Malware on iOS can pretend to power off iPhone to silently monitor with camera, microphone

Researchers have successfully developed a rather sophisticated attack technique targeting iOS devices. The special feature of this technique is to use a malware to pretend to turn off the iPhone and then silently monitor the user through the camera and microphone.

Previously, when an iOS device was infected with malware, users could easily remove it by restarting the device. This will remove the malware from the device's memory.

However, recently, security researchers have successfully developed a new technique to avoid the removal of malicious code. The special feature of this technique is to use a malware to pretend to turn off / restart the iPhone and then silently monitor the user through the camera and microphone.

The researchers call this technique "NoReboot" and it doesn't exploit any vulnerabilities in iOS. Therefore, it cannot be patched by Apple but can only be detected when users raise their vigilance.

How is the fake iPhone shutdown/reboot process done?

Usually, to power off/reboot your iPhone, you'll have to press and hold the power and volume buttons until a slider with the option to power off/reboot appears. You will then have to wait about 30 seconds for the action to be completed.

When the iPhone is powered off, its screen goes dark, the camera is turned off, the 3D haptic feedback is unresponsive to long press, the sound from calls and notifications is muted, the vibrations are also turned off.

ZecOps security researchers have developed an attack method that can inject special code into three iOS tasks to fake that iPhone has been powered off by disabling all the above indicators. .

First, when the user presses and holds the power button plus the volume button an interface with a fake power off button will appear. This interface will appear earlier than the real iOS interface so that the victim will soon let go. If the victim does not let go soon, the real iOS power off interface will appear.

When the user swipes to turn off the power on the fake interface, another fake power off interface will appear with an animation no different from the real interface. Next, everything of the iPhone will be disabled except the camera and microphone that will still work for the purpose of tracking the victim.

When the victim turns on the power, a fake boot interface continues to display to avoid suspicion. During that process the camera and microphone continued to work without being affected.

You can watch more videos of ZecOps for more details:

Of course, ZecOps also found a way to get the camera and microphone on the iPhone to work without the indicator appearing on the iOS interface.