Israeli spyware Pegasus

What is the issue?

- WhatsApp sued an Israeli firm, the NSO Group in a court for using its platform to spy on journalists and human rights activists worldwide.
- The surveillance was carried out using a spyware tool called Pegasus, which has been developed by the NSO Group.

Who are the parties involved in the case?

- **WhatsApp** - The world's most popular messaging app, with more than 1.5 billion users worldwide. It is owned by Facebook.
- About a quarter of those users (more than 40 crore) are in India, WhatsApp's biggest market.
- **NSO Group** - A Tel Aviv-based cyber-security company that specialises in surveillance technology.
- It claims to help governments and law enforcement agencies across the world fight crime and terrorism.

What is the story behind?

- WhatsApp sued the NSO Group in a federal court in San Francisco.
- It accused NSO of using its servers to send malware to approximately 1,400 mobile phones and devices (Target Devices) for the purpose of conducting surveillance of specific WhatsApp users (Target Users).
- The surveillance was carried out between April and May 2019 on users in 20 countries across four continents.
- Will Cathcart, the head of WhatsApp told that the surveillance targeted at least 100 human-rights defenders, journalists and other members of civil society across the world.

What exactly is Pegasus?

- Pegasus works by sending an exploit link, and if the target user clicks on the link, the malware or the code that allows the surveillance is installed on the user's phone.
- A presumably newer version of the malware doesn't even require a target user to click a link.
- Once Pegasus is installed, the attacker has complete access to the target

user's phone.

- The first reports on Pegasus's spyware operations emerged in 2016, when Ahmed Mansoor, a human rights activist in the UAE, was targeted with an SMS link on his iPhone.
- The Pegasus tool at that time exploited a software chink in Apple's iOS to take over the device. So, Apple pushed out an update to fix the issue.
- Pegasus delivers a chain of zero-day exploits to penetrate security features on the phone and installs it without the user's permission.
- **Zero-day exploit** - A completely unknown vulnerability about which even the software manufacturer is unaware, and thus there is no patch or fix available for it.
- In the cases of Apple and WhatsApp, neither was aware of the security vulnerability, which was used to exploit the software and take over the device.
- In May 2019, the Pegasus was being used to exploit WhatsApp and spy on potential targets.
- WhatsApp issued an urgent software update to fix the security bug that was allowing the spyware to exploit the app.

Once installed, what all can Pegasus do?

- It can work on BlackBerry, Android, iOS and Symbian-based devices.
- It can send back the target's private data, including passwords, messages, live voice calls, etc., from popular mobile messaging apps.
- The target's phone camera and microphone can be turned on to capture all activity in the phone's vicinity, expanding the scope of the surveillance.
- Pegasus has the ability to access password-protected devices, being totally transparent to the target, leaving no trace on the device without arousing suspicion in more alert users.
- It has a self-destruct mechanism in case of risk of exposure, and ability to retrieve any file for deeper analysis.

How did Pegasus exploit WhatsApp?

- That's a question for many, given that WhatsApp has always tom-tommed its end-to-end encryption.
- A missed call on the app was all that was needed to install the software on the device - no clicking on a misleading link was required.
- WhatsApp later explained that Pegasus had exploited the video/voice call function on the app, which had a zero-day security flaw.
- It didn't matter if the target didn't take the call - the flaw allowed for the malware to be installed anyway.
- The exploit impacted WhatsApp for Android and iOS; WhatsApp Business for

Android and iOS; WhatsApp for Windows Phone and Tizen (Samsung).

Can Pegasus be used to target just about anyone?

- Technically, yes. But while tools such as Pegasus can be used for mass surveillance; it would seem likely that only selected individuals would be targeted.
- In the present case, WhatsApp has claimed that it sent a special message to the users who it believed were impacted by the attack, to directly inform them about what had happened.
- At least two dozen academics, lawyers, Dalit activists, and journalists were alerted by the company in India.
- It is not known who carried out the surveillance on the Indian targets.
- The NSO Group, while disputing WhatsApp's allegations has said that it provides the tool exclusively to licensed government intelligence and law enforcement agencies and not just to anyone who wants it.

Should we switch to other apps?

- The very popularity of a messaging app makes it a target for hackers, cybercriminals, or other entities.
- Even law enforcement agencies across the world want messages to be decrypted - a demand that WhatsApp is fighting, including in India.
- WhatsApp uses the Signal app protocol for its end-to-end encryption, which seems safe so far.
- It has an advantage over Telegram: Only the secret chats are end-to-end encrypted in Telegram, while on WhatsApp everything is so by default.
- Those rattled by the WhatsApp episode might want to switch to Signal or Wire.
- However, unknown 'zero-day' exploits could exist for virtually every software and app in the world.
- They might be exploited at some point in the future by individuals or agencies determined to do so.

Source: The Indian Express