Ransomware Attack [UPSC Notes]

In November 2022, there was a ransomware attack on the database of the All India Institute of Medical Sciences (AIIMS) affecting its operations significantly leading to the hospital running in manual mode for weeks. This topic becomes important for the cybersecurity segment of the UPSC syllabus. In this article, you can read about ransomware attacks, how they can be prevented, etc.

What is Ransomware?

Ransomware is advanced software used by hackers to block the access of users to crucial databases.

- These cyber criminals demand money in lieu of unblocking data to the respective users.
- In the recent cyberattack on the AIIMS database, the hacker demanded ransom in cryptocurrencies.

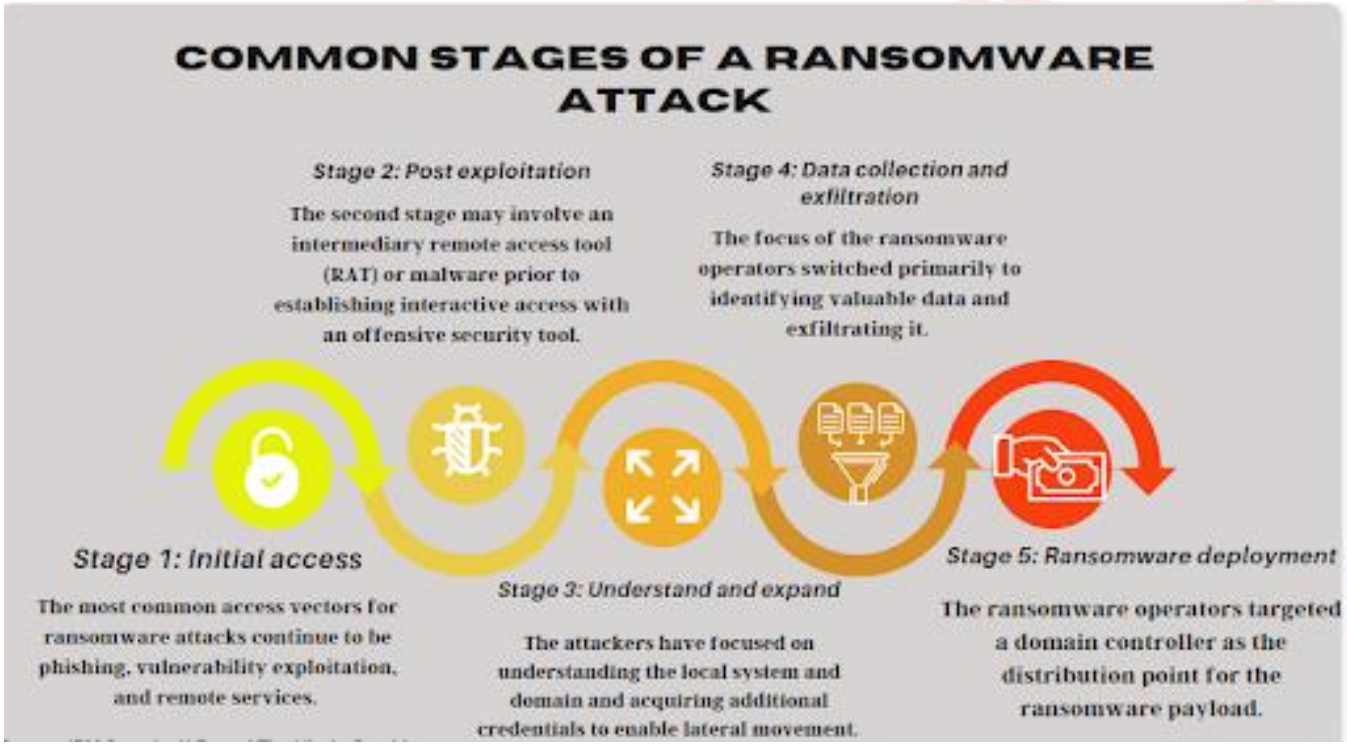

Image Source: The Hindu

Some examples of recent ransomware attacks:

- CryptoLocker
- Petya
- Bad Rabbit
- TeslaCrypt

- Locky
- Jigsaw

Ransomware Attack Implications

According to **Interpol's first-ever Global Crime Trend report,** ransomware was the second highest-ranking threat after money laundering, at 66%. It is also expected to increase the most (72%).

- About 70 per cent of organisations in India have been hit by a ransomware attack in the last three years while 81 per cent of organisations feel that they could be the target of ransomware attacks.
- The Indian Computer Emergency Response Team (CERT-IN) in its India Ransomware Report 2022 stated that there is a 51-percent increase in the number of ransomware attacks across multiple sectors including critical infrastructure.

Image source: The Hindu

Agencies to deal with the cyber threat:

- The **Indian Computer Emergency Response Team (CERT-In)** established in 2004 is the national nodal agency that collects, analyses and circulates inputs on cyber-attacks.
- The National Critical Information Infrastructure Protection Centre has been set up for the protection of national critical information infrastructure.

- The **Cyber Swachhta Kendra (Bot-Net Cleaning and Malware Analysis Centre)** has been launched for the detection of malicious software programmes and to provide free tools to remove them.
- The **National Cyber Coordination Centre** works on creating awareness about existing and potential threats.

Ransomware Attack Best Practices

Best practices recommended by the CERT-In for dealing with ransomware:

- Maintain an **offline database of the important files in encrypted form**.
- All accounts should have **strong and unique passwords**, an **account lockout policy**, and **multi-factor authentication** for all services.
- A **host-based firewall** should be installed to only allow connections to such shares via server message block from a limited set of administrator machines.