India: Damning new forensic investigation reveals repeated use of Pegasus spyware to target high-profile journalists

8-10 minutes ⋮ 12/28/2023

Amnesty International, in partnership with The Washington Post, has unearthed shocking new details about the continued use of NSO Group's highly invasive spyware Pegasus to target prominent journalists in India, including one who had previously been a victim of an attack using the same spyware.

> Our latest findings show that increasingly, journalists in India face the threat of unlawful surveillance simply for doing their jobs, alongside other tools of repression including imprisonment under draconian laws, smear campaigns, harassment, and intimidation
>
> *Donncha Ó Cearbhaill, Head of Amnesty International's Security Lab.*

Forensic investigations by Amnesty International's Security Lab confirmed that Siddharth Varadarajan, Founding Editor of The Wire, and Anand Mangnale, the South Asia Editor at The Organised Crime and Corruption Report Project (OCCRP), were among the journalists recently targeted with Pegasus spyware on their iPhones, with the latest identified case occurring in October 2023.

The use of Pegasus, a type of highly invasive spyware, developed by Israeli surveillance firm NSO Group, comes amid an unprecedented crackdown by the Indian authorities on freedom of peaceful expression and assembly, which has had a chilling impact on civil society organizations, journalists, and activists.

"Our latest findings show that increasingly, journalists in India face the threat of unlawful surveillance simply for doing their jobs, alongside other tools of repression including imprisonment under draconian laws, smear campaigns, harassment, and intimidation," said Donncha Ó Cearbhaill, Head of Amnesty International's Security Lab.

"Despite repeated revelations, there has been a shameful lack of accountability about the use of Pegasus spyware in India which only intensifies the sense of impunity over these human rights violations."

Forensic evidence reveals Pegasus activity

Amnesty International's Security Lab first observed indications of renewed Pegasus spyware threats towards individuals in India during a regular technical monitoring exercise in June 2023, a number of months after media reported that the Indian government was seeking to procure a new commercial spyware system.

In October 2023, Apple issued a new round of threat notifications globally to iPhone users who may have been targeted by "state-sponsored attackers". More than 20 journalists, and opposition politicians in India were reported to have received the notifications.

As a result, Amnesty International's Security Lab undertook a forensic analysis on the phones of individuals around the world who received these notifications, including Siddharth Varadarajan and Anand Mangnale. It found traces of Pegasus spyware activity on devices owned by both Indian journalists.

The Security Lab recovered evidence from Anand Mangnale's device of a zero-click exploit which was sent to his phone over iMessage on 23 August 2023, and designed to covertly install the Pegasus spyware. The phone was running iOS 16.6, the latest version available at the time.

A zero-click exploit refers to malicious software that enables spyware to be installed on a device without requiring any user action from the target, such as clicking on a link.

The Security Lab also identified an attacker-controlled email address used as part of the Pegasus attack on his device. 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).

Anand Mangnale's phone was vulnerable to this zero-click exploit at the time of the attack. It is currently unclear if the exploit attempt resulted in a successful compromise of his device.

The attempted targeting of Anand Mangnale's phone happened at a time when he was working on a story about an alleged stock manipulation by a large multinational conglomerate in India.

A more detailed technical analysis of the exploit and accompanying forensic evidence is available on the Amnesty Tech Security Lab website.

A history of spyware abuse

Amnesty International has previously documented how Siddharth Varadarajan was targeted and infected with Pegasus spyware in 2018. His devices were later forensically analysed by a technical committee established by the Supreme Court of India in 2021 in the wake of the Pegasus Project revelations.

In 2022, the committee concluded its investigation, but the Supreme Court has not made the findings of the technical report public. The court noted, however, that the Indian authorities "did not cooperate" with the technical committee's investigations.

Siddharth Varadarajan was targeted again with Pegasus on 16 October 2023. The same attacker-controlled email address used in the Pegasus attack against Anand Mangnale was also identified on Siddharth Varadarajan's phone, confirming that both journalists were targeted by the same Pegasus customer.

There are no indications that the Pegasus attack was successful in this case.

"Targeting journalists solely for doing their work amounts to an unlawful attack on their privacy and violates their right to freedom of expression. All states, including India, have an obligation to protect human rights by protecting people from unlawful surveillance," said Donncha Ó Cearbhaill

Reporters at The Washington Post reached out to NSO Group for their response to these latest findings.

The company said, "While NSO cannot comment on specific customers, we stress again that all of them are vetted law enforcement and intelligence agencies that license our technologies for the sole purpose of fighting terror and major crime. The company's policies and contracts provide mechanisms to avoid targeting of journalists, lawyers and human rights defenders or political dissidents that are not involved in terror or serious crimes. The company has no visibility to the targets, nor to the collected intelligence."

NSO Group states that it sells its products only to government intelligence and law enforcement agencies. Indian authorities have until today provided no clarity or transparency on whether they have procured or used the Pegasus spyware in India.

“Amnesty International is calling on all countries, including India, to ban the use and export of highly invasive spyware, which cannot be independently audited or limited in its functionality,” said Donncha Ó Cearbhaill.

The organization is also calling for the findings of the Supreme Court Technical Committee Report on Pegasus use in India to be immediately released. The Indian government should also conduct an immediate, independent, transparent, and impartial investigation into all cases of targeted surveillance, including into these latest revelations.

To ensure transparency, Indian authorities should also publicly disclose information about any previous, current or future contracts with private surveillance companies, including with NSO Group.”

Background

In October 2022, OCCRP reported based on analysis of commercial trade databases, that India’s main domestic intelligence agency, the Intelligence Bureau, got a shipment of hardware from NSO Group matching the description of equipment used to run the Pegasus system in April 2017. The earliest Pegasus attacks identified by Amnesty International in India occurred in early July 2017.

In 2020, Amnesty International and Citizen Lab revealed how human rights defenders were targeted in a coordinated operation using commercial off-the-shelf spyware in India.

In 2021, as part of the Pegasus Project, Amnesty International in partnership with Forbidden Stories revealed how numerous civil society members and journalists in India were targeted and infected using NSO Group’s Pegasus spyware, including Siddharth Varadarajan.

The Security Lab will continue to monitor and provide support to civil society around the world who are concerned about spyware attacks and unlawful digital surveillance.

Amnesty International thanks the Digital Security Lab at Reporters Without Borders for their outreach and analysis support as part of this investigation.

If you are a human rights defender, activist or journalist who has received a similar security alert from Apple or other platforms, contact us for digital forensics support.