Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally

amnesty.org/en/latest/news/2021/07/the-pegasus-project/

July 18, 2021

July 19, 2021

NSO Group's spyware has been used to facilitate human rights violations around the world on a massive scale, according to a major investigation into the leak of 50,000 phone numbers of potential surveillance targets. These include heads of state, activists and journalists, including Jamal Khashoggi's family.

> The Pegasus Project lays bare how NSO's spyware is a weapon of choice for repressive governments seeking to silence journalists, attack activists and crush dissent, placing countless lives in peril.
>
> *Agnès Callamard, Secretary General of Amnesty International.*

The Pegasus Project is a ground-breaking collaboration by more than 80 journalists from 17 media organizations in 10 countries coordinated by Forbidden Stories, a Paris-based media non-profit, with the technical support of Amnesty International, who conducted cutting- edge forensic tests on mobile phones to identify traces of the spyware.

"The Pegasus Project lays bare how NSO's spyware is a weapon of choice for repressive governments seeking to silence journalists, attack activists and crush dissent, placing countless lives in peril," said *Agnès* Callamard, Secretary General of Amnesty International.

"These revelations blow apart any claims by NSO that such attacks are rare and down to rogue use of their technology. While the company claims its spyware is only used for legitimate criminal and terror investigations, it's clear its technology facilitates systemic abuse. They paint a picture of legitimacy, while profiting from widespread human rights violations."

"Clearly, their actions pose larger questions about the wholesale lack of regulation that has created a wild west of rampant abusive targeting of activists and journalists. Until this company and the industry as a whole can show it is capable of respecting human rights, there must be an immediate moratorium on the export, sale, transfer and use of surveillance technology."

In a written response to Forbidden Stories and its media partners, NSO Group said it "firmly denies… false claims" in the report. It wrote that the consortium's reporting was based on "wrong assumptions" and "uncorroborated theories" and reiterated that the company was on

a “life-saving mission”. A fuller summary of NSO Group’s response is available here.

The Investigation

At the centre of this investigation is NSO Group’s Pegasus spyware which, when surreptitiously installed on victims’ phones, allows an attacker complete access to the device’s messages, emails, media, microphone, camera, calls and contacts.

Over the next week, media partners of The Pegasus Project – including The Guardian, Le Monde, Süddeutsche Zeitung and The Washington Post – will run a series of stories exposing details of how world leaders, politicians, human rights activists, and journalists have been selected as potential targets of this spyware.

From the leaked data and their investigations, Forbidden Stories and its media partners identified potential NSO clients in 11 countries: Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Togo, and the United Arab Emirates (UAE).

NSO Group has not taken adequate action to stop the use of its tools for unlawful targeted surveillance of activists and journalists, despite the fact that it either knew, or arguably ought to have known, that this was taking place.

> The Pegasus Project revelations must act as a catalyst for change. The surveillance industry must no longer be afforded a laissez-faire approach from governments with a vested interest in using this technology to commit human rights violations.
>
> *Agnès Callamard, Secretary General of Amnesty International*

“As a first step, NSO Group must immediately shut down clients’ systems where there is credible evidence of misuse. The Pegasus Project provides this in abundance,” said *Agnès* Callamard.

Khashoggi family targeted

During the investigation, evidence has also emerged that family members of Saudi journalist Jamal Khashoggi were targeted with Pegasus software before and after his murder in Istanbul on 2 October 2018 by Saudi operatives, despite repeated denials from NSO Group.

Amnesty International’s Security Lab established that Pegasus spyware was successfully installed on the phone of Khashoggi’s fiancée Hatice Cengiz just four days after his murder.

His wife, Hanan Elatr was also repeatedly targeted with the spyware between September 2017 and April 2018 as well as his son, Abdullah, who was also selected as a target along with other family members in Saudi Arabia and the UAE.

In a statement, the NSO Group responded to the Pegasus Project allegations saying that its "technology was not associated in any way with the heinous murder of Jamal Khashoggi". The company said that it "previously investigated this claim, immediately after the heinous murder, which again, is being made without validation".

Journalists under attack

The investigation has so far identified at least 180 journalists in 20 countries who were selected for potential targeting with NSO spyware between 2016 to June 2021, including in Azerbaijan, Hungary, India and Morocco, countries where crackdowns against independent media have intensified.

The revelations show the real-world harm caused by unlawful surveillance:

- In Mexico, journalist Cecilio Pineda's phone was selected for targeting just weeks before his killing in 2017. The Pegasus Project identified at least 25 Mexican journalists were selected for targeting over a two-year period. NSO has denied that even if Pineda's phone had been targeted, data collected from his phone contributed to his death.
- Pegasus has been used in Azerbaijan, a country where only a few independent media outlets remain. More than 40 Azerbaijani journalists were selected as potential targets according to the investigation. Amnesty International's Security Lab found the phone of Sevinc Vaqifqizi, a freelance journalist for independent media outlet Meydan TV, was infected over a two-year period until May 2021.
- In India, at least 40 journalists from nearly every major media outlet in the country were selected as potential targets between 2017-2021. Forensic tests revealed the phones of Siddharth Varadarajan and MK Venu, co-founders of independent online outlet The Wire, were infected with Pegasus spyware as recently as June 2021.
- The investigation also identified journalists working for major international media including the Associated Press, CNN, The New York Times and Reuters as potential targets. One of the highest profile journalists was Roula Khalaf, the editor of the Financial Times.

"The number of journalists identified as targets vividly illustrates how Pegasus is used as a tool to intimidate critical media. It is about controlling public narrative, resisting scrutiny, and suppressing any dissenting voice," said *Agnès* Callamard.

"These revelations must act as a catalyst for change. The surveillance industry must no longer be afforded a laissez-faire approach from governments with a vested interest in using this technology to commit human rights violations."

Exposing Pegasus infrastructure

Amnesty International is today releasing the full technical details of its Security Lab's in-depth forensic investigations as part of the Pegasus Project.

The Lab's methodology report documents the evolution of Pegasus spyware attacks since 2018, with details on the spyware's infrastructure, including more than 700 Pegasus-related domains.

"NSO claims its spyware is undetectable and only used for legitimate criminal investigations. We have now provided irrefutable evidence of this ludicrous falsehood," said Etienne Maynier, a technologist at Amnesty International's Security Lab.

There is nothing to suggest that NSO's customers did not also use Pegasus in terrorism and crime investigations, and the Forbidden Stories consortium also found numbers in the data belonging to suspected criminals.

"The widespread violations Pegasus facilitates must stop. Our hope is the damning evidence published over the next week will lead governments to overhaul a surveillance industry that is out of control," said Etienne Maynier.

In response to a request for comment by media organizations involved in the Pegasus Project, NSO Group said it "firmly denies" the claims and stated that "many of them are uncorroborated theories which raise serious doubts about the reliability of your sources, as well as the basis of your story." NSO Group did not confirm or deny which governments are NSO Group's customers, although it said that the Pegasus Project had made "incorrect assumptions" in this regard. Notwithstanding its general denial of the claims, NSO Group said it "will continue to investigate all credible claims of misuse and take appropriate action based on the results of these investigations".

Topics

Press Release