Computer virus : A computer virus is a malicious program that self-replicates by copying itself to another program. The purpose of creating a computer virus is to infect vulnerable systems, gain admin control and steal user sensitive data.

Here the list of 40 computer virus :

1. **Trojan horse :** In computing, a Trojan horse, or Trojan, is any malicious computer program which misleads users of its true intent. Trojans may allow an attacker to access users' personal information such as banking information, passwords, or personal identity. It can infect other devices connected to the network. Ransomware attacks are often carried out using a Trojan.
2. **Remote Access Trojan :** It is a type of malware that controls a system through a remote network connection. While desktop sharing and remote administration have many legal uses, "RAT" connotes criminal or malicious activity. A RAT is typically installed without the victim's knowledge, often as payload of a Trojan horse, and will try to hide its operation from the victim and from security software and other anti-virus software.
3. **Xafecopy Trojan :** It is a malware software targeting the Android operating system, Malicious code is downloaded onto the device without the knowledge or consent of the user.[5] The app clicks on web pages that use the Wireless Application Protocol (WAP) billing method, and Xafecopy subscribes the phone to a number of services which charge money directly to the user's mobile phone bill..
4. **WannaCry ransomware :** It was a May 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.
5. **Yankee Doodle :** It is said when Yankee Doodle was executed, the virus itself becomes the memory resident. Yankee Doodle infects all .com and .exe files.
6. **Nimda:** It used Emails, server vulnerabilities, shared folders and file transfer to spread itself. The primary purpose of the virus was to slow down the internet traffic considerable causing a DoS attack.
7. **Morris Worm :** The virus which affected approximately 10% of all the computers that were being connected to the internet. The virus had the capability to slow down the computer up to the least point at which it becomes unusable.
8. **Conficker :** It is a type of computer virus that usually targets Microsoft Windows Operating system. This virus uses flaws of Windows operating system to fetch the administrator password via dictionary attacks while forming a botnet.
9. **Storm Worm :** The virus easily tricks the victims to click on the fake links that were already infected by the virus turning any Windows computer into a botnet.
10. **Skynet :** It is a very kind virus which makes the victims PC slow very kindly as well as it turns the computer screen red. This virus infects all .exe files on the computer.
11. **Zeus:** This is a type of Trojan horse malware that spreads mainly through drive-by downloads and phishing schemes. Due to its special stealth technologies, this malware has become the largest botnet on the Internet.

12. **Mydoom :** The virus spread through email which contains the text message “andy; I’m just doing my job, nothing personal, sorry.” When the victim opens the mail the malicious code automatically downloaded and then steal the victim’s whole contacts of email. From where it spread to the victim’s friend, relatives, and colleagues.
13. **SQL Slammer :** It dramatically slowed down general Internet traffic SQL Slammer mainly targeted on the servers by generating random IP addresses and discharging the worm to those IP addresses.
14. **CodeRed :** It affects Microsoft Index Server 2.0 and the Windows 2000 Indexing service on computers running Microsoft Windows NT 4.0 and Windows 2000, which run IIS 4.0 and 5.0 Web servers. The worm uses a known buffer overflow vulnerability contained in the Idq.dll file.
15. **Melissa :** This is a virus based on a Microsoft Word macro If victims download this virus via email, this can spread itself to first 50 individuals in an email list.
16. **Sasser :** This virus attacks the security controller Local Security Authority Subsystem Service as it had a buffer overflow vulnerability. This targets mostly Windows OS and can prove very dangerous to critical infrastructure.
17. **Stuxnet :** It was found to have shut down one-fifth of the centrifuges in Iranian nuclear power plants. This virus was first identified in the year 2010 and targets mostly industrial computer system.
18. **Cryptolocker :** It’s a ransomware Trojan that spreads via email attachments. It almost has been compromised nearly 500,000 computers and encrypted its files until the ransom amount has been paid.
19. **Klez :** This virus infects victim’s computer through an e-mail message, replicated itself and then sent itself to people in the email address book. this virus is capable to disable the antivirus system that’s installed on victim’s computer.
20. **Netsky :** This virus spread itself through e-mails and Windows networks. The Netsky virus spoofs e-mail addresses and propagates through a 22,016-byte file attachment. After spreading itself, it can cause DoS (Denial of Service) attack. After doing the attack system collapse while trying to handle the amount of internet traffic.
21. **Leap-A :** The virus targeted Mac systems and it used the iChat instant messaging app to propagate across vulnerable Mac Computers. After infecting the Mac computer, the virus spread itself to all iChat contacts and sends a message to each and every person.
22. **Slammer :** The virus is powerful enough to bring down an entire system.
23. **Pikachu :** The virus was designed as an actual email that included the Pokemon character, Pikachu. The email carried an image of the Pokemon, but with that imaged unsuspecting children released a Visual Basic 6 program called pikachupokemon.exe that removed the contents of directories.
24. **ILoveu** : It did was use social engineering to get people to click on the attachment**;** in this case**,** a love confession. The attachment was actually a script that poses as a TXT file, due to Windows at the time hiding the actual extension of the file. Once clicked, it will send itself to everyone in the user’s mailing list and proceed to overwrite files with itself, making the computer unbootable.

25. **Flashback :** It propagates itself by using compromised websites containing JavaScript code that will download the payload. Once installed, the Mac becomes part of a botnet of other infected Macs.

26. **Locky :** It is ransomware malware released in 2016. It is delivered by email (that is allegedly an invoice requiring payment) with an attached Microsoft Word document that contains malicious macros.

27. **Tiny Banker Trojan,:** It is also called Tinba, is a malware program that targets financial institution websites. It is a modified form of an older form of viruses known as Banker Trojans, yet it is much smaller in size and more powerful. It works by establishing man-in-the-browser attacks and network sniffing.

28. **Bashlite :** It is malware which infects Linux systems in order to launch distributed denial-of-service attacks.

29. **Regin :** It is a sophisticated malware and hacking toolkit

30. **Gameover Zeus :** It is a peer-to-peer botnet based on components from the earlier ZeuS trojan. It is believed to have been spread through use of the Cutwail botnet

31. **Flame:** That attacks computers running the Microsoft Windows operating system Flame can spread to other systems over a local network (LAN) or via USB stick.

32. **Shamoon :** It can spread from an infected machine to other computers on the network. Once a system is infected, the virus continues to compile a list of files from specific locations on the system, upload them to the attacker, and erase them. Finally the virus overwrites the master boot record of the infected computer, making it unusable.

33. **SpyEye :** It is a malware program that attacks users running Google Chrome, Firefox, Internet Explorer and Opera web browsers on the Microsoft Windows operating system.

34. **ZeroAccess :** It is a Trojan horse computer malware that affects Microsoft Windows operating systems. It is used to download other malware on an infected machine from a botnet while remaining hidden using rootkit techniques.

35. **Waleda :** It is also known by its aliases Waled and Waledpak, was a botnet mostly involved in e-mail spamand malware.

36. **Alureon :** It is a trojan and bootkit created to steal data by intercepting a system's network traffic and searching for: banking usernames and passwords, credit card data, Paypal information, social security numbers, and other sensitive user data.

37. **Daprosy worm :** It was a malicious computer program that spreads via local area network (LAN) connections, spammed e-mails and USB mass storage devices. Infection comes from a single read1st.exe file where several dozen clones are created at once bearing the names of compromised folders.

38. **Kenzero :** It is a virus that is spread across peer-to-peer networks and is programmed to monitor the browsing history of victims.

39. **Mocmex :** It is a trojan, which was found in a digital photo frame in February 2008. It was the first serious computer virus on a digital photo frame. Mocmex downloads files from remote locations and hides randomly named files on infected computers.

40. **Memz trojan:** It is a computer virus and trojan horsemade for Microsoft Windows. Memz was originally created by Leurak for YouTuberdanooct1's Viewer-Made Malware series. The virus gained notoriety for its unique and complex payloads, which automatically activate after each other, some with delay.