Chapter 3 – Computer Security

What are computer viruses, worms and Trojan horses?

Apart from the various types of attacks to the security aspects discussed earlier, there still exist few more destructive programs, which impose threats to our systems in various ways. Their creators develop these programs with the sole objective of 'Destruction'. We shall discuss in this chapter about such programs viz. computer viruses, worms as well as Trojan horses in detail. This will enable us to take precautionary measures in order to save ourselves from these additional threats.

1. Computer Viruses:

1.1 General Concept:

There is nothing magical about computer viruses. A virus is simply a computer program, which is stored somewhere on the disk. But unlike the other programs, this program is not available separately. It will try to hide itself by attaching to some legitimate program. Still, it is to be called a computer program. There is very much similarity between a computer virus and a biological virus. *Both invade the body/machine and attach to cell/program and once lodged, they monitor the activity of the host in order to replicate themselves.*

1.2 Why viruses are developed?

The virus programs are normally written with an objective of destructive effects. A virus cannot do anything that was not written into its program. It is the creation of intelligent computer programmer but with the harmful intentions. There are other harmful programs like worms, Trojan horses etc. A program is not a virus unless it has the ability to *replicate* itself.

There are several ways and intentions with which the viruses are written. These range from complete destruction of host system, to simple pass-time nuisance activities. Sometimes viruses are used to stop from copying legitimate programs, or just to prove someone's knowledge, to simply make fun out of it & so forth.

1.3 How do they work?

Similar to their biological counterpart, the computer viruses also require some *carriers*. As biological viruses may use animals, insects, water or air as a medium for propagation, computer viruses need carriers like some legitimate executable programs, boot sectors, partition tables etc. to *carry* them to the host for further destruction and replication. When infected code gets executed by some means (using these carriers), the virus launches itself into memory and performs according to its program.

There are specific stages in viruses, called the *Life Cycle* of a virus. The first stage is called *Pre-trigger* stage or the *dormant* stage. In this stage viruses lie dormant, and does not do any destruction. (This act is also similar in the biological virus.) It is hard to detect a virus in this stage. The second stage called *trigger* stage is the one in which virus performs any destruction. A trigger can be made to set off at a given time, given number of times a program is run, physical condition of disk, specific date or time, any other event or just anything which might have been thought of by its developer. Once this trigger goes off, the destructive action

mentioned in the virus program executes to carry out the destruction. This is said to be the final stage as it causes actual damage it is supposed to do. *Virus programs enter into the system either by way of copying the carrier programs (exe, com, bat, sys & similar files) or copying anything from a disk with infected boot sector or partition table or even through E-mail or Website contents.* Also, the replication activity of viruses is transparent to the user.

1.4 Virus classifications:

There are several classes/types of viruses with some of them discovered recently. They are classified according to what they infect. The two major classes of viruses are: ***1.Boot sector/partition table viruses*** and ***2.File viruses***. Afterwards few other classes have also included as the new breed of viruses started coming in. These newer classes of viruses include ***3.Multipartite viruses***, ***4.Polymorphic viruses, 5. Stealth viruses*** and ***6.Macro viruses***. Working of each of these types is as explained below:

1. **Boot sector/partition table viruses:** Infect the boot sector, Master Boot record (MBR) or the partition table of the disks. These are the sensitive areas of the system which when controlled, it becomes much more easier for the viruses to carry out further replication. The code in these locations gets loaded in memory at the system startup and hence is a good target for these viruses. Examples of this type include *Michelangelo, Monkey, Brain, Stoned, Pentagon, Print screen etc.*
2. **File viruses:** As the name implies, these viruses infect files. These files normally include executable files such as .exe, .com, .bat etc. In general viruses do not infect data files, because they are not *executed.* But this does not mean that the data files are totally secure from viruses. These may even be targeted in the destruction stage of other viruses. Examples are *Jerusalem, Die Hard 2, Concept, Cascade* etc.
3. **Multipartite viruses:** These types of viruses are a combination of both boot sector as well as file viruses. They first infect the executable *files* and when these files are run the viruses further infect the *boot sectors/partition tables.* Thus they can infect in both the ways. Examples are *Tequila, Flip, Invader* etc.
4. **Polymorphic viruses:** These are newer type of viruses, which encrypt its code in various ways, so that it appears differently with each infection. Obviously these will be more difficult to detect. Examples include *Phoenix, Evil, Proud, Stimulate etc.*
5. **Stealth viruses:** Viruses using certain techniques to avoid detection by antivirus utilities are of this type. Such viruses may hide themselves in some other position than the detectable one, or keep the infected file's size and date the same as original and so on. Examples are *Whale, Frodo, Joshi* etc.
6. **Macro viruses:** This is newer type of viruses which infect the macros (small stored procedures to carry out multiple jobs at a keystroke) within a document or template. Whenever the infected document/template is run, the macro virus activates. Generally for word processing the template used is the file called normal.dot. When new files are created, based on this template the virus infects them all. Examples include *W.32, Nuclear, Word concept* etc.

1.5 Virus detection, prevention and recovery:

There are several precautions one can take in order to safeguard from virus infection. Even then if the virus still creeps in, one has to follow the detection and elimination procedures further. The safety measures or precautions for virus prevention are rightly called the *Golden Rules* or the *Commandments* as given below. While it is difficult to protect the system totally, using these rules one may prevent from the virus infections to a great extent.

The Golden Rules for virus prevention:

- Always keep backup of your data/programs.
- Keep floppies Write-protected (especially if they are bootable.)
- Do not copy anything in your system from any unknown source.
- Restrict the use of machine to only authorized users.
- Never download mail attachments, unknown content from Internet.

Even after using these precautions, if the virus creeps into your system, it can be detected in various ways apart from using a virus scanner for it. This is due to the indications or *symptoms* given out by their existence. These include the following.

Virus Symptoms:

- Computer system seems to be running too slow than normal
- Floppy disk or hard disk is accessed suddenly without any reason.
- Programs do something unusual or do not work normally
- Files, folders disappear mysteriously or contain garbage.
- System crashes often without any reason
- Computer does not boot completely at all
- System memory or disk space reduces without logical reason.
- Unusual error messages appear on screen
- Programs take more time to load than normal.
- Change in data/program file sizes is observed.

Recovery procedure:

If these symptoms are observed, they may indicate the presence of virus in your system. To eliminate virus when observed or detected in the system, one should carry out some specific steps called as *Recovery procedure.* If you use the Anti-virus softwares, they will do this job for you. Many such products exist including McaFee, Norton, F-prot, AVG & so on. One must ensure to update these utilities frequently, to stay safe from the newer viruses, which keep coming. Apart from using the tools, one must create a *Rescue disk* that should be a clean, uninfected bootable disk with required set of tools. This can be used to diagnose, detect & eliminate viruses from the system.

2. Worms:

2.1 General concept:

Apart from the virus programs discussed above, there exists one more type of malicious program in computer world called as a *Worm.* Unlike its cousin - the virus, worms do not require any type of *carriers.* This term was coined from the word *Tapeworm,* which used to copy itself in tapes (used in older computer systems) way back in 1060s. Those days the worm code was considered harmless and was used for just fooling-around with others. But then, hackers considered this as a tool for destruction purposes and the development on the other side continued. This gave rise to the recent *Melisa* or *I Love You* worms, which created havoc through the Internet across the world.

2.2 How do they work?

Worms are normally observed in Networked environment rather than in stand-alone environments and spreads itself by replication similar to that in virus. Some of the worms are coded using the scripting tools such as Java-script, VBScript, and Activex. The recent developed worms carry out their destruction through widespread use of Internet. Once lodged on to a system, worms keep replicating themselves by placing themselves in the memory of various infected systems. They use the network to copy from one node to other. The destructions caused by worms include - bringing down your network's speed, using your address book to send anonymous mails to other hosts, undesirably disclosing your valuable information to the world, resource eating etc. *Worms can choke or congest the network, thus bringing it to a crawling speed!*

2.2 Detection, prevention and recovery:

Normally, all the recent anti-virus utilities are capable of detecting most of the worm codes as well as disinfect them. The indication of worms may be the terrible slowness of the network, although there are several other reasons for this. Worms do not modify a program nor attach themselves to it and hence may be *seen* or *detected* separately unlike the virus. Still, some newer type of worms hide themselves inside the Email source, HTML scripts, web page sources etc. to remain undetected. As far as the prevention is concerned, using some safety measures like detection tools, not opening any content from unknown source, it may be possible to prevent from their attacks.

3. Trojan horses:

3.1 General concept:

Yet another type of malicious program observed is a Trojan Horse, sometimes simply called *Trojan*. The name has a funny history behind it. In the Greek kingdom, a wooden horse was gifted to the enemy and taken inside their fort. This actually contained soldiers inside it, which came out and fought with the enemy taking them by surprise. Our trojan horse in computer works with a similar principle. Even if it claims to be a genuine program, in fact it is a malicious one. It is supposed to do something useful, while all it does is totally different and that is destructive.

3.2 How do they work?

Trojans - as specified, always claim to be a genuine program. *If it were not a genuine program, rather one would not copy or try it out!* It may say it is a new game released, some kind of a utility program newly developed, or something similar. Once copied/downloaded on to a host and executed, actually it may do something like formatting hard disk, erasing files/folders and so on. They may work either like a *Time Bomb* (based on some value, number as triggering condition) or like a *Logic Bomb* (destructing after satisfying some logical event or condition). *It is also possible that the Trojan horse program may be working normally for some time, just to fool the user that it is doing something useful.*

There are some types of Trojans, which include some form of *self-destruction* which means the Trojan program itself gets deleted after triggering condition along with other destruction. (*Can this be very much analogous to a human bomb!*) Examples of Trojan horse program include **12 tricks Trojan**, actual file name CORETEST.COM (claims as hard disk benchmarking program!) **Nortstop Trojan,** filename NORTSTOP.EXE or NORTSTOP.ZIP

(claims to be an antivirus public domain utility!)

3.3 Detection, prevention and elimination:

One major difference between Trojan horse and worms or viruses is that the *Trojans do not self-replicate*. This reduces the amount of destruction caused by them compared to other malicious programs. Another limitation of them is that they are available separately. Hence it is possible to find out that the harm is caused by the running program, label it as Trojan and discard it. But beware! *It is also possible that the Trojan horse programs may be working like Backdoors and passing the valuable information from your system back to hackers!*

It is hence difficult to *detect* a Trojan, unless using some good utility. Now a days, many anti-virus utilities also check for them as well. Unless one tries out a Trojan program, it is hard to know whether it is genuine or not. In such case, one can try it (if it is absolutely necessary) on some separated machines and then using on regular once confirmed. The prevention mechanism says, never download/copy any content from unknown source, or when in doubt. The elimination is obviously the deletion of the program identified as a Trojan.

End of Chapter 3 – Notes for Internet Security, B.Sc. I.T. Semester V