Rahul, Prashant Kishor, ex-EC Lavasa on list of spyware targets

Analysis confirms Pegasus attack or attempts on 10 Indian numbers, says report

SPECIAL CORRESPONDENT
CHENNAI

Former Congress president Rahul Gandhi, former Election Commissioner Ashok Lavasa, election strategist Prashant Kishor, Trinamool Congress leader Abhishek Banerjee and Union Ministers Ashwini Vaishnaw and Prahlad Patel appeared on a leaked list of "potential" or actual targets for spying by the Israeli company NSO's Pegasus spyware, news website *The Wire* and other international publications reported on Monday.

Two mobile phones used by Mr. Gandhi appeared on the list – one was added in 2018 when he was the president of the Congress and the other after the 2019 Lok Sabha election, according to the reports. Numbers belonging to at least five of Mr. Gandhi's close friends and other Congress officials, including Sachin Rao and Alankar Sawai, also figured on the list, which has the names of dozens of journalists, activists and healthcare experts.

At least one number once used by Pakistan Prime Minister Imran Khan as well as hundreds of others in the country also appeared on the list.

The phones targeted were infiltrated by a malicious software called Pegasus, which is sold by the NSO Group. The spyware can secretly unlock the target's phone, computer or other devices, collect information and transfer it to another device without the permission of the user. The Israeli company has said it sells Pegasus only to government agencies to fight terrorism and other serious crimes and that it does not operate the spyware licensed to its clients.

Those who were targeted in India included *The Wire's* editors Siddharth Varadarajan and M.K. Venu, journalist Sushant Singh and Mr. Kishor, a forensic analysis found. The phone of Mr. Kishor, who worked with the Trinamool in West Bengal and the DMK in Tamil Nadu that went to the polls in April, was found to have been compromised as recently as July 14.

Investigations confirmed the Pegasus attack, or signs of potential targeting, on phones linked to 10 Indian numbers and 27 phones around the world, according to *The Guardian*.

CONTINUED ON ▸ PAGE 12
MORE REPORTS ▸ PAGE 13

Decoding Pegasus

Pegasus is a spyware, developed and licensed by an Israeli company, NSO Group. It can be used to infiltrate smartphones that run on both iOS and Android operating systems, and turn them into surveillance devices. A low down:

- Pegasus's method of attack is called zero-click attacks, which do not require any action by the user. The spyware can hack a device simply by giving a **missed WhatsApp call**
- It will **alter call logs** so that the user has no knowledge of what happened
- It can also be **installed manually** on a device or over a wireless transceiver
- If it fails to connect with its command-and-control server for more than 60 days, it **self-destructs and removes all traces**
- If it detects that it was installed on the wrong device or SIM card, it will **self-destruct**
- Amnesty International noted that despite issuing security updates, Android and **iOS devices were breached**
- To stay safe, users need to ensure that software in devices is updated and all apps are installed directly through the offical stores. **No suspicious email or text should be clicked**
- **Once the spyware enters the device, it installs a module to track call logs, read messages, emails, calendars, Internet history, and gather location data to send the information to the attacker**