Experiment No:10

**Aim:**  To study about various types of viruses.

**Theory:**

1. **Boot Sector Virus**

From a user perspective, boot sector viruses are some of the most dangerous. Because they infect the master boot record, they are notoriously difficult to remove, often requiring a full system format. This is especially true if the virus has encrypted the boot sector or excessively damaged the code.They typically spread via removable media. They reached a peak in the 1990s when floppy disks were the norm, but you can still find them on USB drives and in email attachments. Luckily, improvements in BIOS architecture have reduced their prevalence in the last few years.

1. **Direct Action Virus**

A direct action virus is one of the two main types of file infector viruses (the other being a resident virus). The virus is considered “non-resident”; it doesn’t install itself or remain hidden in your computer’s memory. It works by attaching itself to a particular type of file (typically EXE or COM files). When someone executes the file, it springs into life, looking for other similar files in the directory for it to spread to. On a positive note, the virus does not typically delete files nor hinder your system’s performance. Aside from some files becoming inaccessible, it has a minimal impact on a user and can be easily removed with an antivirus program.

1. **Resident Virus**

Resident viruses are the other primary type of file infectors. Unlike direct action viruses, they install themselves on a computer. It allows them to work even when the original source of the infection has been eradicated. As such, experts consider them to be more dangerous than their direct action cousin. Depending on the programming of the virus, they can be tricky to spot and even trickier to remove. You can split resident viruses into two areas; fast infectors and slow infectors. Fast injectors cause as much damage as quickly as possible and are thus easier to spot; slow infectors are harder to recognize because their symptoms develop slowly.

1. **Multipartite Virus**

While some viruses are happy to spread via one method or deliver a single payload, Multipartite viruses want it all. A virus of this type may spread in multiple ways, and it may take different actions on an infected computer depending on variables, such as the operating system installed or the existence of certain files. They can simultaneously infect both the boot sector and executable files, allowing them to act quickly and spread rapidly. The two-pronged attack makes them tough to remove. Even if you clean a machine’s program files, if the virus remains in the boot sector, it will immediately reproduce once you turn on the computer again.

1. **Polymorphic Virus**

According to Symantec, polymorphic viruses are one of the most difficult to detect for an antivirus program. It claims antivirus firms need to “spend days or months creating the detection routines needed to catch a single polymorphic”. Since antivirus software can only blacklist one variant of a virus – but a polymorphic virus changes its signature (binary pattern) every time it replicates. To an antivirus program, it looks like an entirely different piece of software, and can, therefore, elude the blacklist.

1. **Spacefiller Virus**

Also known as “Cavity Viruses”, spacefiller viruses are more intelligent than most of their counterparts. A typical modus operandi for a virus is to simply attach itself to a file, but space fillers try to get into the empty space which can sometimes be found within the file itself. This method allows it to infect a program without damaging the code or increasing its size, thus enabling it to bypass the need for the stealthy anti-detection techniques other viruses rely on. Luckily, this type of virus is relatively rare, though the growth of Windows Portable Executable files is giving them a new lease of life.

**Conclusion:** Hence various types of viruses were studied.