REMINDER: Emailed to a group account. Do NOT reply using email group account.
For comments or inquiries email infosec@pjlhuillier.com.

INFOSEC 101
CONFIDENTIALITY • INTEGRITY • AVAILABILITY

August 31, 2012 Release # 181

-- Begin Transmission --

Mobile Apps: New Frontier of Cybercrime – Part 3

Mobile Apps : New Frontier for Cybercrime

What are the threats affecting current mobile platforms?

More and more people are shifting to smartphones, tablets and other devices powered by the previously discussed operating systems. This signifies its being a viable target for several cybercriminal attacks to infect devices and spread malicious activities. Among all other mobile app stores, the *Android Market* has been targeted with several incidents of malicious apps containing Trojans or backdoors. Because of *Android*'s open nature policy and lax regulations for app developers, it is easier for attackers to upload and distribute malware disguised as apps via the *Android Market.* Moreover, third-party app stores expose more potential risks to users.

Because different malwares are targeting the Android operating system, they are categorized depending on their techniques and payload:

Data Stealer: Steals information stored in the mobile device and sends it to a remote user

Premium Services Abuser: Subscribes the infected phone to premium services without user consent

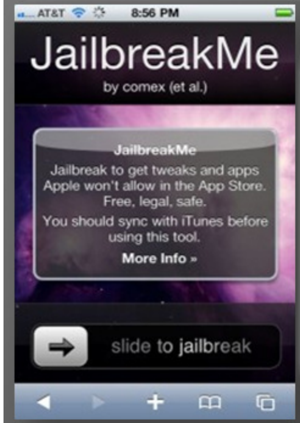
Click Fraudster: Mobile devices are abused via clicking online ads without users' knowledge (pay-per-click)

Malicious Downloader : Downloads other malicious files and apps

Spy Tools: Tracks user's location via monitoring GPS data and sends this to third party

Rooter: Gains complete control of the phone, including their functions

Cybercriminals have also created and distributed malware using the names of popular apps such as games that are not yet available on the *Android Market. Android* users anticipating these games are the likely victims of this ruse. A recent example is a fake version of Temple Run found in the *Android Market*.



AT&T 8:56 PM

JailbreakMe
by comex (et al.)

JailbreakMe
Jailbreak to get tweaks and apps Apple won't allow in the App Store. Free, legal, safe.
You should sync with iTunes before using this tool.
More Info »

slide to jailbreak

Jailbreaking Tool for iOS Exploits Vulnerabilities

Unlike *Android*, *iOS* is limited to apps available in the *iTunes App Store*. This grants *iTunes* complete control of the apps available to users. However, this does not guarantee that *iOs* is without its share of threats. *JailBreakMe* is a jailbreaking tool for *Apple* devices. This tool exploits two separate vulnerabilities that may result in execution of arbitrary code. This tool, detected as TROJ_PIDIEF.HLA, also enables a remote user to gain unauthorized control of the affected device. *iOS jailbreaking* is the process of removing the limitations imposed by Apple on devices running the iOS operating system through the use of hardware/software exploits — such devices include the iPhone, iPod touch, iPad, and second generation Apple TV.

Cybercriminals may use the same technique to push malware onto *iOS*-based device. *Apple* has already released security patches to address these vulnerabilities.

What makes Android Market the most targeted mobile app store?

One main reason for the *Android Market*'s vulnerability toward threats is its openness with distributing apps and ease of enlisting as a developer. It's easy for cybercriminals to register as a developer, download apps (or create one), insert malicious code, and re-upload it to the *Android Market.*

Google is constantly developing and updating the *Android OS,* but the *Android Market*'s security is designed differently. The *Android Market* relies mainly on its community of developers and users to review and report any possible malicious or Trojanized versions of an app.

To be continued…

-- End of Transmission –

Information Security: It's a Shared Responsibility
REFERENCE(S): [Mobile Apps - New Frontier of Cybercrime](#)
INTERNAL USE ONLY: For circulation within the PJ Lhuillier Group of Companies only.