacturers license Android and apply their own modifications to the base operating system. Therefore, there are many versions of Android operating worldwide.

Android has a large community of developers writing applications (apps) for Android devices. These apps can be downloaded from Google Play, the online store run by Google for music, ebooks, and Android apps, or from third-party sites. As of mid-2012, there were more than 600,000 apps available for Android, and Google Play alone had downloaded 20 billion apps.

The Android development team has invested heavily in Android security and has published an extensive document on the security features of Android.[1] However, the Android versions in production have generally been heavily modified by the device manufacturers, and security features are often compromised in these versions.

Furthermore, the manufacturers are often slow in sending operating system updates to their mobile devices. Even worse, they may stop updating older models while they are still in use. According to a Bit9 report, manufacturers Samsung, HTC, Motorola, Sanyo, LG, and Sony are slow in upgrading their phones. Duo Security collected results from 20,000 Android phones that uses its X-Ray vulnerability tool and found that 50% of these phones had unpatched vulnerabilities.

Android's problem of security vulnerabilities due to its fragmented marketplace is compounded by its large base of application programmers writing apps with no verification by Google. As Juniper Networks said,

> "These days, it seems all you need is a developer account that is relatively easy to anonymize, pay $25, and you can post your application. With no upfront review process, no one checking to see that your application does what it says, just the world's largest majority of smartphone users skimming past your application's description page with whatever description of the application the developer chooses to include."

Though Google provides some validation of apps that it provides through its Google Play store, apps sold through third-party stores are unvalidated. Thus, hackers can easily include malicious code in these apps. It appears that the main source of Android infections comes from unvalidated apps obtained through third-party sites. Compounding this problem is that cybercriminals are creating fake Google Play stores to sell malicious apps.

There has been malicious software distributed that attempts to spread Android infections from one phone to another via Bluetooth or Wi-Fi, but so far these have not created a wide-spread problem.

Because smartphones and tablets are much newer in the marketplace than PCs, mobile malware detection utilities are not as advanced and security updates for these utilities are slow to be propagated.

With the combination of Android's market penetration, its security vulnerabilities, malicious apps, and immature anti-virus software, it is no wonder that Android has become the hacker's choice for mobile devices. Coupled with user ignorance of malware threats and the fact that more data is going mobile, malicious infections of Android devices will continue to escalate.

The Threats

Though the variety of malicious threats is large, there seems to be a few that are reported to be predominant.

Preloaded Apps

Preloaded apps delivered with Android devices by many manufacturers have security vulnerabilities. In particular, many of them do not properly enforce the permissions-based security model that requires apps to explicitly request permission from users to access personal information. This security hole is often exploited by hackers to collect sensitive information from users.

Toll Fraud

According to Juniper Networks, SMS toll fraud represents half of malicious attacks on Android devices. These malicious apps use SMS Trojans to send text messages in the background to premium-rate

[1] Android Open Source Project Security, http://source.android.com/tech/security/index.html

numbers (numbers that charge a fee for each call). These result often in huge surcharges to a user's monthly bill. The cybercriminal gets a cut of the generated revenue.

Rootkits

A rootkit is a type of Trojan that keeps itself hidden from detection. It enables an attacker to have root access to the operating system. A rootkit can intercept system API calls and as a result can do whatever the hacker wants to the device and to the user's data. One particular rootkit described in the literature logs a user's location and his keystrokes and sends these to a malicious third party.

What About Apple and iOS?

So far, we have focused on Android. But what about the other major player in the mobile marketplace, Apple, with its iOS mobile operating system and its iPhones and iPads?

Interestingly, there seems to be no significant threats that have been detected that target Apple's mobile platform. There are several reasons for this. For one, iOS is not open source. There is only one iOS in the marketplace, and its source code is not available for hackers to study. Thus, if it has security vulnerabilities (which it certainly must have), these are generally not known.

Furthermore, though older Android operating system versions are often not updated, Apple guarantees upgrades for two years.

Android's security weaknesses reside not only in its vulnerabilities, but in its lack of regulation for apps written by third parties. Apple validates all apps written for iOS and offers them only in its App Store. iOS will not load apps that do not carry an Apple certification.

Perhaps the best tribute to Apple's mobile security comes from Kaspersky Lab. They noted in May, 2012, that they expect iPhone and iPad to be infected by malware within the year. To be sure, all of the malware detection vendors hope that this will be true. However, Kaspersky's prediction is testimony to the fact that malware has not yet reached Apple mobile devices.

With all being said, hackers simply find it easier to attack Android than iOS.

Summary

So what can Android users do to protect their mobile devices? It seems that there are three guidelines (short of switching to an iPhone or iPad):

1. Stop being complacent about mobile security and accept it as a looming threat.
2. Become more proactive in protecting their Android mobile devices with anti-malware software.
3. Install applications only from the Google Store, and avoid applications that look suspicious or sound too good to be true.

Acknowledgements

The following sources provided information for this article:

50% of Android devices face vulnerabilities, *TG Daily*; September 17, 2012.
Android under fire again for poor vulnerability patching, *CSO*; September 12, 2012.
Android devices Have Unpatched Vulnerabilities, *PM News*; September 2012.
iPhone Malware: Kaspersky Expects Apple's IOS To Be Under Attack By Next Year, *Huffington Post*; June 15, 2012.
Android security threats increase by 1,200 percent, *The Inquirer*; May 23, 2012.

Researchers reveal new rootkit threat to Android security, *Network World*; April 23, 2012.
Enterprise Mobility: Android Security Is a Major Threat: 10 Reasons Why, *eWeek*: April 4, 2012.
Android Alert: Five Security Threats You Didn't Know About, *PCWorld*; April 3, 2012.
Cracks appear in face of Apple's iOS security, *NBC News*; March 26, 2012.
"Significant" security threats found in Android devices, *SC Magazine*; December 2, 2011.
Android Security: Threat Level None?, *Information Week*; September 18, 2011.
Android OS Security Threats, *TechJaws*; April 5, 2011.
Android Security Risks Found, *TechJaws*; November 3, 2010.
2 out of 3 Android apps use private data 'suspiciously.' Google protections 'insufficient, *The Register*; September 30, 2010.
Android, *Wikipedia*