Topic wise content

https://t.me/vishnuiasmentor

https://www.youtube.com/channel
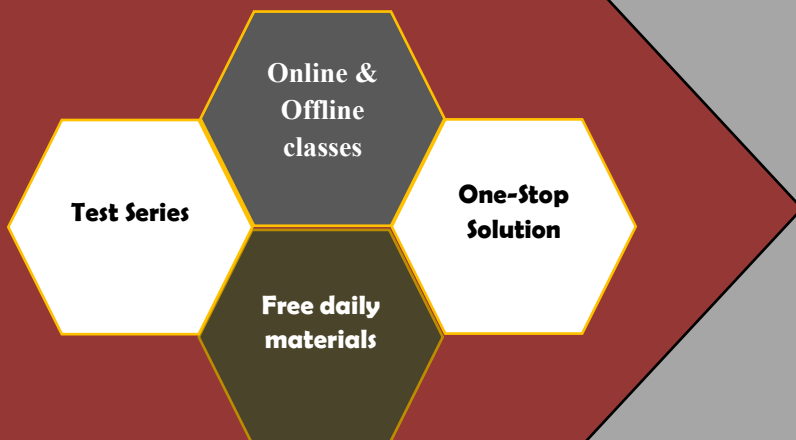
Spyware Pegasus

Notes for civil services preparation

Spyware Pegasus

- The recent digital security breach by a spyware called **Pegasus** compromisedbphones of multiple activists, journalists and lawyers in India. The spyware was ablento track multiple user applications like messages, emails, audio calls, browsernhistory, contacts including end-to-end encrypted data. The whole incident brought forward the issue of digital security and the ways to achieve it with minimum loopholes.

Key Highlights

- The phones of affected people were reportedly **compromised by using a vulnerability in WhatsApp** which allowed the **Pegasus spyware software** to be **installed,** by initiating a WhatsApp voice call with the target.
- This specific vulnerability in WhatsApp has **now been mended.**
- The **Indian government has sought an explanation from WhatsApp** after it was revealed that Indian citizens were spied upon using Pegasus.

Pegasus

- It is a spyware developed by the **Israeli cyber arms firm NSO Group Technologies.**
- It mainly uses **exploit links,** clicking on which installs Pegasus on the target's phone.
- **Citizen Lab** which has investigated several cases of Pegasus infections showed through its research that **social engineering is a very common strategy** to deliver the most sophisticated spyware.
- Pegasus does so by **exploiting vulnerabilities in the phone's operating systems (OS).**
- **Lookout,** which is a cybersecurity company, had **partnered with Citizen Lab** to **investigate Pegasus** and found that it had exploited three zero-day vulnerabilities in iOS to successfully attain all the user access of the phone.
- A **zero-day vulnerability** is a flaw in a software or hardware that is previously unknown to the party responsible.
- In WhatsApp case, a **specially crafted call** was used to trigger a buffer overflow, which in turn was **used to take control of the device.**
- Pegasus is **state-of-the-art spyware** and **NSO charges an exorbitant sum for its product and services.**

Challenges

- **Multiple ways and various technologies** like social engineering, exploiting user apps and then using the vulnerabilities make this issue hard to solve.
- The Google Play Store and the Apple App store have thousands of apps with **undiscovered vulnerabilities** that could potentially be exploited by firms such as NSO to target individual users.
- By mainly targeting WhatsApp only the **focus is shifted from other potential means** through which it can be used further and leave a far bigger impact.
- **Lack of awareness and specialists in digital security** makes this a vulnerable sector.
- **Terrorists and other anti-social elements** have started using more of cyberspace which provides them with more getaways.

Solutions

Users

- It is important to keep the **phone updated for ensuring the security** of the devices, both the applications and the firmware. It is necessary to be **self-aware about digital security** because compromise in that could lead to a situation of total surveillance.

Government

- It needs to **investigate into the matter** so that such future incidents can be prevented.
- It should make **stricter rules and restrictions for the applications** made available in the country and monitor the most commonly used applications without breaching the privacy of the individuals.
- **Laws** on digital privacy and security need to be implemented more strictly.
- **Digital literacy** should be increased to spread **awareness about cyber threats.**
- **Computing environment** and **Internet of Things** (It is a network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators and connectivity which enables these things to connect, collect and exchange data) with current tools, patches, updates need to be secured.
- **Artificial Intelligence (AI)** should be used for predicting and accurately identifying digital attacks and breaches.
- The need of the hour for the Indian government is to develop core skills in data integrity and data security fields, while also setting stringent cyber security standards to protect individuals and

institutions of national importance, to make sure that the unity of the nation and the integrity of the individuals stay safe and secure.