Apple issues update after cyber weapon captured

August 26 2016

Apple released its latest iOS version, 9.3.5, which the New York Times said was meant to fix three security vulnerabilities in Apple products

Apple iPhone owners on Friday were urged to install a quickly released security update after a sophisticated attack on an Emirati dissident exposed vulnerabilities targeted by cyber arms dealers.

Researchers at Lookout mobile security firm and Citizen Lab at the

University of Toronto said they uncovered a fierce, three-pronged cyber attack targeting a dissident's iPhone "that subverts even Apple's strong security environment."

Lookout and Citizen Lab worked with Apple on an iOS patch to defend against what was called "Trident" because of its triad of attack methods, the researchers said in a joint blog post.

"We were made aware of this vulnerability and immediately fixed it with iOS 9.3.5," Apple said in a released statement.

Trident is used in spyware referred to as Pegasus, which a Citizen Lab investigation showed was made by an Israel-based organization called NSO Group.

It was acquired by the US firm Francisco Partners Management six years ago, according to Lookout and Citizen.

Lookout referred to Pegasus as the most sophisticated attack it has seen, sneakily accessing calls, cameras, email, passwords, apps and more on iPhones.

The spyware was detected when used against Ahmed Mansoor, a human rights activist in the United Arab Emirates, who has been repeatedly targeted using spyware.

Phishing scheme

After receiving a suspicious text with a link, he reported the matter to Citizen Lab, which worked in conjunction with San Francisco-based Lookout to research the affair.

"The attack sequence, boiled down, is a classic phishing scheme: send

text message, open web browser, load page, exploit vulnerabilities, install persistent software to gather information," the joint blog post said.

"This, however, happens invisibly and silently, such that victims do not know they've been compromised."

Mansoor received text messages on August 10 and 11 promising that secrets about detainees being tortured in UAE jails could be accessed by clicking on an enclosed link, researchers said.

Had he fallen for the ruse, the Trident chain of "zero-day exploits" would have broken into his iPhone and installed snooping software.

Once infected, Mansoor's iPhone would have been turned into a "spy in his pocket" capable of tracking his whereabouts and conversations, Citizen Lab said.

Mansoor was targeted five years ago with FinFisher spyware and again the following year with Hacking Team spyware, according to Citizen Lab research.

"The use of such expensive tools against Mansoor shows the lengths that governments are willing to go to target activists," the researchers said.

Although the cyber attack on Mansoor was not linked to a specific government, Citizen Lab said indicators pointed to the UAE.

UAE authorities did not comment on the matter.

Lookout and Citizen believe the spyware has been "in the wild for a significant amount of time."

"It is also being used to attack high-value targets for multiple purposes,

including high-level corporate espionage on iOS, Android and Blackberry."

Citizen Lab has also found evidence that "state-sponsored actors" used NSO weapons against a Mexican journalist who reported on high-level corruption in that country and on an unknown target in Kenya.

The NSO tactics included impersonating sites such as the International Committee of the Red Cross, the British government's visa application processing website, and a wide range of news organizations and major technology companies, the researchers said.

Cyber arms dealers

Mansoor's decision to enlist Citizen Lab instead of falling into the trap gave researchers a rare chance to expose the work of "shady cyber arms dealers" who command high prices for morally questionable services, Lookout vice president of security research Mike Murray told AFP.

Invoices posted online have shown that hackers can charge tens of thousands of dollars per target hit with their software.

"The smartphone is a valuable target, and breaking into it is a valuable skill set," Murray said.

"People who can do this, and with wiggle room in their moral code, have realized the business opportunity."

NSO Group has been around since 2010 and the capture of one of its weapons was billed as a first.

Studying Trident has helped cyber defenders find ways to spot spyware that had been operating unseen, and they are "actively catching it in the

wild now," Murray said.

He declined to reveal anything about other targets, saying that they were people likely to be under surveillance in other ways by local authorities.

Citizen Lab saw the attack on Mansoor as further evidence that "lawful intercept" spyware has significant abuse potential, and that some governments can't resist the temptation to use such tools against political opponents, journalists and human rights defenders.