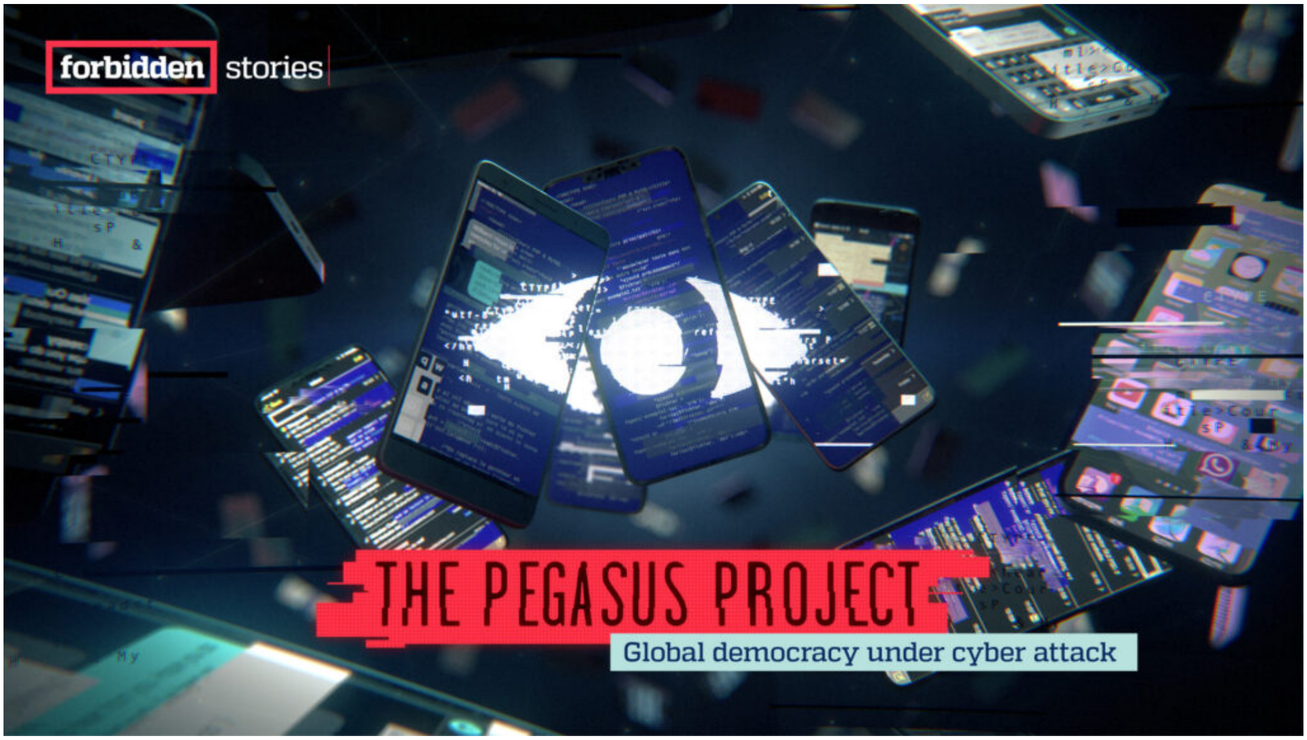
About The Pegasus Project

forbiddenstories.org/about-the-pegasus-project/

An unprecedented leak of more than 50,000 phone numbers selected for surveillance by the customers of the israeli company NSO Group shows how this technology has been systematically abused for years. The Forbidden Stories consortium and Amnesty International had access to records of phone numbers selected by NSO clients in more than 50 countries since 2016.



NSO Group asserts that the product it sells to government clients – most commonly referred to as **Pegasus** – is intended to “collect data from the mobile devices of specific individuals, suspected to be involved in serious crime and terror.” Pegasus has extensive capabilities: the spyware can be installed remotely on a smartphone without requiring any action from its owner. **Once installed, it allows clients to take complete control of the device**, including accessing messages from encrypted messaging apps like WhatsApp and Signal, and turning on the microphone and camera.

The Forbidden Stories consortium discovered that, contrary to what NSO Group has claimed for many years, including in a recent transparency report, **this spyware has been widely misused**. The leaked data showed that **at least 180 journalists** have been selected as targets in countries like India, Mexico, Hungary, Morocco and France, among others. Potential targets also include **human rights defenders, academics, businesspeople, lawyers, doctors, union leaders, diplomats, politicians and several heads of states**.

In a letter shared with Forbidden Stories and its partners, NSO Group contended that the consortium's reporting was based on "wrong assumptions" and "uncorroborated theories." NSO Group insisted that the analysis of the data by journalists who were part of the Pegasus Project relied on a "misleading interpretation of leaked data from accessible and overt basic information, such as HLR Lookup services, which have no bearing on the list of the customers targets of Pegasus or any other NSO products."

HLR refers to Home Location Register – a database that is essential to operating cellular phone networks. A person with direct knowledge of NSO's systems, speaking on the condition of anonymity, told journalists from the Pegasus Project that an HLR lookup is a key step of determining certain characteristics of a phone, such as whether it is turned on or in a country that allows Pegasus targeting.

Asked about those findings by Forbidden Stories, NSO Group denied and said "it will continue to investigate all credible claims of misuse and take appropriate action based on the results of these investigations."

The consortium met with victims from all over the world whose phone numbers appeared in the data. The forensic analyses of their phones – conducted by Amnesty International's Security Lab and peer-reviewed by the Canadian organization Citizen Lab – was able to **confirm an infection or attempted infection with NSO Group's spyware in 85% of cases**, or 37 in total. Such a rate is remarkably high given the state-of-the-art spyware is supposed to be undetectable on the device in compromises.

Journalists from the Pegasus Project – **more than 80 reporters from 17 media organizations in 10 countries coordinated by Forbidden Stories** with the technical support of Amnesty International's Security Lab – sifted through these records of phone numbers and were able to take a peak behind the curtain of this surveillance weapon, which had never been possible to this extent before.

Among the victims were several journalists from the Pegasus Project, such as Siddarth Varadarajan, an Indian investigative journalist and founder of the news site The Wire, who was hacked in 2018 and Szabolcs Panyi, an investigative reporter for Direkt36 in Hungary whose phone was compromised during a seven-month period in 2019.

All shared a general sense of powerlessness when informed about the cyber attacks they had suffered. "We've been recommending each other this tool or that tool, how to keep [our phones] more and more secure from the eyes of the government," Azerbaijani journalist

Khadija Ismayilova said. “And yesterday I realized that there is no way. Unless you lock yourself in [an] iron tent, there is no way that they will not interfere into your communications.”

Amnesty International’s Security Lab also identified new ways through which Pegasus can be installed on a phone, such as through a security flaw in iPhones that has been frequently used since 2019 and was still detected as recently as in July 2021. Well-informed sources shared concerns about **countless vulnerabilities linked to Apple’s messaging service iMessage**, a problem they say has gotten worse over the years.

The leaked data suggests that the spyware is used much more carelessly than advertised. In the transparency report published in June 2021, the Israeli company stressed that Pegasus was “not a mass surveillance technology” and was “used only where there [was] a legitimate law enforcement or intelligence-driven reason.” Yet, **more than 10,000 phone numbers were selected for surveillance by NSO Group’s Moroccan client alone over a two-year period**.

The project shines a harsh light on the business of NSO Group, which, despite claiming it vets its clients based on their human rights track records, decided to sell its product to authoritarian regimes such as Azerbaijan, the United Arab Emirates and Saudi Arabia. Insiders disclosed the **important role played by the Israeli Ministry of Defense when it came to picking NSO Group’s clients**. Multiple sources corroborated the fact that Israeli authorities pushed for Saudi Arabia to be added to the list of customers despite NSO Group’s hesitations. The company’s lawyer denied “NSO Group takes governmental direction regarding customers.”

The revelations stemming from this international collaborative investigation throw into **question the safeguards put in place to prevent misuse of cyber weapons like Pegasus** and, more specifically, NSO Group’s commitment to creating “a better, safer world.”

The Pegasus Project media partners:
The Guardian, Le Monde, The Washington Post, Süddeutsche Zeitung, Die Zeit, Aristegui Noticias, Radio France, Proceso, OCCRP, Knack, Le Soir, Haaretz/TheMarker, The Wire, Daraj, Direkt36, PBS Frontline.

With the technical support of **Amnesty International’s Security Lab.**

The Pegasus Project | All the articles