The secret behind “unkillable” Android backdoor called xHelper has been revealed

reader comments

3 with 3 posters participating

Share this story

In February, a researcher detailed a widely circulating Android backdoor that’s so pernicious that it survives factory resets, a trait that makes the malware impossible to remove without taking unusual measures.

The analysis found that the unusual persistence was the result of rogue folders containing a trojan installer, neither of which was removed by a reset. The trojan dropper would then reinstall the backdoor in the event of a reset. Despite those insights, the researcher still didn’t know precisely how that happened. Now, a different researcher has filled in the missing pieces. More about that later. First, a brief summary of xHelper.

A backdoor with superuser rights

The malicious Android app poses as a performance enhancer that removes old and unneeded files. Antivirus provider Malwarebytes has detected it on 33,000 devices, mainly located in the United States, while AV from Russia-based Kaspersky Lab

found it on 50,000 devices. There’s no evidence xHelper has ever been distributed through Google Play.

Once installed, xHelper installs a backdoor that remotely installs apps downloaded from an attacker-controlled server. It also executes commands as a superuser, a powerful privilege setting that gives the malware unfettered system rights. Besides that, the backdoor has access to sensitive data, including browser cookies used to sign in to sites automatically. Once the backdoor is installed, the fake cleaner app disappears from the main screen and program menu and can only be viewed by inspecting the list of installed apps in the system settings.

February’s post was penned by Malwarebytes researcher Nathan Collier. He reported the ordeal one user had in ridding her phone of the malware. Although the AV removed two xHelper variants and a related trojan from her device, xHelper would reinfect the device within an hour. xHelper came back even after she performed a factory reset.

Collier determined that the reinfections were the result of an undetectable file contained inside a hidden folder. The folder was impossible to remove through normal means. It remained unclear precisely how the folder got on infected phones. Collier ruled out the possibility the folder and file came preinstalled on the device. Also unclear was why the file was undetectable by AV and precisely how the malicious file was executed after the AV or a reboot removed the infection.

Triada

Last week, Kaspersky Lab researcher Igor Golovin published a post that filled in some of the gaps. The reinfections, he said, were the result of files that were downloaded and installed by a notorious trojan known as Triada, which ran once the xHelper app was installed. Triada roots the devices and then uses its powerful system rights to install a series

of malicious files directly into the system partition. It does this by remounting the system partition in write mode. To make the files even more persistent, Triada gives them an immutable attribute, which prevents deleting, even by superusers. (Interestingly, the attribute can be deleted using the chattr command.)

A file named install-recovery.sh makes calls to files added to the /system/xbin folder. That allows the malware to run each time the device is rebooted. The result is what Golovin described as an "unkillable" infection that has extraordinary control over a device.

"It is very easy to get infected by xHelper," Golovin told me. "Devices that are attacked by this malware could lack OS security fixes and stay vulnerable for rooting and installing this kind of malware. Moreover, it's very hard for users to remove this malware once it is installed. This means the user base of xHelper can rapidly grow and xHelper can stay active on attacked devices for a long time."

Poisoning the well

The researcher initially thought that it might be possible to remove xHelper by remounting the system partition in write mode to delete the malicious files stored there. He eventually abandoned that theory.

"Triada's creators also contemplated this question, and duly applied another protection technique that involved modifying the system library /system/lib/libc.so," Golovin explained. "This library contains common code used by almost all executable files on the device. Triada substitutes its own code for the mount function (used to mount file systems) in libc, thereby preventing the user from mounting the /system partition in write mode."

Fortunately, the reinfection method divined in last week's

report works only on devices running older Android versions with known rooting vulnerabilities. Golovin, however, held out the possibility that, in some cases, xHelper may maintain persistence through malicious files that come preinstalled on phones or tablets.

People can disinfect devices by using their recovery mode, when available, to replace the infected libc.so file with the legitimate one included with the original firmware. Users can then either remove all malware from the system partition or, simpler still, reflash the device.

Golovin’s analysis provides a valuable case study of a clever technique that may be used again, should new rooting vulnerabilities be found in current versions of Android. The insights could prove helpful both to end users who are comfortable using more advanced features of their phones, as well as security professionals tasked with securing Android devices.

It’s a “very good write up, and [I’m] glad someone was able to reproduce it more thoroughly than I could,” Collier said. It “all seems feasible.”

https://arstechnica.com/?p=1668757