A Fake Signal App Was Planted On Google Play By China-Linked Hackers

F forbes.com/sites/thomasbrewster/2023/08/30/malicious-signal-app-planted-on-google-play-by-china-linked-cyber-spies/

Thomas Brewster August 30, 2023

China-linked spies snoop on Signal via rogue Google Play and Samsung Galaxy Store apps, researcher claims. (Photo illustration by Jakub Porzycki/NurPhoto via Getty Images)

NurPhoto via Getty Images

A fake version of the private messaging app Signal has found a way onto Google Play and appears to be linked to a Chinese spy operation, researchers claimed on Wednesday.

The hackers, dubbed by researchers at cybersecurity company ESET as GREF, also released a version on Samsung's Galaxy Store. The main aim of the fake Signal, which was called Signal Plus Messenger and functioned the same as the legitimate version, is to spy on communications of the real app, according to ESET researcher Lukas Stefanko.

The standard version of Signal allows users to link the mobile app to their desktop or Apple iPad. The malicious Signal Plus Messenger abused that feature by automatically connecting the compromised device to the attacker's Signal in the background, so all messages were passed onto their account, Stefanko told *Forbes*. That happens “without the user noticing anything or accepting any notification, it is all done in silence,” he said. According to Stefanko, who published a blog and a YouTube video on the machinations of the attack, this was the first documented case of spying on a victim’s Signal via secret “autolinking.”

While the attacks show how Chinese-linked hackers have found a way to get around security checks by two of the world’s biggest tech companies, it also marks an unprecedented attempt to snoop on Signal communications.

Signal president Meredith Whittaker told *Forbes*, “We’re glad that the Play store took this pernicious malware masquerading as Signal off their platform, and we hope they do more in the future to prevent predatory scams via their platform. We’re deeply concerned for anyone who trusted and downloaded this app. We urge Samsung and others to move rapidly to remove this malware.”

A fresh attack on Uyghurs?

According to Stefanko, the same code seen in Signal Plus Messenger was previously used to target Uyghurs.

He found evidence that the same hacking crew also created a malicious Telegram app called Flygram, which was available on Google Play and the Samsung Galaxy Store. Stefanko said that links to download the app was also shared in a Telegram group for Uyghurs.

Stefanko said that while there were fewer than 500 downloads of the fake Signal on Google Play, he believed the attacks were likely targeted, meaning the attackers weren’t going after a broad set of users, but specific individuals.

The fake Telegram may have had a wider impact, though. According to Stefanko, FlyGram was able to access Telegram backups if the user enabled a specific feature in the malware. It was activated by at least 13,953 user accounts.

While Google removed both apps after ESET warned the tech giant, Samsung has not yet taken any action, despite being notified back in May.

Neither Google nor Samsung had responded to requests for comment.

Follow me on Twitter. Check out my website. Send me a secure tip.

Thomas Brewster