Pegasus Project: How Phones of Journalists, Ministers, Activists May Have Been Used to Spy On Them

thewire.in/government/project-pegasus-journalists-ministers-activists-phones-spying

Photo: Bruno/Germany via Pixabay

Government

An international collaborative reporting project has established the frightening extent to which governments around the world, including India, could be using surveillance tools in ways that have nothing to do with national security.

Siddharth Varadarajan

Listen to this article:

Government

Rights

Tech

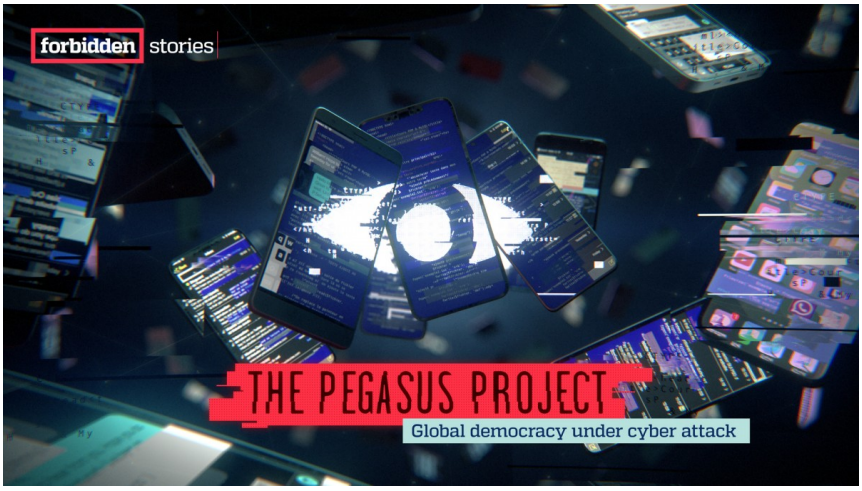
18/Jul/2021

New Delhi: A leaked database of thousands of telephone numbers believed to have been listed by multiple government clients of an Israeli surveillance technology firm includes over 300 verified Indian mobile telephone numbers, including those used by ministers, opposition leaders, journalists, the legal community, businessmen, government officials, scientists, rights activists and others, according to an investigation by *The Wire* and 16 media partners.

Forensic tests conducted as part of this project on a small cross-section of phones associated with these numbers revealed clear signs of targeting by Pegasus spyware in 37 phones, of which 10 are Indian. Without subjecting a phone to this technical analysis, it is not possible to conclusively state whether it witnessed an attack attempt or was successfully compromised.

NSO Group, the Israeli company which sells Pegasus worldwide, says its clients, are confined to “vetted governments”, believed to number 36. Though it refuses to identify its customers, this claim rules out the possibility that any private entity in India or abroad is responsible for the infections which *The Wire* and its partners have confirmed.

The leaked database was accessed by Paris-based media nonprofit Forbidden Stories and Amnesty International and shared with *The Wire, Le Monde, The Guardian, Washington Post Die Zeit, Suddeutsche Zeitung* and 10 other Mexican, Arab and European news organisations as part of a collaborative investigation called the ‘Pegasus Project’.



Forbidden Stories, which accessed the data, says it comprises records of phone numbers selected as targets by NSO clients, a claim the company formally denied while conceding that its clients might have used these numbers for “other purposes”.

A majority of the numbers identified in the list were geographically concentrated in 10 country clusters: India, Azerbaijan, Bahrain, Hungary, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia and the United Arab Emirates.

Each of these countries have been identified in the past by experts at Citizen Lab – a digital surveillance research organisation based out of the University of Toronto that laid the groundwork for WhatsApp’s 2019 lawsuit against the NSO Group – as having been a region

of focus for Pegasus operators.

Working together with the technical lab of Amnesty International, a team of over 80 journalists coordinated by Forbidden Stories sought to identify and verify the individuals to whom these numbers belong and then conduct a forensic examination of the phones in use by them for the period covered by the data, which, in the Indian case was approximately mid-2017 to mid-2019.

Also read: FAQ: On the Pegasus Project's Digital Forensics

The Indian Telegraph Act and Information Technology Act prescribe procedures that must be followed for lawful interception. Different countries have different laws but the use of hacking to deliver surveillance spyware in India by any individual, private or official, is an offence under the IT Act.

The Wire will be revealing the names it has been able to verify under different categories, in a step by step fashion with its partners over the next few days.

The numbers of those in the database include over 40 journalists, three major opposition figures, one constitutional authority, two serving ministers in the Narendra Modi government, current and former heads and officials of security organisations and scores of businesspersons.

The presence of a number in the database indicates its likely selection as a target for surveillance but whether a phone was actually hacked and infected can only be established through forensic examination of the device – more easily done if the instrument in question is an iPhone.

Among the numbers in the Pegasus Project database is one that was registered in the name of a sitting Supreme Court judge. However, *The Wire* has not been able to confirm whether the number, which the judge gave up before it was added to the list, was still being used by him for WhatsApp and other encrypted messaging apps when the number was selected. Until such time as we are able to establish the number's actual user during the period in question, we are withholding the name of the judge.

The Wire and its partners will also not be revealing the identity of any names that appear to be the subject of counter-terrorism or state-to-state espionage, with the exception of 13 heads of state or government around the world.

Committed to privacy rights, says Indian government

In a response to detailed questions sent by Pegasus Project partners to the Prime Ministers' Office earlier this week, the Ministry of Electronics and Information Technology said that "India is a robust democracy that is committed to ensuring the right to privacy to all

its citizens as a fundamental right" and that the "allegations regarding government surveillance on specific people has no concrete basis or truth associated with it whatsoever."

Without specifically denying that Pegasus is being used by the government, the MEITY response said, "Each case of interception, monitoring, and decryption is approved by the competent authority… The procedure therefore ensures that any interception, monitoring or decryption of any information through any computer resource is done as per due process of law."

Also read: Old RTI Response Enough To Deny Govt-Pegasus Link, Media Didn't Do Due Diligence: MeitY

In fact, the procedure for lawful interception involves not just written, time-bound authorisation in each instance but the use of the telecom or computer resource intermediary as well, who is supposed to enable the interception, and does not cover the activities proscribed by Section 43 of the IT Act under the definition of "hacking".

Hacking an individual's smartphone is a necessary step in subjecting an individual to surveillance by spyware such as Pegasus.

NSO says data 'may be' linked to its customers

Though the NSO Group insists the leaked database is "not a list of numbers targeted by governments using Pegasus", it told *The Wire* and Pegasus Project partners in a letter from its lawyers that it had "good reason to believe" the leaked data "may be part of a larger list of numbers that might have been used by NSO Group customers for other purposes".

Asked what these "other purposes" could be, the company changed tack and claimed that the leaked records were based on "publicly accessible, overt sources such as the HLR Lookup service" – and that it had no "bearing on the list of the customer targets of Pegasus or any other NSO products".

HLR lookup services are used to test whether a phone number of interest is currently on a network.

If the leaked numbers represent the output of an HLR Lookup service, as NSO itself suggests, the fact that the data is from countries known to have been a region of focus for Pegasus operators in the past raises two questions: were they all generated by the same service provider? Were they all consolidated and held in one place for some common purpose?

While HLR lookups have obvious commercial relevance for telemarketers, telecom security experts say they could well be an integral part of spyware-driven surveillance. “Here’s the most important reason why you would use an HLR lookup,” Karsten Nohl, chief scientist for Security Research Labs in Berlin, told the Pegasus Project. “You would know that the phone is on” – and hence available for hacking.

NSO disputes the suggestion that Pegasus could have been used to target 50,000 persons, implying that the scale of targeting across all government clients is around 5,000 a year.

The sensitivity of the information involved – governments which select high-profile individuals for potential hacking and surveillance would hardly like the details or metadata of their targeting to be known by a foreign government or private entity – further adds to the questions which the leaked database and NSO’s firm denial that this has any connection to Pegasus raise.

None of the governments involved have an incentive to shed light on the issue. However, in countries that are governed by the rule of law, the possibility that a massive and illegal surveillance programme is being used to target prominent individuals from all walks of life – including political opponents and journalists – poses a clear threat to democracy and will raise demands for an independent probe.

The Pegasus Project is a collaborative investigation that involves more than 80 journalists from 17 news organisations in 10 countries coordinated by Forbidden Stories with the technical support of Amnesty International’s Security Lab. Read all our coverage here.