Malware sneaks into iOS through Apple's official distribution channels

Taking advantage of distribution channels of unapproved applications for testing purposes, malicious code has quietly sneaked into iOS users' devices.

Malware creators have discovered not one but two methods of getting inside the iOS ecosystem, Apple's fenced garden. They use "TestFlight" as well as "WebClips" to trick iPhone and iPad users into installing malicious apps with the ability to steal cryptocurrencies and passwords or perform other malicious activities without being detected. prevent.

Apple always warns about the dangers of sideloading and insists on its own testing process. It's been a long time since Apple required all apps to pass security assessments to be included in the App Store.

The testing process was mostly successful in preventing malicious apps from entering Apple devices. There are of course some exceptions.

But recently, a new report published by security firm Sophos says that some malicious apps have found a way to bypass Apple's app censorship system.

A new campaign called CryptoRom is actively spreading fake crypto apps to iOS and Android users. Since Android allows sideloading, users are at higher risk of voluntarily downloading and installing malware. But the other worry is that Apple's thorough security review process is also being bypassed.

The first method that the CryptoRom team used was to take advantage of TestFlight, a platform that allows iOS users to download and install uncensored apps. Users can download the TestFlight app on the App Store and then download uncensored apps through the app.

By taking advantage of TestFlight, cybercriminals can easily distribute applications filled with malicious code.

The second method is even simpler so it will be more intimidating. CryptoRom uses WebClips, a feature Apple provides to distribute malicious code. Basically WebClips adds website links directly to the iPhone home screen. It has an icon. As a result, cybercriminals can disguise malicious links as a normal app from a legitimate service or platform.

Currently, the guys behind CryptoRom are spreading their malicious apps on social networks, dating sites and dating apps. In other words, they are using social campaigns association to defraud users. Therefore, to be on the safe side, you should not download apps from a source other than the official App Store.