1. LockBit Ransomware

Prelims Syllabus: Information Technology

Mains Syllabus: GS-III Awareness in the fields of IT, Space, Computers, robotics, Nano technology, bio-technology and issues relating to intellectual property rights.

Why in News?

- Recently, it has been found that LockBit ransomware was found to be targeting Mac devices.

About the News:

- Earlier in January 2023, the LockBit gang was reportedly behind a cyber-attack on U.K. postal services, causing international shipping to grind to a halt.
- A ransomware is a type of malware that hijacks computer data and then demands payment (usually in bitcoins) in order to restore it.

What is LockBit Ransomware?

- LockBit, formerly known as “ABCD” ransomware, is a type of computer virus that enters someone's computer and encrypts important files so they can't be accessed.
- The virus first appeared in September 2019 and is called a "crypto virus", because it asks for payment in cryptocurrency to unlock the files.
- LockBit is usually used to attack companies or organizations that can afford to pay a lot of money to get their files back.

- The people behind LockBit have a website on the dark web where they recruit members and release information about victims who refuse to pay.
- LockBit has been used to target companies in many different countries, including the U.S., China, India, Ukraine, and Europe.

Modus Operandi:

- It hides its harmful files by making them look like harmless image files. The people behind LockBit trick people into giving them access to the company's network by pretending to be someone trustworthy.
- Once they're in, LockBit disables anything that could help the company recover their files and puts a lock on all the files so that they can't be opened without a special key that only the LockBit gang has.
- Victims are then left with no choice but to contact the LockBit gang and pay up for the data, which the gang may sell on the dark web - whether the ransom is paid or not.

LockBit Gang:

- The LockBit gang is a group of cybercriminals who use a ransomware-as-a-service model to make money.
- They create custom attacks for people who pay them and then split the ransom payment with their team and affiliates.
- They are known for being very prolific and avoiding attacking Russian systems or countries in the Commonwealth of Independent States to avoid getting caught.

Why is LockBit targeting macOS?

- LockBit is targeting macOS as a way to expand the scope of their attacks and potentially increase their financial gains.
- While historically ransomware has mainly targeted Windows, Linux, and VMware ESXi servers, the gang is now testing encryptors for macOS.
- The current encryptors were not found to be fully operational, but it is believed that the group is actively developing tools to target macOS.
- The ultimate goal is likely to make more money from their ransomware operation by targeting a wider range of systems.

How to Protect against LockBit Ransomware?

Strong Passwords:

- Account breaches often happen because of weak passwords that are easy for hackers to guess or for algorithm tools to crack. To protect oneself, choose strong passwords that are longer and have different types of characters.

Multi-Factor Authentication:

- To prevent brute force attacks, use additional security measures like biometrics (such as fingerprint or facial recognition) or physical USB key authenticators along with your passwords when accessing your systems.
- Brute force attacks are a type of cyber-attack where attackers try to guess a password by repeatedly trying different combinations of characters until they find the right one.

Reassess Account Permissions:

- Limiting user permissions to stricter levels is important to reduce security risks. This is especially critical for IT accounts with administrative access and for resources accessed by endpoint users.
- Ensure that web domains, collaborative platforms, web meeting services, and enterprise databases are all secured.

System-wide Backups:

- To protect against permanent data loss, it's important to create offline backups of your important data.
- Make sure to periodically create backups to ensure that you have an up-to-date copy of your systems. Consider having multiple backup points and rotating them, so you can select a clean backup in case one becomes infected with malware.

Recent Steps Taken in India against Cyber Crime:

- **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.
- **Legislations in India:**
  - ✓ 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 and refers to any kind of software that is designed to cause damage to a single computer, server, or computer network. 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.