They Are Watching You: Israeli-Made Spyware Used to Monitor Journalists and Activists Worldwide

By OCCRP

In Hungary, Szabolcs Panyi exposed spy intrigue and murky arms deals. In India, Paranjoy Guha Thakurta probed the ties between business and political interests. In Azerbaijan, Sevinj Vaqifqizi caught vote-rigging on tape.

Separated by thousands of miles, these journalists have one thing in common: their governments considered them a threat.

All three were among dozens of journalists and activists around the world whose smartphones were infected by Pegasus: spyware made by Israeli firm NSO Group that is able to secretly steal personal data, read conversations, and switch on microphones and cameras at will.

The attacks were revealed by The Pegasus Project, an international collaboration of more than 80 journalists from 17 media organizations, including OCCRP, and coordinated by Forbidden Stories.

What Does 'Selected for Targeting' Mean?

The phones of Panyi, Thakurta, and Vaqifqizi were analyzed by Amnesty International's Security Lab

and found to be infected after their numbers appeared on a list of over 50,000 numbers that were allegedly selected for targeting by governments using NSO software. Reporters were able to identify the owners of hundreds of those numbers, and Amnesty conducted forensic analysis on as many of their phones as possible, confirming infection in dozens of cases. The reporting was backed up with interviews, documents, and other materials.The strongest evidence that the list really does represent Pegasus targets came through forensic analysis.

Amnesty International's Security Lab examined data from 67 phones whose numbers were in the list. Thirty-seven phones showed traces of Pegasus activity: 23 phones were successfully infected, and 14 showed signs of attempted targeting. For the remaining 30 phones, the tests were inconclusive, in several cases because the phones had been replaced.

Fifteen of the phones in the data were Android devices. Unlike iPhones, Androids do not log the kinds of information required for Amnesty's detective work. However, three Android phones showed signs of targeting, such as Pegasus-linked SMS messages.

In a subset of 27 analyzed phones, Amnesty International researchers found 84 separate traces of Pegasus activity that closely corresponded to the numbers' appearance on the leaked list. In 59 of these cases, the Pegasus traces appeared within 20 minutes of selection. In 15 cases, the trace appeared within one minute of selection.The strongest evidence that the list really does represent Pegasus targets came through forensic analysis.

Amnesty International's Security Lab examined data from 67 phones whose numbers were in the list. Thirty-seven phones showed traces of Pegasus activity: 23 phones were successfully infected, and 14 showed signs of attempted targeting. For the remaining 30 phones, the tests were inconclusive, in several cases because the phones had been replaced.

Fifteen of the phones in the data were Android devices. Unlike iPhones, Androids do not log the kinds of information required for Amnesty's detective work. However, three Android phones showed signs of targeting, such as Pegasus-linked SMS messages.

In a subset of 27 analyzed phones, Amnesty International researchers found 84 separate traces of Pegasus activity that closely corresponded to the numbers' appearance on the leaked list. In 59 of these cases, the Pegasus traces appeared within 20 minutes of selection. In 15 cases, the trace appeared within one minute of selection.

In a series of responses, NSO Group denied that its spyware was systematically misused and challenged the validity of data obtained by reporters. It argued that Pegasus is sold to governments to go after criminals and terrorists, and has saved many lives. The company, which enjoys close ties to Israel's security services, says it implements stringent controls to prevent misuse. NSO Group also specifically denies that it created or could create this type of list.

But instead of targeting only criminals, governments in more than 10 countries appear to have also selected political opponents, academics, reporters, human rights defenders, doctors, and religious leaders. NSO clients may have also used the company's software to conduct espionage by targeting foreign officials, diplomats, and even heads of state.

> Based on the geographical clustering of the numbers on the leaked list, reporters identified potential NSO Group clients from more than 10 countries, including: Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Togo, and the United Arab Emirates.

Journalists and Activists in the Crosshairs

In the coming days, OCCRP and other Pegasus Project partners will release stories highlighting the threat of surveillance through misuse of NSO Group software around the world. But to start with, we will focus on some of the most egregious cases: the use of spyware to surveil, harass, and intimidate journalists and activists — and those close to them.

Among those on the list were multiple close relations of Jamal Khashoggi, the Washington Post columnist who was murdered and dismembered by Saudi operatives in the country's Istanbul consulate. Forensic analyses show that Khashoggi's Turkish fiancée, Hatice Cengiz, and other loved ones and colleagues were successfully compromised with NSO Group software both before and after Khashoggi's 2018 killing. (NSO Group said that it has investigated this claim and has denied its software was used in connection with the Khashoggi case.)

Sandra Nogales, the assistant of star Mexican journalist Carmen Aristegui, was also targeted with Pegasus through a malicious text message, according to a forensic analysis of her phone.

Aristegui had already known that she was a Pegasus target. Her case was featured in a 2017 report by Citizen Lab, an interdisciplinary laboratory at the University of Toronto. Still, "it was a huge shock to see others close to me on the list," Aristegui told The Pegasus Project.

"My assistant, Sandra Nogales, who knew everything about me — who had access to my schedule, all of my contacts, my day-to-day, my hour-to-hour — was also entered into the system."

Several reporters in OCCRP's network were among the at least 188 journalists on the list of potential targets. They include Khadija Ismayilova, an OCCRP investigative journalist whose uncompromising reporting has made her a target of the kleptocratic regime of the country's president, Ilham Aliyev. Independent forensic analysis of Ismayilova's Apple iPhone shows that Pegasus was used consistently from 2019 to 2021 to penetrate her device, primarily by using an exploit in the iMessage app.

Ismayilova is no stranger to government surveillance. Roughly a decade ago, her reporting led her to be threatened with compromising videos that she learned to her horror had been shot with hidden cameras installed in her home. She refused to back down, and as a result had the footage broadcast across the internet.

But even after this, Ismayilova was shocked by the all-consuming nature of her surveillance by Pegasus.

"It's horrifying, because you think that this tool is encrypted, you can use it… but then you realize that no, the moment you are on the internet they [can] watch you," Ismayilova said. "I'm angry with the governments who produce all of these tools and sell it to the bad guys like [the] Aliyev regime."

Panyi and his colleague András Szabó, both OCCRP partner journalists in Hungary, also had their phones successfully hijacked by Pegasus, potentially granting their attackers access to sensitive data like encrypted chats and story drafts. As investigative journalists at one of the country's few remaining independent outlets, Direkt36, they had spent years investigating corruption and intrigue as their country became increasingly authoritarian under the rule of Prime Minister Viktor Orban.

Now they found out that they were the story.

For Panyi, the descendant of Jewish Holocaust survivors, something stung in particular: that the software had been developed in Israel, and exported to a country whose leadership regularly flirts

with antisemitism.

“According to my family memory, after surviving Auschwitz, my grandmother’s brother left to Israel, where he became a soldier and soon died during the Arab-Israeli war of 1948,” Panyi wrote in a first-person account of learning he had been hacked. “I know it is silly and makes no difference at all, but probably I would feel slightly different if it turned out that my surveillance was assisted by any other state, like Russia or China.”

The alleged surveillance list includes more than 15,000 potential targets in Mexico during the previous government of President Enrique Peña Nieto. Many were journalists, like Alejandro Sicairos, a reporter from Sinaloa state who co-founded the journalism site RíoDoce. Data seen by The Pegasus Project show Sicairos’ phone was selected as a target for NSO Group’s software in 2017 shortly after his colleague, prominent journalist Javier Valdéz, was shot dead near RíoDoce’s office.

Others on the list were regular people thrust into activism by Mexico’s chaos and violence. Cristina Bautista is a poor farmer whose son, Benjamin Ascencio Bautista, was one of 43 students abducted in Iguala, in the Mexican state of Guerrero, in 2014 and remains missing until this day. The case shook Mexican society to its core and prompted Bautista and other parents to take to the streets in protest, and to assist independent experts in their own investigations.

The vocal stance taken by Bautista and other parents put them directly in the sights of Mexican authorities and Peña Nieto, who denounced the protests as destabilizing the country.

“Oh yeah, they were watching us! Whenever we went, a patrol followed us,” she said.

“They were chasing us.”

A “Natural Tool” for Autocrats

While The Pegasus Project exposes clear cases of misuse of NSO Group’s software, the company is just one player in a global, multi-billion-dollar spyware industry.

Estimated by NSO managers to be worth approximately $12 billion, the mobile spyware market has democratized access to cutting-edge technology for intelligence agencies and police forces that, in years past, could only dream of having it.

“You’re giving lots more regimes an intelligence service,” said John Scott-Railton, a senior researcher at Citizen Lab. “Like a foreign intelligence service in a box.”

Like many private spyware companies, NSO Group’s stock in trade is so-called “zero-day exploits” — previously undiscovered flaws in commercial software that can allow third parties to gain access to devices, such as mobile phones. Pegasus and other top tools enjoy a particular strength: They are often able to infect devices silently, without the user even having to click a link.

Such tools have given governments the edge amid the widespread adoption of encrypted messaging applications, such as WhatsApp and Signal, which otherwise supposedly allow for users to communicate beyond the reach of state surveillance. Once devices are successfully compromised, however, the contents of such apps become readily available, along with other sensitive data like messages, photographs, and calls. Meanwhile, the ubiquity of mobile phone cameras and microphones means they can be easily accessed by spyware clients as remote recording devices.

> While The Pegasus Project exposes clear cases of misuse of NSO Group's software, the company is just one player in a global, multi-billion-dollar spyware industry.

"In order to bypass [encrypted messaging] you just need to get to the device at one or the other end of that communication," said Claudio Guarnieri, head of Amnesty International's Security Lab. Pegasus does just that. "Pegasus can do more [with the device] than the owner can. If Signal, for example, encrypts the message… [an attacker] can just record using the microphone, or take screenshots of the phone so you can read [the conversation]. There is virtually nothing from an encryption standpoint to protect against this."

In fact, there isn't much anyone can do to protect themselves from a Pegasus attack. Guarnieri is skeptical of applications that claim they are completely secure, and instead recommends mitigating the risks of spyware by practicing good cybersecurity hygiene. "Make sure to compartmentalize things and divide your information in such a way that even if an attack is successful, the damage can be minimized."

At its heart, The Pegasus Project reveals a disturbing truth: In a world where smartphones are ubiquitous, governments have a simple, commercial solution that allows them to spy on virtually whoever they want, wherever they want.

"I think it's very clear: Autocrats fear the truth and autocrats fear criticism," said Scott-Railton of Citizen Lab.

"They see journalists as a threat, and Pegasus is a natural tool for them to target their threats."

Published by the good folks at The Elephant.

The Elephant is a platform for engaging citizens to reflect, re-member and re-envision their society by interrogating the past, the present, to fashion a future.

Follow us on Twitter.