UPSC PREPARATION

Pegasus Spyware - Overview

Pegasus spyware is malicious software that is designed to enter a device,gather your data, and then forward it to a third party without the consent of the user.

The Pegasus snooping controversy led to multiple disruptions in the Lok Sabha in the monsoon session 2021 of the parliament.

Pegasus Spyware in Detail

- Pegasus was developed in 2010 by the Israeli firm, the NSO Group.
- Pegasus spyware was first discovered in an iOS version in 2016 and then a slightly different version was found on Android.
- Pegasus spyware is able to read the victim's SMS messages and emails, listen to calls, take screenshots, record keystrokes, and access contacts and browser history.
- Hackers can hijack the phone's microphone and camera, turning it into a real-time surveillance device.
- Pegasus can send back to the hacker the target’s private data, including, contact lists, calendar events, passwords, text messages, and live voice calls 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 evolved from a crude system that was reliant on social engineering to software that can compromise a phone without the user having to click on a single link. This is called Zero-click attack.

Targets of Pegasus Spyware

- Media outlets said they had identified more than 1,000 people in over 50 countries whose numbers were on the list.
- They include business executives, activists, politicians and heads of state and many royal family members of Arab. More than 180 journalists were also found to be on the list, from organisations including the New York Times, CNN and Al Jazeera.
- According to the reports, many of the numbers were clustered in 10 countries: Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia and the United Arab Emirates,

Evolution of Pegasus Spyware

- In 2016, It infected smartphones using a technique called “spear-fishing”: the hackers send malicious links to the target via text messages and emails.
- In 2019, Pegasus was able to infiltrate a device with a missed call on WhatsApp and could even delete the record of this missed call. This makes it difficult for the user to know that they were targeted.
- In the same year, WhatsApp said Pegasus exploited a bug in its code to infect more than 1,400 iPhones and Android phones. These include journalists, government officials and human rights activists. It soon fixed the bug.

- July 2021: The Pegasus Project, an international investigative journalism effort, revealed that various governments used the software to spy on opposition politicians, government officials, activists, journalists and many others. It said the Indian government used it to spy on around 300 people between 2017 and 2019.

International Mechanisms to Mitigate Cybercrime

- Budapest Convention is an international convention It seeks to address Internet and computer crime (cybercrime) by improving investigative techniques, harmonizing national laws, and increasing cooperation among nations. It came into force on 1st July 2004. India is not a signatory to this convention.
- International Telecommunication Union is a specialized agency within the United Nations. It plays an important role in the development and standardisation of telecommunications and cybersecurity issues.

How can one detect the Pegasus Spyware?

Researchers at Amnesty International have developed a tool to see whether your phone is targeted by spyware. The tool is called Mobile Verification Toolkit (MVT), the tool is aimed to help you identify if the Pegasus spyware has targeted your phone. It works with both Android and iOS devices.

NSO's stand on the issue

- The NSO has said that it sells its technologies only to law enforcement and intelligence agencies of governments for the purpose of saving lives through preventing crime and terror acts.
- the group said, It does not operate the system and has no visibility to the data.
- As per the company's website, NSO products are used exclusively by government intelligence and law enforcement agencies to fight crime and terror.

Conclusion:

Providing as much of information on the Pegasus Spyware to software and security vendors can help to fix the vulnerabilities exploited by the attackers. The governments must take measures such that the Spyware is not misused by political parties and intelligence institutions.

Frequently Asked Questions

How does Pegasus spyware get on your phone?

Zero-click exploits use bugs in popular apps like iMessage, FaceTime and WhatsApp. Pegasus can infiltrate a device using the protocol of the app once bugs are found.

Who owns Pegasus spyware?

The Pegasus spyware, developed by Israeli software company NSO Group to fight crime and terror.