Detect spyware that infects iMessage even if the user has not read the message

An analysis report by Amnesty International recently revealed that a type of military-grade spyware successfully broke into the iPhones of journalists by sending them iMessage messages that the recipients did not even click. to enter.

This spyware is developed by the Israeli company NSO Group, a private company specializing in selling high-end hacking tools whose customers include governments in many countries. As reported by Amnesty International and 17 other newspapers, NSO Group's Pegasus software was used by these customers to hack into the phones of at least 37 journalists, activists, politicians, and journalists. business leaders around the world. NSO Group denies this allegation, and asserts that the report contains many serious false content as well as lack of credible evidence.

According to a report by Amnesty International, the method they use to analyze the phones of the targeted victims, thereby detecting whether they have been tampered with by the Pegasus software. The organization found evidence of a type of iMessage attack called "zero-click", which has been targeting journalists since 2018, and this shows the alarming security of the phone line. iPhones from Apple. This type of zero-click attack does not require any interaction on the part of the victim to break into their phone!

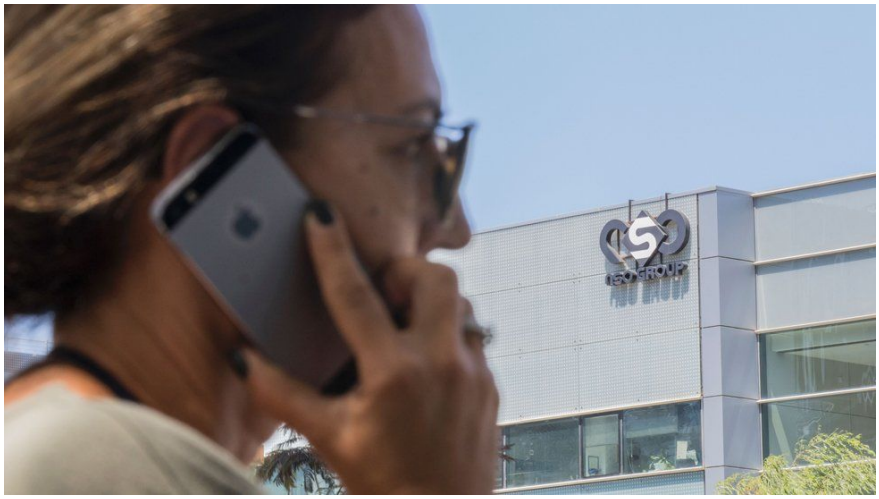
Amnesty says it analyzed a fully updated iPhone 12, belonging to an Indian journalist, with signs of tampering following a June 16 zero-click attack. .

"These latest findings show that NSO Group customers can now remotely interfere with any iPhone model and any recent iOS version," the report said.

Bill Marczak, a researcher at the University of Toronto's Citizen Lab specializing in digital surveillance, posted on Twitter that his lab had also found evidence of zero-click messaging attacks being used to Break into the latest iPhone models.

Marczak said that some such attacks focus on exploiting Apple's ImageIO vulnerability, which allows Apple devices to read and display images.

Amnesty also found evidence of a zero-click attack targeting an Azerbaijani journalist in 2020, but related to Apple Music. Accordingly, their analysts could not be sure whether Apple Music was used to infect phones with spyware, or if the spyware came from another application. The organization has also reported the results to Apple and hopes the company will study the matter more closely.



According to Amnesty, NSO Group customers have previously used a series of attacks to send malicious links to victims, and victims' devices were only infected after they had clicked on the link.

As for Apple, the company asserts that the iPhone remains one of the safest consumer devices on the planet.

"The attacks described above are very sophisticated, cost millions of dollars to develop, often have a short lifecycle, and are used to target specific individuals" - chief security engineer of Apple, Ivan Krstic, said, adding that Apple has always prioritized security updates, and that the vast majority of users are not at risk of such attacks.

NSO Group says its software is used to fight terrorism and crime. The company also says that once the products are sold to customers, they will not operate them and have no information on how they are deployed.

Previously, NSO Group was accused of facilitating device hacks of journalists. Facebook sued NSO Group in October 2019 on the grounds that the company's tools were used to hack WhatsApp accounts of journalists, politicians, social activists. Asking the hacker to call the victim's WhatsApp is enough to hack their phone!