Google fixes APK nightmare-waiting-to-happen, sends patch to partners

July 11 2013, by Nancy Owano

(Phys.org) —As if Android was not getting enough press about exploit opportunities, a Bluebox Security expert let the world know earlier this month that its security team discovered a Master Key vulnerability where hackers could sidestep app verification and install Trojans that can sail through verification without any problems. With this exploit, a hacker can modify a normal Android application package file (APK) without having to break the app's cryptographic signature. That's the ticket. The signature break would have sent off red flags. (Explains *Threatpost*: Applications are digitally signed to establish or confirm the identity of the developer and the signatures make sure that future updates come from only the developer of the application.)

In his blog, Jeff Forristal, CTO of San Francisco-based Bluebox, wrote:

"The Bluebox Security research team – Bluebox Labs – recently discovered a vulnerability in Android's security model that allows a hacker to modify APK code without breaking an application's cryptographic signature, to turn any legitimate application into a malicious Trojan, completely unnoticed by the app store, the phone, or the end user."

The vulnerability could affect nearly 900 million devices—any Android phone released in the last four years.
What's more, Bluebox Security was able to modify an Android device manufacturer's application, he said, to the point where the team had access to all permissions on the device. These might be troubling implications for a vulnerability capable of affecting 900 million devices, especially at a time when BYOD policies are not uncommon in some businesses.

All this can be viewed as much ado about something or might pan out to be much noise about nothing, because Google addressed the problem in a number of ways. Google updated Google Play, to provide checks that can block malicious attempts, so that any Android device user, by sticking to the Google Play area if intending to install any app or update, would not be at risk. Also, according to reports, the latest version of Android, has a built-in app-scanning system to check on apps coming from sources other than Google Play and a phone could block malicious code.

Google, meanwhile, has issued a patch to its hardware partners in the Open Handset Alliance. Manufacturers and carriers need to push it out to end users. Users who are unsure about their device models could check with the manufacture or mobile carrier. Google's Gina Scigliano, Android Communications Manager, said a patch was provided to partners and that some OEMs such as Samsung were shipping the fix to the Android devices.

Forristal said more details about the Android vulnerability will be made known during the Black Hat USA 2013 event in Las Vegas which opens on July 27. His presentation is described as a case study showcasing the technical details of Android security bug 8219321, disclosed to Google in February 2013.

"The vulnerability involves discrepancies in how Android applications are cryptographically verified and installed, allowing for APK code modification without breaking the cryptographic signature; that in turn is a simple step away from system access and control."
He will tell how the vulnerability was located, and the exploit created. "Working PoCs for major Android device vendors will be made available to coincide with the presentation," according to the blurb.

More information: bluebox.com/corporate-blog/blu … -android-master-key/

Citation: Google fixes APK nightmare-waiting-to-happen, sends patch to partners (2013, July 11) retrieved 27 April 2024 from
https://phys.org/news/2013-07-google-apk-nightmare-waiting-to-happen-patch-partners.html