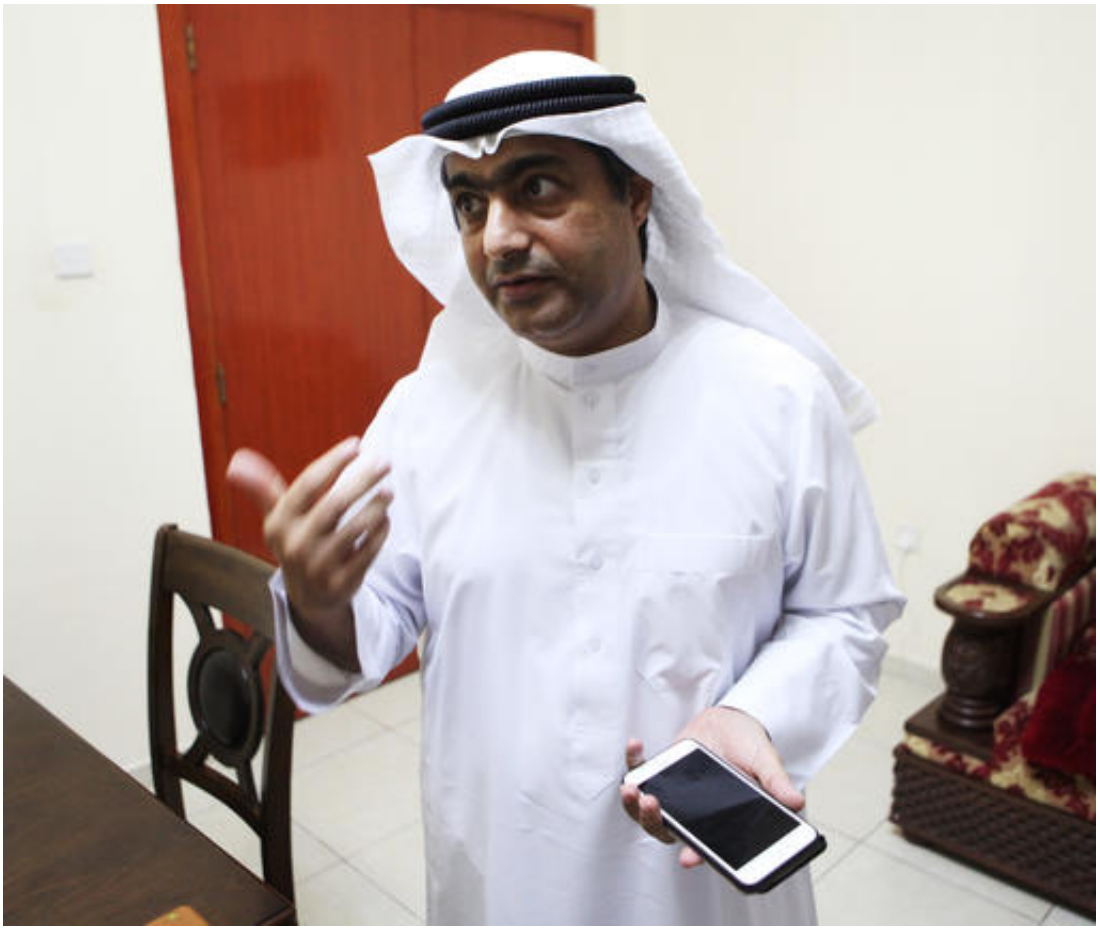
Activist discovers iPhone spyware, sparking security update

August 26 2016, by Raphael Satter, Jon Gambrell And Daniella Cheslow



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 suspicious text message that appeared on Ahmed Mansoor's iPhone promised to reveal details about torture in the United Arab Emirates' prisons. All Mansoor had to do was click the link.

Mansoor, a human rights activist, didn't take the bait. Instead, he reported it to Citizen Lab, an internet watchdog, setting off a chain reaction that in two weeks exposed a secretive Israeli cyberespionage firm, defanged a powerful new piece of eavesdropping software and gave millions of iPhone users across the world an extra boost to their digital security.

"It feels really good," Mansoor said in an interview from his sand-colored apartment block in downtown Ajman, a small city-state in the United Arab Emirates.

Cradling his iPhone to show The Associated Press screenshots of the rogue text, Mansoor said he hoped the developments "could save hundreds of people from being targets."

Hidden behind the link in the text message was a highly targeted form of spyware crafted to take advantage of three previously undisclosed weaknesses in Apple's mobile operating system.

Two reports issued Thursday, one by Lookout, a San Francisco mobile security company, and another by Citizen Lab, based at the University of Toronto's Munk School of Global Affairs, outlined how the program could completely compromise a device at the tap of a finger. If Mansoor had touched the link, he would have given his hackers free reign to eavesdrop on calls, harvest messages, activate his camera and drain the phone's trove of personal data.

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)

Apple Inc. issued a fix for the vulnerabilities Thursday, just ahead of the reports' release, working at a blistering pace for which the Cupertino, California-based company was widely praised.

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

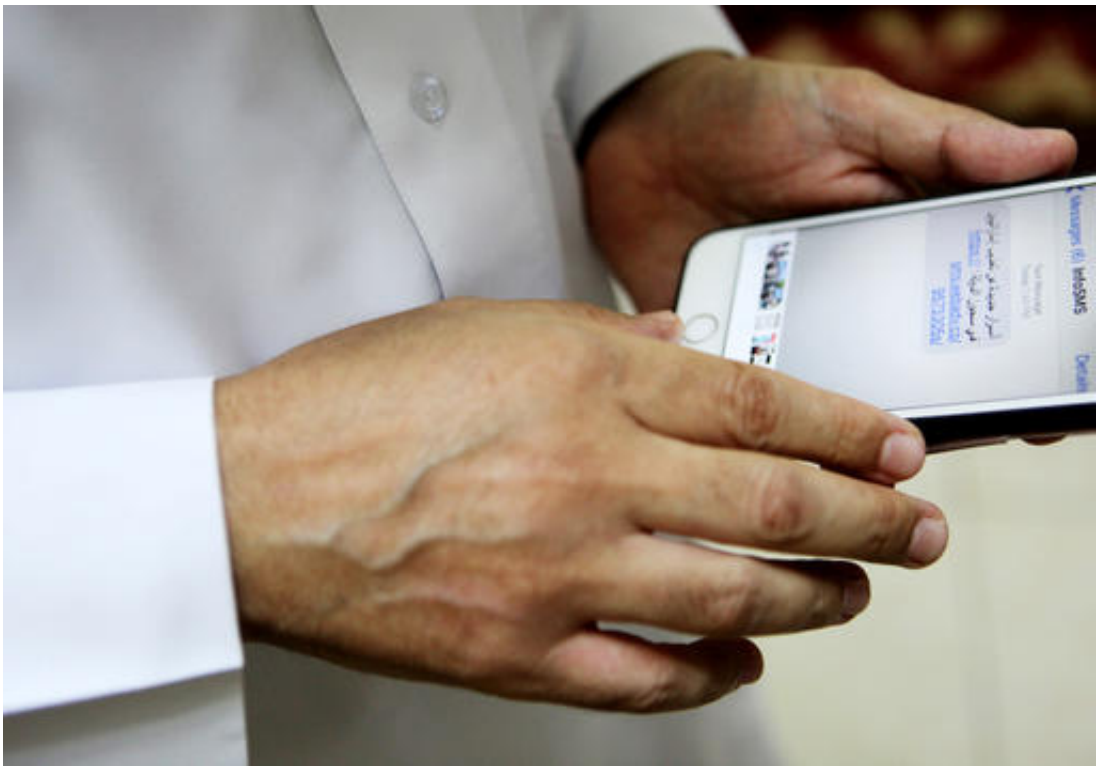
A soft-spoken man who dresses in traditional white robes, Mansoor has

repeatedly drawn the ire of authorities in the United Arab Emirates, calling for a free press and democratic freedoms. He is one of the country's few human rights defenders with an international profile, close links to foreign media and a network of sources. Mansoor's work has, at various times, cost him his job, his passport and even his liberty.

Online, Mansoor repeatedly found himself in the crosshairs of electronic eavesdropping operations. Even before the first rogue text message pinged across his phone on Aug. 10, Mansoor already had weathered attacks from two separate brands of commercial spyware.

When he shared the suspicious text with Citizen Lab researcher Bill Marczak, they realized he'd been targeted by a third.

Citizen Lab and Lookout both fingered a secretive Israeli firm, NSO Group, as the author of the spyware. Citizen Lab said that past targeting of Mansoor by the United Arab Emirates' government suggested that it was likely behind the latest hacking attempt as well.



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)

Executives at the company declined to comment, and a visit to NSO's address in Herzliya showed that the firm had recently vacated its old headquarters—a move recent enough that the building still bore its logo.

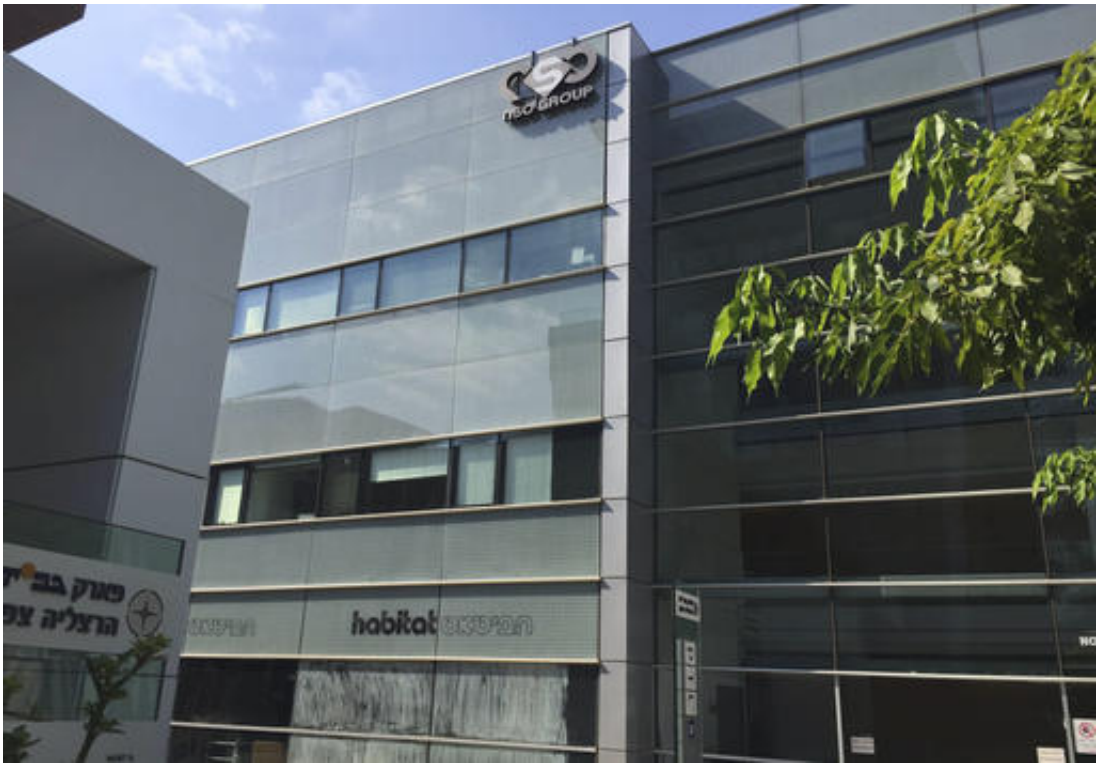
In a statement released Thursday, which stopped short of acknowledging that the spyware was its own, the NSO Group said its mission was to provide "authorized governments with technology that helps them combat terror and crime."

The company said it couldn't comment on specific cases.

Marczak said he and fellow-researcher John Scott-Railton turned to Lookout for help to pick 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," Murray said of the software's makers. "They have a hair-trigger self-destruct."

Working over a two-week period, the researchers found that Mansoor had been targeted by an unusually sophisticated piece of software which some have valued at $1 million. He told AP he was amused by the idea that so much money was being poured into watching him.



Logo of the Israeli NSO Group company is displayed on a building where they had offices until few months ago is seen in Herzliya, Israel, Thursday, Aug. 25, 2016. 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. (AP Photo/Daniella Cheslow)

"If you would give me probably 10 percent of that I would write the report about myself for you!"

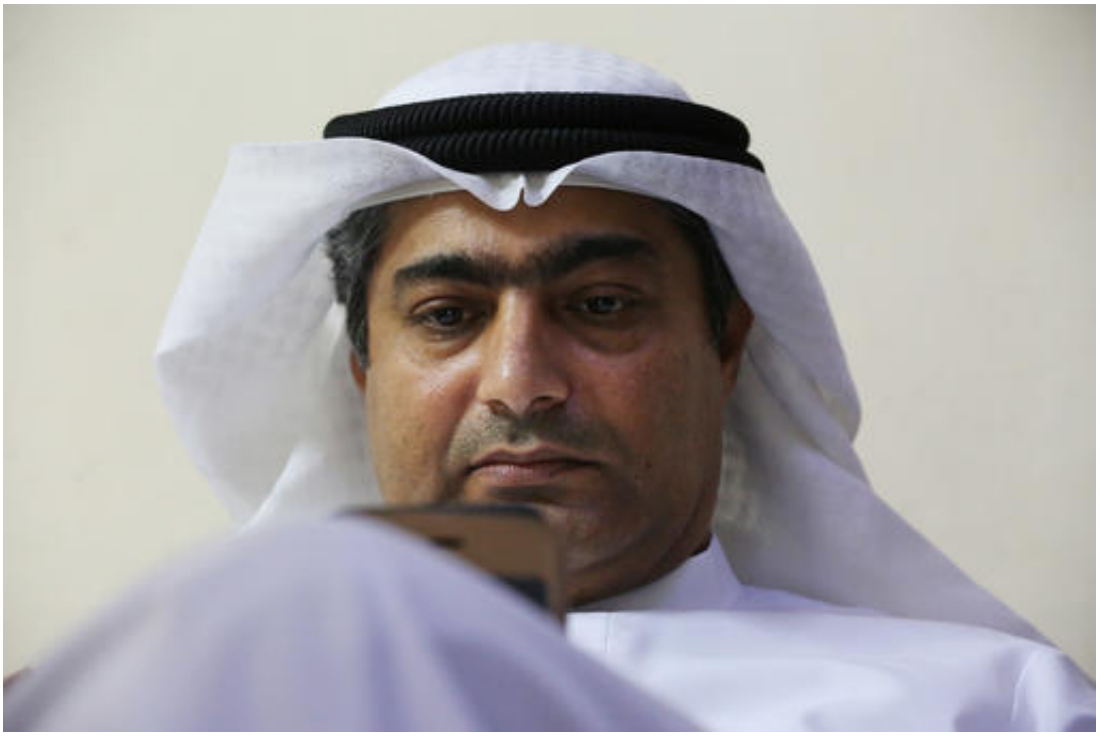
The apparent discovery of Israeli-made spyware being used to target a dissident in the United Arab Emirates raises awkward questions for both countries. The use of Israeli technology to police its own citizens is an uncomfortable strategy for an Arab country with no formal diplomatic ties to the Jewish 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.

There are awkward questions, too, for Francisco Partners, the private equity firm which owns the NSO Group. Francisco is only an hour's drive from the headquarters of Apple, whose products the cybersecurity firm is accused of hacking.

Messages left with Francisco partners' offices in London and San Francisco went unreturned. Israeli and Emirati authorities did not return calls seeking comment.

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

He also noted that Israeli Prime Minister Benjamin Netanyahu has cultivated warmer ties with Arab Gulf states.



Human rights activist Ahmed Mansoor uses his iPhone 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)

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

© 2016 The Associated Press. All rights reserved.

Citation: Activist discovers iPhone spyware, sparking security update (2016, August 26) retrieved 28 April 2024 from https://phys.org/news/2016-08-activist-iphone-spyware.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.