Awake

Bitdefender
Malware Report

Top 5 Android Malware Innovations

Back in their early days, smartphones could hardly be described as “smart.” Big, bulky, underpowered and austere, these gadgets could run a game or two, store contacts, keep the daily agenda or – if properly synchronized –access the work e-mail.

By the time social networking reached its heyday, cell carriers started offering data plans and mobile devices were already packing enough punch under the shiny hood to compete with the office PC at work. Nowadays, one in four mobile phones is a smartphone and the number is rising so fast that, by 2014, mobile internet use will likely overtake desktop internet use.

Google’s Android was the last major operating system to join a market that was heavily disputed by Apple’s iOS and Microsoft’s Windows Mobile. However, the open architecture and the less restrictive requirements for third-party application development dramatically boosted its popularity. Between September 2008 and September 2011, Android has become so popular that it is now present on 53% of the worldwide mobile devices, including tablets, as revealed in the Q3 2011 Gartner Report[1].

Just like any popular operating system, Android opened a huge niche for cyber-criminals, who rushed to port personal PC malware and other cons to the new environment. Regular malware and spyware one would expect to encounter on Internet-connected devices are completed now with dialer Trojans – the nightmare of the dial-up world in the ‘90s, as well as with premium-rate SMS senders.

The 400,000 applications available on the official Android Market have been downloaded more than 10 billion times altogether. These Android packages downloaded from either the official Market or from third-party ones are still the main vectors of infection. Here is a short rundown of the most remarkable pieces of malware that have brought considerable innovations to the Android malware landscape, gathered from the official Android Market and other third party markets as well.

1. Android.Trojan.RootSmart

Threat level: Severe

Spreading: Through repackaged legit applications on third-party Android markets, especially through applications that help the user configure their phones.

Specialties: The largest known mobile botnet

Effect: If executed, the Trojan uses a vulnerability in the Android OS (the GingerBreak root exploit) that allows it to run the malicious code with root privileges. Once it has infected the mobile device, the Trojan starts collecting cell ID and geo-location data along with the usual IMEI and IMSI information. It also installs a backdoor that allows an attacker to take control of the device, send SMS messages to premium numbers, call premium telephony services, or access pay-per-TV services in China. This is one of the most sophisticated pieces of malware targeting mobile users and is also responsible for the largest mobile botnet to date.

2. Android.Trojan.DroidDream

Threat level: Medium

Spreading: The first known Android Trojan to be found on the official Android Market. It was distributed with more than 50 applications, ranging from games to music creators and wallpaper changers.

Specialties: First Trojan available from the official Market

Effect: DroidDream tries to root the phone using the two different exploits Exploid and Rage against the Cage to break out of the Android security container. When the device has been successfully rooted, the Trojan can install other pieces of malware without the user’s intervention. It subsequently proceeds to harvest some information about the environment, such as IMEI, IMSI, Device Model, SDK Version, Language and Country then connects to a remote server to announce that it has successfully infected a device. It proceeds with the installation of a secondary payload, a service that can download anything on the infected file, as per the wishes of the remote attacker.

---

[1] For Q3 2011 Gartner Report please visit: http://www.gartner.com/it/page.jsp?id=1848514

Bitdefender

3. Android.Trojan. FakeInst

Threat level: moderate

Spreading: Third-party Russian websites, via APKs disguised as mobile browsers or other utilities.

Specialties: server-side polymorphism to evade AV detection

Effect: This is one of the first Android Trojans to use polymorphism to mutate from one infection to another. Although the technique is not new on Windows systems, this is the first known piece of malware for Android that tries to obfuscate its code to actively deter detection and analysis.

If infected with Trojan. FakeInst, the Android device starts sending premium-rate SMS messages, and then points the user to a web page offering the genuine web browser or utility that the user wanted to install in the first place.

4. Android.Trojan. FakeUpdates

Threat Level: medium

Spreading: Repackaged commercial applications for Android available on third-party markets.

Specialties: Under the pretext of application updates, it fetches and installs other pieces of malware

Effect: The Trojan is distributed along with a legit application that has been repackaged. Upon installation, the Trojan deploys a service called GoogleServicesFrameworkService that starts along with the host application. When it has been successfully set in place, the Trojan connects to a C&C service and fetches a list of applications to be installed on the smartphone. The Trojan also displays a notification in the status bar area to confuse the user into installing the alleged update and grant the new application up to 10 privileges prior to the installation. The user remains unsuspicious as he thinks that the update targets an application which he already trusts, since it already was installed on the device.

5. Android.Trojan.KuSaseSMS

Threat level: low

Spreading: Via infected links sent from one victim to another.

Specialty: Spreads to the victim’s contacts by social engineering

Effect: Discovered in June 2011 by Bitdefender, Android.Trojan.KuSaseSMS promotes itself through SMS messages sent by two clean applications that were available on the Android Market at the time. These two video stream viewers had an option to recommend the player to friends, but, as it turned out, the alleged download links from the SMS sent to the friends were actually pointing to copies of Android. Trojan.KuSaseSMS. Once Trojan.KusaseSMS is downloaded and installed, it sends 6 SMS to number “10086”. In order to spread the Trojan, the applications’ authors had the unwary users recommend their friends to install malware, thus opening the way to advanced social engineering on mobiles.