“Joker”—the malware that signs you up for pricey services—floods Android markets

reader comments

31 with 22 posters participating

Share this story

September has been a busy month for malicious Android apps, with dozens of them from a single malware family alone flooding either Google Play or third-party markets, researchers from security companies said.

Known as Joker, this family of malicious apps has been attacking Android users since late 2016 and more recently has become one of the most common Android threats. Once installed, Joker apps secretly subscribe users to pricey subscription services and can also steal SMS messages, contact lists, and device information. Last July, researchers said they found Joker lurking in 11 seemingly legitimate apps downloaded from Play about 500,000 times.

Late last week, researchers from security firm Zscaler said they found a new batch comprising 17 Joker-tainted apps with 120,000 downloads. The apps were uploaded to Play gradually over the course of September. Security firm Zimperium, meanwhile, reported on Monday that company researchers found 64 new Joker variants in September, most or all of which were

seeded in third-party app stores.

And as ZDNet noted, researchers from security firms Pradeo and Anquanke found more Joker outbreaks this month and in July respectively. Anquanke said it had found more than 13,000 samples since it first came to light in December 2016.

“Joker is one of the most prominent malware families that continually targets Android devices,” Zscaler researcher Viral Gandhi wrote in last week’s post. “Despite awareness of this particular malware, it keeps finding its way into Google’s official application market by employing changes in its code, execution methods, or payload-retrieving techniques.”

Digital sleight of hand

One of the keys to Joker’s success is its roundabout way of attack. The apps are knockoffs of legitimate apps and, when downloaded from Play or a different market, contain no malicious code other than a “dropper.” After a delay of hours or even days, the dropper, which is heavily obfuscated and contains just a few lines of code, downloads a malicious component and drops it into the app.

Zimperium provided a flow chart that captures the four pivot points each Joker sample uses. The malware also employs evasion techniques to disguise download components as benign applications like games, wallpapers, messengers, translators, and photo editors.

The evasion techniques include encoded strings inside the samples where an app is to download a dex, which is an Android-native file that comprises the APK package, possibly along with other dexes. The dexes are disguised as mp3 .css, or .json files. To further hide, Joker uses code injection to hide among legitimate third-party packages—such as org.junit.internal, com.google.android.gms.dynamite, or com.unity3d.player.UnityProvider—already installed on the phone.

“The purpose of this is to make it harder for the malware analyst to spot the malicious code, as third-party libraries usually contain a lot of code and the presence of additional obfuscation can make the task of spotting the injected classes even harder,” Zimperium researcher Aazim Yaswant wrote. “Furthermore, using legit package names defeats naïve

[blocklisting] attempts, but our z9 machine-learning engine enabled the researchers to safely detect the aforementioned injection tricks.”

The Zscaler writeup details three types of post-download techniques to bypass Google’s app-vetting process: direct downloads, one-stage downloads, and two-stage downloads. Despite the delivery variations, the final payload was the same. Once an app has downloaded and activated the final payload, the knock-off app has the ability to use the user’s SMS app to sign up for premium subscriptions.

A Google spokesman declined to comment other than to note that Zscaler reported that the company removed the apps once they were privately reported.

Day after day

With malicious apps infiltrating Play on a regular, often weekly, basis, there’s currently little indication the malicious Android app scourge will be abated. That means it’s up to individual end users to steer clear of apps like Joker. The best advice is to be extremely conservative in the apps that get installed in the first place. A good guiding principle is to choose apps that serve a true purpose and, when possible, choose developers who are known entities. Installed apps that haven’t been used in the past month should be removed unless there’s a good reason to keep them around.

Using an AV app from Malwarebytes, Eset, F-Secure, or another reputable maker is also an option, although they, too, can have difficulty detecting Joker or other malware.

https://arstechnica.com/?p=1710247