Spyware find highlights depth of hacker-for-hire industry

December 17 2021, by Frank Bajak

Egyptian politician Ayman Nour speaks during a news conference organized by Muslim Brotherhood for former Egyptian president Mohammed Morsi, in Istanbul, on June 20, 2019. Security researchers say they'd discovered two different types of commercial military-grade spyware on the phone of Nour, a leading exiled Egyptian dissident, documenting for the first time a hack by a little-known competitor of Israel's notorious NSO Group. Credit: AP Photo/Burhan Ozbilici, File

Security researchers said Thursday they found two kinds of commercial spyware on the phone of a leading exiled Egyptian dissident, providing new evidence of the depth and diversity of the abusive hacker-for-hire industry.

One piece of malware recently found on an iPhone belonging to Ayman Nour, a dissident and 2005 Egyptian presidential candidate who subsequently spent three years in jail, originated with the increasingly embattled NSO Group of Israel. That company was recently blacklisted by Washington. The other was from a company called Cytrox, which also has Israeli ties. This was the first documentation of a hack by Cytrox, a little-known NSO Group rival.

The spyware was uncovered by digital sleuths at the University of Toronto's Citizen Lab, who said two different governments hired the competing mercenaries to hack Nour's phone. Both instances of malware were simultaneously active on the phone, investigators said after examining its logs. The researchers said they traced the Cytrox hack to Egypt but didn't know who was behind the NSO Group infection.

The researchers said in a report that the intrusions highlight how "hacking civil society transcends any specific mercenary spyware company."

In detailing the Cytrox infection, the researchers said they found the phone of a second Egyptian exile, who asked not to be identified, also hacked with Cytrox's Predator malware. But the bigger discovery, in a joint probe with Facebook, was that Cytrox has customers in countries beyond Egypt including Armenia, Greece, Indonesia, Madagascar, Oman, Saudi Arabia, and Serbia.

Facebook's owner, Meta, announced on Thursday a flurry of takedowns of accounts affiliated with seven surveillance-for-hire firms—including

Cytrox—and notified about 50,000 people in more than 100 countries including journalists, dissidents and clergy who may have been targeted by them. It said it deleted about 300 Facebook and Instagram accounts linked to Cytrox, which appears to operate out of North Macedonia.

Cytrox's last known CEO, Ivo Malinkovski, could not be located for comment. He scrubbed his LinkedIn page earlier this month to remove mention of his Cytrox affiliation—though a coffee mug with the company name was in his profile photo. The business intelligence website Crunchbase says Cytrox was founded in a Tel Aviv suburb in 2017.

Citizen Lab researcher Bill Marzak said investigators found the malware on Nour's iPhone after it was "running hot" in June. He said the Cytrox malware appears to pull the same tricks as NSO Group's Pegasus product—in particular, turning a smartphone into an eavesdropping device and siphoning out its vital data. One captured module records all sides of a live conversation, he said.

Nour said in an interview from Turkey that he was not surprised by the discovery, as he's sure he has been under Egyptian surveillance for years. Nour said he suspected Egyptian military intelligence in the Cytrox hack. An Egyptian foreign ministry spokesman did not respond to calls and texts requesting comment.

Cytrox was part of a shadowy alliance of surveillance tech companies known as Intellexa that was formed to compete with NSO Group. Founded in 2019 by a former Israeli military officer and entrepreneur named Tal Dilian, Intellexa includes companies that have run afoul of authorities in various countries for alleged abuses.

A logo adorns a wall on a branch of the Israeli NSO Group company, near the southern Israeli town of Sapir, Aug. 24, 2021. Israel's Defense Ministry said in a statement Monday, Dec. 6, 2021, that it is tightening supervision over cyber exports—a move that follows a series of scandals involving Israeli spyware company NSO Group. The ministry said the countries purchasing Israeli cyber technology would have to sign a declaration pledging to use the products "for the investigation and prevention of terrorist acts and serious crimes only." Credit: AP Photo/Sebastian Scheiner, File

Four executives of one such firm, Nexa Technologies, were charged in France this year for "complicity of torture" in Libya while criminal charges were filed against three company executives for "complicity of torture and enforced disappearance" in Egypt. The company allegedly sold spy tech to Libya in 2007 and to Egypt in 2014.

On its website, Intellexa describes itself as "EU-based and regulated, with six sites and R&D labs throughout Europe," but lists no address. Its web page is vague about its offerings, although as recently as October it said that in addition to "covert mass collection" it provides systems "to access target devices and networks" via Wi-Fi and wireless networks. Intellexa said its tools are used by law enforcement and intelligence agencies against terrorists and crimes including financial fraud.

The Associated Press left messages for Dilian and also tried to reach Intellexa through a form on its website, but received no response.

In addition to his involvement in Intellexa, Dilian ran afoul of authorities in Cyprus in 2019 after showing off a "spy van" there to a Forbes reporter. His company was reportedly fined $1 million as result. He also founded and later sold to NSO Group a company called Circle Technologies, which geolocated cellphones.

The hacker-for-hire industry is facing increased scrutiny as well as regulatory and legal pressure. That includes a call by a group of U.S. lawmakers this week to sanction NSO Group, Nexa and their top executives.

The Biden administration last month added NSO Group and another Israeli firm, Candiru, to a blacklist that bars U.S. companies from providing them with technology. And Apple announced last month that it was suing NSO Group, with the tech giant calling the company's employees "amoral 21st century mercenaries." Facebook sued NSO Group in 2019 for allegedly violating its WhatsApp messenger app.

Earlier this month, Israel's Defense Ministry said it was tightening oversight over cybersecurity exports to prevent abuse.

Citzen Lab researchers, who have been tracking NSO Group exploits

since 2015, are skeptical. If NSO Group were to disappear tomorrow, competitors could step in without missing a beat with off-the-shelf replacement spyware, they say.

The firms targeted by Facebook in the takedowns announced Thursday included four Israeli companies: Cobwebs, Cognyte, Black Cube, and Bluehawk CI, as well India-based BellTroX and an unknown organization in China. They provide a variety of different kinds of surveillance activity, ranging from simple intelligence collection through fake accounts to wholesale intrusion.

Nour urged international action against hacker-for-hire firms, "whether it comes from Israel or anywhere else. In the end, the biggest problem is those who use these digital monsters to eat and kill innocent people." That includes nonviolent activists and journalists including Nour's late friend, Jamal Khashoggi.

The Saudi journalist was slain in 2018 at his country's Istanbul consulate and is also believed to have been targeted by phone-surveillance software.