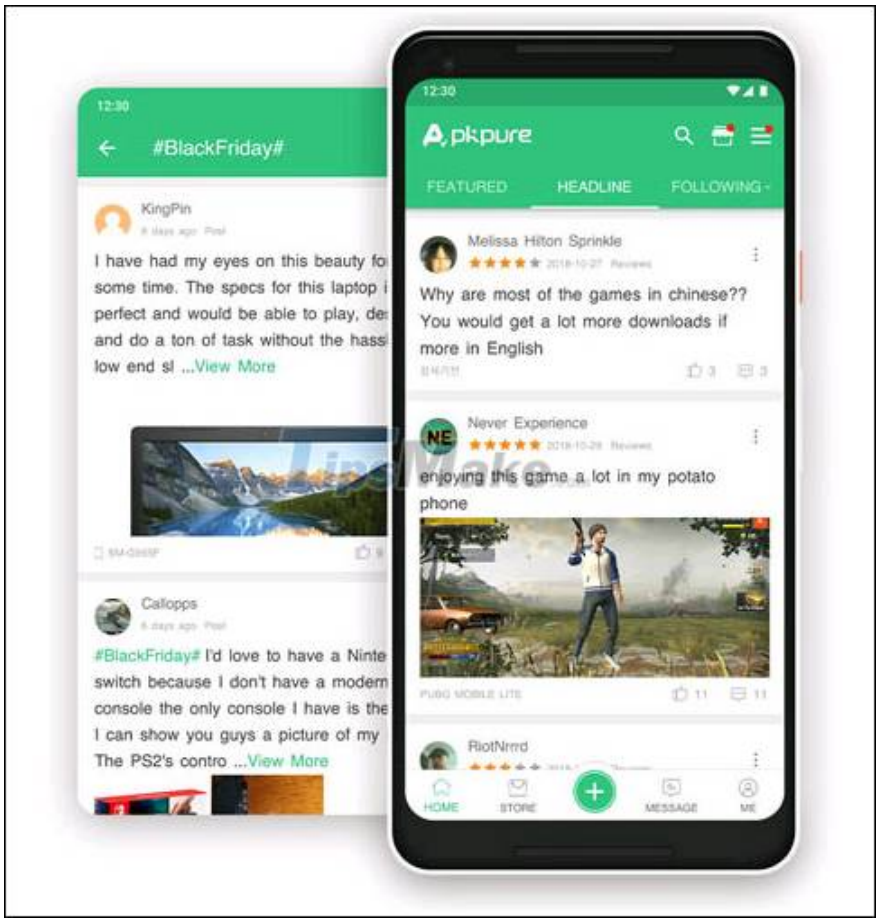
Hackers are taking advantage of the Store to distribute malware

APKPure, one of the world's largest online app stores, a Google Play Store alternative, has been identified as infected with a dangerous strain of malware.

This cheeky attack allows threat actors to actively distribute Trojan malware to Android devices to download apps slowly, which could lead to a large-scale, damaging infection campaign. unpredictable.

More specifically, according to the initial investigation by researchers from Doctor Web and Kaspersky, the APKPure App version 3.17.18 is said to have been tampered with, with malicious code attached. At the same time, hackers will also try to trick users into downloading and installing malicious applications associated with malicious code built into the APKpure application.



" *This Trojan belongs to the dangerous Android.Triada family of malware, possessing the ability to download, install and uninstall software without the user's permission* ," said the Doctor Web team.

According to Kaspersky experts, version 3.17.18 has been intentionally tweaked to integrate the Ads SDK to act as a Trojan spreading tool, designed to deliver other types of malware to the victim's device. " *This component can do a number of tasks such as: displaying ads on the lock screen; opening browser tabs; collecting information about the device; and most annoying is downloading other malware* " According to a Kaspersky researcher.

To overcome the situation, the APKPure side also released a new version for the app (version 3.17.19) on April 9 to remove the malicious component. The developers behind the app distribution platform said in the release notes that they "Fixed a potential security issue, made APKPure Return to a safe state".

There have not been any reports of the damage that APKpure users experienced related to this incident

Infection of malicious code on app store platforms

APKPure is not the only third-party Android app store infected with malware. Earlier this week, Doctor Web researchers also found 10 apps compromised by the Joker (Bread) trojan on Huawei's AppGallery platform. It was also the first time that the malware was detected in the Chinese company's official app store.

Infected applications often come with hidden code that allows it to connect to a command and control server (C2 server) operated by the attacker, to download additional payloads on the device. infected.

In addition, the researchers said there was also 'some other version of Android.Joker' released on Google Play. They are found in apps like Shape Your Body Magical Pro, PIX Photo Motion Maker and a few other names. All of these apps have been removed from the Play Store.