

Google says attackers worked with ISPs to deploy Hermit spyware on Android and iOS

A sophisticated spyware campaign is getting the help of internet service providers (ISPs) to trick users into downloading malicious apps, according to research published by Google's Threat Analysis Group (TAG) (via *TechCrunch*). This corroborates earlier findings from security research group Lookout, which has linked the spyware, dubbed Hermit, to Italian spyware vendor RCS Labs.

Lookout says RCS Labs is in the same line of work as NSO Group – the infamous surveillance-for-hire company behind the Pegasus spyware – and peddles commercial spyware to various government agencies. Researchers at Lookout believe Hermit has already been deployed by the government of Kazakhstan and Italian authorities. In line with these findings, Google has identified victims in both countries and says it will notify affected users.

As described in Lookout's report, Hermit is a modular threat that can download additional capabilities from a command and control (C2) server. This allows the spyware to access the call records, location, photos, and text messages on a victim's device. Hermit's also able to record audio, make and intercept phone calls, as well as root to an Android device, which gives it full control over its core operating system.

Apps containing Hermit were never made available via the Google Play or Apple App Store

The spyware can infect both Android and iPhones by disguising itself as a legitimate source, typically taking on the form of

a mobile carrier or messaging app. Google's cybersecurity researchers found that some attackers actually worked with ISPs to switch off a victim's mobile data to further their scheme. Bad actors would then pose as a victim's mobile carrier over SMS and trick users into believing that a malicious app download will restore their internet connectivity. If attackers were unable to work with an ISP, Google says they posed as seemingly authentic messaging apps that they deceived users into downloading.

Researchers from Lookout and TAG say apps containing Hermit were never made available via the Google Play or Apple App Store. However, attackers were able to distribute infected apps on iOS by enrolling in Apple's Developer Enterprise Program. This allowed bad actors to bypass the App Store's standard vetting process and obtain a certificate that "satisfies all of the iOS code signing requirements on any iOS devices."

Apple told *The Verge* that it has since revoked any accounts or certificates associated with the threat. In addition to notifying affected users, Google has also pushed a Google Play Protect update to all users.

<https://www.theverge.com/2022/6/25/23183046/google-hermit-spyware-isp-android-ios>