VISHNU
I A S

Topic wise content

https://t.me/vishnuiasmentor

https://www.youtube.com/channel

Pegasus Spyware

Notes for civil services preparation

UPSC

General Studies

Pegasus Spyware

- Recently, it has been reported that **Pegasus**, the **malicious software**, has allegedly been used to secretly monitor and spy on an extensive host of public figures in India.

About Pegasus:

- It is a type of malicious software or **malware classified as a spyware.**
- It is **designed to gain access to devices, without the knowledge of users**, and gather personal information and relay it back to whoever it is that is using the software to spy.
- Pegasus has been **developed by the Israeli firm NSO Group** that was set up in 2010.
- The earliest version of Pegasus discovered, which was captured by researchers in 2016, **infected phones through what is called spear phishing** – text messages or emails that trick a target into clicking on a malicious link.
- Since then, however, NSO's attack capabilities have become more advanced. Pegasus infections can be achieved through so-called **"zero click" attacks**, which do not require any interaction from the phone's owner in order to succeed.
- These will often exploit "zero-day" vulnerabilities, which are flaws or bugs in an operating system that the mobile phone's manufacturer does not yet know about and so has not been able to fix.

Targets:

- Human Rights activists, journalists and lawyers around the world have been targeted with phone malware sold to authoritarian governments by an Israeli surveillance firm.
- Indian ministers, government officials and opposition leaders also figure in the list of people whose phones may have been compromised by the spyware.
- In 2019, **WhatsApp filed a lawsuit** in the US court against Israel's NSO Group, alleging that the firm was incorporating **cyber-attacks** on the application by infecting mobile devices with malicious software.

Recent Steps Taken in India:

- **Cyber Surakshit Bharat Initiative:** It was launched in 2018 with an aim to spread awareness about cybercrime and building capacity for safety measures for Chief Information Security Officers (CISOs) and frontline IT staff across all government departments.
- **National Cyber security Coordination Centre (NCCC):** In 2017, the NCCC was developed to scan internet traffic and communication metadata (which are little snippets of information hidden inside each communication) coming into the country to detect real-time cyber threats.
- **Cyber Swachhta Kendra:** In 2017, this platform was introduced for internet users to clean their computers and devices by wiping out viruses and malware.
- **Indian Cyber Crime Coordination Centre (I4C):** I4C was recently inaugurated by the government.
- National Cyber Crime Reporting Portal has also been launched pan India.

- **Computer Emergency Response Team - India (CERT-IN):** It is the nodal agency which deals with cybersecurity threats like hacking and phishing.

Legislation:

- **Information Technology Act, 2000**.
- **Personal Data Protection Bill, 2019.**

International Mechanisms:

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

Types of Cyber Attacks

- **Malware:** It is short for malicious software, refers to any kind of software that is designed to cause damage to a single computer, server, or computermnetwork. Ransomware, Spy ware, Worms, viruses, and Trojans are all varieties of malware.
- **Phishing:** It is the method of trying to gather personal information using deceptive e-mails and websites.\
- **Denial of Service attacks:** A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users.
- DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.
- **Man-in-the-middle (MitM) attacks:** Also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction.
- Once the attackers interrupt the traffic, they can filter and steal data.
- **SQL Injection:** SQL stands for **Structured Query Language**, a programming language used to communicate with databases.
- Many of the servers that store critical data for websites and services use SQL to manage the data in their databases.
- A SQL injection attack specifically targets such kinds of servers, using malicious code to get the server to divulge information it normally wouldn't.
- **Cross-Site Scripting (XSS):** Similar to an SQL injection attack, this attack also involves injecting malicious code into a website, but in this case the website itself is not being attacked.
- Instead the malicious code the attacker has injected, only runs in the user's browser when they visit the attacked website, and it goes after the visitor directly, not the website.

- **Social Engineering:** It is an attack that relies on human interaction to trick users into breaking security procedures in order to gain sensitive information that is typically protected.