

Human rights group: Employee targeted with Israeli spyware

August 1 2018, by Raphael Satter



In this Aug. 25, 2016, file photo, the logo of the Israeli NSO Group company is displayed on a building where they had offices until few months ago in Herzliya, Israel. Human rights group Amnesty International says that a member of its staff was targeted by Israeli-made spyware from the NSO Group. An Amnesty official says the hacking attempt is emblematic of the increased digital risk faced by activists worldwide. (AP Photo/Daniella Cheslow, file)

An Amnesty International employee has been targeted with Israeli-made

surveillance software, the human rights group said Wednesday, adding to a growing number of examples of Israeli technology being used to spy on human rights workers and opposition figures in the Middle East and beyond.

In a 20-page report, Amnesty outlined how it believes a hacker tried to break into an unidentified staff member's smartphone in early June by baiting the employee with a WhatsApp message about a protest in front of the Saudi Embassy in Washington.

The London-based [human rights](#) organization said it traced the malicious link in the message to a network of sites tied to the NSO Group, an Israeli surveillance company implicated in a series of digital break-in attempts, including a campaign to compromise proponents of a soda tax in Mexico and an effort to hack into the phone of an Arab dissident that prompted an update to Apple's operating system.

Joshua Franco, Amnesty's head of technology and human rights, said the latest hacking attempt was emblematic of the increased digital risk faced by activists worldwide.

"This is the new normal for human rights defenders," Franco said.

NSO said in a written statement that its product was "intended to be used exclusively for the investigation and prevention of crime and terrorism" and that allegations of wrongdoing would be investigated. In response to a series of written questions, the company said past allegations of customer misuse had, in an undisclosed number of cases, led to the termination of contracts.

Amnesty's findings were corroborated by internet watchdog Citizen Lab, based at the University of Toronto's Munk School of Global Affairs. The watchdog has been tracking NSO spyware for two years.

In its own report , released Wednesday, Citizen Lab said it so far had counted some 175 targets of NSO spyware worldwide, including 150 people in Panama identified as part of a massive domestic espionage scandal swirling around the country's former president.

The Amnesty International report said the organization identified a second human rights activist, in Saudi Arabia, who was targeted in a similar way to its staffer. Citizen Lab said it found traces of similar hacking attempts tied to Qatar or Saudi, hinting at the use of the Israeli spyware elsewhere in the Gulf.

Any possible use of Israeli technology to police dissent in the Arab world could raise uncomfortable questions both for Israel, which still sees itself as a bastion of democracy in the region, and for countries with no formal diplomatic ties to the Jewish state.

For Amnesty's Franco, it was a sign of an out-of-control trade in high-tech surveillance tools.

"This is a huge market that's completely opaque and under-regulated," he said.

© 2018 The Associated Press. All rights reserved.

Citation: Human rights group: Employee targeted with Israeli spyware (2018, August 1) retrieved 19 July 2024 from <https://phys.org/news/2018-08-human-rights-group-employee-israeli.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.