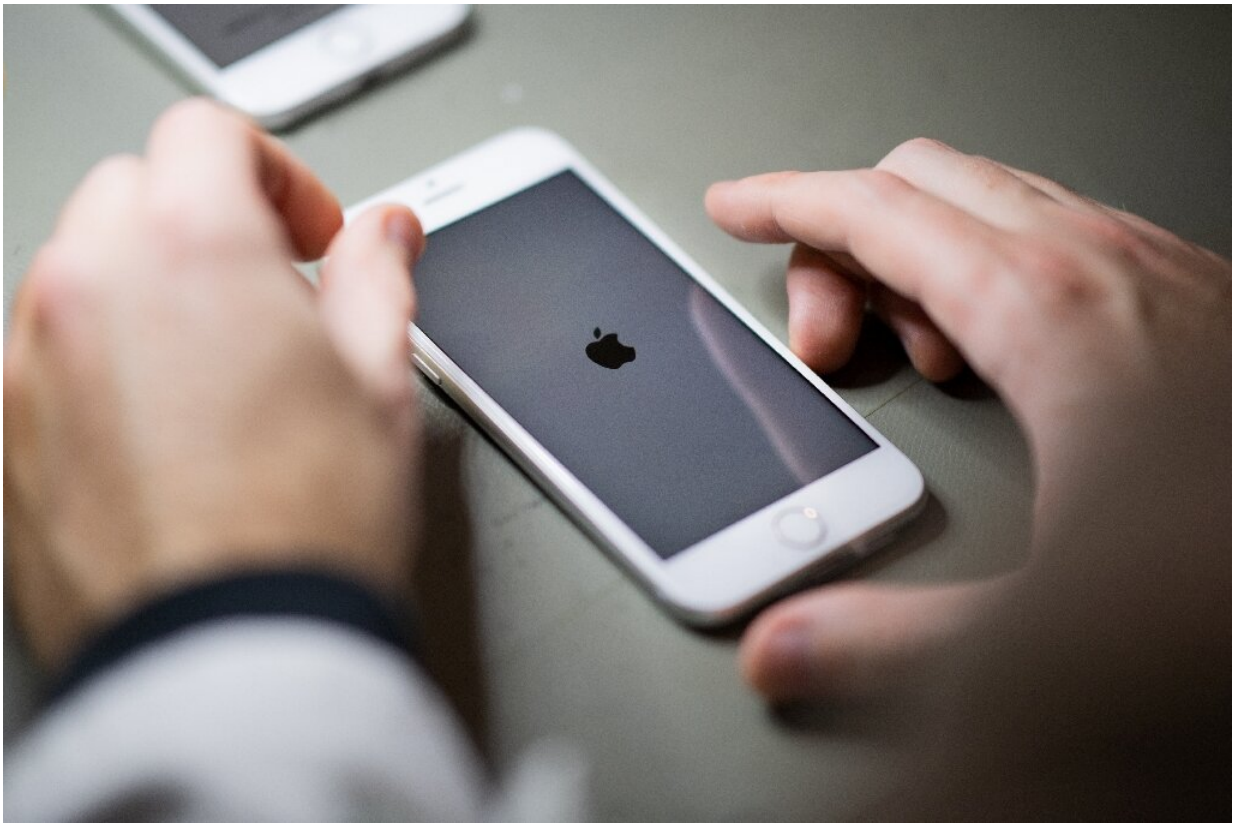
Apple security flaw: How do 'zero-click' attacks work?

September 14 2021, by Katy Lee



You don't even need to click on anything for 'zero-click' malware to infect your phone.

Apple has spent the past week rushing to develop a fix for a major security flaw which allows spyware to be downloaded on an iPhone or

iPad without the owner even clicking a button.

But how do such "zero-click" attacks work, and can they be stopped?

What is a 'zero-click' hack?

Spying software has traditionally relied on convincing the targeted person to click on a booby-trapped link or file in order to install itself on their phone, tablet or computer.

"Zero-click takes that threat to the next level," said John Scott-Railton, senior researcher at Citizen Lab, the Toronto University cybersecurity centre which discovered the Apple flaw.

With a zero-click attack, the software can sneak its way onto the device without the person needing to be fooled into clicking on the link.

That grants would-be spies much easier access, not least in an era when people have grown increasingly wary of clicking on suspicious-looking messages.

In this case, the malware exploited a hole in Apple's iMessage software to stealthily install Pegasus, a hugely invasive piece of software that essentially turns a phone into a pocket listening device.

Allegations that the software has been used by governments worldwide to eavesdrop on human rights activists, business executives and politicians sparked a global scandal in July.

Will I know if my phone is infected?

A simple answer: "No," said Scott-Railton.

"There's nothing you can do as a user to protect yourself from infection, and nothing you're going to see when you're infected," he told AFP.

That is partly why Apple has taken the threat so seriously, he said.

Scott-Railton urged Apple users to install the software update released by the tech giant on Monday.

Apple announced a fix for the problem just under a week after Citizen Lab reported it on September 7.

A fix of this speed is "a rarity, even for a big company", Scott-Railton said.

Why are messaging apps so vulnerable?

Revelations of Apple's iMessage flaw come after messaging service WhatsApp discovered in 2019 that it, too, had a zero-click vulnerability that was being used to install Pegasus on phones.

Scott-Railton said the ubiquity of such apps meant it was not surprising that the NSO Group, the scandal-hit Israeli company behind Pegasus, had used them to sneak onto people's devices.

"If you find a phone, there's a good chance that there's a popular messaging app on it," he explained.

"Finding a way to infect phones through messaging apps is an easy and quick way to accomplishing what you want."

The fact that messaging apps allow people to be identified with their phone numbers, which are easily locatable, also "means that there are a huge target for both nation-states and commercial mercenary hacking

operations like NSO," he said.

Can such hacks be stopped?

Vivien Raoul, chief technical officer at French cybersecurity firm Pradeo, said the discovery of the iMessage flaw was "a good start for reducing the ports of entry, but it's unfortunately not enough to stop Pegasus".

Malware-makers can simply look for other weaknesses in widely used apps, which inevitably include flaws from time to time due to their complexity, say experts.

Google's mobile operating system Android and Apple's iOS regularly "correct a large number of vulnerabilities", Raoul said.

NSO, whose recruits include former elite members of Israeli military intelligence, has formidable resources of its own to invest in the hunt for weak spots, while hackers also sell access to them on the dark web.

Citation: Apple security flaw: How do 'zero-click' attacks work? (2021, September 14) retrieved 26 April 2024 from https://techxplore.com/news/2021-09-apple-flaw-zero-click.html