iPhones running latest iOS hacked to deploy NSO Group spyware

bleepingcomputer.com/news/security/iphones-running-latest-ios-hacked-to-deploy-nso-group-spyware/

Sergiu Gatlan

By
Sergiu Gatlan

- July 19, 2021
- 05:03 AM
- 2

Human rights non-governmental organization Amnesty International and non-profit project Forbidden Stories revealed in a recent report that they found spyware made by Israeli surveillance firm NSO Group deployed on iPhones running Apple's latest iOS release, hacked using zero-day zero-click iMessage exploits.

"Amnesty International has observed evidence of compromise of the iPhone XR of an Indian journalist (CODE INJRN1) running iOS 14.6 (latest available at the time of writing) as recently as 16th June 2021," the report reads.

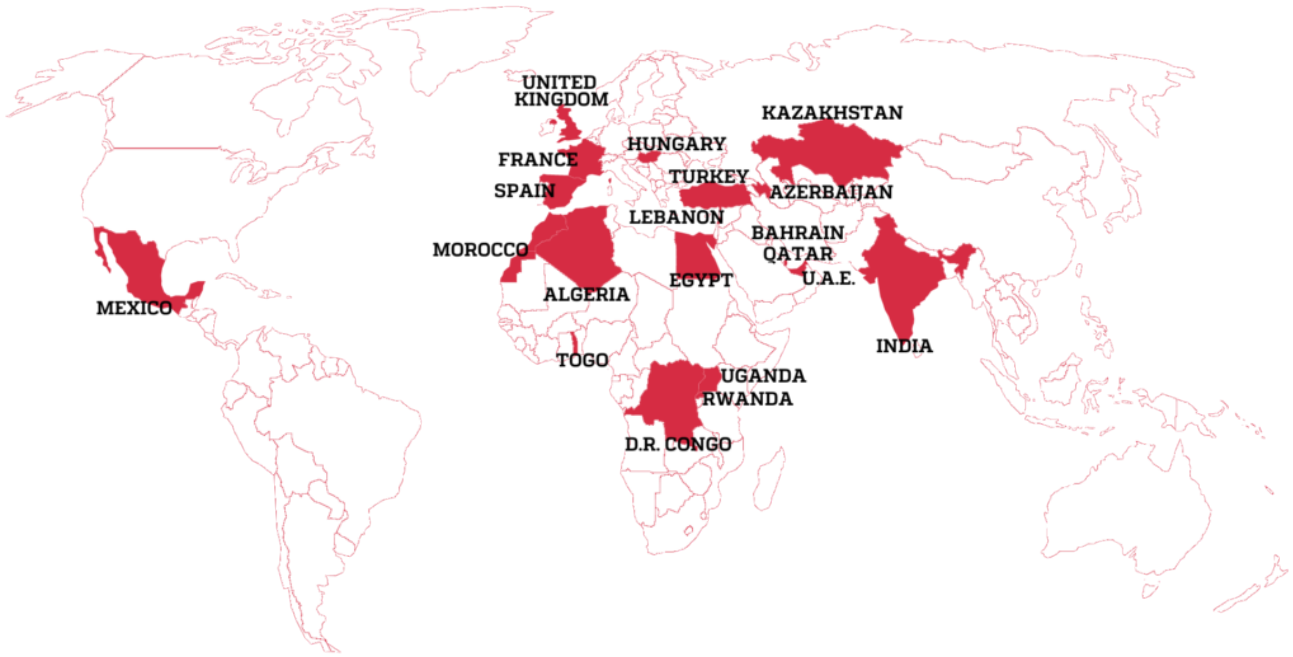
"Lastly, Amnesty International has confirmed an active infection of the iPhone X of an activist (CODE RWHRD1) on June 24th 2021, also running iOS 14.6.

"Most recently, a successful "zero-click" attack has been observed exploiting multiple zero-days to attack a fully patched iPhone 12 running iOS 14.6 in July 2021."

The NGO also sad that it reported this information to Apple, who said that they are investigating the matter.

"Attacks like the ones described are highly sophisticated, cost millions of dollars to develop, often have a short shelf life, and are used to target specific individuals," Ivan Krstić, head of Apple Security Engineering and Architecture, told The Washington Post.

"While that means they are not a threat to the overwhelming majority of our users, we continue to work tirelessly to defend all our customers, and we are constantly adding new protections for their devices and data."



Countries where journalists were targeted with spyware (Forbidden Stories)

Findings confirmed by Citizen Lab's peer review

Bill Marczak, a research fellow at academic research lab Citizen Lab, also revealed that an independent peer review of Amnesty's report said that the forensic methodology is sound and led to additional evidence supporting the report's findings.

Citizen Lab was able to independently observe NSO Pegasus spyware deployed on an iPhone 12 Pro Max running iOS 14.6 (the OS's latest release), hacked via a zero-day zero-click iMessage exploit, which does not require interaction from the target.

The researchers also discovered zero-click iMessage attacks that led to Pegasus being installed on an iPhone SE2 phone running iOS version 14.4 and an iPhone SE2 device running iOS 14.0.1.

"The mechanics of the zero-click exploit for iOS 14.x appear to be substantially different than the KISMET exploit for iOS 13.5.1 and iOS 13.7, suggesting that it is in fact a different zero-click iMessage exploit," Citizen Lab added.

Pegasus is a spyware tool developed by NSO Group and marketed as a surveillance tool "licensed to legitimate government agencies for the sole purpose of investigating crime and terror."

"These most recent discoveries indicate NSO Group's customers are currently able to remotely compromise all recent iPhone models and versions of iOS," Amnesty International and Forbidden Stories said in their report.

> It also indicates that Apple has a MAJOR blinking red five-alarm-fire problem with iMessage security that their BlastDoor Framework (introduced in iOS 14 to make zero-click exploitation more difficult) ain't solving.
>
> — Bill Marczak (@billmarczak) July 18, 2021

NSO Group spyware used in high-profile attacks

This is just one of a long string of reports and papers documenting NSO Group's Pegasus spyware being used to spy on human rights defenders (HRDs) and journalists worldwide.

For instance, two years ago, Facebook sued Israeli cyber-surveillance firm NSO Group and its parent company for creating and selling a WhatsApp zero-day exploit.

The zero-day exploit was later used to hack and infect the devices of high-profile targets such as government officials, diplomats, and journalists with spyware.

Researchers at Citizen Lab revealed in 2018 that they found some Pegasus licensees using it actively for cross-border surveillance and in countries with a history of abusive behavior by state security services.

In collaboration with Microsoft, Citizen Lab also reported last week that they found links between another Israeli surveillance firm known as Candiru to new Windows spyware dubbed DevilsTongue deployed on targets' computers via now patched Windows zero-day vulnerabilities.

"Candiru is a secretive Israel-based company that sells spyware exclusively to governments," Citizen Lab said. "Reportedly, their spyware can infect and monitor iPhones, Androids, Macs, PCs, and cloud accounts."

Microsoft researchers discovered "at least 100 victims in Palestine, Israel, Iran, Lebanon, Yemen, Spain, United Kingdom, Turkey, Armenia, and Singapore," with the list of victims including "politicians, human rights activists, journalists, academics, embassy workers, and political dissidents."

Related Articles:

Newly found zero-click iPhone exploit used in NSO spyware attacks

Google: Predator spyware infected Android devices using zero-days

Protect your iPhone's data with this backup software deal

Bearded Barbie hackers catfish high ranking Israeli officials

Newly found Android malware records audio, tracks your location

- Amnesty International
- Citizen Lab
- Forbidden Stories
- iOS
- iPhone
- NSO Group
- Pegasus Spyware
- Spyware

Sergiu Gatlan

Sergiu Gatlan is a reporter who covered cybersecurity, technology, Apple, Google, and a few other topics at Softpedia for more than a decade. Email or Twitter DMs for tips.

- Previous Article
- Next Article

Comments

- 
  Some-Other-Guy - 10 months ago
  -
  -

  Meanwhile, in other news.....

  Still no spyware, ransomware or other malware affecting my Windows XP box after 7 years ONLINE!

- 
  NoneRain - 10 months ago
  -
  -

  https://www.psychologyhelp.com/

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: