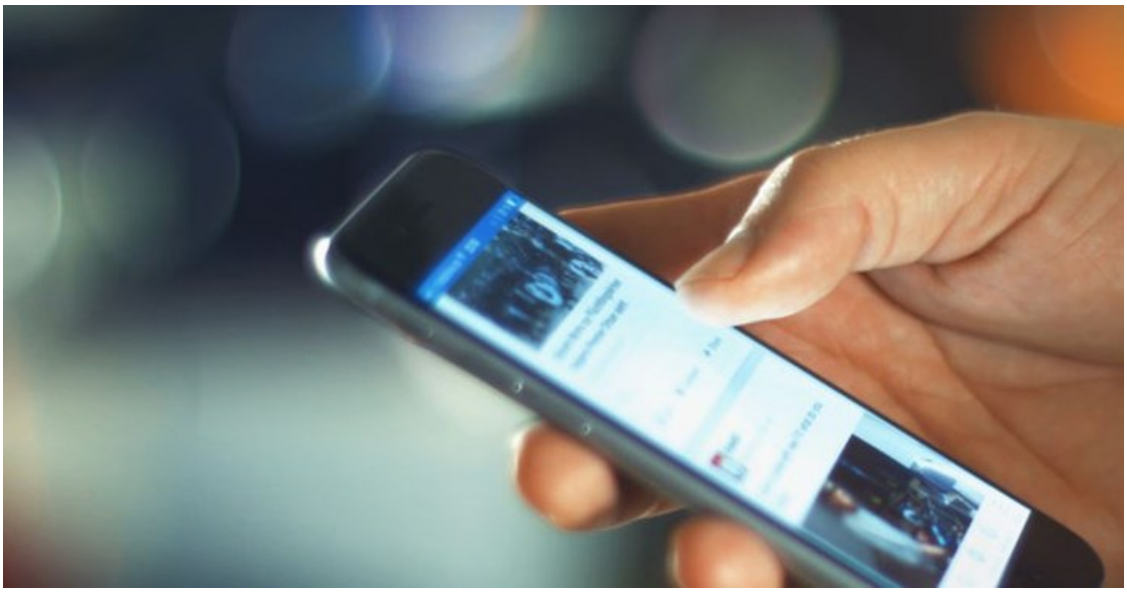
Dangerous security flaw in Android permissions

Check Point researchers have reported a flaw to Google, spotted in one of Android's security mechanisms. Based on Google's policy which grants extensive permissions to apps installed directly from Google Play, the flaw exposes Android users to several types of attacks, including ransomware, banking malware, and adware. According to Google, this issue is already being dealt with in the upcoming version of Android, “Android O”.



© Alexander Kirch via 123RF

Technical background:

In Android version 6.0.0, “Marshmallow”, Google introduced a new permission model for apps. The new model consists of several groups of permissions, with permissions considered as “dangerous” granted only during runtime. This means that during the first time an app tries to access a “dangerous” resource, the user is required to approve the necessary permission.

In addition to the “dangerous” permissions, another category exists, which contains a single permission – System_Alert_Window. Unlike the other permissions, to grant it, the user must go through several menus (Settings -> Apps -> Draw over other apps) and manually allow an app to use it.

The reason System_Alert_Window is unique is the extensive capability it withholds, by enabling an app to display over any other app without notifying the user. This entails a significant potential for several malicious techniques, such as displaying

fraudulent ads, phishing scams, click-jacking, and overlay windows, which are common with banking Trojans. It can also be used by ransomware to create a persistent on-top screen that will prevent non-technical users from accessing their devices.

According to the findings, 74% of ransomware, 57% of adware, and 14% of banker malware abuse this permission as part of their operation. This is clearly not a minor threat, but an actual tactic used in the wild.

The flaw:

Since Google understood the problematic nature of this permission, and the apparent risks for user privacy it created the distinct process mentioned above to approve it. However, this soon caused problems, as this permission is also used by legitimate apps, such as Facebook, which requires it for its Messenger chat heads feature. Since most users won't be able to approve the permission manually, such apps could be hurt by it.

As a temporary solution, Google applied a patch in Android version 6.0.1 that allows the Play Store app to grant run-time permissions, which are later used to grant System_Alert_Window permission to apps installed from the app store. This means that a malicious app downloaded directly from the app store will be automatically granted this dangerous permission.

The impact:

Based on the research, nearly 45% of the applications using the System_Alert_Window permission are apps from Google Play. With the granting of the permission to apps installed from the app store, Google effectively bypasses the security mechanism introduced in the previous version. Google relies heavily on "Bouncer", which scans apps uploaded to Google Play, to keep harmful apps out of it. Unfortunately, malicious apps successfully infiltrate Google Play time after time. FalseGuide and Skinner discovered on Google Play are two recent examples.

Google is working on a fix

After the company reported this flaw, Google responded it has already set plans to protect users against this threat in the upcoming version "Android O". This will be done by creating a new restrictive permission called Type_Application_Overlay, which blocks windows from being positioned above any critical system windows, allowing users to access settings and block an app from displaying alert windows.

How to stay protected in the meantime?

- **Beware of fishy apps:** Users should always beware of malicious apps, even when downloading from Google Play. Look for the comments left by other users, and grant only permissions which have relevant context for the app's purpose.
- **Implement advanced security measures:** Just as you protect your PC with dedicated security solutions, you should also make sure to protect your mobile device using a protective solution capable of identifying and blocking known and unknown malware.