**Computer Viruses**

A computer virus is **a malware program** that is written to have **access** to a computer without its owner’s permission. These kinds of programs are primarily **written to steal or destroy computer data**.

There are different types of computer viruses that can **be categorized according to their origin**, storage location, files they infect and destructive nature.

1. **Boot Sector Virus.** Boot Sector virus infects the storage device’s master boot record (MBR). These viruses inject their code to hard disk’s partition table. It then gets into the main memory once the computer restarts. Booting problems, unstable system performance and inability to locate hard disk are common issues that can appear after getting infected. The virus can affect any file after getting into the main memory. Examples: Form, Disk Killer, Stone virus, Polyboot.B. Protection: Make sure that the disk you are using is write-protected. Do not start/restart the computer with unknown external disks connected.

2. **Direct Action Virus**. This virus quickly gets into **the main memory**, infects **all programs/files/folder** and then **deletes itself**. In most cases, **they don’t delete system files** but change the system’s **overall performance**.: Use antivirus scanner. Direct action virus is **easy to detect** and all infected files can be **restored completely**.

4**. Web Scripting Virus**. A web scripting virus **destroys web browser security** and allows attackers to inject client-side scripting into the web page. It is used **to attack large sites** like social networking, user review or email. It can send **a large amount of spam and damage files on sever**. Protection: **use cookie security or install real-time protection software for the web browser**.

5. **Directory Virus.** Directory Virus infects the file by **changing the DOS** **directory information** When you **run a program**, DOS **first loads and executes the virus code before** running the actual program code. It becomes very difficult to locate the original file after getting infected. Example: Dir-2. Protection: Install the antivirus to relocate the misplaced files.

5. **Polymorphic Virus**. The polymorphic virus **encodes themselves** using different encryption keys and algorithms each time they **infect a program or create a copy of itself**. Because of different encryption keys, it becomes very difficult for the antivirus software to find them. **It can affect any file**. Protection: Install advanced, high-end antivirus software.

7**. Memory Resident Virus**. These viruses live **in primary memory (RAM)** and get activated whenever **you switch on the compute**r. They affect all files currently running on the desktop. It can affect any file running on PC and files that are being copied or renamed.

8. **Macro Virus**. This virus is written **in the macro language**, so it may run automatically when the **document is opened** and **it can easily spread to other files too**. It depends on the application rather than the operating system. It can affect: .mdb, .PPS, .Doc, .XLs files. Protection: Disable macros and **don’t open emails from unknown sources**. Alternatively, you can install modern antivirus software that can **detect macro virus easily**.

12. **Trojan Horse**. Trojan Horse (or Trojan) is a type of malware that looks legitimate. Users are typically **tricked into loading and executing it on the system**. It can destroy/modify all the files, crash the computer, modify the registry, and is strong enough to give hackers **remote access to your PC**.

13.**Computer worms**. Worm is a program that **replicates itself in order to spread to other co**mputers. It **relies on networks (mostly emails) a**nd security holes to travel from one system to another.

10. **Multipartite virus**. They usually **stay in memory and infect the hard disk**. Once it gets into the system, it infects all drives by changing all applications’ content. You will soon start noticing performance lag and low virtual memory available for user applications.