Windows malware tries to infect Android devices connected to PCs

By Lucian Constantin

Published: 2014-01-23 · Archived: 2026-04-05 21:15:50 UTC

A new computer Trojan program attempts to install mobile banking malware on Android devices when they're connected to infected PCs, according to researchers from Symantec.

This method of targeting Android devices is unusual, since mobile attackers prefer social engineering and fake apps hosted on third-party app stores to distribute Android malware.

"We've seen Android malware that attempts to infect Windows systems before," Symantec researcher Flora Liu, said Thursday in a blog post. "Android.Claco, for instance, downloads a malicious PE [portable executable] file along with an autorun.inf file and places them in the root directory of the SD card. When the compromised mobile device is connected to a computer in USB mode, and if the AutoRun feature is enabled on the computer, Windows will automatically execute the malicious PE file."

"Interestingly, we recently came across something that works the other way round: a Windows threat that attempts to infect Android devices," Liu said.

The new malware, dubbed Trojan.Droidpak by Symantec, drops a DLL file on the Windows computer and registers a new system service to ensure its persistence across reboots. It then downloads a configuration file from a remote server that contains the location of a malicious APK (Android application package) file called AV-cdk.apk.

The Trojan program downloads the malicious APK, as well as the Android Debug Bridge (ADB) command line tool that allows users to execute commands on Android devices connected to a PC. ADB is part of the official Android software development kit (SDK).

The malware executes the "adb.exe install AV-cdk.apk" command repeatedly to ensure that if an Android device is connected to the host computer at any time, the malicious APK is silently installed on it. However, this approach has a limitation — it will work only if an option called "USB debugging" is enabled on the Android device.

USB debugging is a setting normally used by Android developers, but it's also required for some operations that are not directly related to development, like rooting the OS, taking screen captures on devices running old Android versions or installing custom Android firmware. Even if this feature is rarely used, users who turn it on once to perform a particular task may forget to disable it when they don't need it anymore.

The malicious APK distributed by this Windows malware is detected by Symantec as Android.Fakebank.B and masquerades as the official Google Play application. Once installed on a device, it uses the name "Google App Store" and the same icon as the legitimate Google Play app.

The malware appears to target online banking users from South Korea.

“The malicious APK actually looks for certain Korean online banking applications on the compromised device and, if found, prompts users to delete them and install malicious versions,” Liu said. It also intercepts SMS messages received by the user and sends them a remote server.

The targeting of online banking apps and the theft of SMS messages that can contain transaction authorization sent by banks suggest the motivation of this malware’s authors is bank fraud.

Even if this particular threat targets users from a single country, malware coders commonly borrow ideas from each other and replicate successful attack methods.

Liu advised users to turn off the USB debugging feature on their Android devices when not it’s not needed and to be wary of connecting their mobile devices to computers they don’t trust.
