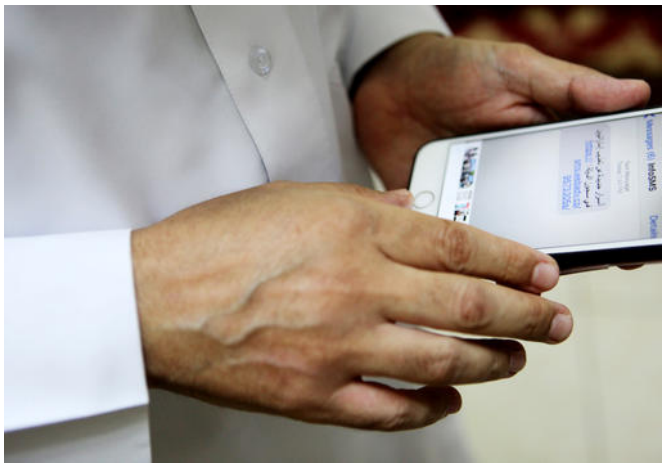
Apple boosts iPhone security after Mideast spyware discovery

25 August 2016, by Raphael Satter And Daniella Cheslow



Human rights activist Ahmed Mansoor shows Associated Press journalists a screenshot of a spoof text message he received in Ajman, United Arab Emirates, on Thursday, Aug. 25, 2016. Mansoor was recently targeted by spyware that can hack into Apple's iPhone handset. The company said Thursday it was updated its security. The text message reads: "New secrets on the torture of Emirati citizens in jail." (AP Photo/Jon Gambrell)

A botched attempt to break into the iPhone of an Arab activist using hitherto unknown espionage software has trigged a global upgrade of Apple's mobile operating system, researchers said Thursday.

The spyware took advantage of three previously undisclosed weaknesses in Apple's mobile operating system to take complete control of iPhone devices, according to reports published Thursday by the San Francisco-based Lookout smartphone security company and internet watchdog group Citizen Lab. Both reports fingered the NSO Group, an Israeli company with a reputation for flying under the radar, as the author of the spyware.

"The threat actor has never been caught before," said Mike Murray, a researcher with Lookout, describing the program as "the most sophisticated spyware package we have seen in the market."

The reports issued by Lookout and Citizen Lab—based at the University of Toronto's Munk School of Global Affairs—outlined how an iPhone could be completely compromised with the tap of a finger, a trick so coveted in the world of cyberespionage that in November a spyware broker said it had paid a $1 million dollar bounty to programmers who'd found a way to do it. Such a compromise would give hackers full control over the phone, allowing them to eavesdrop on calls, harvest messages, activate cameras and microphones and drain the device of its personal data.

Arie van Deursen, a professor of software engineering at Delft University of Technology in the Netherlands, said both reports were credible and disturbing. Forensics expert Jonathan Zdziarski described the malicious program as a "serious piece of spyware."

Apple said in a statement that it fixed the vulnerability immediately after learning about it, but the security hole may have gone unpatched had it not been for the wariness of an embattled human rights activist in the United Arab Emirates.

Ahmed Mansoor, a well-known human rights defender, first alerted Citizen Lab to the spyware after receiving an unusual text message on Aug. 10. Promising to reveal details about torture in the United Arab Emirates' prisons, the unknown sender included a suspicious-looking link at the bottom of the message.

Human rights activist Ahmed Mansoor speaks to Associated Press journalists in Ajman, United Arab Emirates, on Thursday, Aug. 25, 2016. Mansoor was recently targeted by spyware that can hack into Apple's iPhone handset. The company said Thursday it has updated its security. (AP Photo/Jon Gambrell)

Mansoor wasn't convinced. Not only had he been imprisoned, beaten, robbed and had his passport confiscated by the authorities over the years, Mansoor had also repeatedly found himself in the crosshairs of electronic eavesdropping operations. In fact Mansoor already had the dubious distinction of having weathered attacks from two separate brands of commercial spyware. And when he shared the suspicious text with Citizen Lab researcher Bill Marczak, they realized he'd been targeted by a third.

Marczak, who'd already been looking into the NSO Group, said he and fellow-researcher John Scott-Railton turned to Lookout for help picking apart the malicious program, a process which Murray compared to "defusing a bomb."

"It is amazing the level they've gone through to avoid detection," he said of the software's makers. "They have a hair-trigger self-destruct."

Working feverishly over a two-week period, the researchers found that Mansoor had been targeted by an unusually sophisticated piece of software which likely cost a small fortune to arm.

"Ahmed Mansoor is a million-dollar human rights defender," Scott-Railton said.

In a statement which stopped short of acknowledging that the spyware was its own, the NSO Group said its mission was to provide "authorized governments with technology that helps them combat terror and crime."

The company said it had no knowledge of any particular incidents. It said it would not make any further comment.

Human rights activist Ahmed Mansoor speaks to Associated Press journalists in Ajman, United Arab Emirates, on Thursday, Aug. 25, 2016. Mansoor was recently targeted by spyware that can hack into Apple's iPhone handset. The company said Thursday it has updated its security. (AP Photo/Jon Gambrell)

The apparent discovery of Israeli-made spyware being used to target a dissident in the United Arab Emirates raises awkward questions for both countries. The use of Israeli technology to police its own citizens is an uncomfortable strategy for an Arab country with no formal diplomatic ties to the Jewish state. And Israeli complicity in a cyberattack on an Arab dissident would seem to run counter to the country's self-description as a bastion of democracy in the Middle East.

Authorities in both countries did not return calls seeking comment.

Attorney Eitay Mack, who advocates for more transparency in Israeli arms exports, said his country's exports of surveillance software were not closely policed.

"Surveillance is not considered a lethal weapon," Mack said. And Israeli regulations "don't take into consideration human rights or that it would be used by a government to oppress dissidents."

He noted that Israeli Prime minister Benjamin Netanyahu has cultivated ties with Arab Gulf states. Netanyahu in 2014 urged Saudi Arabia and the United Arab Emirates to join him in the war on terrorism.

"Israel is looking for allies," Mack said. "And when Israel finds allies, it does not ask too many questions."