4.0 INTRODUCTION

The world of computers and Information Technology is going through an era of electronic terrorism, in the form of virus. It is a problem that is potentially so dangerous that it threatens the proper functioning of the computer system in today's information age.

In this unit, we would discuss about the evolution of virus, the menace caused by them, the process of infection, classification of viruses, types of viruses, the prevention and the cure against them.

4.1 OBJECTIVES

At the end of this unit you should be able to:

- define computer viruses and its evolution
- explain the damage a virus can do
- define the process of virus infection
- identify different types of viruses depending or their area of bperation/infection
- describe/apply virus preventive measures.

4.2 THE EVOLUTION OF VIRUS

The concept of virus dates back to 1949, when John Von Neumann submitted a paper putting forward the concept of a "Self Replicating" program; the idea seemed impossible and was dropped. Subsequently, the first virus like program appeared in the form of a recreational game called "CODE-WARS" at the Bell Labs of American Telephone and Telegraph Company. In "Code-wars" two players were to code a set of programs that would destroy the other players programs. Realising the potential danger of such programs, the authors did not reveal the presence of such programs. Concurrently, at Massachusetts Institute of Technology, students were carrying out experiments with computer, which no body had ever tried. Their relatively harmless hobby of messing up with other programs gave rise to the idea and concept of computer viruses.

The first commercial application of viruses was in 1985, when two Pakistani brothers, in order to keep track of software piracy used Brain Virus (also known as Pakistani virus) on their low cost software sold from their outlet in Lahore. Hidden in nearly every disk they sold, was an extra program not supplied by the original manufacturer a snippet of computer code, self-replicating in nature that would infect an unauthorised user's computer by disrupting his operations. These self-replicating programs multiplied so fast that, today, they are a threat to the smooth operation of a computer.

4.3 THE MENACE

The virus, whether biological or electronic is an information disorder. Biological viruses are tiny genetic codes DNA or RNA that take over the machinery of a living cell and are capable of making thousands of replicas of the original virus. Like its biological counterpart, a computer virus carries in it an instructional code that makes copies of itself.

Lodged in a host computer, the typical virus takes temporary control of the computer disk operating system. When the infected system comes in contact with an uninfected computer, the virus passes onto the uninfected machine and, thus spreads like a forest fire, infecting machines after machine with which it comes in contact.

Computer viruses are computer programs, which are a collection of coded instructions. The basic difference between a normal program and a virus is that viruses are self-replicating, they have the capability of executing themselves without being asked for. Computer virus is a very broad term in itself and includes not only viruses, but also Worms and Trojans.

Trojans are similar to viruses. They move around as valid programs, sometimes getting executed with flashy opening screens describing them as - "Word Processor" or a "Database package". Trojans are programs that claim to do something but do something completely different and in the process damage information stored on a computer system. Trojans do not infect other software.

Worms travel longer distances by storing themselves in critical areas of the disk from where they get loaded and have with them sufficient code to transfer themselves outward from the system they infect. Worms have been known to damage and infect entire LANs.

Apart from self-replication, another devastation caused by viruses is data loss. A virus can also take steps to avoid its detection. That makes viruses even more dangerous, because you may come to know about the infection when it has struck. Even though all viruses are developed with a specific characteristic, most of them result in data-loss.

Most viruses are designed to perform simple feats but in order to do so, they:

- Corrupt the most sensitive area of the disk the File Allocation Table (FAT) or the directory area.

- Modify the interrupt organisation of the system, meaning when a read or write to screen operation takes place, it is routed through the virus code in the memory resulting in unresolvable interrupt clashes where a program opens up a file simultaneously for read-write access and the virus interrupts every operation.

Even though the virus may have no instructions built into it to destroy data, it can nevertheless render a disk full of files absolutely useless.

4.4 THE PROCESS OF INFECTION

To understand how a virus infects a system, we go; back to the elementary working of a computer. On booting, the system carries out the ROM instructions, the first being the power on Self Test (POST), which is followed by the bootstrap process of' reading the boot record and loading of the disk operating system. In MS-DOS, it involves the loading of IBMDOS.COM, IBMBIO.COM and COMMAND.COM along with some optional files like CONFIG.SYS and AUTOEXEC.BAT. The booting process culminates into the system prompt displayed on the VDU.

The infection may begin as soon as a computer; system boots from a contaminated disk or executes an infected program. Whatever viruses are present gets activated, which immediately begin to spread throughout the system.

Another important aspect that needs mention here is the Interrupt mechanism. All input/output activities on a PC are carried out by interrupts. The interrupt mechanism in itself is very complex. We will try to understand it with an example. Let us say, a. user wishes to save his program and presses the required keys on the key board. This treated as an interrupt. The main memory has specific routines to handle these user requests. One such set of routines exists in the ROM-BIOS and the another is in the DOS program in the memory, loaded from IBMBIO.COM. The routine that services the interrupt requests are termed as Interrupt Service Routines (ISR's) and are located in the memory with their addresses. Then interrupt request activates a number and not the routine address, thus, there exists a table with the interrupt numbers and the corresponding routine address in DOS. When an interrupt request is made, the CPU looks up the table, performs the required routines and transfers the control back to the program.

The contents of ISR address table being in the RAM is vulnerable to modification by user programs and that is what a virus does-modify the ISR's address.

4.5 CLASSIFICATION OF VIRUSES

Viruses are classified on the basis of their mode of existence and there are three categories of viruses:

1. BOOT Infectors

2. SYSTEM Infectors

3. GENERAL EXECUTABLE PROGRAM Infectors.

4.5.1 BOOT Infectors

As the name suggests, they are characterised by the fact that they physically reside in the boot sector [0 (zero)] sector of the disk. A system infected by such a virus will have the virus residing in a particular area of the disk rather than in a program file. These viruses get loaded soon after the Power on Self Test and control the system and remains in control at all times. They sometimes have the capability to trap soft booting (i.e. CTRL ALT DEL) and remain in control even if the system is booted from a non-infected floppy, thereby contaminating the clean floppy.

Boot infectors displaces information originally residing on the location, which they occupy. While writing onto the boot sector, the virus ensures that the boot record is not deleted. Once the virus is loaded, it automatically transfers control to the area where the boot record is available. The reason behind doing this is that the boot record contains instructions to read IBMBIO.COM and IBMDOS.COM and if these files are not readable, access to the disk is not possible, and so the virus becomes ineffective.

Boot infectors typically create "Bad sectors". Boot infectors are the types, which once loaded would stay in the memory until the system is shut off, and until the disk reformats.

4.5.2 SYSTEM Infectors

This second category of viruses' deals with the components of the system itself. All machines without exception require an operating system in order to create an environment in which the operator works. In MS-DOS, COMMAND.COM contains all the internal commands. If no such command file exists, commands such as COPY, DIR etc. are not loaded onto the memory when the machine is booted. The System Infectors attach themselves to a file such as COMMAND.COM or other memory resident files and manipulate these files.

System infectors differ from Boot infectors in the sense that system infectors gain control after the computer is booted: and infects the hard disk or bootable floppies, which contain the appropriate system files only. They have another peculiarity that they may activate after a given period of time or may instantly begin subtle modifications in system processing such as, increasing the time to perform system functions, scrambling of data, or modification of systems error messages or information messages.

4.5.3 GENERAL .COM or .EXE Infectors

From the infection point of view, these viruses are most dangerous and devastating of the three classes of viruses. They attach themselves to program files and can spread to almost any executable program in any system. These viruses change the original program instructions into a "jump" to its own code and follows that code with a return to the original program. As a result, whenever the program is executed, the virus gets loaded and executed first and then allows the original program to proceed. It remains memory resident and infects each and every program that is loaded for execution.

By attaching themselves to EXE or COM files, they alter the file size and sometimes multiple infections renders program files too large to be accommodated in the memory.

4.6 SOME VIRUS

The virus list has become a non-ending entity with new viruses joining the list every other day. We would be discussing some of the most commonly prevalent viruses in the computer industry. However, this list is incomplete.

1. Scores Virus

These viruses are prevalent in Macintosh machines. Scores virus has a built in time trigger that activates at two, four and seven days after the disk has became infected. The consequences are varied ranging form printing problems, system crashes and malfunctioning of disk operations. This virus does not directly affect data files, but erasure of this virus requires deletion of all files.

2. Brain Virus

This is one of the first viruses that came into being. Also known as the Pakistani virus, it was, developed by the Pakistani brothers to keep track of low cost software, those were sold out of their outlet in Lahore. The virus pops up a screen saying "Welcome to the Dungeon". This virus is known to destroy data and are highly contagious.

3. Lehigh Virus

This virus originated at the Lehigh University Computer Centre. This virus stays in the stack space of COMMAND.COM. With the booting of a PC from an infected disk, the virus is spread through commands such as COPY, TYPE, DIR etc. On any other disk with COMMAND.COM the virus code gets copied to the other disk and a counter is incremented on the parent. When the counter reaches a value of 4, all files of the disk gets erased. The boot sector gets ruined and also the FAT.

4. Friday the 13th

This virus attacks not only the COMMAND.COM but also other executable files. When a .COM or .EXE file is executed for the first time after booting, the virus captures a specific interrupt and inserts its own code; after which, whenever any .EXE file is executed, the virus code is written to the end of the file resulting in increase in size of the file by 1808 bytes. In COM files the virus code is written to the beginning of the file.

The increase in size of the EXE and COM files causes the program to become too large to be loaded into the memory. Also after a certain interval of time, delays are inserted resulting in considerable slowing down of the programs. The worst disaster occurs, if the infected .EXE or .COM is executed when the system date is Friday the 13th, all files get deleted.

5. Sunnyvale Slug

This does a variety of things like displaying a message "Greetings form Sunnyvale. Can you find me?" and also sometimes modifies the COPY Command resulting in deletion of files instead of copying.

6. Raindrops

This virus infects COM files. It intercepts the load and execute function of MS-DOS. It checks whether the file is EXE or not, if the file is not an EXE file, the first three bytes of the file are replaced by a jump instruction at the end of the file, where it gets attached after encryption. This results in dropping or showering of characters on the screen like raindrops and is also accompanied by appropriate sound effects.

7. Happy Birthday 30th

This virus gets activated on January 5th, if any of the infected program get executed, and will ask the user to type "Happy Birthday 30th". It might destroy all the data stored on a disk. The symptoms of this virus are that the computer memory is reported 6KB less than actual e.g. 634 KB instead of 640 KB.

Following is a list of prominent viruses that have created havoc on may machines across the globe. A comprehensive list cannot be built as every other day a new virus gets included into it.

Name	Also known as	Name	Also known as
Marijuana	(Stoned)	Tequila	
Joshi	(Happy Birthday Joshi)	Slow	
Flip		BFD	
Eddie	(Dark Avenger)	World peace	
Jerusalem	(Jerusalem Ver A to E,)	Kanishka	

	(Friday the 13th)		
		Disk-washer	
Serum	(Yankee Doodle, Version A, B)	Alfa	
Kinky	(Fellowship)	Trikal	
V2000		Mummy	
Zealot	(Keypress)	Mubamk	
Changu-Mangu		Charas	
March-6th	(Michael Angelo)	Feist	
Frodo	(4096, 100 Years)	Boabob	
Desi	(Made in India)	Monkey	
Datalock		ExeBug	
Gravity	(Raindrops, 1701,17XX) (1701/1704 Version A, B)		
		Feist	
Hong_Kong		NewBug	
Liberty		1403	
Form			
Pronto	(15XX)	G3	
Taiwan		Cansu	
Invader	(And-CAD)	Dong_2	
Generic	(Keydrop)	Long- 1	
Possessed	(Poss)	Khobar	
Black Monday		PFO	
Plastique		Die-Hard-2	
Bosh		Bloomington	
Dir-2		Fat-avenger	
Gumnam		Green-Catapillar	
		Angelina	

4.7 PREVENTION

Even though the computer industry has found a somewhat plausible solution to the virus problem in the form of vaccines, it is always advisable to follow the dictum "Prevention is better than cure". Moreover, the viruses are made faster than the vaccines. It is a good practice to follow some simple precautionary measures, which can reduce the possibility of a virus attack. The precautionary measures are:

- The CHKDSK command can be incorporated to the AUTOEXEC.B AT to check the disk. If the number of hidden files increase, the matter should be looked into.

- **Do not copy pirated software on your system.**

- Write protect tags should be used on the original software diskettes.

- Proper backup of all data and program files should be kept.

- Copying of files should be done carefully, a better practice is to write the COPY command in a batch file with CHKDSK command.

- Used floppies should be reformatted.

- Avoid letting the system to be used by unauthorised users.

- Restrict the use of outside floppies

- Do not download suspicious shareware programs.

4.8 THE CURE

The viruses are not omnipotent. Viruses can be cured with anti-viral programs. The anti-viral programs perform one or more of the following functions:

- prevention
- detection
- vaccination
- inoculation
- identification, and/or
- damage control.

A good anti-viral utility is one which checks whether the system has been infected or not. These programs stop the virus from infecting the system. They do not allow the modification of executable files, so that a file virus cannot get a foothold.

Some of them refuse to let any program make itself resident in RAM unless allowed by the user. Others do not allow the user to run a program unless it is on a list of approved and tested applications. The detectors warn the user of the presence of a virus after it is loaded into the machine or disk. These programs maintain a file with a list of checksum values of the executable files. The identifiers rely on the fact that when the virus replicates, it makes a copy of itself.

The vaccinators inject some code into the executable files. When the vaccinated file is run, the injected code performs an integrity check on the program being executed and warns if any changes have been made.

The innoculators insert the virus signature into infected areas or files at appropriate locations. When the virus performs their self-detection, they find their signature and believe that the memory/disk/file is already infected and so do not infect.

The better equipped anti-viral programs control damages. They may be preventive or restorative. Preventive techniques include stopping attempts at direct access such as formatting and deleting, or even write protecting the hard disk while testing unfamiliar software. The restorative process is achieved by maintaining a copy of the CMOS information, boot sector information, the file allocation table etc. in a safe area like a floppy.

As a virus can hide itself in many different ways, it is difficult to detect all viruses with just one anti-viral program. Moreover, the virus writers keep altering the viral code, so that any existing anti-viral programs cannot detect it. The point to remember is that there, is no cent per cent foolproof anti-virus program available and, in principle there never will be.

4.9 OPEN INDENT QUESTIONS AND ACTIVITIES

1. Make a list of at least 10 viruses with their characteristics.
2. Make a list of anti-virus packages you are using at your centre.

4.10 SUMMARY

This unit discussed about the threat faced by computer virus. It explains the evolution characteristics of the virus and the damage they can do to a computer. We studied different types of viruses and their characteristics. It also discussed about different preventive measures that should be taken to get rid of computer viruses. With the development of computer field, new viruses/vaccine software may come.

Therefore, one has to keep track of latest development in this field and know how to counter these problems.