

Pegasus Espionage Case and Government of India

Dr. Sayyad Yasinbhai Gulabbhai

HOD Department of Political Science, Agsti, Art's Commerce and Dadasaheb Rupwate Science College Akole, Ahmednagar Maharashtra
422601, India
yasinsayyad1970[at]gmail.com

Abstract: *The French and Israeli governments have ordered an investigation into the spying scandal. However, the Indian government rejected the demand for an inquiry, claiming that it was an international conspiracy and defaming India. In the Rajya Sabha on Thursday, Union Minister for Information Technology, Communications and Electronics Ashwini Vaishnav rejected the opposition's demand for an inquiry, alleging that the case was an attempt to tarnish India's democracy. The Forbidden Stories in France covered the Pegasus case by 17 news organizations, including The Wire, The Washington Post and The Guardian. There was a worldwide outcry after that. The spying case was found in 14 other countries including India. French President Emmanuel Macron's government has ordered a 24 - hour probe into the alleged hacking of his mobile phone. If the evidence in the case is true, Macron said on Tuesday, it is a very serious matter and will try to ascertain the manner in which various reports have come from the media.*

Keywords: International conspiracy, hacking, cyber security, spyware, Pygmalus

1. Introduction

1.1 How 'Pegasus' is used

The Committee to Protect Journalists has reported 38 cases of spyware being used against journalists in nine countries since 2011. Eva Galperin, director of cyber security at the Electronic Frontier Foundation (EFF), was the first researcher to identify cyber - attacks against journalists and human rights activists in Mexico, Vietnam and elsewhere. She says, "In 2011, malware was installed on your computer via email. After 2014, with the advent of smartphones, spying on journalists on the phone became more common. Journalists were caught red - handed trying to provide specific information about a possible scam or their families. The malware is installed on the target person's phone after clicking on the link provided. "Now the process of installing 'Pegasus' spyware on the smart is being done more cleverly. Now that person doesn't even need to click. So the complexity of these attacks has increased even more. After successful installation on the phone, 'Pegasus' spyware gives NSO customers full access to their devices so they can also read messages from encrypted messaging apps like Signal, What Sapp or Telegram. Pegasus can be activated at any time until the phone is shut down. It can be reactivated after the phone is turned on.1

According to Claudio Gueneri, director of Amnesty International's security lab, Pegasus operators can remotely record audio and video on the phone, access data from the messaging app, use GPS to track location, and learn about passwords and authentication keys. Spying governments are pursuing a policy of exposing themselves by infecting the phone and getting information quickly so that it is not exposed.2

1.2 Pigassus project

Ismailova is one of 200 journalists from around the world selected by NSO clients. The report of the joint project 'Pegasus Project', which was attended by more than 80 journalists from 17 media organizations in ten countries, was released today. It was organized by Forbidden Stories and provided technical support by Amnesty International's

security lab. Forbidden Stories and Amnesty International have 50, 000 records of phone numbers chosen by NSO customers to monitor. According to an analysis of these records, at least 180 journalists from 20 countries were selected by 10 NSO clients. These customers were from monopoly countries (Bahrain, Morocco and Saudi Arabia) as well as democracies (India and Mexico). It included Hungary and Azerbaijan in Europe, as well as Togo and Rwanda in Africa. And the targets they chose included journalists, human rights activists, political opponents, entrepreneurs, and even heads of state.3

1.3 Pegasus and India

Founded in 2010, the NSO Group is considered to be the father of Pegasus. Pegasus is a spyware that allows a remote controller to hack into someone's smartphone. It also transmits information, content from the phone to the microphone and camera. NSO has always insisted that Pegasus is not sold to any private entity or government. In a letter to The Wire and co - operatives, the NSO reiterated that it only sells its spyware to a few experienced governments. The NSO will not confirm whether the Indian government is a customer or not. However, the existence of Pegasus in the phones of journalists and other people in India and the people selected for hacking show that one or more authorized organizations are actively using this spyware.

The Narendra Modi government has so far not explicitly denied the official use of Pegasus. However, he has denied the allegations, saying "Pegasus" could be used to monitor some people in India. This was made clear in a reply to a letter sent to the Ministry of Electronics and Broadcasting by members of the Pegasus project on Saturday.

Nine of the 13 iPhones tested in India were targeted, and seven of them had clear evidence of Pegasus.9 Android phones were also checked. One of them was found to be 'Pegasus'. It is not possible to say for sure about the remaining 8 phones. This is because the Android phone log does not provide such information, which cannot be used to confirm the existence of 'Pygmalus'.

Volume 11 Issue 7, July 2022

www.ijsr.net

Licensed Under Creative Commons Attribution CC BY

It is not clear from the combined findings whether the numbers of the journalists who have been found have been successfully tracked and obtained. The findings show that between 2017 and 2019, they were selected by official agencies to be targeted. A special digital forensic analysis conducted by AI's security lab found that the mobile phones of six Indian journalists on the list contained 'Pegasus'.⁴

Who exactly is the target in India?

- Founding Editor of The Wire and M. K. Venu is included in this list. Premshankar Jha, Rohini Singh and columnist Swati Chaturvedi, who worked for 'Wire', are also said to have been targeted.
- Rohini Singh had reported on the business of Union Home Minister Amit Shah's son Jai Shah and Prime Minister Narendra Modi's aide Nikhil Merchant. He also unveiled some deals between Union Minister Piyush Goyal and industrialist Ajay Piramal.
- It is mentioned that Sushant Singh, the deputy editor of The Indian Express, who was constantly trying to expose the Raphael scandal in 2018, was also under surveillance.
- Vijaya Jain of The Hindu, Shirish Gupta and Prashant Jha, editor of Hindustan Times, important journalists of media like India Today, Network 18, The Hindu and Indian Express are found in the list.
- Congress leader Rahul Gandhi's two mobile numbers, political strategist Prashant Kishor, former election official Ashok Lavasa, ministers Ashwin Vaishnav, Pralhad Patel and Trinamool Congress leader Abhishek Banerjee are also on the list.
- The watch list also includes eight mobile numbers of former Supreme Court Justice Ranjan Gogoi, a female Supreme Court employee accused of molestation, her husband and brother.⁵

2. Conclusion

Pegasus is a spyware developed by NSO Group, an Israeli cyber security company. This is a program that if put in a smartphone phone, all its information will be in the hands of hackers. The person who needs to be targeted is sent a link via Pegasus via SMS, WhatsApp or any other means. The special thing is that even after the phone is hacked, you will not know anything. This spyware is so strong that it can even hack an iPhone. Pegasus can work even when your phone is locked. The time has come for Pygmy spyware. This is underlined in a joint international investigative journalism project with The Wire and 16 other media organizations. The Israeli company Spyware Pegasus is being used by governments around the world to spy on journalists, MPs, politicians and relatives of politicians. The investigation has been dubbed the 'Pegasus Project'. The leaked information of thousands of telephone numbers listed by several government customers of the Israeli intelligence technology agency includes more than 300 Indian mobile numbers. The mobile numbers have been used by ministers, opposition leaders, journalists, lawyers, businessmen, government officials, scientists, human rights activists and others, according to the research project 'Project Pegasus'.

References

- [1] Jay muzoomdar, new delhi, The Indian Express, 1Nov2019
- [2] 19 July 2021 vayar news
- [3] Finijrukart, 19 july 2021 vayar news
- [4] 19 July 2021 vayar news
- [5] Chacke post in Marathi july 2021