85 Google Play apps with 8 million downloads forced fullscreen ads on users

reader comments

32 with 23 posters participating

Share this story

Researchers found 85 Google Play apps with more than 8 million downloads that forced users to view fullscreen ads.

The apps, which posed as photography and gaming programs, contained a family of adware that was highly disruptive to end users. Once installed, the apps displayed ads in full screen—a setting that forced users to view the entire duration of an ad before being able to close the window or get back to the app. The apps showed an ad every five minutes, but the people operating the platform had the ability to remotely change the frequency.

AndroidOS_Hidenad.HRXH, as the adware is called, used several tricks to evade detection and removal. A half-hour after being installed, for instance, an app would hide its icon and create a shortcut on the device home screen. (That's according to a write-up from Trend Micro, the security firm that found the apps.) Hiding the icon prevented the apps from being uninstalled by dragging and dropping the icon uninstall section of the device screen. Android 8 and later versions require user confirmation before an app can create a shortcut, but even if users of these versions didn't agree, the icon

would nonetheless remain hidden.

An app would also record two timestamps, “the current time (the device’s system time) as ‘installTime,’ and the network time, whose timestamp is retrieved by abusing a publicly available and legitimate RESTful application programming interface (API), then stored as networkInstallTime.'”

Later, the app would register an Android component, known as a “Broadcast Receiver,” that let the app send or receive system or application events. The purpose: to help monitor if a user was present after the infected device woke up.

Trend Micro researcher Ecular Xu wrote:

> *Every time the user unlocks the device, the adware will perform several checks before it executes its routines. It first compares the current time (the device’s system time) with the timestamp stored as installTime; it then compares the current network time (queried via a RESTful API) with the timestamp stored as networkInstallTime. With these, the adware-embedded app can determine if it has been installed on the device long enough, with the default delay time configured to 30 minutes. To a certain extent, using network time can evade time-based detection techniques or triggers employed by traditional sandboxes, as the app’s time settings can be configured by simply using networkInstallTime.*

If an app determined it had been installed for longer than 30 minutes, it would initiate the hiding of the icon and the creation of the shortcut.

Xu continued:

> *The app also registers another Broadcast Receiver for android.intent.action.USER_PRESENT dynamically to check if the user has unlocked the device. Once conditions are met, advertisements will be displayed on the screen. Similar to*

> *how it hides the icon, it also checks for time before displaying advertisements. It also uses installTime and networkInstallTime to identify how long it has been installed on the device. Apart from that, it also checks the last advertisement to make sure that it doesn’t show the same ad too frequently.*

The list of apps included Super Selfie Camera, Cos Camera, Pop Camera, and One Stroke Line Puzzle. Each of those titles has been downloaded 1 million times, which accounts for about half of the total number of downloads. Other apps (which included Background Eraser, Meet Camera, Pixel Blur, Hi Music Play, and One Line Stroke) each had about 500,000 downloads. The remaining apps are published here.

Trend Micro privately reported the apps to Google. Google then removed the apps from Play.

https://arstechnica.com/?p=1554139