Computer Virus

Computer virus is a type of malicious software program (“malware”) that, when executed, replicates by reproducing itself (copying its own source code) or infecting other computer programs, data files or the boot sector of the hard drive by modifying them. When this replication succeeds, the affected areas are then said to be infected with a computer virus.

The term virus is also commonly, but inaccurately, used to refer to other types of malware. Malware encompasses computer viruses along with many other forms of malicious software, such as computer “worms”, Trojan horses, keyloggers, rootkits, spyware, adware etc. The majority of active malware threats are actually trojan horse programs or computer worms rather than computer viruses.

Types of Computer Virus

There are various types of computer viruses, classified in terms of techniques, origin, the types of files affected, damage, OS or platform attacked, as well as the places they hide. Its relatively hard to answer how many different types of computer viruses there are but below covers the main core concepts of the common types:

Resident viruses: These are permanent viruses dwelling in RAM memory. In this case, they would be in a position to overcome, as well as interrupt, all operations that the system executes. Their effects include corrupting programs and files that are closed, opened, renamed or copied.

Overwrite viruses: These viruses delete information that is in the infected files. In this case, the infected files would be rendered totally or partially useless. Unfortunately, you would only clean the infected file by deleting it completely, therefore losing original content.

Direct action viruses: This virus replicates itself, then acts when executed. Subject to satisfaction of particular conditions, the virus infects files located in the folders or computer directory. It is also in directories specified in the autoexec.bat path. In most cases, it is located in hard drive's root directory and takes particular action when the computer boots.

File infectors: This virus infects executable files or programs. On running the programs, the virus would be activated, then be able to carry out its damaging effects. Most of the existing viruses are in this category.

Boot (sector) viruses: This virus infects the hard disk's or floppy drive's boot sector. This would make the computer unable to boot. These viruses can, however, be avoided by ensuring that the floppy disks or hard drive is well protected. Never start the computer using unknown disk drive or floppy disk.

Directory viruses: This virus alters paths indicating a file's location. In this case, when the infected program is executed, you will be running the program unknowingly, since the virus has moved the original program and file to another location. This therefore makes it impossible to locate the moved files

Macro virus: This virus affects files created using particular programs or applications containing macros. The mini-programs increase their ability to automate some operations, in which case they would be performed as single actions.

Sources of Computer Viruses

- **Freeware** - short for "free software" downloaded without any fee. Some freeware are malware with hidden agenda on your computer.
- **Flashed drive**: It is usual to get virus from a flash drive or any other storage device that was used on an infected PC.
- **Email attachment**: if you receive an email from someone you don't know asking to click on a link or open a file attachment, there may be a potential hazard on your PC. If the email claims to be from DHL

then the email address should have like “@DHL.com” email address and not “@yahoo.com” or “@gmail.com”

- **Cracked software**: Most people download cracked and illegal versions of software online are unaware of the reality that they may contain virus sources as well.
- **Booting from CD**: if an Infected CD is used to boot an uninfected PC, there is possibility that the system can be infected
- **Malicious websites:** Some websites can install an adware (with other software) that you keep seeing unnecessary ads right from the moment you turn the internet on. The solution is a combination of an **ad-blocker** along with an antivirus.
- Through Bluetooth file transfer

Virus warning sign

The following are some of the virus warning signs:

- Application don’t work properly
- Disk can’t be accessed
- File size changes for no apparent reason
- Un-commanded disk drive activity
- Unusual error messages
- System slows down, freezes or crashes
- Appearance of strange character
- A sudden decrease in available memory
- Loss of document

Virus detection and prevention control

- Do not open any files attached to an email from an unknown, suspicious or untrusted source
- Install and regularly update antivirus
- Use a complex password
- Protect your computer from Internet intruders – use firewalls
- Do not download any software from unknown sources
- Backup your files on a regular basis

List of antivirus

- BitDefender
- Kaspersky antivirus
- ESET NOD32 antivirus
- Norton antivirus
- Avira antivirus
- AVG
- Zone alarm
- McAfee