Researchers unearth malicious Google Play apps linked to active exploit hackers

reader comments

44 with 30 posters participating

Share this story

Researchers have found more malicious Google Play apps, one of which exploits a serious Android rooting vulnerability so the app can take screenshots and collect other types of sensitive user information.

Camero exploits CVE-2019-2215, a potent vulnerability discovered in October by Google's Project Zero vulnerability research group, researchers from Trend Micro reported on Monday. The use-after-free flaw makes it easy for attackers to gain full root privileges on Pixel 1 and Pixel 2 phones and a host of other Android models. Google patched the vulnerability in October, a few days after Project Zero researcher Maddie Stone reported it was likely under active attack by either exploit developer NSO Group or one of its customers. All three apps are no longer available in Play.

Camero connected to a command and control server that has links to SideWinder, the code name for a malicious hacking group that has been targeting military entities since at least 2012. The app then downloaded attack code that exploits CVE-2019-2215 or a separate exploit in the MediaTek-SU driver that installs an espionage app called callCam. callCam

collected a variety of sensitive user data including:

- Location
- Battery status
- Files on device
- Installed app list
- Device information
- Sensor information
- Camera information
- Screenshot
- Account
- Wi-Fi information
- Data of WeChat, Outlook, Twitter, Yahoo Mail, Facebook, Gmail, and Chrome

To escape detection, callCam hid its icon after installation. It also used a complex cryptographic routine to encrypt stolen data before it was sent to attacker-controlled servers. callCam was also available as a standalone Google Play offering that advertised itself as a call and camera app. A third app, called FileCrypt Manager, meanwhile, installed callCam by abusing Android accessibility permissions to display screen overlays. Underneath, the app installed a series of apps that eventually ended with callCam.

While a certificate in one of the apps suggests the campaign has been active since March, Web search caches here and here show that Camero and callCam received only five and one install, respectively, from Google Play. The number of FileCrypt Manager installs wasn’t immediately clear. Google removed the apps, so they are no longer available in the official Google Play store. It remains unclear if the apps are available elsewhere.

TrendMicro researchers Ecular Xu and Joseph C. Chen said the control servers to which the apps are connected are suspected of being part of the SideWinder infrastructure. A URL linking to one of the apps in Google Play is also found on one of the

control servers. In 2018, researchers at Kaspersky Lab said SideWinder mainly targeted Pakistani military groups and had been active since at least 2012. Last month, a security researcher said on Twitter that SideWinder was likely behind attacks that exploited a now-patched vulnerability in the Equation Editor that’s part of Microsoft Office.

People who want to check Android phones for infections can find indicators of compromise on the above-linked TrendMicro report. Google representatives had no comment for this post other than to confirm the apps have been removed from Play.

https://arstechnica.com/?p=1639397