Revealed: leak uncovers global abuse of cyber-surveillance weapon

theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus

Stephanie Kirchgaessner, Paul Lewis, David Pegg, Sam Cutler, Nina Lakhani, Michael Safi July 18, 2021

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

Spyware sold to authoritarian regimes used to target activists, politicians and journalists, data suggests

The investigation by the Guardian and 16 other media organisations suggests widespread and continuing abuse of NSO's hacking spyware. Illustration: Guardian Design

The investigation by the Guardian and 16 other media organisations suggests widespread and continuing abuse of NSO's hacking spyware. Illustration: Guardian Design

Human rights activists, journalists and lawyers across the world have been targeted by authoritarian governments using hacking software sold by the Israeli surveillance company NSO Group, according to an investigation into a massive data leak.

The investigation by the Guardian and 16 other media organisations suggests widespread and continuing abuse of NSO's hacking spyware, Pegasus, which the company insists is only intended for use against criminals and terrorists.

Pegasus is a malware that infects iPhones and Android devices to enable operators of the tool to extract messages, photos and emails, record calls and secretly activate microphones.

The leak contains a list of more than 50,000 phone numbers that, it is believed, have been identified as those of people of interest by clients of NSO since 2016.

Forbidden Stories, a Paris-based nonprofit media organisation, and Amnesty International initially had access to the leaked list and shared access with media partners as part of the Pegasus project, a reporting consortium.

The presence of a phone number in the data does not reveal whether a device was infected with Pegasus or subject to an attempted hack. However, the consortium believes the data is indicative of the potential targets NSO's government clients identified in advance of possible surveillance attempts.

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.

Forensics analysis of a small number of phones whose numbers appeared on the leaked list also showed more than half had traces of the Pegasus spyware.

The Guardian and its media partners will be revealing the identities of people whose number appeared on the list in the coming days. They include hundreds of business executives, religious figures, academics, NGO employees, union officials and government officials, including cabinet ministers, presidents and prime ministers.

The list also contains the numbers of close family members of one country's ruler, suggesting the ruler may have instructed their intelligence agencies to explore the possibility of monitoring their own relatives.

The disclosures begin on Sunday, with the revelation that the numbers of more than 180 journalists are listed in the data, including reporters, editors and executives at the Financial Times, CNN, the New York Times, France 24, the Economist, Associated Press and Reuters.

The phone number of a freelance Mexican reporter, Cecilio Pineda Birto, was found in the list, apparently of interest to a Mexican client in the weeks leading up to his murder, when his killers were able to locate him at a carwash. His phone has never been found so no forensic analysis has been possible to establish whether it was infected.

NSO said that even if Pineda's phone had been targeted, it did not mean data collected from his phone contributed in any way to his death, stressing governments could have discovered his location by other means. He was among at least 25 Mexican journalists apparently selected as candidates for surveillance over a two-year period.

Without forensic examination of mobile devices, it is impossible to say whether phones were subjected to an attempted or successful hack using Pegasus.

NSO has always maintained it "does not operate the systems that it sells to vetted government customers, and does not have access to the data of its customers' targets".

In statements issued through its lawyers, NSO denied "false claims" made about the activities of its clients, but said it would "continue to investigate all credible claims of misuse and take appropriate action". It said the list could not be a list of numbers "targeted by governments using Pegasus", and described the 50,000 figure as "exaggerated".

The company sells only to military, law enforcement and intelligence agencies in 40 unnamed countries, and says it rigorously vets its customers' human rights records before allowing them to use its spy tools.

bar graph grey version
The Israeli minister of defence closely regulates NSO, granting individual export licences before its surveillance technology can be sold to a new country.

Last month, NSO released a transparency report in which it claimed to have an industry-leading approach to human rights and published excerpts from contracts with customers stipulating they must only use its products for criminal and national security investigations.

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

However, the broad array of numbers in the list belonging to people who seemingly have no connection to criminality suggests some NSO clients are breaching their contracts with the company, spying on pro-democracy activists and journalists investigating corruption, as well as political opponents and government critics.

That thesis is supported by forensic analysis on the phones of a small sample of journalists, human rights activists and lawyers whose numbers appeared on the leaked list. The research, conducted by Amnesty's Security Lab, a technical partner on the Pegasus project, found traces of Pegasus activity on 37 out of the 67 phones examined.

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.

The analysis also uncovered some sequential correlations between the time and date a number was entered into the list and the onset of Pegasus activity on the device, which in some cases occurred just a few seconds later.

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

The presence of a number in the data does not mean there was an attempt to infect the phone. NSO says there were other possible purposes for numbers being recorded on the list.

Rwanda, Morocco, India and Hungary denied having used Pegasus to hack the phones of the individuals named in the list. The governments of Azerbaijan, Bahrain, Kazakhstan, Saudi Arabia, Mexico, the UAE and Dubai did not respond to invitations to comment.

The Pegasus project is likely to spur debates over government surveillance in several countries suspected of using the technology. The investigation suggests the Hungarian government of Viktor Orbán appears to have deployed NSO's technology as part of his so-calledwar on the media, targeting investigative journalists in the country as well as the close circle of one of Hungary's few independent media executives.

The leaked data and forensic analyses also suggest NSO's spy tool was used by Saudi Arabia and its close ally, the UAE, to target the phones of close associates of the murdered Washington Post journalist Jamal Khashoggi in the months after his death. The Turkish prosecutor investigating his death was also a candidate for targeting, the data leak suggests.

Claudio Guarnieri, who runs Amnesty International's Security Lab, said once a phone was infected with Pegasus, a client of NSO could in effect take control of a phone, enabling them to extract a person's messages, calls, photos and emails, secretly activate cameras or microphones, and read the contents of encrypted messaging apps such as WhatsApp, Telegram and Signal.

Explainer graphic grey version
By accessing GPS and hardware sensors in the phone, he added, NSO's clients could also secure a log of a person's past movements and track their location in real time with pinpoint accuracy, for example by establishing the direction and speed a car was travelling in.

Viktor Orbán accused of using Pegasus to spy on journalists and critics

Read more

The latest advances in NSO's technology enable it to penetrate phones with "zero-click" attacks, meaning a user does not even need to click on a malicious link for their phone to be infected.

Guarnieri has identified evidence NSO has been exploiting vulnerabilities associated with iMessage, which comes installed on all iPhones, and has been able to penetrate even the most up-to-date iPhone running the latest version of iOS. His team's forensic analysis discovered successful and attempted Pegasus infections of phones as recently as this month.

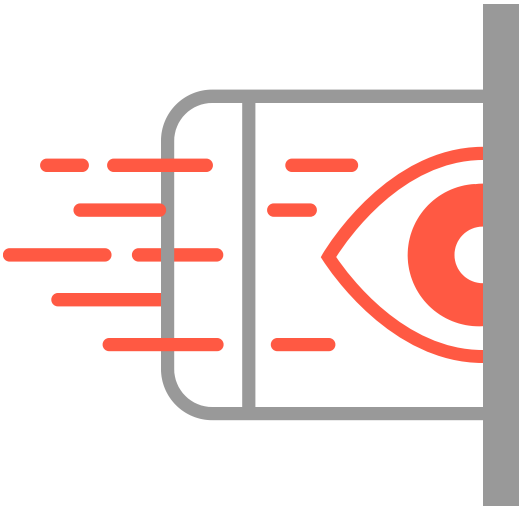
Apple said: "Security researchers agree iPhone is the safest, most secure consumer mobile device on the market."

NSO declined to give specific details about its customers and the people they target.

However, a source familiar with the matter said the average number of annual targets per customer was 112. The source said the company had 45 customers for its Pegasus spyware.

- *Additional reporting: Dan Sabbagh in London, Shaun Walker in Budapest, Angelique Chrisafis in Paris and Martin Hodgson in New York.*

- **Show your support for the Guardian's fearless investigative journalism today so we can keep chasing the truth**



Topics
Reuse this content