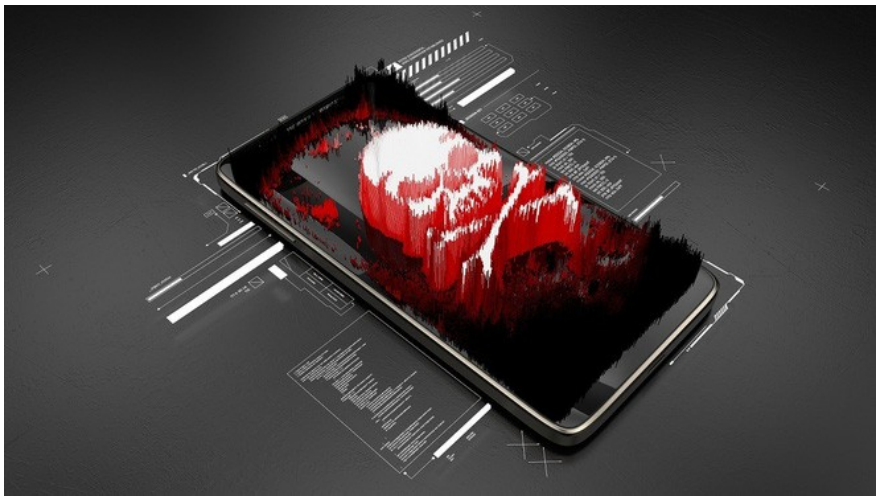
# Discover a new offensive campaign, targeting iPhone users with iOS 12.2 and below

By deceiving users into accessing fake web sites, malicious code on it will crack iPhone and allow hackers to record calls and sounds, eavesdrop on user messages.

The crisis from Covid-19 virus is changing the lifestyle of people around the globe. Buying goods online, working remotely, communicating via chat applications, . a series of internet applications have witnessed a surge in usage. This also means that users face more attacks from hackers.

In early March, security firm Trend Micro said about a cyberattack campaign targeting users in Southeast Asia with sophisticated spyware called LightSpy. Subsequently, Kaspersky's Global Research and Analysis Group also published some important details about the attack targeting smartphone users through links on various forums and media channels.



In this offensive campaign, websites containing malicious code will be designed by hackers like the original websites that victims often visit. When the victim visits the malicious website, the exploit chain that is installed on it will deploy malicious software to the victim's smartphone.

The malware is currently targeting iPhones running iOS 12.2 and below, and the latest iPhones for iOS 13.4 are not being attacked in this campaign. Android users are also targeted by hackers. In addition, Kaspersky has detected the existence of malware targeting Mac, Linux and Windows computers, along with Linux-based routers.

To trick users into visiting this malicious website, hackers often spread its link through forum posts as well as popular social networks. When the victim accesses this malicious website, malware will crack the victim's device and allow the hacker to record calls and sounds, read messages from certain applications.

According to Kaspersky's recommendation, to avoid becoming a victim of this attack, as well as similar attacks, users avoid clicking on suspicious links, especially if they are shared on social networks.

- Check the authenticity of the website by checking the URL link format or spelling of the company name, checking domain registration data. Do not visit websites until they are sure they are valid.

- Install reliable security applications for your device to effectively protect against threats.