

COMPUTERS AND VIRUSES - AN OVERVIEW

Isaac Tanam

B Eng M Eng PGDC CCP MNSE MCOAN

ECWA Information & Computer Science Institute, Jos

Presented at the Sensitisation Workshop for Computer Professional in Plateau State, May 1998

ABSTRACT:

Since the invention of the mechanical computer by Charles Babbage in 1828, and the birth of the first digital computer during the second world war, several generations of computers have been born. With each generation of computers comes increased efficiency and reduced size. It may also be added that even though the size of the computer is reduced, its capacity and capabilities have increased. This increase in capacity and capability increases the need for file sharing, and by extension, virus sharing. This paper takes an overview of the computer, the way they are affected by virus and how to prevent and/or "cure" virus infected computers.

BRIEF COMPUTER OVERVIEW

The computer is an electronic machine which has the ability to receive, store and process data to produce information for decision making. Decisions made could either be a management decision to improve productivity or for control of automatic machines, which is what computers were originally made for. The function of modern day computer has moved from simple mathematical calculations to more complex data processing, word processing, image processing among others, says Petrillo, (1993).

The computer consists of two major parts, the hardware and the software. One without the other is of no value.

THE HARDWARE:

The physical components of the computer form the hardware. These include the following:

1. **The Keyboard:-** This is the typewriter-like board containing alphabets, numbers, punctuations, special characters as well as special function keys. These keys do different things at different situations. The keyboard is the means by which the user communicates with the computer and is therefore referred to as an input device. Other input devices are the mouse, joystick, modem, etc.

2. **The Monitor:-** This is the TV-like part of the computer. This helps the user, through the screen, monitor the operations going on in the computer. If any operation is not successful, an error message is displayed on the screen. The monitor is the means by which the computer communicates with the user. It is therefore referred to as an output device. Other output devices are the printers, speakers, and other physical operations that occur as a result of information generated by the computer.

3. **Computer Casing:-** This part of the computer is erroneously called the CPU by computer beginners.

The casing houses various components (discussed shortly) that form the "real" computer. The CPU is just one of these components, and is probably among the smallest part in the casing.

The part housed by the casing include the following:

(a) **CPU:-** CPU stands for Central Processing Unit. It is the "brain" of the computer and controls the activities of all other components of the entire computer system. It is sub-divided into two main units.

(i) **The Arithmetic and Logical unit:-** This carries out all forms of calculations such as addition, multiplication, division, subtraction, exponenciation, etc., and make comparisons between units of data (Brightmem and Dimsdale, 1986). Changing font type and/or size requires such complex calculations.

(ii) **The Control unit:-** This unit of the CPU controls the operations of all the hardware (Brightmen and Dimsdale, 1986). It determines which component is sending data and to where. In other words, it selects, interprets and executes the program instructions as available in the primary storage (discussed below). It performs the overall supervision of all the units.

(b) **Disk Drives (Secondary Storage):-** Disk drives are the storage houses for programs, data and information. There are two types of disk drives, hard disk drive and floppy disk drive. Capacity of floppy drives vary from 360KB - 1.44MB while that of hard disk vary from 10MB - over 3.5GB. These values are large when compared with computer used in the 60's or early 70's. Today there are variations of both types of disks in terms of their location in the computer and/or size. Generally though, hard disks

are permanently in the casing while the floppy disk drives use disks that are removable, and so could be used to move data from one computer to another. Disks are permanent storage devices. Another permanent storage device are magnetic tapes. These have capacities of the hard disk but are very slow in operation. They are generally used for backup purposes.

- (c) **Main (Primary) Storage:-** The main storage is where data currently being processed, and the program processing them are stored. Once a program and data are in the main storage, they can be accessed directly at any time by another program stored here. For this reason, the main storage is sometimes called the Random Access Memory (RAM) or simply memory. This is probably the most important part in the computer, for no program can be used unless it is brought into the memory. Likewise data being processed. Common RAM sizes are 256KB, 512KB, 640KB, 1MB and can be as large as 64MB in modern systems.

Depending on the size of your computer RAM, you can have more than 2 programs running at the same time.

Note that the life of programs and data stored and immediately the computer is powered off, storage here is only temporary. Any unsaved work is lost at power off, be it accidental or intentional.

THE SOFTWARE:

A computer without software is only as good as a piece of decoration in the office or the sitting room. When you want the computer to do a thing, you simply give it the instruction along with the rules on how to carry out the instruction. A set of rules and instructions written to do a thing in the computer is called a program. These programs are what is referred to as software. Softwares are developed by programmers, now called software engineers. Each is designed for a specific task. No software can do what it is not designed for.

Software may be grouped into two broad classes namely Application software and Systems software.

1. Application Softwares are those programs written to do some productive work. The table below shows some job processes and examples of some

available programs used for the processing.

Job Process	Example of Program
Word Processing	<ol style="list-style-type: none"> 1. WordPerfect 2. Microsoft Word 3. Page Maker 4. Ventura 5. Word Star, etc.
Database Management	<ol style="list-style-type: none"> 1. dBase 2. Alpha 3. Data Perfect 4. Microsoft Access, etc.
Spreadsheet	<ol style="list-style-type: none"> 1. Lotus 123 2. Microsoft Excel 3. PlanPerfect 4. Quatro Pro, etc.
Accounting	<ol style="list-style-type: none"> 1. Dac Easy 2. Quicken 3. Peach Tree, etc
Image Processing	<ol style="list-style-type: none"> 1. CorelDraw 2. DrawPerfect 3. Microsoft PowerPoint 4. Word Perfect Draw 5. AutoCAD 6. Harvard Graphics, etc.
Others	As required by client

2. Systems software are those developed for system control and maintenance. Most of them are used for disk, file and memory management. Operating systems, diagnostic programs and anti-virus program fall under this category.

COMPUTER VIRUSES

Computer viruses have been in existence for many years but were hardly ever noticed because of the low level of computer usage. Until recently, as the number of computer users increases and inter-connectivity also increases, leading to extensive file

(information) sharing, viruses were never much of a problem and so were never a matter of much concern.

Today, with the increase in network activity, and heavy (probably over) dependence on ready-made software, the speed and ease of virus spread and the harm they cause have become a thing of major concern, to both computer professionals and computer users. It has therefore become necessary to cry out their existence, the harm they can do and how to prevent or cure computers already infected.

Simply speaking, a computer virus is a program written just like any other software. What differentiates a virus from other programs is its ability to replicate. Viruses spread by copying themselves from one place to another. This is what really makes them very dangerous. Unlike most copy activities, when a virus copies itself, you do not know until it starts its designed operation on your computer.

Effects of Viruses:

The harm done by a virus depends on the type of virus. Some of the effects of a virus on a computer include the following:

1. Slows down the computer.
2. Virtual reduction of memory.
3. Displays unusual and unexpected messages on the screen, some of which may appear funny or annoying.
4. Deletes file(s) from the infected disk.
5. Formats the hard drive.
6. Scramble FAT

While many viruses simply display messages on the screen when active, there are those that remain in the background, doing their designed harm. Most dangerous viruses behave this way. Those that "make noise" easily get caught.

Research reveals that only 35% of all known viruses are deliberately harmful but even the so-called harmless viruses can cause trouble if not detected, even though they were not meant to be. This is because most of them are designed and written by kids who are inexperienced and are only trying their hands on the little programming they were taught at school. In the process of their practice they develop viruses, most un-

intentional. In the process of trying to correct theirs, they make them worst by producing variants of the same virus.

There are thousands of viruses and their variants. Below is a list of just a few.

AIDS	Christmas Tree	HIV
Alabama	Civil_War.245	Israeli
Alexander	Crazy_Priest	Jerusalem
Amoeba	Crucifix 2914	Joke Program
AntiChrist	Damage	Joshua
AntiCMOS	Dark Lord	Jump
April.EXE	Dark Avenger	La_la
Arab	Dark End	Leprosy
Bad Taste	DataCrime	Lesson_1.305
Bad Boy	Datalock	Manotoba
BadGuy	December 24th	MichelAngelo
Banana	Demon	Mindless.423.B
Bandit	Devil_Dance	SADAM
Barcelona	Die_Hard	Stoned
Beer	Dr Q	Surprise
Blood	Father Christmas	Wizard.312
Brothers	Foetus	Xmas in Japan
Bugs	Genesis 217	Yankee
Busted.572	Helicopter	Yankee_Doodle.2167
Chemist	Hello (A and B)	Zeleng

Types of Viruses and mode of Transmission:

Four types of viruses are known to exist. These include the following:

1. **Boot Sector Viruses (BSV):-** These type of viruses affect only the boot sector of the disk, whether floppy or hard disk. The way these viruses affect the disk is to copy itself to the boot area of the disk and moves the real system files to a different area of the disk. When you try to boot from that disk, the virus goes into the memory and tries to run the booting program from the disk. If this fails, you get the message "Non-system disk", even though you are sure it is. Even with this, the virus remains in memory.

When you insert a clean diskette into a boot sector infected computer, the boot sector of the diskette get infected. If you leave this diskette in the drive of a clean computer and try to boot from it, whether the booting is successful or not, the virus copies itself to the boot sector of the computer and so it spreads.

2. **File (program) viruses:-** These type of viruses infect only program files, files with the extension .EXE, .COM, .SYS, and sometimes .OVL. These viruses are spread when you share files with infected computers, either through a network or copying programs. Even when you purchase a software in its original diskette, there is a chance of infection from such diskettes. E-mail is a potential means of transmission of viruses.

Once an infected program goes into your hard drive, any attempt to run this program places the virus in the memory. The virus remains there even when you exit the program. A program loaded into the memory immediately gets a copy of the virus and so it spreads from program to program and from computer to computer.

This type of viruses affect the files by copying itself into a portion the executable file. The effect is that it either prevents the program from running or the program runs but very slowly. Even when it runs the virus, if it is the "noise making" type, begins to play some tricks on your memory, displaying some unwanted things on the screen along with your work. This is confusing and annoying. The very dangerous one will delete some files from the disk, rewrite the FAT and so scramble it or format the hard disk.

3. **Multipartite viruses:-** These type of virus are the most common. They have the characteristics of BSV and file (program) virus. That is, they can infect boot sector as well as program files. They spread faster because of this.
4. **Macro virus:-** This is relatively a new type of virus but it is fast becoming very popular. Its popularity is due to the fact that these viruses are written in fourth generation languages, such as the macro facilities available in word processors and spreadsheets, hence the name macro viruses.

These viruses are really dangerous because they attack mostly data files, and data files cannot be replaced once lost. For program files, they can always be replaced. While these do not affect the computer much, they can do havoc to data files by adding themselves to your vital information, making them difficult to edit. They are not yet very common in this part of the world, except probably with those hooked to the internet. We would soon have them as we begin to share files or continue to receive E-mails.

Protection against Virus:

There is no complete protection against viruses. However some protection is better than no protection. Following are ways you could employ to prevent virus infestation.

1. Do not share files with anybody. This is the best and sure way to prevent viruses, but unfortunately it is most unrealistic. It is impossible to have a computer without sharing files. If you do not receive data or information from anybody, you must at least buy and instal programs to your computer.
2. Do not leave diskette in your floppy drive (drive A: in particular) while booting up your computer. This would prevent BSV.
3. Backup your files often. This does not prevent viruses but a safeguard against loss of data. Your data are probably more important than your programs.
4. Suspect and be careful with any (and every) file coming into your system.
5. No matter how careful you are, there is always the possibility of viruses sneaking in without you noticing them until they start operation. Your best bet is to buy and install a good antivirus program. Below is a list of some common antivirus program.
 - a. F-Prot Fridrik Skulason
 - b. NAV Norton AntiVirus
 - c. Toolkit Dr Solomon's
 - d. MSAV MicroSoft Antivirus
 - e. CPAV Central Point AntiVirus
 - f. VirusScan McAfee Associate

It must be noted here that file hiding or write protecting files is not a solution to virus infections as some viruses are known to remove the write protection, copy themselves to the file and replace the write protection.

One sure way to prevent virus infestation is to properly install the antivirus program using the install (or setup) file that comes with the program. This would add the TSR virus detection program to either your config.sys or autoexec.bat file. For instance, Toolkit adds the following line to your autoexec.bat:

C:\toolkit\guard

This is usually the first line in the file, and it should be.

You can add virstop.exe as

Device=C:\F-Prot\virstop.exe in config.sys

or **C:\F-PROT\VIRSTOP** in autoexec.bat

Virstop.exe comes with F-Prot. It is best placed in the config.sys for the same reason

toolkit's guard is the first line in the autoexec.bat, that is, to be loaded to memory before any other program gets there and infect it.

These programs remain in memory for as long as your computer is on. When you insert a diskette into your drive and try to read from it, these programs check the boot sector of the diskette for virus, and reports any existence. If you try running a program, the antivirus programs first check the files for virus. If a virus exists in the file this program reports it and freezes your computer. These programs do not remove the virus, they only report their presence. So when you receive such report, the first thing you do should be to turn off your computer, then reboot from a "clean" disk and run your antivirus programs. Remember that using more than one antivirus program for scanning gives you a better protection.

The type of scanning we have are:

- a. Signature scanning
- b. Heuristic scanning
- c. Integrity scanning
- d. Generic decryption
- e. Behaviour Blocker

These are not discussed here for lack of space. Note, however, that no single antivirus program can be said to be the best, for the facilities in one might not be in the other, and the viruses detected and/or removed and repaired by one might not even be detected by another. This explains why you should use more than one antivirus program.

CONCLUSION

The computer is an electronic machine that could be used for almost anything imaginable, except of course making a man. To carry out their functions, computers receive data, process the data received, store or use the information generated for decision making.

As files are shared between computer users, viruses are spread. These viruses can be very harmful, even when they are not meant to be. Therefore, taking a few minutes to protect, and clean your system could save your hours, days or even years of work.

Stop the virus now; they are real.

BIBLIOGRAPHY

- Jaret, D, 1984: The good Computing book for Beginners Low priced Edition.
- Mainelli, T. 1997: Computer Viruses: Understand your PC'S Enemy. Smart Computing in Plain English Vol 8 (6).
- Marshal, P, 1985; Computer Aided Manufacture. The Agric Engineer Vol 40 (1) PP 22-27
- NAV Manual 1992: Using Norton Antivirus For Windows.
- Nwoye, M. C. 1990: Computer Application in Selection of, and Rating of a Single-Packed Air-conditioner. The Nigerian Engineer Vol 25 (4) PP 24-31
- Olutoye, F. A. 1988: The Computer and it's importance in Engineering. The Unilorin Engineer vol 1.