1773

# COMPUTERS UNDER ATTACK
# Logic Bombs, Viruses, Worms, Trozan Horse

ANIL KUMAR GROVER

This paper analyses various viruses that attack the functioning of a computer. The effects of these viruses on the operating systems are examined. Several suggestions have been given to avoid these viruses and thereby keep the computer system healthy.

In our day to day life we never bother about the various insects and other semi-living disasters but when we enter the field of Computers without having any knowledge about these insects (commonly known as Viruses), it is really harmful. Unfortunately this disease is created by Doctors of this field also known as the professionals or the persons who claim themselves to be the superusers of Computer. A Virus is actually a maliciously authored piece of software which interferes with normal functioning of your system and corrupts data.

The kind of Viruses spreading these days are not easily detectable. These Viruses are hidden programs (they are not dumb programs) and, they are not easily detectable in DOS partitions.

## CLASSES OF VIRUSES

A virus is a computer program that "infects" other legitimate programs by modifying them to include a copy of itself to additional executable program code or operating system commands, spreading from computer to computer, system to system and network to network. It eventually performs the function that it was designed to do — erase a hard disk, lock up the keyboard, or display a screen message.

The most dangerous aspect of a typical virus is that its first task is to replicate itself. Not all viruses are harmful or unwanted. You might design one yourself that compresses files to save storage space. You might also write a virus that hunts down and destroys a destructive virus in your system.

### *(i) Worm*

A worm is a section of code that searches for unused computer memory and

Mr. Anil Kumar Grover is Technical Assistant, Computer Centre, Shri Ram College of Commerce, University of Delhi, Delhi.

then replicates itself to fill up that space. It eventually uses up so much memory that the computer can no longer function and the system "crashes".

A worm is usually different from a virus in that its main task is simply to replicate itself many times. It is also different in that it often maintains communication ties with the original program code in memory.

### *(ii) Logic Bombs*

A logic bomb is a section of damaging computer code that is programmed to go off based on some predetermined event; for example, dates such as June 12th or April 1 or Friday the 13th. It also could be based on a condition not met : for example, a social security number (say 321-75-2345) that is not on the executable files or it can create a separate date file with this content or replace existing one with it.

### *(iii) Trojan Horse*

A program that does something "on the sly" which the programmer intended, but the user would disapprove of. Many people use the term "Trojan" to refer to a non-replicating malicious program.

## HOW TO KEEP YOUR SYSTEM HEALTHY

You cannot eliminate the possibility of getting a computer virus but you can reduce the risk. Adopt an institution or a company or a group wide security policy and publicize it to all persons of it concerned. This policy should have top-management support and should describe the various sanctions to be imposed on individuals who fail to follow rules.

The following suggestions are for preventing and minimizing damage from microcomputer viruses ;

### *(i) Allow no Direct Downloading of Software from Public Bulletin Board Systems*

Any useful program that any person wishes to download should be quarantined (scanned) first. This program should be examined and tested by a knowledgeable individual before being released to the department. Tests should be performed using virus detection software and actual execution of the program should be done on a floppy based system. Avoid testing new programs on hard disk systems so that the hard disk does not become infected.

When testing the program, be sure to advance the system clock to catch any time delayed logic bombs, especially Friday the 13th, April Fool's Day, 1st of every year and so on. When you do install a new program on your hard drive you must set up a subdirectory for it. Do not put it on to your root directory. Many PC viruses have affected only the current directory that they were located in.

*(ii) Write Protect Tabs to Executable and Other System Files :*

Those files whose names end in "COM" or "EXE" or "SYS" or "OVL" etc. are called executable or system files. One must be very careful at the time of using these files on removable disks; in other words, anything should not be copied on it; as a remedy the disks must be write protected with a tab. For hard disks (or also for floppies), you can use the DOS "attribute" command to mark a file as read-only.

You may also establish read-only status more effectively with some virus prevention programs like PCtools, Norton Disk Doctor. This inhibits a virus from corrupting these valuable programs. You should also periodically check programs for size and/or date changes.

*(iii) When Using a PC that is Shared by Many Users, turn the Machine off before you begin to work on it*

A number of viruses can hide in RAM (i.e. be memory resident) to infect any subsequent users. Always turn the system power off to clear the computer completely.

*(iv) Boot Floppy based Systems only from a known Write Protected Boot Diskette*

This will ensure that the operating system installed is legitimate.

*(v) Boot a Hard Disk System from the Hard Disk Drive*

There is evidence that it is easier to write a more general virus that can override a larger number of floppy disk controllers than hard disk controllers. By booting from your known hard disk programs you are minimizing your risk of infection.

*(vi) Provide Physical and/or logical Security for your Computers*

Lock up your computers to prevent unauthorized access. Consider installing access protection software to prevent anyone from getting access to the computer without password authorization.

*(vii) Install Virus Protection Software*

On your computers to alert you to any unusual activities,— for example, format hard disk.

*(viii) Back Up, Back Up, Back Up !!!*

This is the most fundamental security step to be done on a regular basis in any organization. A regular backup routine will help to restore lost data and/ or programs. It does not guarantee that the backups will be completely clean but at least it will give you some files from which to work.

## SOFTWARE THAT HELPS

There are a number of good programs that can help to minimize your risk in this area. They are often described as antivirus or vaccine software. According to the Computer Virus Industry Association (CVIA) in the U.S., such viruses fall into three basic categories :

### *(a). Class I*

This kind of softwares are designed to prevent initial infection and to halt the reproduction process. Typically, it disables any writing to the protected files. Once it is installed on the system, the user often is presented with a choice to allow writing to a particular file or not. Sometimes it can be overly intrusive on your work habits.

### *(b) Class II*

These programs are designed to detect infection. They work by performing a variety of activities, which include calculating checksums (an algorithm that produces a number determined by the sum of the bytes in a program) or signatures and comparing them to a previously recorded number.

### *(c) Class III*

These programs identify the type of virus that is affecting your system and once it is identified, they are often programmed to remove the virus. They are successful only on known viruses and do not usually provide much help on new viruses or old viruses that have been modified. They can still be very useful because known viruses have a tendency to reappear.

Many of these packages residein RAM while you are running your usual applications. The antivirus program will "pop up" when a predetermined event occurs to ask you if you wish to allow it to happen-write to a file, format the disk. If you answer affirmatively, your application program continues working. If you say no, the memory-resident software stops the questionable action.

## INTRODUCTION OF SOME VIRUSES

There are numerous viruses, each with its own speciality. However to give introduction to all is quite difficult; a few viruses are introduced hereunder:

### *Friday the 13th and other Destructive Viruses*

A good example of a destructive virus was discovered at Lehigh University in November 1987. It affected IBM compatible microcomputers by altering the COMMAND.COM file used to boot the machines. Its first task was to copy itself to any uninfected COMMAND.COM file with which it had contact. When its internal counter detected that it had achieved this purpose four times, it would write all zeros to the first 32 sectors of any diskette or hard disk it could reach at that moment. This destroyed the boot sector and root directory of these disks. Usually making the data unrecoverable. Once the virus was discovered and isolated, it was relatively easy to determine if a diskette was infected. The virus would change the last date of update for the COMMAND.COM file.

The good example of the Virus infection is the "Brain" virus conceived by the Alvi brothers of Lahore, Pakistan, which is generally known as "Pakistani Brain Virus"; it was made in 1985. The two brothers had been writing computer software and selling it from their shop, Brain Computer Services. Dismayed when people started to copy their software without permission, the older brother decided to include some additional code in the programs that would proclaim, the user would have to contact the Alvi brothers (phone number was provided) to fix their systems.

The Alvi brothers soon started selling their own pirated copies of brand name computer programs, such as Lotus 1-2-3 and WordStar, for as cheaply as $1.50 each. Some tourists who bought the copies, especially Americans, were given programs with the Brain virus attached; while local customers were given a clean version. These virus laden programs were brought back to the United States where, it is estimated, they infected over 100,000 diskettes. Although the Alvi brothers stopped selling the contaminated disks in mid 1987, the virus kept popping up at various locations throughout 1988.

### *The Brain Virus*

The Brain virus is easily recognized because it changes the volume label of any infected floppy or hard disk to "Brain". It also marks some disk sectors as bad and modifies several command files. Several altered versions of the Brain virus that do more severe damage also have been reported.

### *The Israili Virus*

A prime example of the Logic bomb is "Israili" or "Friday the 13th" virus. First sighted at Hebrew University in late 1987 the virus was designed to erase all files and timed to go off on Friday, May 18, 1988. This was the 40th anniversary of the creation of the state of Israel. It also was designed to copy itself to other programs on every Friday and every 13th of the month.

It was detected early because it kept making copies of itself on the sarne program and slowed down computer response. Some programs contained 400 copies of the bomb. The virus had infected home, university, and never got to fully perform its mission. But it did destroy some data and programs.

### The Misis Virus

Misis is a very small boot sector virus from Russia. It stores itself in low system memory and overwrites the interrupt sector of the table. This makes the system potentially unstable. This virus triggers on every 16th boot sector access, and contains several phrases of Russian text which can be viewed on displays with a Russian screen driver.

## HOW TO ELIMINATE THE VIRUSES

To diagnose a virus is actually 'half of the work done'. Although there are numerous tools to diagnose a disk for suspected viruses as Scan, Utscan, Nashot, Micro Soft Anti Virus, Virus Killer etc., a few of them are described hereunder :

### Scanner or Viruscan

This is a memory resident program which identifies pre-existing virus infections and prevents viruses from spreading throughout your system. It monitors and scans programs as they are loaded and prevents infected programs from executing. It also scans specific areas of the system — the boot sector, partition, hidden files, Command Interpreter and itself, when it is first executed.

It identifies the virus strain which has caused the infection in all cases of the known viruses. It remains active in your system at all times after it is loaded.

Scanner comes in various versions (0.3v1 to 8.33V) as it is updated time to time to keep the requirement of the user. The 0.8V35 version of Scanner can identify 34 major virus strains and numerous sub varieties for each strain. The 34 viruses include the twelve most common viruses which account for over 95% of all reported PC infections. These common viruses include :

- Pakistani Brain
- Alameda
- Cascade (1701/1704)
- Ping Pong
- Stoned
- Lehigh
- Den Zuk,
- Datacrime (1208/1168)

— Fu Manchu
— Vienna (DOS 62)
— April First

These viruses infect one of the following areas :

The hard disk partition table; the DOS boot sector of hard disks or floppies; or one or more executable files within the system. The executable files may be operating system programs, system device drivers, .COM files, .EXE files, .OVL files or any other which can be loaded into memory and executed. Scanner identifies the area or file that has become infected and indicates the name of the virus that has infected each area. When the infection is identified, the VIRUSCAN non-resident system scanner should be used to scan the entire system and determine the extent of the infection.

a) *Operation*

First place Scanner on a write protected floppy prior to installing it. This will ensure a valid copy in the event that the program becomes infected.

To Install scanner place the following line as the First entry in your autoexec. bat file as Scanner.

Then copy the file Scanner.exe. to the root directory of our bootable hard drive (usually C:)

Scanner will then become active each time the system is powered on or re-booted. It will check.

At the time of powered on or re-booted, it will check the critical areas of the system for viruses, including itself, and then monitor all program loads. As programs are loaded, scanner will scan the programs looking for viruses. If a virus is found scanner will display a warning message and name of the infected files. The infected program will then be terminated.

b) *Virus Removal*

What do you do if a virus is found? Well ! now we have a facility of CLEAN for removal of viruses, but in case of damage by a Boot sector virus or Partition table, one must need an experienced person because these infections can damage the hard disk totally or can destroy the booting facility provided by that particular floppy disk or hard disk. Following are some of the minor ways to remove the viruses :

i) *Boot Sector Infections*

Power down the system. Power up and boot from an uninfected write protected floppy. Execute the DOS SYS command to attempt an overwrite of the boot sector. This works in many cases. If this does not work, backup all data files and perform a low level format of the disk.

ii) *Executable File Infections :* Remove all infected files. Replace from the original distribution diskettes.

iii) *Partition Table Infections :* Without a removal utility, the only option is to low level format the media.

c) *How to use Viruscan (Virus Scanner)*

If a new virus pops up somewhere just add its signature to the list below and scan your disks with virscan after using the following format :

Format of a virus signature entry (3 lines, no comments in between)

| | |
|---|---|
| <Virus name> | (max. 30 characters) |
| <affected items> | (COM, EXE, SYS, OVL, BIN or BOOT separated by a blank) |
| <Virus signature> | (Hex-string, no separators, max. 80 characters) |

## EFFECTS OF VIRUSES ON VARIOUS OPERATING SYSTEMS/ PLATFORMS

It is sometimes unbelievable to see a virus infect other than DOS partitions. Even LAN/WAN, Windows, Unix operating system, OS-2 etc. are not untouched with the shadow of this dungeon. Few facts are described here, which show its relation with other platforms.

a) *Viruses on Network Systems (LAN/WAN)*

Even after having a lot of security on Network systems, the viruses do inhabit and infect networks. The maximum damage occurs if the server is booted off an infected disk since it will allow the virus to spread to all the nodes that access the server-and reduce the FATs to electronic confetti. For this reason alone, we should boot the server only through the hard disk. But keep a clean, bootable write protected floppy handy — so that the same version of bootable operating system should help us in case of hard disk failure.

Files on a network server are relatively safe, because the NOS (Network Operating System) prevents users from writing to the server if the required write permission has not been granted. So, most viruses cannot infect the server.

In case of WAN (Wide Area Network) the chances of viruses become more than with LAN because the area is wide and the systems are not only connected in a finite strength but they are connected with the international machines. When more and more machines get connected to international wide area networks, the risk of infection becomes greater. So it pays to be aware of viruses which could affect your computer-even though they affect someone else.

*Security Technique in Network System*

A set of computers connected in a well managed LAN (Local Area Network), with carefully established security settings, and with minimal privileges for each user is more virus-resistant than the same set of computers if they are **not interconnected**. When all computers have (read only) access to a **common pool of executable** programs, there is usually less need for **diskette swapping and software** exchange between them — and therefore, **less ways through which a** virus can spread. However, if the LAN is not well managed, it could help a virus to spread more efficiently.

### b) *Viruses and Windows*

The Windows platform is different from DOS. It is more complex and rigid. It is more surprising that Viruses have also attacked even in this Platform, although the safeguard technique of Windows as compared to other operating systems is more powerful as it makes tough for programs to modify memory areas reserved for other applications. But one need to be aware that the memory protection is not foolproof; some viruses can be written using Windows own programming toolkit, which is more dangerous. In Windows the viruses have many more places to hide, e.g., in library files, in EXE files; a virus can even infect font files or display drivers.

### c) *Viruses and UNIX*

Unix is a very comprehensive operating system. Although it has no interlink with DOS even then this platform is not safe from the attack of some critical viruses. UNIX's memory and disk protection mechanisms make virus spread practically impossible, as does the fact that most UNIX programs are distributed in source form and compiled on the target machine. The probability of an infection during normal operation is not high. If we use UNIX operating system as a development platform then there are chances of infection. Because the development is occasionally done by users in privileged groups, or even by root, the infection can be dangerous.

Unix system has its own inherent file system security; the damage is fairly limited. All directories with write access are affected, and no intentional permanent or transient damage occurs. As most directories do not have write access, they are safe, unless the virus appears in a program created by root — which is unlikely.

## VIRUS SIGNATURES

Following are few virus signatures of some special class viruses :

***Pakistani Brain Virus***
(Boot Sector Virus)
Sign :
8CC88ED88ED0BC00F0F0FBA0067CA2097C8B0E077C890E0A7CE85700

***Stoned (Marijuana) Virus***
Boot Sector Virus
Sign :
1E5080FC02721780FC0473120AD2750E33C08Ed8A03F04A8017503E80700

***April 1st EXE Virus***
(Execution time virus)
Sign :
2EA31700BB17000E1FB4DECD21B42ACD2181FA0104742281F9BC077506E8C504

***Jerusalem Virus — Version B-2***
(Boot Sector/Command file/Execution time Virus)
Sign :
E99200000000000000000001

***Data Crime II Virus***
Command files/Execution time Virus)
Sign :
5E81EE030183FE00742A2E8A94

***1701/1704 Virus — Version B?***
(Boot Sector/Command file/Execution time virus)
Sign :
31343124464C75F8

***Vienna (DOS62) Virus — A***
(Boot sector/ Command file/Execution time virus)
Sign :
8BFE81C71F008BDE81C61F00

***Israili Boot Virus***
(Boot sector Virus)
Sign :
CD13B80202B90627BA0001

***Bouncing Ball Virus***
(Boot Sector Virus)
Sign :
505380FC4B740880FC4E7403E977018BDA807F013A75058A07EB07

### Other Destructive Viruses with their Standard Messages :

Viruses suddenly appear on the screen, and give a signal of their attack. They sometimes bang in a loud voice, or display a Crucial Message. They are sometimes known by different names as alias. A few interesting facts about some viruses are described hereunder :

*Chinese-Fish*

| | | |
|---|---|---|
| Alias | : | Fish Boot |
| Disk Space | : | 3 sectors |
| Message | : | "Hello I am Fish, Please don't kill me." ...Chinese-Fish |

*Deicide (B)*

| | | |
|---|---|---|
| Disk Space | : | 666 bytes |
| Action | : | First 80 sectors of drive C : clobbered with garbage |
| Message | : | "DEICIDE ! Glenn (666) say BYE BYE HARDDISK ! ! Next time be carefull with illegal stuff. . ." Deicide (B) |

*Invisible*

| | | |
|---|---|---|
| Infects | : | COM.EXE |
| Disk Space | : | 2926 (COM), 2926+15 (EXE) |
| Action | : | Overwrites some files instead of infecting. |
| Message | : | "I am invisible man," . . .Invisible. |

*June 12th*

| | | |
|---|---|---|
| Infects | : | COM, EXE |
| Disk Space | : | 2660 bytes + 16 bytes for EXE (rounding) |
| Action | : | Music and screen display. |
| Message | : | "June 12, the independence of the Philippines" . . .June 12th |

*Kalah*

| | | |
|---|---|---|
| Infects | : | COM files |
| Disk Space | : | 499 bytes |
| Action | : | First 100 tracks of the hard drive are formatted. |
| Message | : | "I don't like Mondays. . ." Kalah (499) |

*Kthulhu*

| | | |
|---|---|---|
| Infects | : | COM files |
| Disk space | : | 512 bytes |
| Action | : | Writes a message on the console, beeps and waits for a key before rebooting. |
| Message | : | "It is coming. Today is my birthday, It has gone" . . .Kthulhu |

| | | |
|---|---|---|
| *Pathogen* | : | *SMEG* |
| Infects | : | COM, EXE |
| Action | : | It writes randomly on the sectors of storage media |
| Message | : | "Your hard disk is being corrupted, courtesy of PATHOGEN !" . . . Pathogen : SMEG |

*Runtime*

| | | |
|---|---|---|
| Infects | : | COM |
| Disk Space | : | 365 bytes |
| Message | : | "Runtime error 412 followed by possible garbage" . .Runtime |

*Su*

| | | |
|---|---|---|
| Alias | : | Susan |
| Infects | : | EXE |
| Disk Space | : | 571 bytes |
| Action | : | Infected files are overwritten and destroyed. |
| Message | : | "Bad command or file name" . . .Su |

*Techno*

| | | |
|---|---|---|
| Infects | : | COM |
| Disk space | : | 1123 bytes |
| Action | : | Music, Videoeffect |
| Message | : | "TECHNO, don't touch the keyboard, COMSPEC=" . . . Techno |

## REFERENCES

1. *A Pathology of Computer Viruses* : By Daved Ferbrache, (Springer — Verlag, 1992).
2. *A Short Course on Computer Viruses* : By Fred Cohen, (ASP Press, 1990).
3. *The Virus Bulletin* : Listed at Quadrant Abingdon, OX14 3YS (England) (Published in UK in 1992).
4. *Computer Viruses Report* : US-based National/International Computer Security Association.
5. *War on Virus* : By Harsh Javery and Suchit Nanda, (Computer Bookshop, 2nd Edition).
6. *PC-Quest* : A Cyber Media Publication (India).
7. *Computers & Viruses* : By Peter J. Denning, (ACM Press/Addison-Wesley, 1990).