Hackers antivirus application preinstalled on Xiaomi phones into malware

What's more tragic when the tools that are considered shields for your device can now turn into malware that paves the way for unauthorized infringement, through the 'variable hand? Virtual 'hackers'.

What's more tragic when the tools that are considered shields for your device can now turn into malware that paves the way for unauthorized infringement, through the 'variable hand? Virtual 'hackers'.

Many famous security researchers have revealed late yesterday that a security application is preinstalled on more than 150 million devices manufactured by Xiaomi, China's fourth-largest smartphone company, can be transformed into tools that allow hackers to gain access to Xiaomi smartphones remotely.

1. If using an Android phone, be careful: You may be being tracked without knowing

More specifically, according to CheckPoint, reported issues appear in one of the applications pre-installed on Xiaomi phones named Guard Provider. Basically, Guard Provider is a security application developed by this manufacturer, including three different antivirus programs that allow users to choose from, namely Avast, AVL and Tencent.

By Guard Provider is designed by Xiaomi to be able to integrate as well as provide many 3rd party programs in a single application, so it will have to use some software development kit (SDK), and According to researchers, doing so is not a good idea, simply because the data of an SDK cannot be isolated, so any problems occur with one of the components. This can all affect the whole application.

1. The unsafe 'feature' on UC Browser allows hackers to take control of Android phones remotely

"One of the most obvious potential drawbacks in using some SDKs in the same application is that they all share the same context and application permissions. Despite the small errors in each SDK Individuals can often be an independent problem, but when multiple SDKs are deployed in the same application, it can lead to more serious vulnerabilities due to the fact that the data of an SDK cannot be her. isolated or split ', the researchers explained.

It turned out before receiving the latest patch, basically Guard Provider application has automatically downloaded antivirus signature updates via an unsecured HTTP connection, allowing an intermediate attacker to access the system. Open WiFi network to block network connection on your device, and also push malicious updates to the system.

"After connecting to the same Wi-Fi network with the targeted device - assume in public places, for example at a restaurant, cafe or business center - an attacker will be able to Access to the photo, video and other sensitive data store of Xiaomi smartphone owners, CheckPoint said.

1. Google: Play Protect helped cut 20% of malicious Android application installations by 2018

However, the actual attack scenario is not so simple.

As explained by CheckPoint, researchers have successfully implemented remote code execution on targeted Xiaomi devices after having to exploit four separate problems in two different SDKs available in the application. Use Guard Provider.

The basic attack was facilitated by Guard Provider using an unsecured HTTP connection, along with a path in the transmission path and the lack of digital signature verification during download and installation. update on device.

'The core issue here is that users often put too much faith in smartphone manufacturers, especially for pre-installed applications on the device and are claimed to be able to help protect itself. Their handset is like Guard Provider's case. This is completely understandable. "

1. Android apps contain malicious code that uses motion sensors to avoid detection

Check Point reported the above problems to Xiaomi, the company has confirmed the incident and said it has fixed the problem in the latest version of Guard Provider application. So if you own Xiaomi smartphone, you should make sure your security software is updated to the latest version to avoid unfortunate incidents to your personal data warehouse.