Ransomware attacks on Indian IT Firms

Why in news?

IT service provider HCL Technologies has shared that it was hit by a ransomware incident within a restricted cloud environment.

What is a ransomware?

- **Ransomware** – It is an *extortion software* designed to lock or *encrypt a device or data* on a system and then *demand a ransom* (money) for its release.
- Attackers usually leave behind a *message with instructions* on the ransom amount, mode of transfer, or instructions on how to contact them for further guidance.
- **Working**
  - *Originates* from a malicious link, email attachment, exploited vulnerability, attack campaign, or worm.
  - *Installs* in victim's machine.
  - *Spreads to other devices* on a network and connects to a command-and-control server controlled by the attacker.

- **Impact** - It can lead to *data loss, productivity losses, and reputational damage*.

Ransomware-as-a-service *business models promote new generation of smaller and smarter gangs are likely to become more prevalent*

How does it differ from malware?

What is the current status of ransomware attacks in India?

- **Indian Ransomware Report** – It is released by India's Computer Emergency Response Team (CERT-In).
  - A *51% increase in ransomware incidents* was reported in first half of 2022 as compared to 2021.
  - A majority of these attacks target data centres, IT, and TeS sectors in the country.
- **State of Ransomware 2023 Report** -It is a 2023 study by Sophos, a cybersecurity company.
  - **Increase in ransomware attack –** Attack on organisations is up from 57% the previous year to *73%*.

- **Drop in successful encryption of data –** It is *77% of reported organisation*, a drop from 78% the previous year.
- **Ransom Paid** – *44% of organisations* payed the ransom to retrieve their data.
- **Highest Impact** – It is in *education sector*, where 79% of higher education organizations surveyed and 80% of lower education organizations surveyed reported such incidents.

Ransomware Attacks
• **Recent attacks** – Akira, Wiperware attacks from Russia and LockBit Black. • **Ransomware attacks in India** – Indian organisations are increasingly targeted by ransomware attacks. • In 2023, a *US-based subsidiary of Infosys* was reportedly targeted by a ransomware attack while Indian drug manufacturer *Sun Pharma* was hit by a cyberattack. • In 2022, a ransomware attack crippled AIIMS for days.

Why do attackers target IT organisations?

- **Repository of valuable data** – They hold sensitive information like personally identifiable data of users, intellectual property, access credentials, and even financial information.
- Higher the value for data, *higher the chances that the ransom will be paid*.
- **Higher vulnerability of the target** – If the data is leaked, it could lead to a drop in their value and replication of software, *devaluing the company thus threatening its revenue streams*.
- Successful attacks could potentially open the channel to target supply chains, adding pressure on companies to pay the ransom.
- **Easy target** – They are among the 1st to adopt new technologies and use *open architecture, which may not have the highest levels of protection* against cyberattacks, making them an easy target.

'***Police'*** *and '****Public Order'*** *are* ***State subjects*** *as per the 7th Schedule of the Constitution of India. Hence States and UTs are responsible for cybercrime prevention, detection etc.*

How to protect against ransomware?

- Cyber awareness training and education
- Continuous data backups
- Patching – Apply recent security updates on system or software.
- User authentication
- Reduce the attack surface – By addressing phishing messages, unpatched vulnerabilities, remote access solutions and mobile malware.
- Deploy anti-ransomware solution.

To know more about cybercrime prevention in India, click here

References

1. The Hindu| Increased Ransomware Attacks in India
2. The Hindu| Ransomware statistics in India
3. Yubico | Image

SHANKAR IAS PARLIAMENT
Information is Empowering