Pegasus infection found on Indian journalists' phones after Apple alert: Amnesty International

Amnesty International announced that it found recent traces of Pegasus spyware, sold only to governments, on two Indian journalists' phones after they received "state-sponsored attacker" alerts from Apple in October.

December 28, 2023 10:51 am | Updated 06:36 pm IST - NEW DELHI

AROON DEEP

Representational image only. The Pegasus spyware, which the Union government has not categorically denied buying or using, allows attackers to extract all the contents of smartphones by leveraging software weaknesses

Security Lab was able to determine after testing their devices, it announced on Thursday. The journalists had received an alert from Apple that they were being targeted by "state-sponsored hacking," following which they provided their phones to Amnesty for testing. NSO Group, the Pegasus spyware's developer, only sells its technology to governments. India's Intelligence Bureau imported hardware from NSO Group in 2017, trade data show.

Vijayakant: DMDK founder, actor, philanthropist, who briefly altered TN's political landscape

To discover more such stories, visit SHOWCASE

Separately, *TheWashington Post* reported that after the security alerts went out in October, government officials put 'pressure' on Apple to offer 'alternative' explanations to the public on why these warnings were sent to Opposition leaders and journalists. Union Ministers and Apple had made a series of misleading and unsubstantiated statements when these alerts went out, such as that these messages had gone out in 150 countries, when no other countries' citizens — or ruling party lawmakers — had reported receiving a warning that week. According to the *Post* report, Praveen Chakravarty, the chairman of the All India Professionals' Congress, was also likely targeted, based on an analysis of his phone by iVerify, a cybersecurity firm.

The Pegasus spyware, which the Union government has not categorically denied buying or using, allows attackers to extract all the contents of smartphones by leveraging software weaknesses that are known to a select few hackers, and sold for millions of dollars. These so-called 'zero day exploits' allow attackers to access all the data on even phones whose software has been fully updated, and access real-time camera and microphone data. Such technology, privacy activists argue, is an unconstitutional form of surveillance. Dozens of Opposition leaders, journalists and activists were targeted by Pegasus until 2021, according to the *Forbidden Stories* collective, which reported on a leak of the spyware's global targets.

'Attack on privacy'

an obligation to protect human rights by protecting people from unlawful surveillance, said Donncha Ó Cearbhaill, head of the Security Lab that uncovered the infections.

"The recovered samples are consistent with the NSO Group's BLASTPASS exploit, publicly identified by Citizen Lab in September 2021 and patched by Apple in iOS 16.6.1 (CVE-2023-41064)," Amnesty said in a statement, referring to a vulnerability that Apple patched through a software update in September.

The Union government refused to cooperate in a Supreme Court-ordered investigation into the 2021 Pegasus revelations. Both Mr. Varadarajan and Anand Mangnale, South Asia Editor at the Organised Crime and Corruption Report Project (OCCRP), had spyware that logs show infected their phones this year. The OCCRP had reported last year that the Intelligence Bureau (IB) obtained Pegasus, citing trade data that *The Hindu* was later able to verify, and interviews with unnamed IB officers. Ten months later, Mr. Mangnale's phone was infected, Amnesty found. The day before, he told *TheWashington Post*, he had sent queries to the Adani group for an investigative story OCCRP was working on about the corporate group.

Mr. Varadarajan's phone was found to be infected on October 16. Both men received alerts from Apple in October saying that their phones had been targeted by "state-sponsored attackers". The Union government said it was investigating these alerts, which were sent to numerous Opposition members of Parliament as well.

The Union government was reportedly looking for Pegasus alternatives after the NSO Group's activities came under global scrutiny, but the spyware's continued use after the furore has only emerged now. The Defence Intelligence Agency's Signal Intelligence Directorate has purchased equipment from Cognyte, a company that has been sued in the United States on similar snooping grounds, *The Hindu* had reported in April.