Saudis behind NSO spyware attack on Jamal Khashoggi's family, leak suggests

theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus

Stephanie Kirchgaessner July 18, 2021

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

Jamal Khashoggi was killed and dismembered at the Saudi consulate in Istanbul, Turkey. Composite: AFP/Getty Images
Jamal Khashoggi was killed and dismembered at the Saudi consulate in Istanbul, Turkey. Composite: AFP/Getty Images
Forensic analysis shows phones of those close to journalist were targeted before and after he was murdered

In the wake of the brutal murder of the journalist Jamal Khashoggi, the NSO Group emphatically denied that its government clients had used its hacking malware to target the journalist or his family.

“I can tell you very clear. We had nothing to do with this horrible murder,” Shalev Hulio, the chief executive of the Israeli surveillance firm, told the US TV news programme 60 Minutes in March 2019. It was six months after Khashoggi, a Washington Post columnist, was killed in Turkey by assassins dispatched by Saudi Arabia, a client of NSO.

Now a joint investigation by the Guardian and other media, based on leaked data and forensic analysis of phones, has uncovered new evidence that the company’s spyware was used to try and monitor people close to Khashoggi both before and after his death.

What is Pegasus spyware and how does it hack phones?

Read more

In one case, a person in Khashoggi’s inner circle was hacked four days after his murder, according to peer-reviewed forensic analysis of her device.

The investigation points to an apparent attempt by Saudi Arabia and its close ally the United Arab Emirates to leverage NSO's spy technology after Khashoggi's death to monitor his associates and the Turkish murder investigation, even going so far as to selectthe phone of Istanbul's chief prosecutor for potentialsurveillance.

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.

Khashoggi was killed and dismembered at the Saudi consulate in Istanbul in October 2018. While the investigation mostly points to Khashoggi's close associates being targeted in the months after the murder, it also identified evidence suggesting that an NSO client targeted the phone of his wife, Hanan Elatr, several months before his death, between November 2017 and April 2018.

The client appears to have used NSO's spyware, Pegasus, which can transform a phone into a surveillance device, with microphones and cameras activated without a user knowing.

Pegasus: the spyware technology that threatens democracy – video
A forensic examination of Elatr's Android phone found that she was sent four text messages that contained malicious links connected to Pegasus. The analysis indicated the targeting came from the United Arab Emirates, a Saudi ally. However, the examination did not confirm whether the device had been successfully infected.

"Jamal warned me before that this might happen," Elatr said. "It makes me believe they are aware of everything that happened to Jamal through me." She added that she was concerned his conversations with fellow dissidents might have been monitored through her phone. "I kept my phone on the tea table [in their Virginia home] while Jamal was talking to a Saudi guy twice a week."

Elatr's number was also contained in a leak of numbers that were selected by clients of NSO as candidates for possible surveillance. Access to the leak was shared with the Guardian and other media by Forbidden Stories, a nonprofit organisation, as part of a collaborative investigation called the Pegasus project. Examination of phones was done by Amnesty International's Security Lab, a technical partner on the Pegasus project.

US intelligence agencies have already concluded that the Saudi crown prince, Mohammed bin Salman, was responsible for ordering the murder of Khashoggi, a former Saudi government insider whose criticism of the kingdom's regime in the pages of the Washington Post was seen as a threat to the Saudi heir.

A team of Saudi agents killed Khashoggi inside the Saudi consulate in Istanbul during his visit there to pick up documents he needed to get married to his fiancee, Hatice Cengiz, who later became an outspoken advocate for accountability over his murder.

Jamal Khashoggi's fiancee, Hatice Cengiz. Photograph: Anadolu Agency/Getty Images
Forensic analysis revealed that Cengiz's phone was first infected with Pegasus just four days after his murder, on 6 October 2018. Her phone was also hacked on two other days in October 2018. Further attempts to hack her phone followed in June 2019, although they did not appear to be successful.Data analysis suggested that Saudi Arabia was behind her hacking. Cengiz said she was not surprised she had been hacked: "I was thinking this after the murder. But what can you do?"

A close friend of Khashoggi, Wadah Khanfar, the former director general of the Al Jazeera television network, was also hacked using Pegasus, with analysis showing that his phone was infected as recently July 2021.

The phone analysis discoveries and leaked phone records suggest that Saudi Arabia and its allies used NSO's spyware in the aftermath of the murder to monitor the campaign for justice led by friends and associates of Khashoggi, while also showing an intent to spy on the official Turkish inquiry into his murder.

Khashoggi associates who were targeted for possible surveillance after his death, according to the leak, include Abdullah Khashoggi, the journalist's son; Azzam Tamimi, a Palestinian-British activist and friend, and Madawi Al-Rasheed, a London-based scholar who co-created an opposition party of expatriate Saudis in the wake of the murder.

The Saudi crown prince, Mohammed bin Salman, who US intelligence agencies have concluded was responsible for ordering the murder of Khashoggi. Photograph: Anadolu Agency/Getty Images

Analysis of Rasheed's phone found evidence of an attempted hack in April 2019, but there was no evidence the spyware was successfully installed.

Other Khashoggi-connected names linked to in the data were Yahya Assiri, a UK-based Saudi activist who documents human rights violations in Saudi Arabia and was in close contact with Khashoggi before his death, and Yasin Aktay, a friend of Khashoggi and a top aide to the Turkish president, Recep Tayyip Erdoğan. No forensics were able to be carried out on their phones.

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.

In an interview, Aktay said he had already been alerted by Turkish intelligence officials that his phone had been hacked after Khashoggi's death because the Saudis were still trying to create a "map" of the journalist's connections. "It was needless," Aktay said of the surveillance. "I was just a friend of his."

İrfan Fidan, the Turkish prosecutor who charged 20 Saudis over the Khashoggi killing. Photograph: Anadolu Agency/Getty Images

The phone number of İrfan Fidan, the Istanbul chief prosecutor who later formally charged 20 Saudi nationals over the killing, also appeared in the list of numbers of possible candidates for surveillance by NSO Group clients.

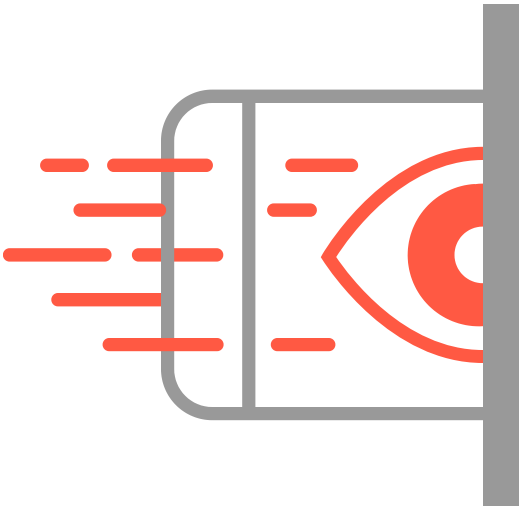
Without forensic examination of their phones, it is not possible to know whether these targets were infiltrated or successfully hacked using Pegasus.

In a statement, NSO said: “Our technology was not associated in any way with the heinous murder of Jamal Khashoggi. We can confirm that our technology was not used to listen, monitor, track, or collect information regarding him or his family members mentioned in your inquiry.”

Agnès Callamard, the secretary general of Amnesty International, which is a partner in the Pegasus project, said new discoveries about Khashoggi-related targets indicated an attempt by Saudi Arabia and others to gather intelligence on the fallout from the killing.

“The targeting indicates a clear intention to know what the prosecutor and a few other high political actors were doing,” she said. “They saw Turkey as the heart of what they needed to control.”

On Tuesday 27 July, at 8pm BST, a panel including Agnès Callamard, secretary general of Amnesty International, will discuss the global implications of the Pegasus project. Book your ticket here.



Topics

Reuse this content