Revealed: murdered journalist's number selected by Mexican NSO client

theguardian.com/news/2021/jul/18/revealed-murdered-journalist-number-selected-mexico-nso-client-cecilio-pineda-birto

Nina Lakhani July 18, 2021

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

Pineda's press credentials among belongings kept by his wife. After going freelance in 2012 he quickly gained a reputation for exclusive crime scene reports. Composite: Nina Lakhani
Pineda's press credentials among belongings kept by his wife. After going freelance in 2012 he quickly gained a reputation for exclusive crime scene reports. Composite: Nina Lakhani
On 2 March 2017, Cecilio Pineda Birto made a broadcast about alleged corruption. Hours later he was dead

The hitmen came for Cecilio Pineda Birto as he swung in a hammock at a carwash, waiting for his pickup to be cleaned.

The 38-year-old freelance reporter was shot dead on 2 March 2017 in Ciudad Altamirano, a town in the southern Mexican region of Tierra Caliente – a battleground for rival organised crime factions.

A few hours earlier, Pineda had in a broadcast on Facebook Live accused state police and local politicians of colluding with a violent local capo known as El Tequilero.

In previous weeks, Pineda had received a string of anonymous death threats. At about the same time, his mobile phone number was selected as a possible target for surveillance by a Mexican client of the spyware company NSO Group.

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.

A successful infection enables an NSO client to access everything on the device, including contacts, chat messages – and precise location. Pineda's phone disappeared from the scene of his murder, so a forensic examination to determine if it was targeted or infected with spyware was not possible.

The gunmen who murdered him could have learned of his location at a public carwash through means not related to NSO's technologies, or its clients. But his attackers knew exactly where to find him, even though the hammock where he lay was not visible from the street.

"People with power can do whatever they want to anyone," said his widow, Marisol Toledo, when told Pineda had been selected for potential targeting. "If they succeeded [in infecting his phone], they would have known where he was at all times."

locator map grey version
One of the alleged hitmen was found dead a few months later, but no one has been prosecuted over the murder.

NSO says its products are only licensed for use by its clients to fight serious crime and terrorism. Yet at least 26 Mexican journalists' phone numbers appear on the leaked data suggesting persons of interest to NSO customers between 2016 and 2017.

Those whose phone numbers appear on the list include freelance investigative reporters, senior editors from the country's major news organisations and the former New York Times bureau chief Azam Ahmed. The data, accessed by Forbidden Stories and Amnesty International, was shared with the Guardian and its 15 media partners.

The carwash where Pineda was shot dead on 2 March 2017.

While the leak reveals phones that were selected as possible targets by NSO's government clients, it is not possible to say whether phones were successfully infected with spyware without forensic analysis of a device.

Lawyers for NSO Group did not comment on whether Pineda's phone had been targeted using its software. However, they said "even if" that were correct, "that does not mean that the NSO Group client or data collected by NSO Group software were in any way connected to the journalist's murder the following month. Correlation does not equal causation, and the gunmen who murdered the journalist could have learned of his location at a public carwash through any number of means not related to NSO Group, its technologies, or its clients."

Pegasus: the spyware technology that threatens democracy – video

Mexico is the world's most dangerous country for reporters outside of warzones. Last month, two journalists were killed within a week, bringing the death toll to at least 86 since 2010, according to the Committee to Protect Journalists. Those most at risk are reporters who investigate the webs of influence and interest woven by organised crime, the security forces and corrupt officials.

> It's not the narcos who have absolute power – it's the narco-politicians.

In Tierra Caliente, where Pineda lived and died, such pacts have long enabled cartels and politicians to cement their power and control this strategically important corridor used to transport drugs, arms and people.

This hot, dry region is heavily militarised, with federal and state security forces and intelligence agencies all operating in the region.

Local journalists must navigate opaque rules and direct threats dictating what must and cannot be covered. Reporters' salaries are extremely low, and many – as Pineda did – rely on so-called gratitude payments for covering events.

"This is the precarious reality in which Cecilio had to support his family, and while there's no justification for accepting payments or gifts, you have to understand the context in which journalists live, work and die in Guerrero," said Vania Pigeonutt, a journalist specialising in organised crime. "It's impossible to keep everyone happy. And it's not the narcos who have absolute power – it's the narco-politicians."

Pineda was afraid of blood, but when he went freelance in 2012 he quickly developed a reputation for exclusive reports from crime scenes. Toledo and former colleagues described him as hard-working, outgoing and socially minded – but also as a womaniser who liked to show off with fake designer clothes and cars bought on credit.

He did not smoke, drink alcohol or take drugs, but loved to eat tacos and watch movies with his two daughters. The family lived in one room, a sweltering converted garage at his mother's house.

"My son told me not to be scared, that he'd be fine," said his mother, Crizanta Birto Melecio, 71, wiping away tears. "But he said: 'If something happens to me, it will be the politicians.'"

Pineda frequently changed numbers because he feared his could be compromised, according to his colleagues and family. At one point, the transcript of a conversation between Pineda, a colleague and a source was published in a national newspaper.

Pineda with his friend Agustín Hernández, right.

Like most local crime reporters, Pineda frequently received death threats. But while other journalists often tried to avoid trouble through self-censorship, Pineda played down the risks, said Agustín Hernández, a close friend and former colleague. “Cecilio would get into problems because he was so direct. We would tell him to take it easy but he always said everything would be fine,” he said.

Still, Pineda had panic attacks and insomnia, and in 2015 he contacted the federal protection mechanism for human rights workers and journalists, a quasi-independent agency within the home affairs ministry.

The Guardian obtained a recording of Pineda’s final meeting with the mechanism in October 2016, when he voiced fears about a threat from the town of San Miguel Totolapan. The officials acknowledged the gravity of the situation but closed Pineda’s case because he refused to relocate to another state.

In the recording, he says he is managing the risks: “The people who could do me harm could hire killers, but they wouldn’t know my whereabouts.”

A few weeks later he was selected as a possible target for surveillance by an NSO client.

A picture of Pineda is displayed on his coffin.

San Miguel Totolapan is a mountainous municipality about 30 miles (50km) south-east of Ciudad Altamirano, and one of Guerrero's main heroin poppy-growing areas.

At the time, the area was controlled by Los Tequileros, a local gang faction that split from the Familia Michoacana cartel in about 2012 and launched a wave of mass kidnappings that left dozens dead.

According to multiple sources, the political godfather of Los Tequileros was Saúl Beltrán Orozco, a local politician from the then ruling Institutional Revolutionary party (PRI). He has denied the allegations. Beltrán was also the local campaign coordinator for Héctor Astudillo, who was elected as state governor after pledging to bring "order and peace".

In December 2016, armed locals captured the mother and friends of Los Tequileros' chief in retaliation for the latest kidnappings. This new faction presented itself as a group of ordinary citizens fed up with crime, and Pineda sympathised with their cause, said Israel Flores, a local journalist. "He started naming the politicians who he believed to be responsible for what was happening. This was a mistake."

But the group was actually aligned with the Familia Michoacana cartel, which was trying to recover lost territory. It is unclear if Pineda knew this, though he reported extensively on the crisis, accusing the state governor and security forces of protecting Los Tequileros.

As the violence intensified, one of NSO's Mexican clients again highlighted Pineda's phone number. Around the same time, the phone numbers of Beltrán and Astudillo also appeared in the data – as did the state's chief prosecutor, Xavier Olea, who would later investigate the journalist's death. Forensic analysis to determine whether the telephones of Beltrán, Astudillo or Olea were targeted was not possible.

Neither Astudillo nor Beltrán responded to a request for comment.

Olea, who was Guerrero's attorney general between December 2015 and April 2018, had himself been given a demonstration of Israeli spyware. In an interview, he described how in early 2016 he was visited by two businessmen – an Israeli and a Mexican – who had been recommended by the federal anti-kidnapping commission.

The men said their software was capable of listening to calls and downloading WhatsApp messages. As part of their demonstration, they hacked the phone of Olea's wife.

Olea said he was impressed by the technology, but the budget for a deal was never approved. Two years later, the state governor agreed to buy the software, Olea said.

Our investigation suggests Pineda was selected as a possible target by Mexico's ministry of defence, NSO's first client. Several state security forces are also believed to have access to spyware and close links between organised crime and politicians has prompted concerns it could end up in the wrong hands.

Bar graph grey version
"The line between the good guys and bad guys isn't clear," said Jorge Rebolledo, a security and intelligence consultant based in Mexico City.

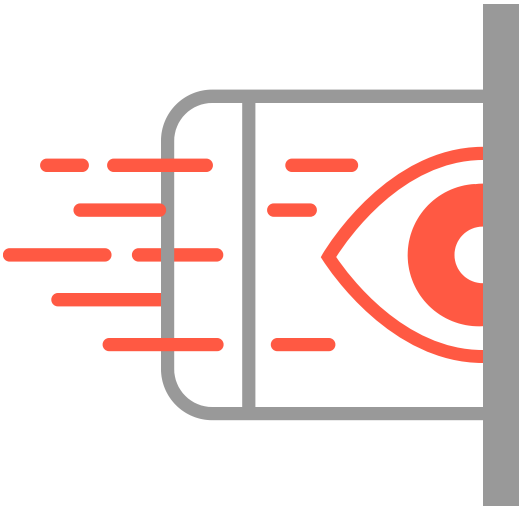
NSO said it did not operate the systems that it sells to vetted government customers to fight crime and terrorism, and did not have access to the data of its customers' targets.

By February 2017, Pineda may have sensed that time was running out. He started reverse-parking his car and repeatedly asked his wife to check if the doors were locked. "That last week he seemed worried and scared," said Toledo. "[But] he never told us any details – the less we know the better."

Pineda broadcast his final report on 2 March, claiming that the state governor and elements of the state police knew exactly where Los Tequileros were hiding.

Within hours, he was dead.

Additional reporting by Paloma Dupont de Dinechin from Forbidden Stories



Topics
Reuse this content