Report reveals Israeli spyware used to target journalists and activists

According to the Guardian, the leak contains a list of more than 50,000 numbers that are believed to be of interest to clients of NSO since 2016 [File: Reuters]

London, July 19 (RHC)-- Activists, politicians and journalists across the world were targeted in a surveillance operation using software sold by the Israeli surveillance company NSO Group, according to

an investigation into a massive data leak by The Guardian, the Washington Post and 15 other media outlets.

The reports released on Sunday said “authoritarian governments” abused the Pegasus software, “hacking 37 smartphones,” according to a report by the Washington Post.

According to the Guardian, the leak contains a list of more than 50,000 numbers that are believed to be of interest to clients of NSO since 2016. However, the mention of phone numbers in the leaked data does not alone mean that those devices were hacked.

The Washington Post said numbers on the list also belonged to heads of state and prime ministers, members of Arab royal families, diplomats and politicians, as well as activists and business executives.

The list also included journalists for media organisations around the world including Agence France-Presse, The Wall Street Journal, CNN, The New York Times, Al Jazeera, France 24, Radio Free Europe, Mediapart, El País, the Associated Press, Le Monde, Bloomberg, the Economist, Reuters and Voice of America, the Guardian said.

According to forensic analysis by Amnesty’s Security Lab, two women close to slain Saudi columnist Jamal Khashoggi were targeted with Pegasus spyware, according to the Washington Post newspaper. The phone of Khashoggi’s fiancée, Hatice Cengiz, was infected with the malware days after his murder in the Saudi consulate in Istanbul in October 2018, the paper, for whom Khashoggi wrote, reported.

Pegasus, a sophisticated surveillance tool developed by the Israel company, infects the user’s smartphone and steals all the phone’s information, including every contact name and phone number, text message, e-mail, Facebook message, everything from Skype, WhatsApp, Viber, WeChat and Telegram.

The list did not identify the clients but the reports said many were clustered in 10 countries – Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia and the United Arab Emirates.

“The surveillance industry works under a cloud of darkness – its products are designed to deceive and skirt culpability,” Natalia Krapiva, Tech Legal Counsel at Access Now, told Al Jazeera.

“Yet we ask ourselves, ‘how could something like this happen?’ Spyware companies simply cannot be trusted to hold themselves accountable. This story, along with the recent revelations of abuses by Cellebrite and Candiru, is another example of why we urgently need to hold these surveillance companies and the governments that use them up to the light.

“The industry has shown that it is incapable of policing itself and governments are hiding behind national security to excuse these surveillance abuses. We need regulation, transparency, and accountability and we need them now,” she told Al Jazeera.

Amnesty International and Forbidden Stories, a Paris-based media non-profit organisation, initially had access to the leak, which they then shared with media organisations from around the world. NSO, which previously pledged to police abuses of its software, firmly denied what it called “false claims.”

“NSO Group firmly denies false claims made in your report,” it said in a release published by the Guardian. “Many of which are uncorroborated theories that raise serious doubts about the reliability of your sources, as well as the basis of your story.”

According to the company, it has good reason to “believe … the claims … are based on a misleading interpretation of leaked data from accessible and overt basic information.” Citizen Lab reported in December that dozens of journalists at Qatar-based Al Jazeera Media Network had their mobile communications intercepted by sophisticated electronic surveillance.

Amnesty International reported in June of last year that Moroccan authorities used Pegasus software to insert spyware onto the cellphone of Omar Radi, a journalist convicted over a social media post.

---

https://www.radiohc.cu/en/noticias/internacionales/264280-report-reveals-israeli-spyware-used-to-target-journalists-and-activists

Radio Habana Cuba