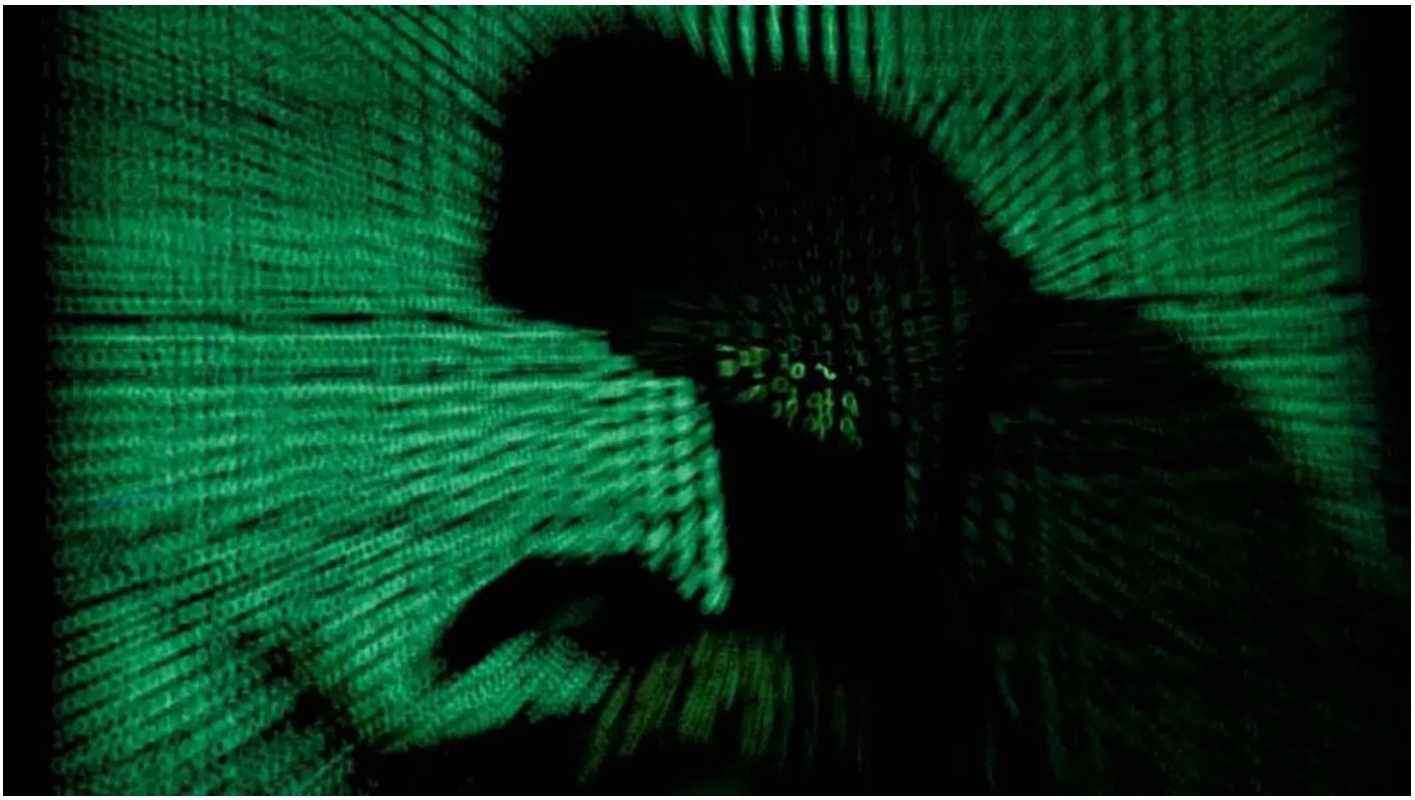
LockBit Ransomware

May 8, 2024 • vajiramandravi.com



About LockBit Ransomware:

- It is **malicious software** designed to block user access to computer systems in exchange for a ransom payment.
- It was formerly **known as "ABCD" ransomware**, but it has since grown into a unique threat within the scope of extortion tools.
- It is a **subclass** of ransomware known as a **'crypto virus'** due to forming its ransom requests around financial payment in exchange for decryption.
- It focuses mostly on enterprises and government organizations rather than individuals.
- It functions as **ransomware-as-a-service** (RaaS). It is now working to create encryptors targeting Macs for the first time.
- **Working**
    - It works as a **self-spreading malware**, not requiring additional instructions once it has successfully infiltrated a single device with access to an organisational intranet.
    - It is also known to **hide executable encryption files** by disguising them in the . PNG format, thereby avoiding detection by system defences.

- Attackers use **phishing tactics** and other **social engineering methods** to impersonate trusted personnel or authorities to lure victims into sharing credentials.
- Once it has gained access, the ransomware prepares the system to release its encryption payload across as many devices as possible.
- It then disables security programs and other infrastructures that could permit system data recovery.

Q1: What is Encryption?

Encryption is a way of scrambling data so that only authorized parties can understand the information. In technical terms, it is the process of converting human-readable plaintext to incomprehensible text, also known as ciphertext.

Source: U.S. announces $10 million bounty for alleged LockBit ransomware creator

---