Google puts malware scanner in Google Play pipeline

October 16 2012, by Nancy Owano

(Phys.org)—A new version of the Google Play app store will enable scanning users' smartphones for malware, according to *Android Police*. The site's report, headlined "A Built-In Malware Scanner," said, "Yes, it's hard to believe, but Google is working on a malware scanner for the Play Store. The string file doesn't lie." The heads-up item said that there are two malware-fighting parts in the Google pipeline:"App Check" will allow Google to check out each application that has already been downloaded, while an application blocker will deliver a warning of any application that looks suspicious. Also according to *Android Police*, there will be a "shut up and download it" button for people who want to proceed anyway.

Presently, Google says on its "Security on Android" page that Google

Play has a rating and review system that allows you to discover more about the app before you install it. Any app that might mislead the user probably has a low star rating and poor comments. Google says users can even flag apps for review if they see something that makes them think it is suspicious."We remove those applications that violate our policies."

In response to the *Android Police* news, security firm Sophos said it viewed the Google Play code. Graham Cluley, senior technology consultant at Sophos, said on *Naked Security* that Sophos examined the new code in Google Play, suggesting Google's intent to build a framework for virus-scanning, in the future. He said functionality will not be available "until at least API level 17 (which will be supported in the version of the Android operating system after Android 4.1 (Jelly Bean)." The functionality may also make use of the Google Safe Browsing API.

Google Play is a rebranded and expanded "Android Market," the formerly named e-store for buying and downloading mobile apps. The promotional description for Google Play reveals the breadth of exposure to media products: "On Google Play you can choose from over 675,000 apps and games, browse the world's largest eBookstore, discover millions of songs, watch the latest and greatest movies and TV shows, and even flip through your favorite magazines."

While mobile devices are rich in choices, they also carry risks for malware as stats indicate. Malware on mobile devices is alive and thriving. The FBI's Internet Crime Complaint Center (IC3), for example, issued a warning this month about increasing levels of malware targeting Android phones.

The IC3 mentioned two such malware threats, Loozfon and FinFisher. Loozfon lures its victims through invitations for work opportunities or for viewing porn and then proceeds to steal information. The FBI said it

is mainly targeted at Japan. FinFisher is capable of taking over the mobile device. Victims are lured through web links or bogus text messages pretending to be system updates. When installed the mobile device can be remotely controlled and monitored.

Interestingly, some tech bloggers as well as forum contributors appear to treat the FBI warning , not holes in Android, with derision. Their reactions can be briefly summed up as follows. "So I have to click on a strange email and then follow an unknown link?" "So I have to click through the warning about malware?" "Give us a break." "If you're that dumb, blame yourself."

Nonetheless, said another group, one cannot underestimate people who are naïve. The FBI, meanwhile, wrote up an advice list for avoiding malware, including this: "If you decide to sell your device or trade it in, make sure you wipe the device (reset it to factory default) to avoid leaving personal data on the device."

They also recommended checking out all defaults that come with a new smartphone. "Turn off features of the device not needed to minimize the attack surface of the device."

They also reiterated the obvious: "Use the same precautions on your mobile phone as you would on your computer when using the Internet."

  More information: www.androidpolice.com/2012/10/ … theres-more-wish-lis