The Pegasus Threat: All you need to know

Spyware developed by an Israeli firm has once again been used for surveillance against journalists, human rights activists and business executives. Smartphones were hacked to gather confidential information, according to an investigation by The Washington Post and 16 media partners.

A world collaborative investigative project has discovered Israeli spyware Pegasus was used to target thousands of people across the globe. In India, at least 300 people are believed to have been targeted, which are two serving Ministers in the Narendra Modi government, three Opposition leaders, one constitutional authority, various journalists and business persons.

The BJP launched a full-blown campaign to counter the opposite allegations on the Pegasus controversy. Home minister Amit Shah on Monday said disruptors and obstructors will not be able to derail India’s development trajectory through their (opposition’s) conspiracies and the monsoon session will bear new fruits of progress.

Shah said the facts and sequence of events are for the entire nation to see. “Today, the monsoon session has started. In what seemed like a perfect cue, late last evening we saw a report that has been amplified by a few sections with only one aim to do whatever is possible and humiliate India at the world stage, peddle the same old narratives about our nation and derail India’s development trajectory,” the home minister said in a statement, a few hours after Congress sought his resignation over the controversy.

How does it work?

‘Pegasus’ is spyware used to snoop into handsets which have

been claimed that even a missed video call on WhatsApp could give Pegasus complete access to users' smartphones.

It enabled the opening up of the handsets and the operator installing the spyware on the device without the owner's acknowledgement.

This resulted in the hacker accessing the user's data including passwords, contacts, calendar events, text messages and even live voice calls from messaging apps easily without the user permission.

The 2019 attacks and WhatsApp's complaint

Pegasus can be installed on your phone without even your awareness just a phone call away and you never come to know it !!

After the 2019 attacks, WhatsApp in its complaint filed in California said the attack happened through its video calling feature.

It said Pegasus is capable of surveillance on three levels: initial data extraction, passive monitoring and active collection.

The software was used to hijack smartphones running on iOS, Android and BlackBerry operating systems. "A buffer overflow vulnerability in WhatsApp VOIP stack allowed remote code execution via specially crafted series of RTCP packets sent to a target phone number," WhatsApp said in its complaint.

The spyware leaves no trace on the device, consumes minimal battery, memory and data consumption and comes with a self-destruct option that can be used any time, the complaint further added.