Assignment :- 03

Que1:- What are fast and slow infectors?

Ans:- A fast infector infects any file accessed, not just run. A slow infector only infects files as they are being created or modified The term fast or slow when dealing with viruses pertains to how often and ~~a~~ under what circumstances they spread the infection. Typically, a virus will load itself into memory when an infected program is run.

Que2:- Explain the following terms:

a) Dropper

A dropper is a program that has been designed or modified to "install" a virus onto the target system. The virus code is usually contained in a dropper in such a way that it won't be detected by virus scanners that normally detect that virus while quite uncommon, a few doppers have been discovered. A dropper is effectively a trojan horse whose payload is installing a virus infection. A dropper which installs a virus only in memory is sometimes called an "injector".

b) Companion Virus

A companion virus is one that, instead of modifying an existing file, creates a new program which is executed instead of the intended program. On exit, the new program executes the original program so that things appear normal. On PCs this has usually been accomplished by creating an infected. COM file with the same as an existing EXE file. Integrity checking antivirus software that only looks modifications in existing files will fail to detect such viruses

c) Activity monitoring programs:

Activity monitors are special software which are used as virus prevention tools. These programs try to prevent infection before it happens by looking for virus-like activity, such as attempts to write to another executable, reformat the disk, etc.

An alternative term for these softwares is BEHAVIOR ~~BLOCK~~ BLOCKER

Ex: SECURE and FluShot + (PC), and Gate Keeper (Macintosh)

d) Virus Simulators

There are three different kinds of programs that are often called "virus simulators".

None of the three generate actual viruses.

The first kind demonstrate the audio and video-effects of some real computer viruses. The second kind are programs that simulate a virtual environment - a virtual computer, with virtual disks, virtual files and virtual viruses on them.

The third kind are programs that generate file containing scan strings used by some scanners to detect real viruses.