Report: Civil society in Jordan under assault by NSO's Pegasus spyware

By Dina Temple-Raston

Published: 2024-02-01 · Archived: 2026-04-05 17:30:11 UTC

An investigation based on interviews, documents and forensic analysis reveals new evidence that the phones of some three dozen journalists, human rights advocates and lawyers in Jordan were infected with Pegasus spyware.

In a report released Thursday, Access Now, a digital rights organization, joined forces with the Citizen Lab, a cybersecurity watchdog organization at the University of Toronto, to document a roster of Pegasus cases in Jordan. The spyware is one of the most notorious hacking tools used by governments to slip into mobile devices and vacuum up their contents.

"Our investigation unveils the widespread hacking," the report said, "demonstrating the relentless nature of this targeted surveillance campaign" in Jordan. While the report suggests the Jordan authorities are behind the campaign, the authors stop short of saying so directly.

Citizen Lab had previously reported that it had been able to confirm that two organizations in Jordan were Pegasus spyware customers. The first publicly confirmed case of the use of Pegasus in Jordan happened in early 2022, when a human rights lawyer named Hala Ahed revealed that forensic artifacts linked to the spyware was found on her phone.

"Ahed's device unsuccessfully targeted with Pegasus spyware for a second time on or around February 20, 2023," the Access Now report said. "The hacking attempt occurred amidst a broader campaign of harassment against her."

'We're proud of our truthfulness'

Daoud Kuttab, an award winning Palestinian-American journalist based in Jordan, was also the subject of a Pegasus spyware attack. He was a Ferris Professor of Journalism at Princeton University and is currently the director of the Community Media Network, an NGO that, among other things, runs a community radio station and a news website in Jordan.

The Community Media Network is unusual in the region because it has earned a kind of Good Housekeeping seal of approval from Reporters Without Borders, which promotes and defends the freedom of expression around the world. The group said the Community Media Network provides unbiased, trustworthy reporting.

"We are proud of our truthfulness, our professionalism," Kuttab told the Click Here podcast in a recent interview ahead of the report's release. He believes he was targeted by Pegasus spyware because he published some stories from the Pandora Papers, a mysterious leak of some 12 million financial documents that revealed where

influential people around the world had stashed their money, including Russian President Vladimir Putin's inner circle and Jordan's King Abdullah.

Kuttab said soon after his network published a piece on shell companies the King allegedly had set up to buy property in the U.S. and the United Kingdom, he got an angry text message from officials in the Jordanian General Intelligence Directorate. He said they wanted him to pull the story.

"I told them that wouldn't do any good because in today's world, you cannot keep bad news away," Kuttab said in an interview. "The best way to deal with a bad story is to present your own story and try to hope that it will go viral."

Eventually, after some back-and-forth, Kuttab did take the story down from his website. But a short time later, he published his account of the entire episode in Foreign Policy Magazine. Not long after that, according to Kuttab, he came to find out much later, his phone was infected with Pegasus spyware.

That was March 2022.

According to the Access Now report, forensic analysis of his phone suggests Kuttab's mobile device was then targeted seven more times, unsuccessfully, until September 2023.

Zero-click exploits

People targeted by Pegasus don't have to click on anything to be infected. The software uses something called a zero-click exploit to crack into a device.

"A zero-click exploit, you wouldn't see anything. You wouldn't get a text message or an email," said John Scott-Railton, a researcher at the Citizen Lab. "Your phone would just be uninfected one minute and then a spy in your pocket the next moment."

Pegasus just finds some vulnerability on your device and takes advantage of it and it is so sophisticated The New York Times Magazine dubbed it "the world's most powerful cyberweapon."

Scott-Railton agrees. "One minute, your phone is yours, filled with your private data. And the next minute, some autocrat, perhaps halfway around the world, is dumping your digital life out on the proverbial table," he told Click Here before this latest report was published. "That's what's so scary about this technology."

NSO Group Technologies, the Israeli company that created Pegasus, says it only sells the tool to nation-states for national security purposes. In fact, one of the spyware's early adopters was Mexico. They used it to spy on the drug cartels and to roll up drug lords. NSO declined an interview request for this article but it has said publicly that anyone using their spyware on targets within civil society is doing so without their permission.

Scott-Railton said that it would be naive to create something like Pegasus and not expect it to be abused. "There's something about it, something about that temptation of total access to a person's innermost world on their phone that just makes it really, really, really prone to abuse," he said.

Human Rights Watch

Amnesty Tech and Human Rights Watch discovered last year that the personal mobile devices belonging to two of its Jordan-based staff were targeted with Pegasus as well. Adam Coogle, a deputy director with HRW's Middle East and North Africa division was hacked with Pegasus through a zero-click attack.

According to the Access Now report, the attack occurred exactly two weeks after HRW published a report on the increasing government repression in Jordan. "We have typically had a relatively adversarial relationship with the authorities, which isn't surprising given the fact that we report on their human rights abuses," Coogle told Click Here in an interview. "Because of that… I'm not terribly surprised that we, or our staff, would be targeted."

Even so, Coogle said that learning he'd been hacked changed his mindset. While he hasn't confirmed the Jordanian government was behind it, he said the whole experience rattled him. "The idea that you are on their radar, you're being directly targeted by a security apparatus of a country is a little bit… unnerving," he said. "And then you start to think about what was on my phone, what could they have potentially gained access to, ad that's a conversation that goes on in your head for a long time."

In the conclusion of its report, Access Now called on the Jordanian government to investigate the allegations of spyware abuse. "We urge all world governments, including Jordan's, to halt the use of Pegasus spyware, and implement an immediate moratorium on the export, sale, transfer, servicing, and use of targeted digital surveillance technologies," it reads. "Until rigorous human rights safeguards are put in place to regulate such practices."

The Jordanian government had not responded to the allegations in the report by press time. Recorded Future News has reached out to them for comment.

No previous article

No new articles

Dina Temple-Raston

is the Host and Managing Editor of the Click Here podcast as well as a senior correspondent at Recorded Future News. She previously served on NPR's Investigations team focusing on breaking news stories and national security, technology, and social justice and hosted and created the award-winning Audible Podcast "What Were You Thinking."
