Kaspersky accused the APT32 hacker group of using the Google Play Store to spread spyware for years

Kaspersky security researchers found a malicious campaign called PhantomLance targeting Android device users.

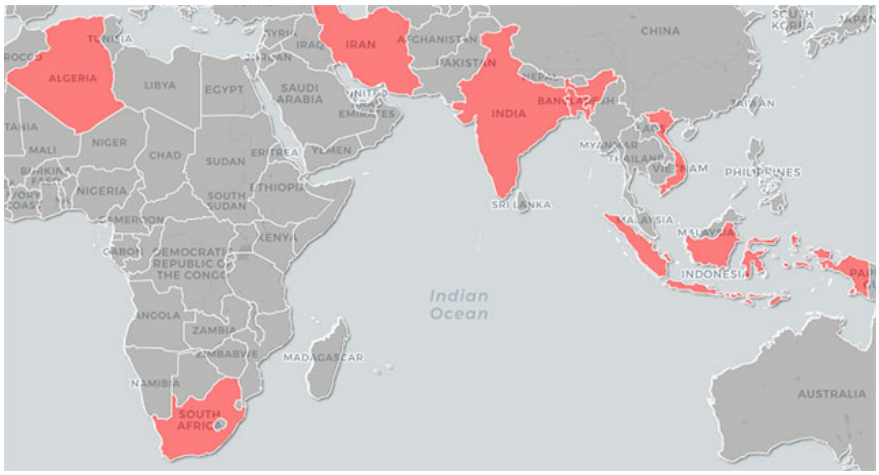
Recently, Kaspersky security researchers discovered a malicious attack campaign called PhantomLance targeting Android device users, possessing malicious payloads as spyware embedded in applications distributed across various platforms, including the Google Play Store and alternative Android app stores such as APKpure and APKCombo.

Specifically, according to Kaspersky's conclusion, PhantomLance has many features that overlap with previously discovered malicious attacks on Windows and macOS due to OceanLotus (also known as APT32), to know more about This hacker group you can read on Wikipedia) is behind the operation. Therefore, it is not without grounds that Kaspersky believes OceanLotus is also the organization behind PhantomLance campaign.

'The campaign has been in operation since at least 2015 and is ongoing, including multiple versions of complex spyware, designed to collect victim data. Along with that is a smart distribution strategy, through dozens of applications on Google Play and other Android application download platforms, " the Kaspersky team said.

Focus on collecting and stealing information

The reason Kaspersky was able to detect the PhantomLance campaign was due to Doctor Web's report of a new backdoor trojan they found on the Play Store, which was designed to be relatively complicated to steal login and financial information. Android users mainly in Southeast Asia, excluding Vietnam. These data include geographic location, call logs, contacts, text messages, list of installed applications and victim's device information.



The country PhantomLance aims to
Not only that, hackers can download and execute various malicious payloads. Therefore, they can adjust the payload to suit the specific environment on the device, such as Android version and installed applications. 'In this way, they can limit the malicious application is overloaded by unnecessary features, and accurately collect the desired data. "

Distributed via multiple Android application download platforms

Kaspersky released a list of Android applications containing PhantomLance malware samples and was later removed from the Play Store by Google in November 2019. Specifically:

Package name	Google Play persistence date (at least)
com.zimice.browserturbo	2019-11-06
com.physlane.opengl	2019-07-10
com.unianin.adsskipper	2018-12-26
com.codedexon.prayerbook	2018-08-20
com.luxury.BeerAddress	2018-08-20
com.luxury.BiFinBall	2018-08-20
com.zonjob.browsercleaner	2018-08-20
com.linevialab.ffont	2018-08-20

Not only the Play Store, PhantomLance is also distributed on a variety of other major Android app download platforms, such as https: // apkcombo [.] Com, https: // apk [.] Support /, https : // apkpure [.] com, https: // apkpourandroid [.] com, and some other platforms.

To avoid being detected and prevented by these platforms, hackers will first upload clean application versions that do not contain any malicious payloads. However, in later updates of the application, malicious payloads will be attached and sent to the victim's device.

"PhantomLance has been going on for more than 5 years and the threat agents have been very successful in trying to bypass the app store's advanced security filters many times with advanced techniques."

Currently, APT32 and PhantomLance campaign are still being closely monitored by Kaspersky.