Viktor Orbán using NSO spyware in assault on media, data suggests

theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests

Shaun Walker July 18, 2021

This article is more than **10 months old**
This article is more than 10 months old

Since Viktor Orbán became prime minister in 2010, Hungary has fallen from 23rd to 92nd in the World Press Freedom Index. Composite: NurPhoto/Rex/Shutterstock
Since Viktor Orbán became prime minister in 2010, Hungary has fallen from 23rd to 92nd in the World Press Freedom Index. Composite: NurPhoto/Rex/Shutterstock

Hungary's far-right government suspected of hacking phones of investigative journalists and targeting owners

Viktor Orbán's government has deployed a new weapon in its war on the media in Hungary, according to forensic analysis of several mobile devices, using some of the world's most invasive spyware against investigative journalists and the circle of one of the country's last remaining independent media owners.

The Pegasus project, a collaborative investigation run by the French nonprofit journalism organisation Forbidden Stories, has reviewed leaked records that suggest a wide range of people in Hungary were selected as potential targets before a possible hacking attempt with the sophisticated Pegasus spyware, sold by the Israeli company NSO Group. In a number of cases, forensic analysis confirmed devices had been infected with Pegasus.

The leaked data includes the phone numbers of people who appear to be targets of legitimate national security or criminal investigations.

Quick Guide

What is in the Pegasus project data?

Show

What is in the data leak?

The data leak is a list of more than 50,000 phone numbers that, since 2016, are believed to have been selected as those of people of interest by government clients of NSO Group, which sells surveillance software. The data also contains the time and date that numbers were selected, or entered on to a system. Forbidden Stories, a Paris-based nonprofit journalism organisation, and Amnesty International initially had access to the list and shared access with 16 media organisations including the Guardian. More than 80 journalists have worked together over several months as part of the Pegasus project. Amnesty's Security Lab, a technical partner on the project, did the forensic analyses.

What does the leak indicate?

The consortium believes the data indicates the potential targets NSO's government clients identified in advance of possible surveillance. While the data is an indication of intent, the presence of a number in the data does not reveal whether there was an attempt to infect the phone with spyware such as Pegasus, the company's signature surveillance tool, or whether any attempt succeeded. The presence in the data of a very small number of landlines and US numbers, which NSO says are "technically impossible" to access with its tools, reveals some targets were selected by NSO clients even though they could not be infected with Pegasus. However, forensic examinations of a small sample of mobile phones with numbers on the list found tight correlations between the time and date of a number in the data and the start of Pegasus activity – in some cases as little as a few seconds.

What did forensic analysis reveal?

Amnesty examined 67 smartphones where attacks were suspected. Of those, 23 were successfully infected and 14 showed signs of attempted penetration. For the remaining 30, the tests were inconclusive, in several cases because the handsets had been replaced. Fifteen of the phones were Android devices, none of which showed evidence of successful

infection. However, unlike iPhones, phones that use Android do not log the kinds of information required for Amnesty's detective work. Three Android phones showed signs of targeting, such as Pegasus-linked SMS messages.

Amnesty shared "backup copies" of four iPhones with Citizen Lab, a research group at the University of Toronto that specialises in studying Pegasus, which confirmed that they showed signs of Pegasus infection. Citizen Lab also conducted a peer review of Amnesty's forensic methods, and found them to be sound.

Which NSO clients were selecting numbers?

While the data is organised into clusters, indicative of individual NSO clients, it does not say which NSO client was responsible for selecting any given number. NSO claims to sell its tools to 60 clients in 40 countries, but refuses to identify them. By closely examining the pattern of targeting by individual clients in the leaked data, media partners were able to identify 10 governments believed to be responsible for selecting the targets: Azerbaijan, Bahrain, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Hungary, India, and the United Arab Emirates. Citizen Lab has also found evidence of all 10 being clients of NSO.

What does NSO Group say?

You can read NSO Group's full statement here. The company has always said it does not have access to the data of its customers' targets. Through its lawyers, NSO said the consortium had made "incorrect assumptions" about which clients use the company's technology. It said the 50,000 number was "exaggerated" and that the list could not be a list of numbers "targeted by governments using Pegasus". The lawyers said NSO had reason to believe the list accessed by the consortium "is not a list of numbers targeted by governments using Pegasus, but instead, may be part of a larger list of numbers that might have been used by NSO Group customers for other purposes". They said it was a list of numbers that anyone could search on an open source system. After further questions, the lawyers said the consortium was basing its findings "on 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 ... we still do not see any correlation of these lists to anything related to use of NSO Group technologies". Following publication, they explained that they considered a "target" to be a phone that was the subject of a successful or attempted (but failed) infection by Pegasus, and reiterated that the list of 50,000 phones was too large for it to represent "targets" of Pegasus. They said that the fact that a number appeared on the list was in no way indicative of whether it had been selected for surveillance using Pegasus.

What is HLR lookup data?

The term HLR, or home location register, refers to a database that is essential to operating mobile phone networks. Such registers keep records on the networks of phone users and their general locations, along with other identifying information that is used routinely in routing calls and texts. Telecoms and surveillance experts say HLR data can sometimes be used in the early phase of a surveillance attempt, when identifying whether it is possible to connect to a phone. The consortium understands NSO clients have the capability through an interface on the Pegasus system to conduct HLR lookup inquiries. It is unclear whether Pegasus operators are required to conduct HRL lookup inquiries via its interface to use its software; an NSO source stressed its clients may have different reasons – unrelated to Pegasus – for conducting HLR lookups via an NSO system.

However, the records also include the numbers of at least 10 lawyers, an opposition politician and at least five journalists.

The phones of two journalists at the Hungarian Pegasus project partner, the investigative outlet Direkt36, were successfully infected with the spyware, including Szabolcs Panyi, a well-known reporter with a wide range of sources in diplomatic and national security circles.

Forensic analysis of his device by Amnesty International stated conclusively it had been repeatedly compromised by Pegasus during a seven-month period in 2019, with the infection often coming soon after comment requests made by Panyi to Hungarian government officials.

Szabolcs Panyi, left, and colleague András Szabó. Photograph: Andras Petho/Direkt36

Pegasus enables the attacker to view all content on a phone, including messages from apps with end-to-end encryption, photographs and GPS location data. It can also turn the device into an audio or video recorder. NSO has claimed the spyware is only meant for use against serious criminals and terrorists.

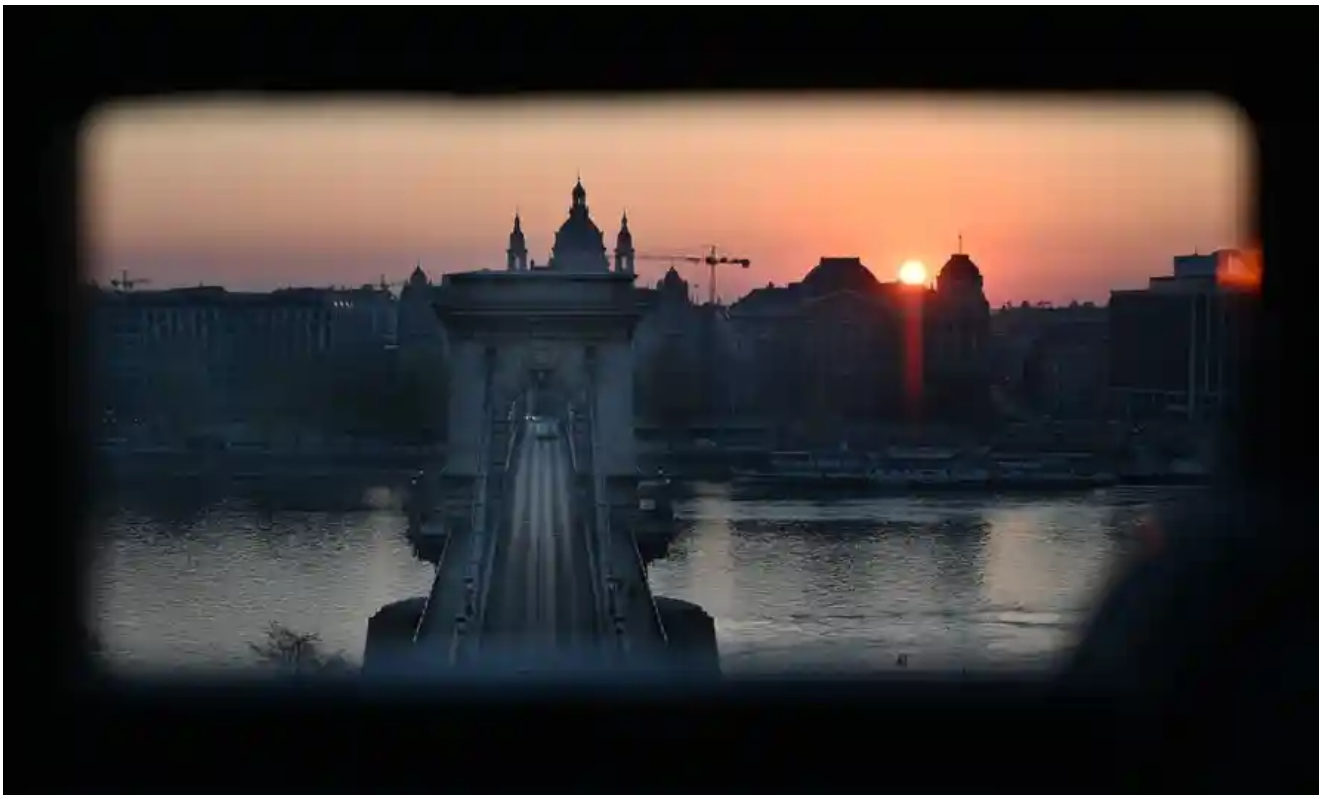
Panyi thinks some in the Orbán government believe independent journalists are part of a conspiracy against them. “I think there’s widespread paranoia and they see much more in our motives and our networks than there actually is,” he said.

“We are not aware of any alleged data collection claimed by the request,” said a Hungarian government spokesperson in response to detailed questions about the targeting of Panyi and others.

NSO Group said it “does not have access to the data of its customers’ targets”, cast doubt on the significance of the leaked data and said it would “continue to investigate all credible claims of misuse and take appropriate action”.

Previously, Orbán’s spokesperson Zoltán Kovács has publicly attacked Panyi, accusing him of “Orbánophobia and Hungarophobia” and describing him as “deep into political activism”.

Since Orbán became prime minister in 2010, Hungary has fallen from 23rd to 92nd in the World Press Freedom Index. Earlier this month, Reporters Without Borders put Orbán on its Enemies of Press Freedom list, the first time an EU leader has featured.



Sunrise in Budapest. There are few remaining Hungarian media outlets that are not under some kind of government control. Photograph: Attila Kisbenedek/AFP via Getty Images

There have been almost no cases of physical violence against journalists in Hungary; instead, Orbán's war of attrition against the media has used different means. These have included harassment of independent journalists, pressure on media owners, withdrawing state advertising funds from critical titles and aggressive takeovers by government-friendly figures.

Orbán's covert war against the media

When his forensics report came through, Panyi sat down in Direkt36's Budapest newsroom, a modest suite of offices inside a grand building one block from the Danube, and sketched out a chart in blue pen.

On the left-hand side: dates on which he sent official requests for comment to the Hungarian government. On the right: dates on which forensic analysis shows his phone was compromised by Pegasus.

The correlation was hard to ignore. On 3 April 2019, for example, Panyi sent a request for comment to several government departments in relation to a story he was working on about a Russian bank that was relocating to Budapest despite concerns it could be a front for Russian intelligence. One day later, Panyi's phone was infected with Pegasus.

There were 11 occasions when a Pegasus infection was confirmed within a few days of a comment request from Panyi to the government, according to Amnesty's analysis.

More than half the comment requests he sent to various government offices during a seven-month period were followed up with an attack. The tactic, he assumes, was for the government to get ahead of the story, work out what he was planning to publish and attempt to identify his sources.

Analysis carried out on the phone of one of Panyi's colleagues at Direkt36, András Szabó, also returned positive results. Direkt36 is one of just a few remaining Hungarian outlets not under some kind of governmental control or influence.

explainer grey background version
Other Hungarians selected for potential targeting include a photographer who worked as a fixer for a visiting foreign journalist, and a well-known investigative journalist, who declined to have forensic analysis done or to be named, citing a fear of losing sources.

Another Hungarian journalist selected as a candidate for possible surveillance was Dávid Dercsényi, who edits a newspaper put out by the authority of Budapest's opposition-run eighth district and previously worked for five years for the website of the independent outlet HVG.

Three numbers linked to Dercsényi, including one belonging to his ex-wife that had been registered in his name, were found in the data.

He expressed puzzlementhis name was in the data. “Mostly I was working on average, not-very-sensitive topics,” he said. He suspects a request for comment sent to the government over a story about the trial of a former Islamic State operative could have drawn attention. He was no longer in possession of any of the three phones appearing in the data, so analysis was not possible.

More than 70 editorial staff at index.hu walked out of the newsroom after submitting resignations following Szabolcs Dull’s dismissal as editor in July 2020. Photograph: Bődey János/Index

The decline of the major online news site Index last year, under pressure from a government-linked businessman, left 24.hu, owned by the wealthy investor Zoltán Varga, as the biggest independent news site in the country.

Varga has long been in Orbán’s crosshairs. In an interview on the terrace of his grand villa in the Buda Hills, he described receiving both enticements and threats from government-linked businesspeople to sell 24.hu and the rest of his sizeable media portfolio, which includes the country’s bestselling women’s magazine. On one occasion, he claims, he was told he would receive generous state advertising subsidies if he made editorial staffing changes.

Pegasus: the spyware technology that threatens democracy – video

“They think everything is about money. But I already have money … Slowly I turned into an enemy,” he said.

He began to notice men in parkedcars outside his home and unwanted eavesdroppers on his business meetings in restaurants. He said sometimes in the middle of a phone call, he would hear a recording of the call played back, from the beginning.On one occasion, a black

helicopter hovered above his house and made three incursions into his garden – an intimidation tactic, he believes. Varga has round-the-clock security at his home and has long been wary of speaking on the phone.

The Hungarian investor Zoltán Varga. Photograph: Central Media Group

He was right to be worried. A few weeks after Orbán won a third consecutive term as prime minister in spring 2018, Varga invited six friends to dinner. Among them was Attila Chikán, a minister in Orbán's first government in the late 1990s, who has since become a staunch critic of the prime minister. The others were wealthy and well-connected businessmen.

Over wine and finger food on Varga's expansive terrace, the men discussed creating a new foundation that among other things would investigate and expose corruption among Hungary's ruling elite. "It was a friendly conversation, it wasn't a coup," said Varga.

Two weeks later he met a government-linked acquaintance for coffee and she demonstratively referenced the dinner, suggesting such meetings could be "dangerous" for him. Varga suspected Orbán's circle had somehow put the meeting under surveillance.

Indeed, the records show all seven people at the dinner were selected as potential candidates for surveillance. Forensic analysis carried out on the handset of one of those present showed clear evidence of a confirmed infection at the time of the dinner. The phone of another participant showed signs of Pegasus activity but not of compromise.

Q&A

What is the Pegasus project?

Show

The Pegasus project is a collaborative journalistic investigation into the NSO Group and its clients. The company sells surveillance technology to governments worldwide. Its flagship product is Pegasus, spying software – or spyware – that targets iPhones and Android devices. Once a phone is infected, a Pegasus operator can secretly extract chats, photos, emails and location data, or activate microphones and cameras without a user knowing.

Forbidden Stories, a Paris-based nonprofit journalism organisation, and Amnesty International had access to a leak of more than 50,000 phone numbers selected as targets by clients of NSO since 2016. Access to the data was then shared with the Guardian and 16 other news organisations, including the Washington Post, Le Monde, Die Zeit and Süddeutsche Zeitung. More than 80 journalists have worked collaboratively over several months on the investigation, which was coordinated by Forbidden Stories.

One of those present expressed surprise the meeting had attracted such attention. "It was a typical Hungarian discussion. We sat down, everybody said: 'Fuck, the situation is really bad,' but then it did not lead anywhere," he said.

Along with Varga's circle, the son and lawyer of the oligarch Lajos Simicska, Orbán's childhood friend turned enemy, also appear to have been candidates for surveillance around the time that Simicska was pressured into selling his critical media holdings to government-friendly figures in 2018.

Ajtony Csaba Nagy, Simicska's lawyer, recalled noticing strange sounds or replayed conversations during phone calls in 2018. "It also happened that some information appeared in the press that we only discussed on the phone, nowhere else," he told Direkt36.

Map grey background version

Hungary, Israel and Pegasus

A former NSO employee confirmed Hungary was among the company's clients. It apparently acquired Pegasus in the aftermath of a 2017 visit to the country by the then Israeli prime minister, Benjamin Netanyahu, a close Orbán ally. NSO has denied it takes any direction from the Israeli government when choosing its customers.

Benjamin Netanyahu and Viktor Orbán shake hands at a joint press conference in Budapest in 2017. Photograph: AFP Contributor/AFP/Getty Images

In response to detailed allegations about Hungary's acquisition and use of Pegasus, a Hungariangovernment spokesperson said: "Hungary is a democratic state governed by the rule of law, and as such, when it comes to any individual it has always acted and continues to act in accordance with the law in force. In Hungary, state bodies authorised to use covert instruments are regularly monitored by governmental and non-governmental institutions."

Hungary has one of the loosest legislative frameworks in Europe for the authorisation of surveillance. There is no judicial oversight if the request is made for national security reasons; only the signature of the minister of justice is required.

Information released to the Hungarian outlet 168 Óra under a freedom of information request showed the justice minister, Judit Varga, approved 1,285 surveillance requests in 2020, which includes all forms of surveillance, not just Pegasus.

In an earlier interview with a Pegasus project partner, Varga said it was a “provocation” to ask whether she would authorise surveillance of a journalist, but said “there are so many dangers to the state everywhere” when asked why she had approved so many requests. The justice ministry did not respond to detailed allegations about Hungary’s use of Pegasus.

The government communications office, when presented with the same allegations, replied with questions of its own: “Have you asked the same questions of the governments of the United States of America, the United Kingdom, Germany or France? In the case you have, how long did it take for them to reply and how did they respond? Was there any intelligence service to help you formulate the questions?”

Orbán has built his political platform on staunchly opposing migration and claiming Hungary is under attack from a network directed by the Hungarian-American financier and philanthropist George Soros.

The leaked data reveals at least one case in which Pegasus appears to have been used in the hope of uncovering – or inventing – a “Soros conspiracy”.

One of the numbers in the data belonged to Adrien Beauduin, a Belgian-Canadian PhD student.

Adrien Beauduin. Photograph: Szabolcs Nagy/Index

On paper, he was the perfect “villain” for the Orbán government: a gender studies student at Central European University (CEU), an institution founded by Soros. At the time, the government was in the process both of ending the teaching of gender studies in Hungary and of forcing CEU out of the country.

Beauduin was arrested at a protest in Budapest in December 2018 and charged with assaulting police officers, which carries a sentence of up to eight years in prison. He denies he was in any way violent towards police.

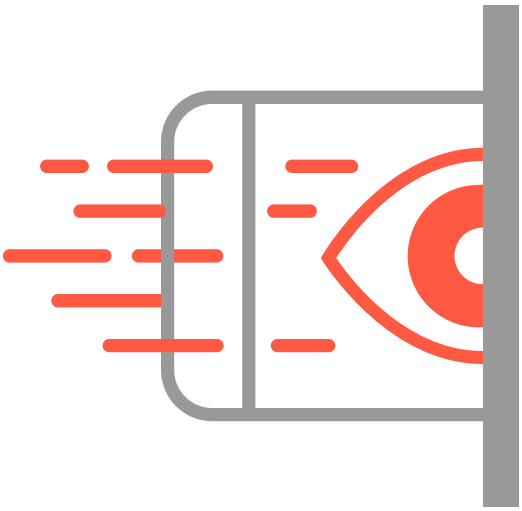
Beauduin’s lawyer, Kata Nehéz-Posony, said there was “no real evidence” against him except for police testimony that was copied word for word from the case of another person arrested.

She said she suspected the arrest was “highly politically motivated”. On 14 December, a few days after the arrest, the then communications chief of Orbán’s Fidesz party publicly noted that “the pro-immigration Soros network is organising violent demonstrations in Budapest”.

Analysis of Beauduin’s phone showed Pegasus activity on the device shortly after this, though no sign of successful infection. Eventually, the most serious charges against him were dropped, suggesting nothing incriminating was found.

A former senior Hungarian counter-intelligence officer who left the service in the early part of the last decade admitted there was a flexible approach to concocting national security reasons for surveillance during his time. “[But] there were two professions we kept our distance from: lawyers and journalists,” he said.

The leaked records, and the analysis of infected devices, suggest that in Orbán’s Hungary today, this is no longer the case.



Topics
Reuse this content