Increasing Ransomware Attacks in India

Why in news?

Recently, e-services at the All-India Institute of Medical Sciences (AIIMS) were crippled and is suspected to be a ransomware attack.

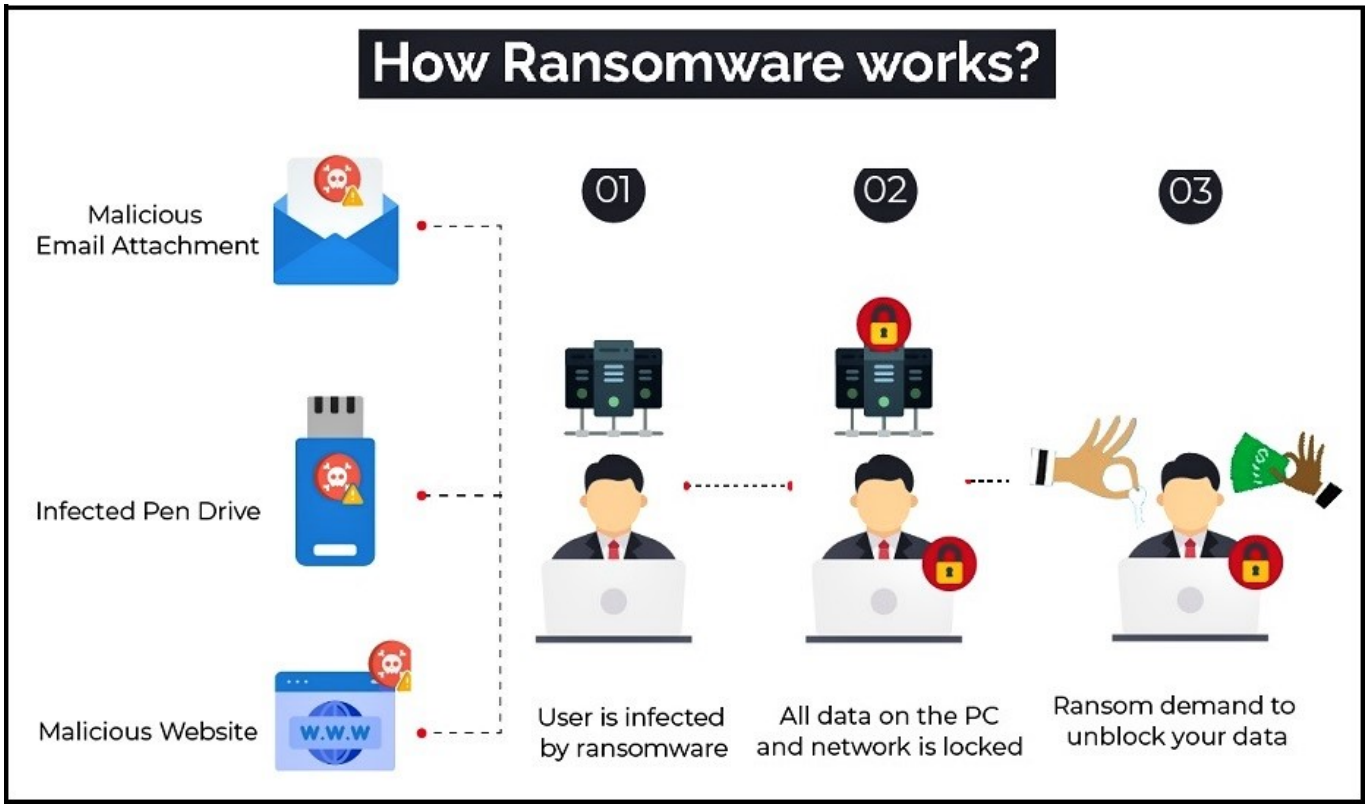
What is the issue?

- **Issue** - AIIMS has a Local Area Network comprising more than 6,500 computers.
- The centralised records were inaccessible and the e-hospital system has been completely shut down.
- A ransomware attack is suspected in this regard.
- **Impacts -** Preliminary findings have indicated that at least five of the AIIMS' servers that hosted data related to more than three crore patients were compromised.
- The institute has been able to provide consultation services to just about one-fifth that number.
- The latest incident has dented the image of the institute which is known for the quality of teaching and research work.
- The Delhi Police's Intelligence Fusion & Strategic Operations have launched investigations.
- The experts from the Indian Computer Emergency Response Team (CERT-in) and National Informatics Centre (NIC) are working on restoring online services.

According to the Interpol's first-ever Global Crime Trend report, ransomware was the second highest-ranking threat after money laundering, at 66%.

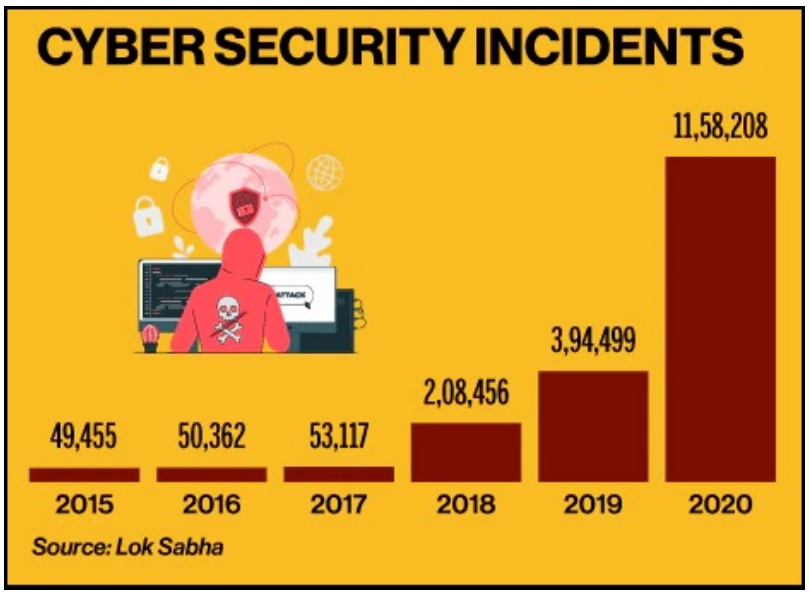
What is Ransomware?

- Ransomware is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access.
- The malware may usually be injected remotely by tricking the user into downloading it upon clicking an ostensibly safe web link sent via email or other means, including hacking.
- It can spread throughout the network by exploiting existing vulnerabilities.
- Ransomware attacks can be accompanied by theft of sensitive data.
- Recently, Spice jet and Oil India had faced a cyber-threat.



How are cyber-attacks dealt in India?

- **Indian Computer Emergency Team (CERT-In)** - CERT-In is the national nodal agency for responding to computer security incidents as and when they occur.
- CERT-In is operational since January 2004.
- The constituency of CERT-In is the Indian Cyber Community.
- CERT-In has been designated to perform the following functions
    - Collection, analysis and dissemination of information on cyber incidents.
    - Forecast and alerts of cyber security incidents.
    - Emergency measures for handling cyber security incidents
    - Coordination of cyber incident response activities.
    - Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.
    - Imparting training to computer system managers.
- **National Cyber Security Coordinator** - The National Cyber Security Coordinator, under the National Security Council Secretariat, coordinates with different agencies at the national level on cybersecurity issues.
- **The National Critical Information Infrastructure Protection Centre** - It has been set up for the protection of national critical information infrastructure.
- **The Cyber Swachhta Kendra** - It is a Botnet Cleaning and Malware Analysis Centre that has been launched for detection of malicious software programmes and to provide free tools to remove them.
- **The National Cyber Coordination Centre** - It works on creating awareness about existing and potential threats.
- **Cyber Crisis Management Plan** - The government has formulated a Cyber Crisis Management Plan for countering cyber-attacks.



What are the best practices recommended by CERT-In?

> *The information tracked by the CERT-In showed that cyber-attacks saw a four-fold jump in 2018 and recorded an 89% growth in 2019.*

- Maintain regularly offline data backups with encryption.
- All accounts should have strong and unique passwords and lockout policy
- Multi-factor authentication for all services
- Disable remote desktop connections
- Have a proper Remote Desktop Protocol logging and configuration, and spam-proof email validation system
- Anti-virus software should be updated
- Users must not open attachments or URL links in uninvited e-mails

References

1. The Hindu | Are ransomware attacks increasing in India?
2. Business Today | Cyber security attacks in India grew in 2020
3. MEITY | CERT-In