Pegasus Spyware

For Prelims: Pegasus spyware**, Zero-click and Zero-day vulnerabilities,** National Cyber Security Strategy**,** Cyber Surakshit Bharat

For Mains: Spyware and Privacy Concerns, Cyber Attacks, Government Initiatives

Source: TH

Why in News?

The **Pegasus spyware** has once again ignited a debate on **privacy and security**. Recent reports by **Amnesty International** point to its utilization in targeting the **phones of two prominent Indian journalists,** prompting inquiries into potential government involvement.

- Amnesty International is a global movement of more than 10 million people who are committed to creating a future where **human rights are enjoyed by everyone.**

What is Pegasus Spyware?

- **About:**
  - Pegasus spyware is a **highly invasive mobile surveillance tool** that can secretly infiltrate and monitor smartphones, collecting data and information from various apps and sources.
  - It was developed by the **Israeli cyber-intelligence firm NSO Group,** which claims to sell it only to government agencies for fighting crime and terrorism.
    - NSO emphasizes mechanisms in place to avoid targeting journalists, lawyers, and human rights defenders not involved in terror or serious crimes.
- **Operating Procedure:**
  - Pegasus uses **“zero-click”** methods to infect devices; it is a malicious software that allows spyware to be installed on a device **without the device owner’s consent.**
    - The spyware doesn't necessitate any user actions for installation, distinguishing it from **regular apps that require explicit user confirmation.**
    - It can exploit vulnerabilities in apps such as WhatsApp, iMessage, or FaceTime, and send a message or a call that triggers the installation of the spyware, even if the user does not open or answer it.
  - Pegasus is a spyware that can **exploit zero-day vulnerabilities** to deploy spyware on Apple products.
    - A zero-day vulnerability is an **undiscovered flaw or bug** in an operating system that the mobile phone’s manufacturer does not yet know about and so has **not been able to fix.**
- **Targets:**
  - Several investigations and reports have revealed that Pegasus spyware has been used to spy on **journalists, human rights activists, lawyers, opposition leaders, and heads of state.**

    - Some of the countries that have been accused of using Pegasus spyware to target their critics and enemies include **Saudi Arabia, Mexico, India, Morocco, Hungary, Azerbaijan, and Rwanda.**
- **Implications:**
    - Pegasus spyware threatens **privacy and security** for individuals and groups exposing corruption, defending human rights, and advocating democracy.
    - It undermines **press freedom by exposing journalists' sources,** methods, and materials, compromising their independence.
    - The spyware poses a risk to the sovereignty and stability of nations, enabling foreign interference and **espionage in internal affairs and decision-making processes.**
- **Challenges:**
    - Pegasus spyware is difficult to detect and remove, as it can hide its presence and activity on the device, and can **self-destruct** if it senses that it is being discovered or analyzed.
    - Pegasus spyware is difficult to regulate and control due to its operation in legal grey areas.
        - NSO Group and its clients commonly deny or evade responsibility for the misuse and abuse of spyware.

Major Types of Cyber Threats

//

Cyber Threat	Description
Malware	Malicious software designed to harm or exploit systems by infecting, disrupting, or gaining unauthorized access.
Phishing	Deceptive attempts to acquire sensitive information, often through fake emails, websites, or messages impersonating trusted entities.
Ransomware	Encrypts data and demands payment (usually in cryptocurrency) for its release, posing significant threats to data integrity.
DDoS Attacks	Overwhelms a system with a flood of traffic, causing service disruption by exhausting resources or bandwidth.
Man-in-the-Middle (MitM)	Intercepts and potentially alters communication between two parties, leading to unauthorized access or information theft.
SQL Injection	Exploits vulnerabilities in SQL databases by injecting malicious code, allowing unauthorized access or data manipulation.
Zero-Day Exploits	Attacks targeting undiscovered vulnerabilities in software before developers can create a patch, posing a serious and often potent threat.
Social Engineering	Manipulating individuals into divulging sensitive information through psychological manipulation or deception.
Insider Threats	Risks originating from individuals within an organization, either intentionally or unintentionally causing harm or data breaches.
Advanced Persistent Threats (APTs)	Prolonged and targeted cyber attacks often linked to espionage, aiming to infiltrate and remain undetected in a network.
Cross-Site Scripting (XSS)	Injects malicious scripts into web pages viewed by others, potentially compromising the security and privacy of users.
Credential Stuffing	Uses stolen usernames and passwords from one breach to gain unauthorized access to other accounts due to individuals reusing passwords.
Internet of Things (IoT) Threats	Exploits vulnerabilities in connected devices, potentially allowing unauthorized access or disruption of IoT networks.
Cryptojacking	Unauthorized use of a computer's resources for cryptocurrency mining, slowing down systems and consuming energy without the user's consent.
Wi-Fi Eavesdropping	Unauthorized interception of wireless communication, where attackers may capture sensitive data transmitted over Wi-Fi networks.

What are the Related Cybersecurity Initiatives?

- **India:**
  - **Information Technology Act, 2000.**
  - **National Cyber Security Strategy.**
  - **Cyber Surakshit Bharat.**
  - **Computer Emergency Response Team - India (CERT-In).**
  - **Critical Information Infrastructure.**
  - **Indian Cyber Crime Coordination Centre (I4C).**
- **International Mechanisms:**
  - **International Telecommunication Union (ITU)**
  - **Budapest Convention on Cybercrime**

Way Forward

- Establish an **international oversight mechanism** to hold companies accountable for any unethical use of surveillance tools and facilitate independent audits.
  - Strengthen national and international legal **frameworks to explicitly address the use of spyware** and protect the privacy and human rights of individuals targeted.
- Conduct **public awareness campaigns** to educate individuals about the risks posed by spyware and how to safeguard their devices against potential infiltration.
- **Strengthen national cybersecurity infrastructure** to proactively detect and neutralize cyber threats, including the continuous monitoring of potential spyware activities.
- Encourage tech companies to adopt **ethical guidelines that align with human rights** principles, promoting responsible corporate behaviour.

UPSC Civil Services Examination, Previous Year Question (PYQ)

Prelims

Q. The terms 'WannaCry, Petya and EternalBlue' sometimes mentioned in the news recently are related to (2018)

(a) Exoplanets
(b) Cryptocurrency
(c) Cyber attacks
(d) Mini satellites

Ans: (c)

Q. In India, under cyber insurance for individuals, which of the following benefits are generally covered, in addition to payment for the loss of funds and other benefits? (2020)

1. Cost of restoration of the computer system in case of malware disrupting access to one's computer
2. Cost of a new computer if some miscreant wilfully damages it, if proved so
3. Cost of hiring a specialized consultant to minimize the loss in case of cyber extortion
4. Cost of defence in the Court of Law if any third party files a suit

Select the correct answer using the code given below:

(a) 1, 2 and 4 only
(b) 1, 3 and 4 only
(c) 2 and 3 only

(d) 1, 2, 3 and 4

Ans: (b)

Q. In India, it is legally mandatory for which of the following to report on cyber security incidents? (2017)

1. Service providers
2. Data centres
3. Body corporate

Select the correct answer using the code given below:

(a) 1 only
(b) 1 and 2 only
(c) 3 only
(d) 1, 2 and 3

Ans: (d)

Mains

Q. What are the different elements of cyber security? Keeping in view the challenges in cyber security, examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy. **(2022)**