C. List few latest viruses on internet and explain.

Types of viruses :

Malware – malware is a broad term that includes more than computer viruses. Worms, Trojans, adware, and even ransomware may all be considered malware. This is any computer code intentionally created to do damage to computer systems, gain unauthorized access to computers, or steal information.

Ransomware – ransomware disables access to computer files by encrypting data. Demands for payment or other requests must be met before the offending software will be unlocked to reinstate access to servers or business files. Even large enterprises and city governments have fallen victim to ransomware attacks in recent months.

Trojans – Trojans typically require the recipient to take some form of action, such as running a program or accessing a malicious website through a link passed by email. A common use of a Trojan attack is first to notify a computer user a virus has infected them. Prompted to click a link or run the attached program to solve the problem, the unsuspecting user falls victim to the Trojan attack.

Latest computer viruses :

1. **Cyborg Ransomware**

Much like the viruses that used to distribute themselves via infected floppy disks (remember those?), Cyborg Ransomware sneaks into computers and encrypts files. Cyborg's most recent evolution is to penetrate WIN 10 systems disguised as Windows updates. To protect your systems from Cyborg – also knows as Aids Info Disk Trojan (AIDS), avoid opening any questionable or unknown file with a "jpg" extension.

Once Cyborg takes over, users are presented with a notification that files are encrypted, and they will not be restored unless a ransom is paid. Ransom amount and instructions are provid ed, typically an amount in the range of $300 USD. Unfortunately, decryption is often not provided – even if the ransom is paid. Once infected, the virus can be removed, but that does not restore access to the files. Typically, the only recovery is removing the virus, then restoring files from recent backups.

2. **GoBrut**

GoBrut is a virus that is one of the most recent computer viruses to be unleashed by hackers. It is not terribly sophisticated in its technology but can wreak havoc just the same. Based on Golang, it uses brute force methodology to decipher passwords and gain access to Windows and Linux systems.

GoBrut can slow down internet access to infected machines. The real threat of this virus is the potential of discovering and leaking confidential information such as passwords, usernames, and more.

3. **Jokeroo**

Jokeroo is a serious piece of malware in the form of ransomware that is offered on underground hacking sites for proliferation by other cyberthieves. It can be distributed through social media sites, including Twitter and others.

Hackers joining in on this Ransomware as a Service (RaaS) scheme receive a portion of the ransom generated from their victims.

4. **CryptoMix Clop Ransomware**

CryptoMix Clop has a different approach. Instead of targeting individual computers, it focuses on attacking complete networks. This creates considerable headaches for IT administrators, as CryptoMix Clop spreads throughout Windows machines, shutting down critical services and processes such as Microsoft Security Essentials and Windows Defender. This results in a system that is defenseless against the virus.

Ransomware then takes over, encrypting files and presenting the ransom note. This is another virus that currently has no free decryption solution available.

5. **Trojan Glupteba**

One of the best-known viruses, the Trojan Glupteba virus rides into computers through other exploitive code or with other malware. It keeps a low profile, with many infected users not even being aware of the attack.

Using the system's IP and port information, it communicates with other websites to gather sensitive information. You may also unknowingly be directed to harmful websites.