Interview

We Do Not Target NSO, but Most Evidence Leads to Them, Says Digital Human Rights Researcher

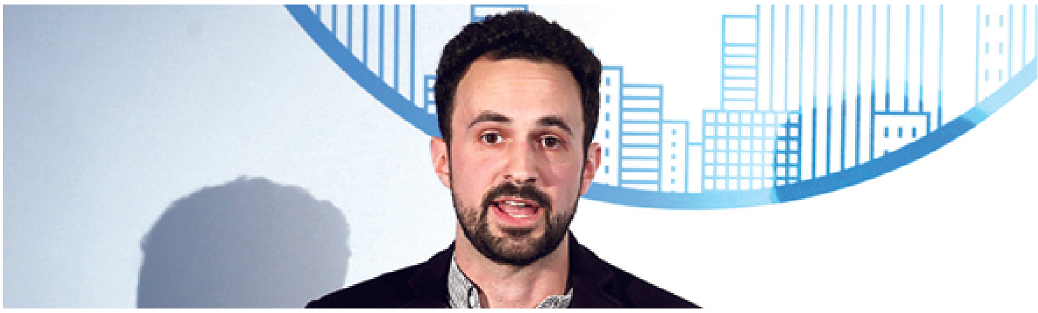
Bill Marczak, a senior research fellow at Citizen Lab and at University of California, Berkeley, is behind much of the research that exposed NSO's operations

Omer Kabir 14:29 04.02.20

TAGS: Citizen Lab NSO Interview Bill Marczak Surveillance Spyware Pegasus

Spyware like Pegasus, developed by Israeli surveillance company NSO Group, is sold to repressive regimes that use them to damage democracy, according to digital researcher Bill Marczak. It is ironic, Marczak said, that democratic countries like Israel facilitate the export of products that undermine democracy. Marczak, a senior research fellow at the University of Toronto's Citizen Lab, a digital and human rights research group focused on cyber-surveillance, and a postdoc at the University of California, Berkeley, spoke to Calcalist following Citizen Lab's announcement last week that Pegasus has been used by a Saudi-linked operator to target New York Times journalist Ben Hubbard. Hubbard, currently the NYT's Beirut Bureau Chief, previously reported on Saudi Arabia and has a book about crown prince Mohammed bin Salman coming out in March.

Marczak, who has helmed much of Citizen Lab's research into NSO's operations in recent years, also led the research published last Tuesday. The research differs from previous Citizen Lab publications about NSO on two aspects. First, it is the first time the group found evidence that Pegasus was used to target an American journalist, though the number targeted was a non-U.S. number. Second, it is the first time NSO's response broke its usual template and was a direct attack of both Hubbard and Citizen Lab.



Digital researcher Bill Marczak. Photo: Orel Cohen

According to Citizen Lab and the New York Times, on June 21, 2018, Hubbard received an SMS in Arabic with the message "Ben Hubbard and the story of the Saudi Royal Family" and a link to a website with the URL arabnews365.com. He passed it on to Citizen Lab, which concluded that the journalist was being targeted, and that had he clicked the link his attackers would have received almost unlimited access to his smartphone's data, as well as the ability to control it remotely.

NSO has firmly denied the accusation. Not every unanswered call, SMS, or video call is Pegasus, a spokesperson told Calclist. "It seems Ben Hubbard forgot or deliberately concealed the fact that last year we worked directly with him, analyzed his claims, and shared our expansive and clear-cut conclusions with him," the spokesperson said. "The timing of the publication, just now, is very interesting. Now that Hubbard has a book to sell, he and Citizen Lab are raising these unsubstantiated claims again."

NSO's spokesperson said that both Hubbard and Citizen Lab are aware of the facts but chose to ignore them. "These hypocritical attacks by Citizen Lab and its camp followers indicate that Citizen Lab, Hubbard, and others are uninterested in the truth, and their commercial ambitions are clearly visible to everyone. It is undoubtedly a trick to increase the book's sales and profit."

Marczak rejects NSO's claims. It is true that not every suspicious message or link is Pegasus, he told Calcalist, but the link included in Hubbard's weird SMS led to a website Citizen Lab previously identified as Pegasus operators. In 2016, Marczak explained, the group received a Pegasus-infected device that contained part of the spyware's source code, which included a list of command and control (C&C) servers used for the spyware's distribution. Marczak developed a fingerprint of sorts based on the way these servers behaved and used it to compile a list of 250 servers that exhibited the same fingerprint.

After Citizen Lab published the information in a 2016 report, all cited servers were removed, Marczak said, but he kept monitoring them, and after a few weeks some servers came back online. They behaved differently now, though, so he developed a new fingerprint and used it to identify a new list of 1,000 Pegasus-linked servers, including the one Hubbard's SMS linked to, he said. "This server is also linked to 20 other servers managed by the same operator, who in the past attacked or tried to attack activists and journalists who criticized Saudi Arabia." Among them, for example, a close friend of murdered Washington Post columnist Jamal Khashoggi.

After NSO responded last week to Citizen Lab's and Ben Hubbard's reports with a comment similar to the one above, the NYT released a comment of its own. Previously, the NYT said, NSO insisted all interactions with Hubbard be off the record, but now that agreement has been broken by the company. The NYT went on to say that NSO did not inspect Hubbard's phone but rather was provided with a screenshot, and told Hubbard the software was not used to target him. Though it had many opportunities to do so, NSO did not explain how it came to this conclusion or agree to say it on record, the NYT said.

> The Times has responded to NSO's statement about @NYTBen speaking with NSO previously, says it had been an off-the-record conversation it's now released from because NSO broke it. pic.twitter.com/081B0RWlfW
> — Kevin Collier (@kevincollier) January 28, 2020

NSO's off-record response was interesting, Marczak said, because they did not explain why they thought Citizen Lab's research or findings were wrong. Their response was an attack, but they did not actually criticize major parts of the research, he added. Marczak also rejects the statement that Citizen Lab is biased against NSO, proffering as evidence Citizen Lab's response to claims that Saudi Arabia's crown prince was behind the hacking of Jeff Bezos' phone and that Pegasus was used to do it.

To see if someone is biased or not, one needs to see if they promote shady reports of Bezos' so-called hack or whether they are on the side of the facts, Marczak said. "We are interested in getting to the truth," he said. Citizen Lab did not jump on these reports like other outlets but rather tried to understand the facts and look at them in a critical way, he added.

Regarding the Bezos hack, Marczak is somewhat skeptical. The company that examined his device released its report to the public, and one of the things Citizen Lab's noticed was that it seemed the examination was not complete, he said. "Bezos received a video, but they found nothing malicious. There was another encrypted version of the video they did not manage to crack, and that is what their claims were based on. The findings are not based on evidence." Citizen Lab's research, however, is always peer-reviewed, he said.

Related stories:

- Israeli Court Agrees to Keep NSO Legal Proceedings in Chambers
- Israel Wants NSO Proceedings to Remain Secret
- Israel's Military Censor Asks for Early Release From Service Following NSO Job Offer

Another claim is that NSO is receiving an unfair share of the criticism, though many companies offer similar technologies and services. Citizen Lab receives suspicious material—messages, links, and files—from outsiders, and tries to connect them to companies, governments, and other powerful players, Marczak explained. "If we succeed, we will write a report. It is true that a lot of our research has to do with NSO, but that is what people receive, provide to us, and we manage to make the connection," he said. "The reason people notice messages connected to NSO is that there was a lot of material published on the subject and because NSO is the biggest player in the sector they also receive more attention than other companies. We are always looking for examples of activity by other companies."

Marczak thinks governments should better regulate technologies like Pegasus. NSO says its technology is used to fight terrorism and crime, and that is true, and governments need access to such abilities—under proper legal supervision, Marczak said. But the problem is that NSO and its competitors also sell to governments with a bad track record regarding human rights, and to repressive regimes like Saudi Arabia, he said. "They may use the software to investigate crime and terrorism, but these products are also used against journalists or activists that criticize the government, to help them evade criticism."

Buzz

The truth behind the Lemonade surge, America's most successful IPO of 2020

05.07.2020 Sophie Shulman

Israeli autonomous vehicle startup VayaVision acquired by Canada's LeddarTech

07.07.2020 Hagar Ravet

AI cancer treatment startup Nucleai raises $6.5 million in series A round

07.07.2020 Meir Orbach

Next Food aiming for $7.5 million in first-of-its-kind IPO

05.07.2020 Meir Orbach

Co-living is wasted on the youth, Israeli startup Willa is offering urban living for midlifers

05.07.2020 Ron Friedman

Software giant Amdocs set to lay off 1,000 employees

02.07.2020 Meir Orbach