Google’s Android and Chrome extensions are a very sad place. Here’s why

Photo Illustration by Miguel Candela/SOPA Images/LightRocket via Getty Images

reader comments

56 with

No wonder Google is having trouble keeping up with policing its app store. Since Monday, researchers have reported that hundreds of Android apps and Chrome extensions with millions of installs from the company’s official marketplaces have included functions for snooping on user files, manipulating the contents of clipboards, and injecting deliberately unknown code into webpages.

Google has removed many but not all of the malicious entries, the researchers said, but only after they were reported, and by then, they were on millions of devices—and possibly hundreds of millions. The researchers aren’t pleased.

A very sad place

“I’m not a fan of Google’s approach,” extension developer and researcher Wladimir Palant wrote in an email. In the days before Chrome, when Firefox had a bigger piece of the browser share, real people reviewed extensions before making them available in the Mozilla marketplace. Google took a different approach by using an automated review process, which Firefox then copied.

“As automated reviews are frequently missing malicious extensions and Google is very slow to react to reports (in fact, they rarely react at all), this leaves users in a very sad place,” Palant said.

Researchers and security advocates have long directed the same criticism at Google’s process for reviewing Android apps before making them available in its Play marketplace. The past week provides a stark reason for the displeasure.

On Monday, security company Dr.Web reported finding 101 apps with a reported 421 million downloads from Play that contained code allowing a host of spyware activities, including:

- Obtaining a list of files in specified directories
- Verifying the presence of specific files or directories on the device
- Sending a file from the device to the developer
- Copying or substituting the content of clipboards.

ESET researcher Lukas Stefanko analyzed the apps reported by Dr.Web and confirmed the findings. In an email, he said that for the file snooping to work, users would first have to approve a permission known as READ_EXTERNAL_STORAGE, which, as its name implies, allows apps to read files stored on a device. While that’s one of the more sensitive permissions a user can grant, it’s required to perform many of the apps’ purported purposes, such as photo editing, managing downloads, and working with multimedia, browser apps, or the camera.

Advertisement

Dr.Web said that the spyware functions were supplied by a software developer kit (SDK) used to create each app. The SDKs help streamline the development process by automating certain types of commonly performed tasks. Dr.Web identified the SDK enabling the snooping as SpinOK. Attempts to contact the SpinOK developer for comment were unsuccessful.

On Friday, security firm CloudSEK extended the list of apps

using SpinOK to 193 and said that of those, 43 remained available in Play. In an email, a CloudSEK researcher wrote:

> *The Android.Spy.SpinOk spyware is a highly concerning threat to Android devices, as it possesses the capability to collect files from infected devices and transfer them to malicious attackers. This unauthorized file collection puts sensitive and personal information at risk of being exposed or misused. Moreover, the spyware's ability to manipulate clipboard contents further compounds the threat, potentially allowing attackers to access sensitive data such as passwords, credit card numbers, or other confidential information. The implications of such actions can be severe, leading to identity theft, financial fraud, and various privacy breaches.*

The week didn't fare better for Chrome users who obtain extensions from Google's Chrome Web Store. On Wednesday, Palant reported 18 extensions that contained deliberately obfuscated code that reached out to a server located at serasearchtop[.]com. Once there, the extensions injected mysterious JavaScript into every webpage a user viewed. In all, the 18 extensions had some 55 million downloads.

On Friday, security firm Avast confirmed Palant's findings and identified 32 extensions with 75 million reported downloads, though Avast said the download counts may have been artificially inflated.

It's unknown precisely what the injected JavaScript did because Palant or Avast couldn't view the code. While both suspect the purpose was to hijack search results and spam users with ads, they say the extensions went well beyond being just spyware and instead constituted malware.

"Being able to inject arbitrary JavaScript code into each and every webpage has enormous abuse potential," he explained. "Redirecting search pages is only the one *confirmed* way in

which this power has been abused.”

https://arstechnica.com/?p=1944202