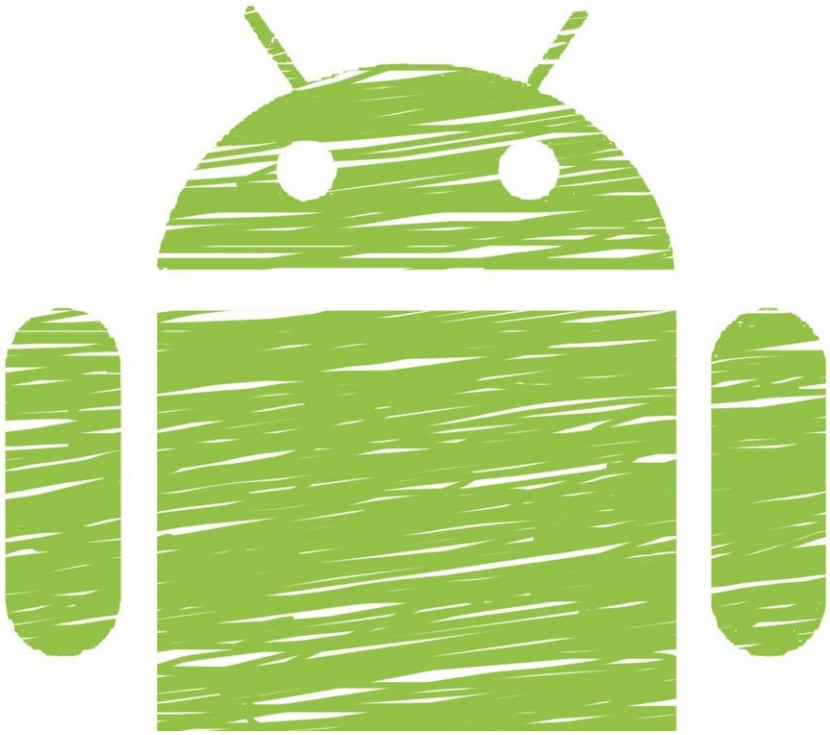
Stubborn strain of Android malware disses resets

February 14 2020, by Nancy Cohen



Credit: CC0 Public Domain

It's being called nasty—oh, the reinfection of it all— and sneaky for good reason: It's all of that, known to headache-watchers as xHelper, which turns out to be of no help at all once infected. The malware xHelper was identified as a trojan dropper.

A trojan dropper? It installs malicious APKs on your phone without your knowledge or permission, said *TechRadar*.

Nathan Collier, malware analyst, Malwarebytes, a company which as its name suggests is in the business of cybersecurity, knows firsthand about this malware-dropper and its persistent use of re-infection tactics.

Android Trojan xHelper is how nasty? Collier wrote that "This is by far the nastiest infection I have encountered as a mobile malware researcher." His work always led him to believe that, though the last option, a factory reset could resolve even the worst infection.

Not this time.

Actually, said Collier, the company knew about this back in 2019. Eventually, reported Dan Goodin in Ars Technica, Malwarebytes would come to learn through its Android antivirus app detection that xHelper was on 33,000 devices "mostly located in the US, making the malware one of the top Android threats."

Consider the report by Symantec back in October 2019.

"Symantec has observed a surge in detections for a malicious Android application that can hide itself from users, download additional malicious apps, and display advertisements."

Symantec nailed its ability to reinstall itself even after users have uninstalled it. Symantec said it was designed to stay hidden. It would not be appearing on the system's launcher.

"The app has infected over 45,000 devices in the past six months." At the very start, the malware's code was relatively simple, but over time the code changed. "Initially, the malware's ability to connect to a C&C

server was written directly into the malware itself, but later this functionality was moved to an encrypted payload, in an attempt to evade signature detection. Some older variants included empty classes that were not implemented at the time, but the functionality is now fully enabled. As described previously, Xhelper's functionality has expanded drastically in recent times."

By November 2019, Bruce Schneier in *Security Boulevard* knew this was not easy in trying to pin down the culprit. "It's a weird piece of malware," he remarked. "That level of persistence speaks to a nation-state actor. The continuous evolution of the malware implies an organized actor. But sending unwanted ads is far too noisy for any serious use. And the infection mechanism is pretty random. I just don't know."

Meanwhile, Collier brought its readers up to recent times, when "a tech savvy user reached out to us in early January 2020 on the Malwarebytes support forum: 'I have a phone that is infected with the xhelper virus. This tenacious pain just keeps coming back.'"

Again, the nastiness resided in its persistence. Collier reported that "Malwarebytes for Android had already successfully removed two variants of xHelper and a Trojan agent from her mobile device. The problem was, it kept coming back within an hour of removal. xHelper was re-infecting over and over again."

Collier said this aspect of the xHelper stands out for him because he could not recall a time that an infection persisted after a factory reset unless the device came with pre-installed malware.

Unlike apps, directories and files remain on the Android mobile device even after a factory reset. Therefore, until the directories and files are removed, the device will keep getting infected. "Luckily, I had Amelia's

help, who was as persistent as xHelper itself in finding an answer and guiding us to our conclusion."

The culprit? In 2020, Collier made some headway. He investigated and this is what he found. "Hidden within a directory named com.mufc.umbtts was yet another Android application package (APK). The APK in question was a Trojan dropper we promptly named Android/Trojan.Dropper.xHelper.VRW. It is responsible for dropping one variant of xHelper, which subsequently drops more malware within seconds."

More of the mystery wafts in: Nowhere on the device did it appear that Trojan.Dropper.xHelper.VRW was installed. "It is our belief that it installed, ran, and uninstalled again within seconds to evade detection—all by something triggered from Google PLAY. The 'how' behind this is still unknown."

Fortunately, Collier wrote about steps to follow, to address xHelper. He had detailed instructions. Collier first of all recommended installing the free Malwarebytes for Android.

He said to install a file manager from Google PLAY that had the capability to search files and directories. Amelia used File Manager by ASTRO. Collier said to disable Google PLAY temporarily, to stop re-infection. More instructions followed in the list.

Collier concluded by taking his readers into the bigger picture: we might have entered a new era in mobile malware. "The ability to re-infect using a hidden directory containing an APK that can evade detection is both scary and frustrating. We will continue analyzing this malware behind the scenes. In the meantime, we hope this at least ends the chapter of this particular variant of xHelper."

Cat Ellis, *TechRadar*: "If you start to see new app and notification icons that you don't recognize, there's a chance that your phone has been infected with this type of malware, though it's not always obvious; malware is often disguised as legitimate system applications, and the icons can be hidden away."

More information: blog.malwarebytes.com/android/ … lp-from-google-play/

Citation: Stubborn strain of Android malware disses resets (2020, February 14) retrieved 2 May 2024 from https://techxplore.com/news/2020-02-stubborn-strain-android-malware-disses.html