Computer Virus

Dr. Leena H. Sarkar

Associate Professor, I/C Principal
Department of Chemistry
J.V.M's Degree College, Airoli, Navi Mumbai 400 708, India.

Abstract : A computer virus is a software program with ability to make copies of self, which can attack or corrupt other applications or files. The most potent and vulnerable threat for computer users is virus attack. Virus attacks hampers important work involved with data and documents. It is very necessary for the users to know about different softwares which can protect their computers from these virus attacks. One must take every possible measure in order to keep the computer systems free from virus attacks. A program that has been modified by a virus is deemed infected. This infected file / program can also become an evolved copy of the original virus program. Every program that gets infected can also act as a virus and thus the infection multiplies similar to biological virus, hence the name computer 'virus'. The ability to infect different programs is the main property of any virus. Every general purpose computer system currently in use is open to viral attack in some secure system, virus tends to spread further when created by some user of the system. A virus has the potential to spread throughout any system which allows file sharing. The computer virus can be generated and introduced by a hacker. The perpetrator gets the satisfaction of demonstrating human superiority over at cybernetic system or hacker stills the information for financial or other gains.

The aim of this paper is to discuss about the different types of computer viruses, their characteristics, working, how they affect the computer systems and also to suggest measures for detecting the virus infection in a computer system and to elaborate means of prevention.

Keywords: **Virus attacks, Computer, cybernetic system, Trojan**.

I. INTRODUCTION

"A computer virus is a kind of software that infects programs, data or dices and can reproduced itself in the same or other form. Despite all preventive measures, the viruses are becoming an order of the day. Viruses are enemies of computers and destroy whatever is stored in it, innocently, calmly and intelligently."

Fred Cahen incidentally coined the term 'Computer Virus'. The terms 'Virus' and 'Worm' were generally used in science fiction novels in the early 1970s. Around the same period researchers at Xerox Crop., created and demonstrated a self replicating code, called viruses.

Study of Virus shows a set of 'undecidable detection problems'. A list could be as follows:

- Detection of a virus by its appearance.
- Detection of a triggering mechanism by its appearance.
- Detection of a evolution of a known virus.
- Detection of a virus by its behavior.
- Detection of a triggering mechanism by its behavior.
- Detection of a viral detector by its behavior.
- Safety of a protection scheme.

Nowadays, networking has become an indispensable part of communication. This results in a virus getting initiated through a particular node or through few nodes and may give an appearance of having originated from some other node. A virus may also get kindled at some stages of a program in an executable file and not necessarily whenever the program is called for.

Experts say that a virus need not be used only for evil purpose. A very interesting theory in compression through virus has been developed. It can be explained that the simple virus can be written to find uninfected executable file, compress them and insert itself into them. The infected program decompresses itself and executes normally on execution. Studies indicate that such a virus could save over 50% of the space taken by the executable files in an average system.

The virus infected programs show a slight decrease in performance on decompression. The compression virus then imposes a specific kind of tradeoff between space and time.

Another example could be that a virus program can be written in such a way to find 'uninfected' executable. It will plant itself at their beginning. These viruses are set to get themselves activated on a specific date and time and this results in the executable programs to get into an indefinite loop and not performing its required job.

And in modern networking with the level of sharing that is prevalent, the entire system would become unusable as of the moment. Antivirus operators might find a great deal of hard work is required to treat the damage caused by such a virus.

II. TYPES OF VIRUSES

2.1 NON-TSR FILE VIRUS

This is the simplest form of virus to write and the least effective, so one is unlikely to be troubled by them. When an infected program is first run the virus code carries out its task checking that an executable file in not infected, then attaching a copy to it. It then runs the original program to which it is attached. In contrast TSR viruses load themselves into memory when they are executed and are able to infect any executable program they can reach from that point.

2.2 BOOT SECTOR VIRUS

This is the other major type of virus. It infects the master boot record. Most of the boot sector consists of a simple, small program that is used to start DOS or whatever operating system is installed. Boot sector viruses replace this with virus code and

typically move the boot sector to another part of the disc. When the PC boot the virus code is executed first. Then the virus runs the real boot sector.

The main symptom in the machines infected with boot sector virus is very slow boot from an infected floppy or master boot record. During this process the virus gets itself saved in memory which in turn affects other files.

2.3 MULTIPARTITE VIRUSES

These combine both techniques. They can infect both sector and files. The file version of 'Tequila' for example infects the Master Boot Record. Once the PC has been booted with an infected MBR, the virus goes and infects entire memory of the accessed EXE files.

2.4 COMPANION VIRUSES

Companion viruses create a .COM companion to an .EXE files. Because DOS executes.COM files before .EXEs the virus is run before the .EXE file of the same name. The virus then runs the original .EXE.

2.5 STEALTH

Stealth covers a variety of techniques that viruses use to disguise their presence from anything as simple as hiding the increase in files size of executable to full blown detection of the tools used to detect the virus and the taking appropriate action to fool them.

2.6 TROJANS

Trojans are not viruses at all. They are programs that hide a malevolent code within a seemingly innocuous program but they do not replicate. For this reasons the chance of being caught out accidentally by Trojans are low.

2.7 MACRO VIRUSES

Macro viruses have been predicted for very short duration. They appeared when Microsoft accidentally sent them from CD-ROM to OEMs. They were called 'Prank Macro'. It is the first virus that will run on both PCs and Macs. It replicates using an auto-executing World Basic macro embedded in a document. When the document is loaded it copies the macro to word's settings file NORMAL.DOT. The file save command is replaced with a program that also saves a copy of the macro in each document.

III. PREVENTION FROM A VIRUS ATTACK

To prevent virus attacks, external device accesses such as pen drive, floppy, etc. to a machine should be limited. In case of floppy discs the simplest form of protection is to place write protect tabs on all discs so that any attempt by a virus to write to the disc would result in an error message. Even in case of checking directory listing in an infected floppy disc can be enough to infect a machine.

In general write protect facilities are not available for hard discs, but in recent times, new hardware products have started appearing in the market which offer users the ability to write protect hard disc. But they are expensive and so they are not widely used.

Nowadays, software products are available in the market which can write protect hard discs. But they are also susceptible to virus attack. In network environment the use of diskless or hard disc only system is becoming popular. Control of software is them restricted to the files server and network administrator only.

Even if one busy and use several antivirus applications the best defense is to avoid infection in the first place. There is no absolute guarantee against infection. But the risk can be minimized by following the guidelines listed below:

- The system should be booted with a write protected and scanned floppy disc, containing the boot, system files and set of files of a qualified virus scanned program.
- Even if there is a hard disc and the PC normally boots from the disc, start by first booting the system with the uninfected and write protected disc boot floppy in the 'A' drive.
- All floppies should be scanned individually and periodically by using a qualified and uninfected virus scanning program.
- Avoid using shared computer for online transactions. If it is mandatory to use, remember to clear history and local cache before closing the browser.

IV. REFERENCES

1. David J. Stang, Computer Virus, Diane Publishing Company, 1992.
2. Verma, S.K. & Mittal, R., Legal Dimensions of Cyberspace. New Delhi, ILI Publisher, 2004.
3. Gurjeet Singh & VidhySandher, 'Emerging of Cybercrime A challenge for new millennium' Aligarh Law Journal.Vol. XIV & XV, year 1999-2000.
4. Dudeja, V.D, Cyber Crime and Law. Vol.1, Commonwealth publisher, Ed. 1st.
5. Richard B. Levin, The computer virus handbook, McGraw-Hill Ryerson, Limited, 1990.
6. Sutar Prafull, Social Media- Digital Media, Multiversity Publication, Pune, 2015.