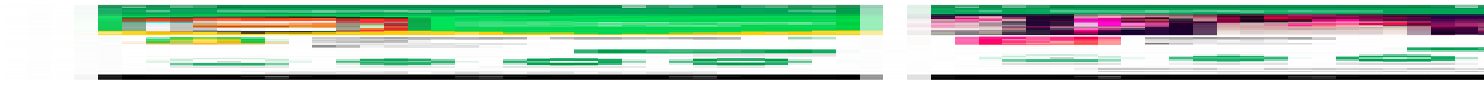
Over 500 Android apps with a combined 100 million downloads found to secretly contain spyware

Unbeknown to the app developers, an advertising software development kit contained code for stealing data from their products' users.

By Danny Palmer | | Topic: Security

- 0
-



Some of the apps which previously used the malicious software -- but which are now clean.

Image: Lookout

More than 500 Android apps, collectively downloaded over 100 million times from the Google Play store, could have been used to secretly distribute spyware to users, thanks to a malicious advertising SDK (software development kit).

More security news

- Android Oreo: Google has just made app installs from unknown sources a lot safer
- Stabbing fruits to breaking your skull: Robot bugs make hacking too easy
- DOJ amends request for data from anti-Trump site
- Cryptocurrency miner malware is enslaving PCs with EternalBlue

Mobile apps -- especially free ones -- commonly use advertising SDKs to deliver ads to their customers through existing advertising networks, thereby generating revenue.

However, security researchers at Lookout have discovered that many app developers inadvertently deployed a rogue SDK called Igexin, which can be exploited for malicious activity.

Google has been informed about Igexin's secret functionality, and all of the compromised apps have now been removed from the Play Store or updated with new, clean versions.

Researchers provided two specific examples of previously-infected apps on Google Play: a photography app called SelfieCity -- downloaded over five million times -- and an app called LuckyCash, which has been downloaded more than a million times. Lookout has confirmed that neither of these apps are now vulnerable to malicious behaviour.

Other infected apps -- not individually identified -- included a game targeted at teenagers with over 50 million downloads, a weather app and a photo app, both with between one million and five million downloads, and an internet radio app with between 500,000 and one million downloads.

Various other apps downloaded from the Google Play Store -- including educational, health and fitness, travel, emoji, and home video camera apps -- were also found to have been compromised.

Ultimately, the ad network has the potential to turn more than 100 million Android phones into malicious spying devices, putting the privacy of users and their employers at risk.

Igexin, which is Chinese in origin, promotes services that claim to leverage data about people, such as their interests, occupation, income and location for the benefit of advertising.

A translated version of the Igexin website, which offers advertising services.

Image: Lookout

Lookout researchers began investigating Igexin when reviewing other apps that communicated with IP addresses and servers known to have distributed malware. They found that many of the apps' requests were being made to an endpoint used by the Igexin ad SDK.

Alarm bells rang because this sort of traffic is commonly used by malware distributors, who specialise in hiding their malicious payloads within apps that appear to be legitimate.

The app developers would have been unaware of the SDK's abuse of app permissions for data collection: this functionality is not immediately obvious, and those behind the malicious code can alter it at any time.

The most exploitative functionality spotted in the Igexin code is log exfiltration, potentially enabling the threat actors to make off with all manner of user data. The apps also employed PhoneStateListener, a legitimate tool in the Android app developers' arsenal, but one with the ability to record details about calls. The infected apps made no indication they could register times of calls and the numbers used.

Despite the offending apps being removed, the vast majority of those who downloaded the dangerous apps are unlikely to be aware that they're even potentially at risk, as apps lack any sort of recall facility; developers must hope that users follow instructions to update their apps.

Although Google keeps the vast majority of its 1.4 billion Android users safe from malware, malicious apps still regularly get through to the official store, with malicious apps often employing various obfuscation techniques circumvent security checks.

Related coverage

Ghost apps live on to torment Android users

Even after they've been removed from the app store, rogue apps can still be causing hassles for the people who downloaded them.

Android alert: This cutesy malware has infected millions of devices

Auto-clicking 'Judy' adware was distributed by over 40 apps in Google's official Android market.