The Guardian

This article is more than **6 months old**

Israeli spyware allegedly used to target Pakistani officials' phones

NSO Group malware may have been used to access WhatsApp messages for 'state-on-state' espionage

Stephanie Kirchgaessner *in Washington*

Thu 19 Dec 2019 13.56 GMT

The mobile phones of at least two dozen Pakistani government officials were allegedly targeted earlier this year with technology owned by the Israeli spyware company NSO Group, the Guardian has learned.

Scores of Pakistani senior defence and intelligence officials were among those who could have been compromised, according to sources familiar with the matter who spoke on the condition of anonymity.

The alleged targeting was discovered during an analysis of 1,400 people whose phones were the focus of hacking attempts in a two-week period earlier this year, according to the sources.

All the suspected intrusions exploited a vulnerability in WhatsApp software that potentially allowed the users of the malware to access messages and data on the targets' phones.

The discovery of the breach in May prompted WhatsApp, which is owned by Facebook, to file a lawsuit against NSO in October in which it accused the company of "unauthorised access and abuse" of its services.

The lawsuit claimed intended targets included "attorneys, journalists, human rights activists, political dissidents, diplomats, and other senior foreign government officials".

NSO has said it will vigorously contest the claim and has insisted that its technology is only used by law enforcement agencies around the world to snare criminals, terrorists and paedophiles.

The alleged targeting of Pakistani officials gives a first insight into how NSO's signature "Pegasus" spyware could have been used for "state-on-state" espionage.

The details also raise fresh questions about how NSO's clients use its spyware.

"This kind of spyware is marketed as designed for criminal investigations. But the open secret is that it also winds up being used for political surveillance and government-on-government spying," said John Scott-Railton, a senior researcher at the Citizen Lab, an academic research group located at the University of Toronto that has worked with WhatsApp to help identify victims of the alleged hacks.

"Spyware companies are clearly contributing to the proliferation of state-on-state technological espionage. No government seems particularly immune. This is probably further stretching the patience of governments around the world with this industry," he added.

The Pakistani embassies in London and Washington declined multiple requests for comment. WhatsApp declined to comment.

Representatives for NSO declined to comment on questions about whether the company's software had been used for government espionage.

The company has previously said it considered it a "misuse" of its product if the software was used for anything other than the prevention of "serious crime and terrorism".

While it is not clear who wanted to target Pakistani government officials, the details are likely to fuel speculation that India could have been using NSO technology for domestic and international surveillance.

The government of the Indian prime minister, Narendra Modi, is facing questions from human rights activists about whether it has bought NSO technology after it emerged that 121 WhatsApp users in India were allegedly targeted earlier this year.

The figure included about two dozen alleged victims who are journalists, activists and human rights lawyers, a fact that prompted Modi opponents in the Indian National Congress to seek a supreme court inquiry into the matter.

Pakistan has not publicised the alleged hack, but there are signs the government, led by the prime minister, Imran Khan, is taking steps to address the matter.

Dr Arslan Khalid, who serves as Khan's top adviser on digital issues, has said in local press reports that the government is working on developing an alternative to WhatsApp to be used for sensitive government data and other classified information. Government officials in Pakistan's ministry of information technology have also reportedly advised officials to stop sharing classified information over WhatsApp and replace smartphones that were purchased before May 2019, according to local press reports.

NSO has repeatedly said that its spyware is only meant to be used to combat terrorism and other crimes, such as child abduction and sex crimes. The company has claimed that the use of its spyware by governments has saved "thousands of lives".

NSO has also put a new human rights policy in place that is meant to "prevent and mitigate" abuse of its spyware. The policy states that NSO customers have "contractual obligations" to limit the use of the company's products to the "prevention and investigation of serious crimes, including terrorism, and to ensure the products will not be used to violate human rights".

NSO has not commented on whether it has pursued any internal investigations into the alleged WhatsApp hack.

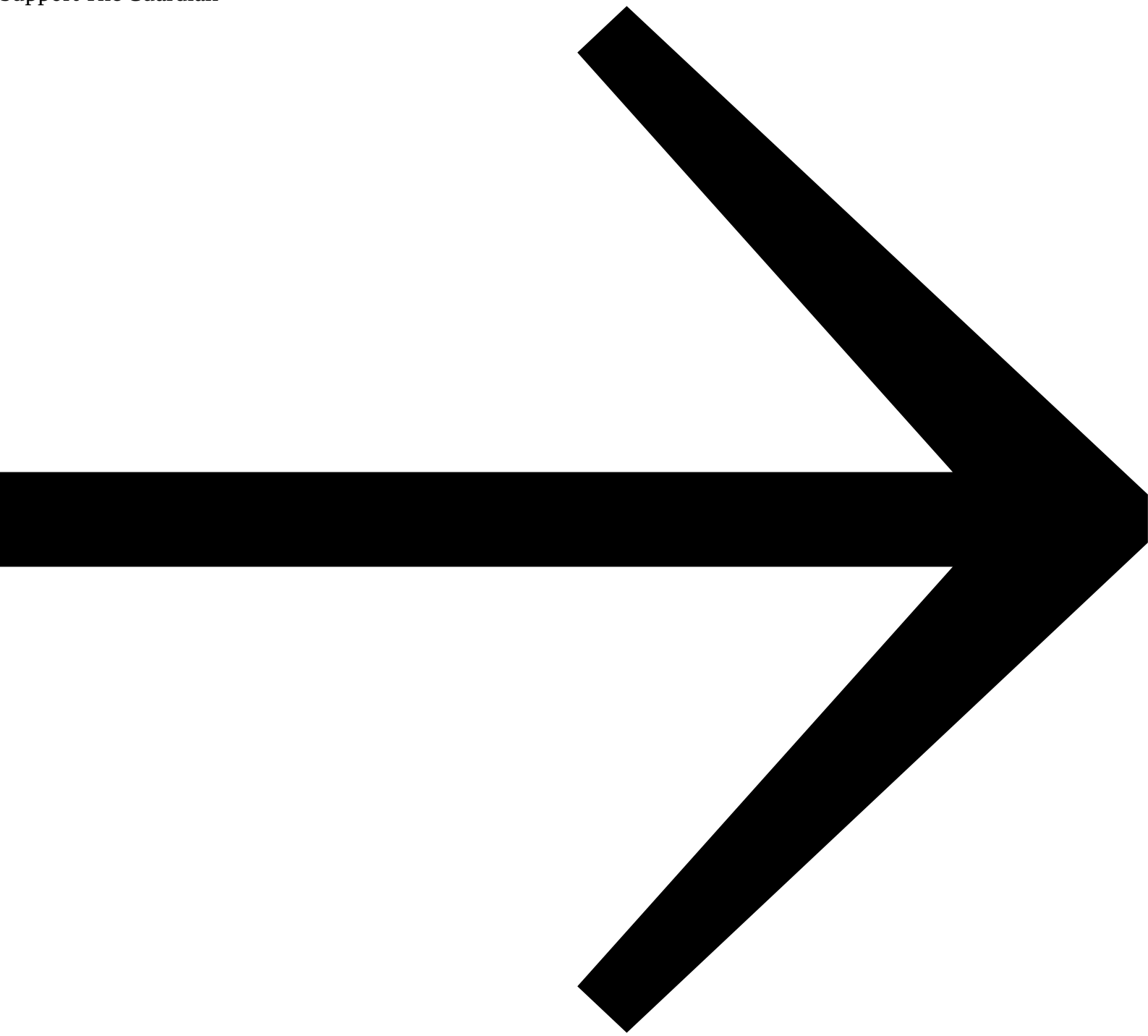
India was first linked to NSO in 2018, when a report by the Citizen Lab identified 36 Pegasus "operators" who were found to be using the malware in 45 countries. One operator, which the Citizen Lab identified and codenamed "Ganges", was found to have been active since 2017 and had infected mobile phones in five locations: India, Bangladesh, Brazil, Hong Kong and Pakistan. The Citizen Lab did not identify who it believed was behind "Ganges" but the data in its report indicated that most of the networks with infections were in India.

Apar Gupta, the executive director of the Internet Freedom Foundation (IFF), said in an interview with the Guardian that the Modi government had been evasive in answering questions by activists about whether or not the government had ever bought or licensed NSO technology.

Ravi Shankar Prasad, the Indian technology minister, said in a tweet on 31 October after news of the alleged Indian victims emerged that India was “concerned at the breach of privacy” on WhatsApp. When pressed about whether the government had any contracts with NSO, the Indian ministry of home affairs said that “no information” existed about the government ever ordering Pegasus, according to local reports.

The Indian embassy in Washington declined to comment.

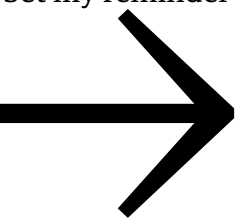
Support The Guardian



Remind me in September

Remind me in September
Email address

Set my reminder



We will use this to send you a single email in September 2020. To find out what personal data we collect and how we use it, please visit our Privacy Policy

We will be in touch to invite you to contribute. Look out for a message in your inbox in September 2020. If you have any questions about contributing, please contact us here.

Topics

- Pakistan
- Hacking
- WhatsApp
- Mobile phones
- South and Central Asia
- Israel
- Middle East and North Africa
- news