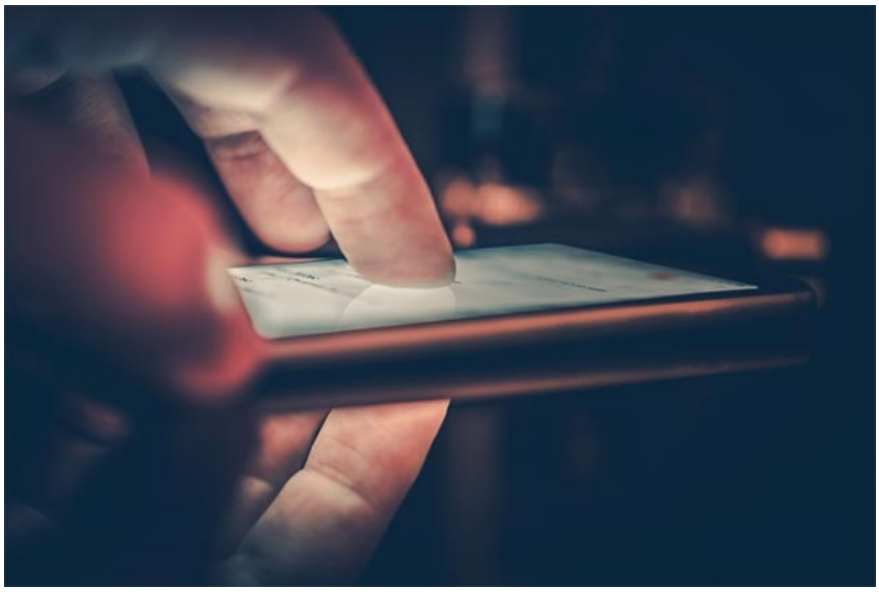
Detect spyware targeting iOS users

Network security researchers have recently discovered the iOS version of a phone spy application, originally designed to target Android devices through applications on Google Play Store.

Network security researchers have recently discovered the iOS version of a phone spy application, originally designed to target Android devices through applications on Google Play Store.

This malware is named Exodus. It is spyware that works on iOS, developed based on the Android version that was discovered by security researchers at LookOut during the analysis of Android models they found last year. .



1. Reveal personal data of more than 1.3 million people from a vulnerability in web application

Unlike the Android variant, the Exodus version on iOS has been distributed outside Apple's official App Store, primarily through phishing sites designed to mimic Italian and Turkmenistan mobile operators to benefit. use lightness from the victim.

Besides, because Apple has always maintained a policy of restricting the application setting directly outside the app store, it is officially the App Store, so the iOS version of Exodus switched to abuse Apple Developer Enterprise program, allowing businesses distribute internal applications directly to their employees without using iOS's App Store, thereby spreading them to personal user devices.

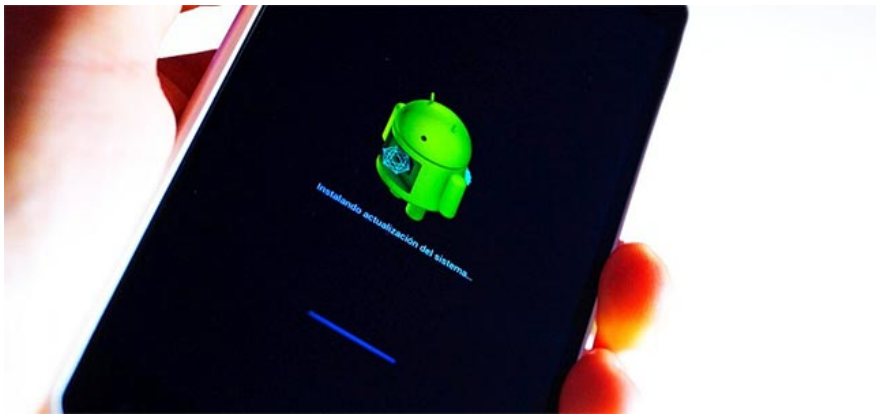
1. Hackers antivirus application preinstalled on Xiaomi phones into malware

This malicious information is shared by LookOut's security experts in a blog post as follows:

"Each phishing site will contain links to a distribution manifest, which contains metadata such as the application name, version, icon and URL for the IPA file. All of these packages used the profile provided with the distribution certificate associated with the company named Connexxa SRL '.

Although the iOS variant of Exodus is less sophisticated than the version on Android, these spyware can still filter important and basic personal information from targeted iPhone devices including , contacts, recording, photos, videos, GPS location and device information.

The stolen data will then be transmitted through HTTP PUT requests to the endpoint on the attacker's command and control server (command and control server), which is a CnC infrastructure like used with the Android version, and also uses the same communication protocols.



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

In addition, some technical details also indicate that Exodus "may be the product of a sponsored spy code development project" and aims to target government or law enforcement agencies. law of the state.

"The operation mechanism of this malicious code includes the use of certificate pinning, general key encryption for communication protocol C2 (C2 communications), and a comprehensive set of monitoring features that are well implemented." , the researchers said.

Developed by an Italian-based company called Connexxa SRL, Exodus appeared on Android at the end of the month before some white-hat hackers from Security Without B Border organization discovered nearly 25 disguised applications. into software services on Google Play Store. Of course these malicious applications were also removed by the tech giant immediately after receiving the notification.

1. The alarming increase in the number of attacks targeted at IoT devices

According to information security researchers obtained, Exodus has been developed for at least 5 years. In addition, Exodus on Android usually includes 3 separate deployment stages. First, malicious code will collect basic identification information, such as IMEI and phone number of the targeted device. The second phase includes multiple binary packages that are responsible for deploying a set of monitoring functions. Finally, at the third stage, malicious code will use 'infamous' DirtyCOW exploits (CVE-2016-5195) to gain root control over infected phones. After successful installation, Exodus can perform a large number of spy requests on the device that is difficult to detect. Besides, the Android variant is also designed to keep running on infected devices even when the user turns off the screen.

While the Android version of Exodus is likely to have infected on 'a few thousand devices or more', it is currently not possible to estimate how many iPhones are infected with the iOS Exodus variant.

After being informed by Lookout researchers about Exodus spyware, Apple immediately revoked the business certificate, preventing malicious applications from being installed on the new iPhone and running on devices. infected.

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

This is the second case in just one year when an Italian software company was caught distributing spyware applications. Earlier last year, another European-based company was also "caught up" distributing "Skygofree", a dangerous spy tool designed exclusively for Android, to help hackers. Full control over remote infection devices.