COMPUTER VIRUSES

Computer Program which can damages computer system and/or destroys or erases data files.

What is computer Virus?

- a computer virus is a type of malicious code or program written to alter the way a computer operates.

- a virus has the potential to cause unexpected or damaging effects, such as harming the system software by corrupting or destroying data.

How does a computer virus attack?

- Once a virus has successfully attached to a program, file, or document, the virus will lie until circumstances cause the computer or device to execute its code.
- In order for a virus to infect your computer, you have to run the infected program, which in turn causes the virus code to be executed.

What a computer virus can do?

- A virus tries to take control of computer system at the first opportunity available.
- It makes copies of itself and try to carry harmful task.
- This process happen so quickly that the user is not aware of the presence of the virus in computer.

Why do people create computer Viruses?

- To take control of a computer for specific task.
- To steal sensitive information such as password, personal details.
- To prove his/her skills
- To disable computer/network

How do viruses spread?

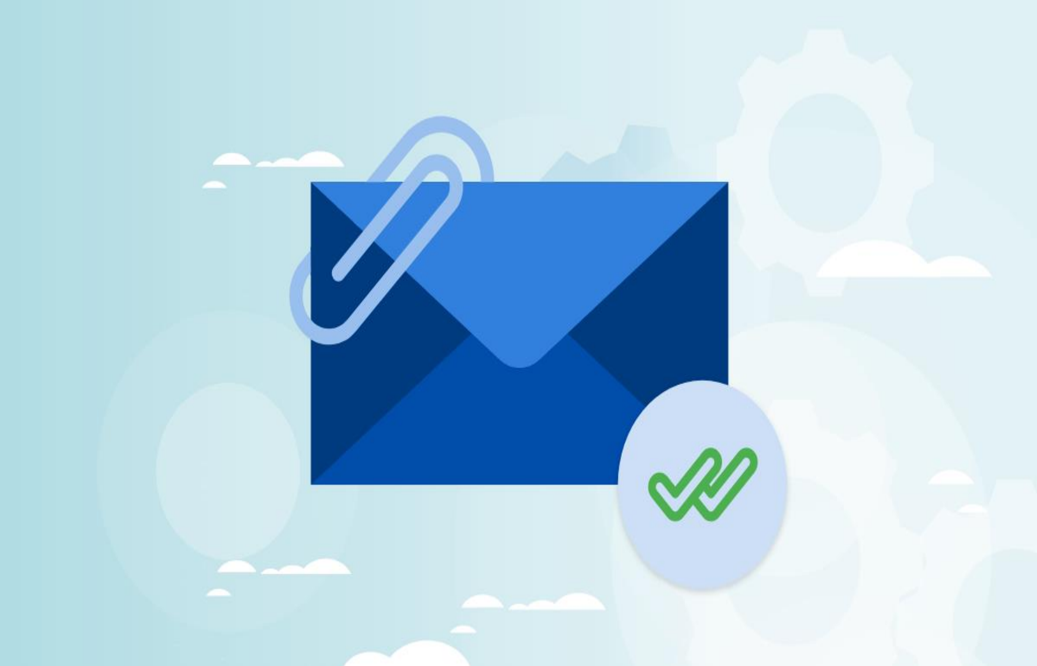
From Removable Media

How do viruses spread?

From Downloads of internet

How do viruses spread?

Attachment of E-mail



Types of computer Viruses

- File Virus
- Boot Sector Virus
- Macro Virus
- Source code Virus

- Armored Virus
- Tunneling Virus
- Stealth Virus
- Encrypted Virus

File Virus

- This type of virus infects the system by appending itself to the end of a file. It changes the start of a program so that the control jumps to its code. After the execution of its code, the control returns back to the main program. Its execution is not even noticed. It is also called **Parasitic virus** because it leaves no file intact but also leaves the host functional.

Boot Sector Virus

- It infects the boot sector of the system, executing every time system is booted and before operating system is loaded. It infects other bootable media like floppy disks. These are also known as **memory virus** as they do not infect file system.

Macro Virus

- Unlike most virus which are written in low-level language(like C or assembly language), these are written in high-level language like Visual Basic. These viruses are triggered when a program capable of executing a macro is run. For example, macro virus can be contained in spreadsheet files.

Source Code Virus

- It looks for source code and modifies it to include virus and to help spread it.

Armored Virus

- An armored virus is coded to make it difficult for antivirus to unravel and understand. It uses a variety of techniques to do so like fooling antivirus to believe that it lies somewhere else than its real location or using compression to complicate its code.

Tunneling Virus

- This virus attempts to bypass detection by antivirus scanner by installing itself in the interrupt handler chain. Interception programs, which remain in the background of an operating system and catch viruses, become disabled during the course of a tunneling virus. Similar viruses install themselves in device drivers.

Stealth Virus

- It is a very tricky virus as it changes the code that can be used to detect it. Hence, the detection of virus becomes very difficult. For example, it can change the read system call such that whenever user asks to read a code modified by virus, the original form of code is shown rather than infected code.

Encrypted Virus

- In order to avoid detection by antivirus, this type of virus exists in encrypted form. It carries a decryption algorithm along with it. So the virus first decrypts and then executes.

Virus Vs Worm

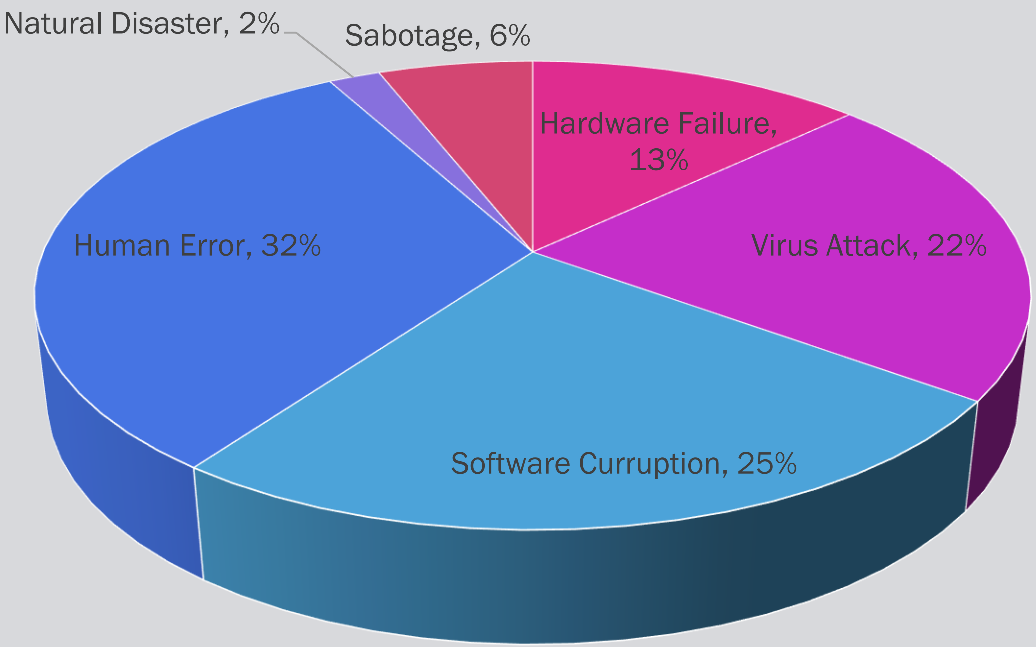
Virus

- Spreads from Program to program or from disk to disk.
- Destroys data and/or erases disk.
- Can’t remove easily.
- Files such as .exe, .sys or .com can be corrupted

Worm

- Uses computer hosts to reproduce themselves.
- Resides in memory rather than disk.
- Can be removed easily.
- Does not modify any stored Programs.

Cause of data Loss due to Computer virus



References

- https://www.geeksforgeeks.org/types-of-virus/