iPhone spyware spotlights Israel's secretive surveillance industry

August 29 2016, by Jean-Luc Renaudie

An Israeli woman uses her iPhone in front of the building housing the Israeli NSO group, on August 28, 2016, in Herzliya, near Tel Aviv

The discovery of sophisticated spyware to infiltrate and remotely take control of iPhones without leaving a trace has put a spotlight on Israel's secretive surveillance industry, considered among the world's most advanced.

Apple rushed out a security update last week after researchers said a prominent Emirati rights activist was targeted by "Pegasus" spyware attributed to Israeli firm NSO Group, based in Herzliya in the country's "Silicon Valley".

NSO Group, now owned by US private equity firm Francisco Partners Management, has flown far under the radar, without even a website.

It is among some 27 surveillance firms headquartered in Israel, according to a recent report from British NGO Privacy International—putting the country of eight million people at the top of the list of such companies per capita.

According to Privacy International, Israel has 0.33 such firms per 100,000 people, while the United States has 0.04.

For the firms involved, the technology is meant to fight crime and terrorism through legal means. Israel's defence ministry must also approve exports of sensitive security products.

But activists question whether enough attention is paid to the potential for abuse of such invasive technology, including whether governments will simply target opponents.

"Opposition activists, human rights defenders, and journalists have been placed under intrusive government surveillance and individuals have had their communications read to them during torture," Privacy International said.

"State agencies are also utilising technologies used for surveillance for offensive and military purposes as well as espionage."

'Spy in his pocket'

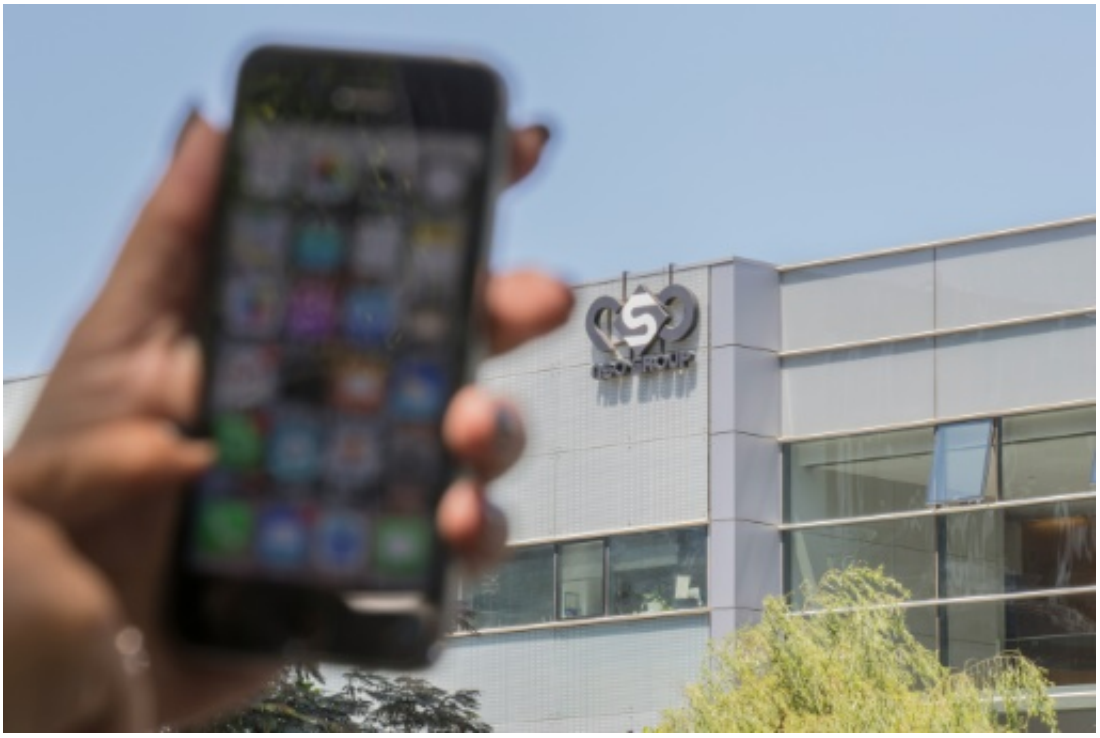
An investigation by Lookout mobile security firm and Citizen Lab at the University of Toronto found the spyware that forced Apple's update last week to be rare and powerful.

Emirati activist Ahmed Mansoor's phone "would have become a digital spy in his pocket, capable of employing his iPhone's camera and microphone to snoop on activity in the vicinity of the device, recording his WhatsApp and Viber calls, logging messages sent in mobile chat apps, and tracking his movements," they said.

He was targeted by a simple text message that asked him to click on a link for information on detainees tortured in the United Arab Emirates.

Targeted by cyber attacks in the past, he became suspicious and forwarded it to Citizen Lab.

NSO did not confirm that it created the spyware used to target Mansoor.



The Israeli NSO Group, now owned by US private equity firm Francisco Partners Management, has flown far under the radar, without even a website

But it said in a statement that it "sells only to authorised governmental agencies, and fully complies with strict export control laws and regulations".

"Moreover, the company does not operate any of its systems; it is strictly a technology company."

Israel's defence ministry, for its part, did not respond to a request for comment.

Code-crackers

Daniel Cohen, a cyber-terrorism expert at Israel's Institute for National Security Studies, said the country's expertise in such products stems in part from its military, which puts a premium on cyber-warfare training.

Most Jewish Israelis are required to serve in the military, whose Unit 8200 for signal intelligence and code-cracking is considered an incubator for future start-ups.

"Israel is among the world leaders in everything involving the cyber sector," Cohen said.

"After leaving the military, such experts take advantage of their knowledge to create start-ups or get hired at exorbitant salaries by existing firms."

Cohen said there are more than 300 cyber-related firms in Israel, though most create products to protect institutions against cyber attacks.

"Less than 10 percent of firms in the cyber sector have pursued an offensive niche, meaning technologies allowing the infiltration of computer systems," he said.

Companies with Israeli roots have provided technology to monitor Internet and phone communication to secret police in Uzbekistan and Kazakhstan as well as Colombian security forces, according to Privacy International.

They have also reportedly exported to Trinidad and Tobago, Uganda, Panama and Mexico, it said.

One case drew particular attention in 2011, when Internet-monitoring technology by Allot Communications was reportedly sold on by a distributor to Iran, Israel's arch-enemy.

Citizen Lab said: "Clearly, additional legal and regulatory scrutiny of the 'lawful intercept' market, and of NSO Group's activities in relation to the attacks we have described, is essential."

"While these spyware tools are developed in democracies, they continue to be sold to countries with notorious records of abusive targeting of human rights defenders."