Computer Viruses

The terms "computer virus" and "virus" are used very loosely to describe "trouble" with computers. Computers are designed to read and follow instructions, computer viruses are programs similar to other computer programs. Computer viruses differ from other programs in their intended (or not intended) damaging behaviour.

Computer viruses have been made more illustrious by Hollywood movies such as "Independence Day", "The Net" and "Sneakers" who clearly portray one of the behaviours of viruses, the disruption of the normal behaviour or functionality of a computer system.

Viruses, worms, Trojan horses, and logic bombs are all unwanted, uninvited, potentially dangerous software, but there are important distinctions among them. Table 7.1 is one grouping for troublesome, unwanted programs. There is no univer-

Table 7.1 - Differentiation of 'Trouble' Programs by Host Requirements

Term	Requires Host?	Replicates?
Virus	*Yes*. A virus goal is to live through infections of other programs (hosts). Many viruses attempt to hide from being discovered.	*Yes*. Viruses make copies of themselves, infecting system boot sectors, master boot sectors, programs, or data
Worm	*No*. A host is not required, because worms typically 'live' as real programs on systems operating	*Yes*. A worm makes copies of itself as it finds the opportunity.
Trojan horse	*No*. The Trojan Horse is the program masquerading as a useful program while holding disruptive instructions.	*No*. Most Trojan horses activate when they are run and often destroy the structure of the current drive (FATs, directory, etc.), obliterating themselves in the process.
Bug, Logic bomb, Time bomb	*Yes*. Programmers cannot write a bug without also writing other code — although it's fair to say that most programmers do not intentionally write bugs. Logic bombs and time bombs are intentionally inserted in otherwise "good" code.	*No*. This code generally has better things to do than making copies of itself. Logic bombs and time bombs wish to remain hidden, with only their effects being visible. Bugs do just about every-

sally agreed grouping of troublesome programs, but groupings usually involve how these programs are started (triggered), their behaviour, and how they spread.

A host program is similar to a host organ sustaining the existence of an organic virus. To replicate is the ability a program has to make copies of itself (sustain life) to expand its infection and minimise the potential of existing viruses being destroyed.

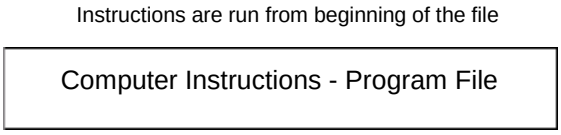
Storing Data & Instructions - The Corruptible File System

Discussions about viruses, misbehaving programs, should begin a reminder that computer programs are instructions for the computer to perform tasks. These computer programs are most commonly stored in the storage devices of the computer system, such as the Hard Disk and Floppy Diskettes.

The computer programs may either be the creations of the computer user, or by the supplier who may include hundreds of different files on the system to perform the tasks for which the computer was designed and acquired.

A simplification is to consider that a computer program is stored on your computer hard disk like the following block, where instructions for the computer to perform are read by the computer from left to right.

Diagram 7.1 A computer program file



Virus Types

Table 7.2 General Virus Types

What they are called	What they infect
File virus	Executables (program files). These
Macro virus	Data files. These are able to infect
Boot virus	Boot sectors of hard drives and floppy disks. These are not able to infect
Multipartite virus	Both executable files and boot sectors. These are able to infect over

When discussing viruses, the virus is often distinguished between four different types as shown in the Table 7.2. The File Virus, Macro Virus, Boot Virus, and Multi-partite virus.

Because a macro virus infects files, it technically is a file virus. However, because the layout of information in data files is quite different from normal program files, the anti-virus developers have had difficulty in developing detection and removal techniques and originally designated the viruses in a different category, which remains today.

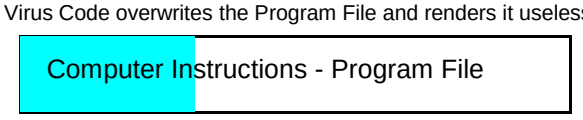
The incredible growth in macro viruses is also a good reason to highlight this group for its increasing disruption of work.

File Virus

A file virus attaches itself to a program file (the host) and uses different techniques to infect other program files. Three techniques for infecting an executable file is described here: overwrite, pre-pend, and append.

An *overwriting virus* places itself at the beginning of the program, directly over the original program code, so the program is now damaged. When you try to run this program, nothing happens except for the virus infecting another file.

Diagram 7.2 Overwriting Virus

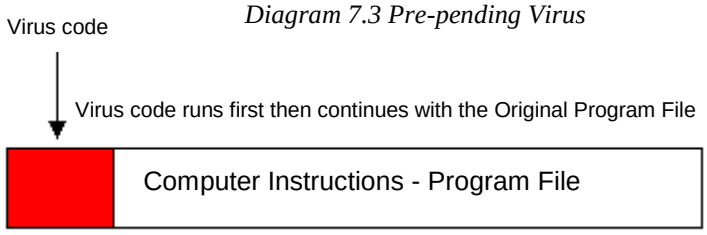


Such viruses are easier to detect, apprehend and destroyed by users and support staff. This virus spreads poorly.
The pure *pre-pending virus* may simply place all of its code at the top of your original program. When you run a program infected by a pre-pending file virus,

the virus code runs first, and then your original program runs.

An *appending virus* places a "jump" at the beginning of the program file, moves

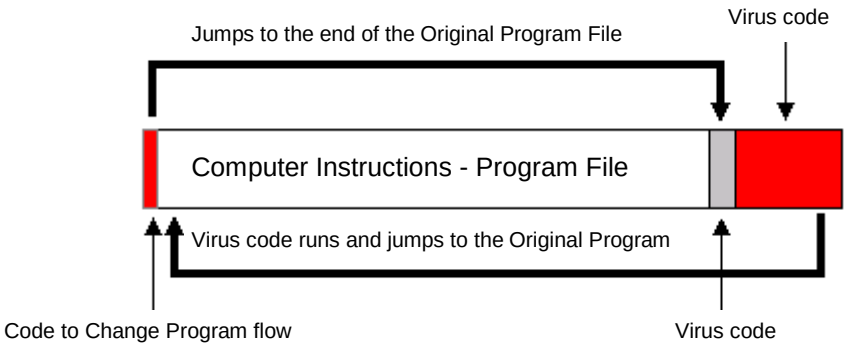
Diagram 7.3 Pre-pending Virus



the original beginning of the file to the end of the file, and places itself between what was originally the end of the file and what was originally at the beginning of the file. When you try to run this program, the "jump" calls the virus, and the virus runs. The virus then moves the original beginning of the file back to its normal position and then lets your program run.

The file viruses which proliferate, survive by infecting other files usually ‘infect’

Diagram 7.4 - Appending Virus



store a part of itself in computer memory (go memory-resident.) By staying alive in the computer RAM, a virus can monitor all actions and infect other program files.

If a file virus is memory resident, then it can infect another program file by waiting until that program file is opened by the operating system to run, while the file is open the virus attaches to that file. That file becomes infected (i.e., become a "carrier"), and it will go on to infect other program files.

File Based viruses have been most prevalent on MS-DOS based operating systems due to the poor ability of this operating system to secure against intrusions, and because there are so many machines using MS-DOS and MS-DOS based operating systems. (Microsoft Windows 95, and Windows NT support MS-DOS programs to a great extent so some programs live through these newer operating systems.)

File Based viruses have not been as prevalent for Microsoft Windows 95 nor Microsoft Windows NT because of the different ways in which these operating systems deal with files. Because Windows 95/NT supports MS-DOS programs, MS-DOS viruses live-on to some extent under the Windows OS.

Macro Virus

Macro Viruses commonly refers to viruses that infect documents created, used within other Programs. Macros are used by programs such as Microsoft Word, Microsoft Excel to allow users to customize and enhance the built-in capabilities of these products. To allow these enhancements, Applications Programs such as Microsoft Word, include a complete programming language that can be used for programming and customising the application environment.

Macro viruses work by making use of the programming language capabilities within Microsoft Word and similar products. By using the same techniques used on standard File Based Viruses. Macro viruses infect and spread by overwriting, pre-pending, appending, and a complete mixture.

Macro viruses are mostly prevalent for Microsoft Windows 95/NT applications since these have been the applications (such as Microsoft Word) that have a broad market and an extensive programming language. Specialised languages designed for use between different applications, such as Java and Postscript present a problem for applications using these programming languages without restraints against the programming languages causing destructive commands to be used.

Macro Viruses are exploding because people share data files more frequently than they share program files. As infected document files are shared more documents on different users machines become infected and an increasing number of virus infections propagate.

Macro Viruses are potentially more dangerous than normal File Based viruses because of the greater likelihood of their spreading, and because of the increasing probability that it will change your document without your knowledge.

An example of changes difficult to detect: A spelling mistake caused by a virus in a ten page document is difficult to find or realise. A numeric change by a virus in a ten page document of accounting numbers is more difficult to find and the side-effects may be huge.

Data! Data! Data$

As world economies increasingly become more dependent on information and the technology which provides the infrastructure, your data becomes more and more important to your business and career. Unwanted, unwarranted, and undetected changes to your data caused by viruses become more and more dangerous.

Boot Virus

Boot viruses infect System Boot Sectors (SBS) and Master Boot Sectors (MBS).

The MBS is located on all physical hard drives configured for use with IBM PC compatibles. It contains, among other data, information about how a physical disk is divided into logical disks, and a short program that can interpret the partition information to find out where the SBS is located. The SBS contains, among other data, a program whose purpose is to find and run an operating system.

Because these system areas are read during the booting process on all IBM-compatibles, boot viruses are operating system-independent and are therefore able

to propagate more effectively than file viruses.

The Booting Process

To better understand boot viruses, it is necessary to understand the booting process.

When an IBM compatible computer is turned on, the computer is physically configured to pass control to a part of the computer called the BIOS. The BIOS (Basic Input/Output System), controls the computer start-up process, initialises the Power On Self Test (POST) to check for the existence and 'normal' functionality of a number of the devices for a computer such as the keyboard, screen.

The Term 'boot' refers to the ability of the computer to 'pull itself up by its boostraps.' An old American saying that applies to how the computers can now start themselves up, unlike previous machines which required a lot of user intervention to start the operating system and other parts of the computer.

After the POST, the BIOS starts the operating system to take over the rest of the work.

No Diskette

Normally, no diskette is present, and the Master Boot Sector on the hard drive is read. The Master Boot Sector tells the BIOS how the hard disk is organised and where to find the System Boot Sector. Then the System Boot Sector of the hard drive is read, and the BIOS transfers control to the instructions in the SBS.

This process is the same for all IBM PC based systems including machines running MS-DOS, Windows, Windows 95, Windows NT, and OS/2.

Diskette in the Floppy Disk during Start Up.

The BIOS normally looks for the System Boot Sector on the floppy, reads it and attempts to execute the instructions.

If the diskette does not contain a recognisable System Boot Sector then you will see the following message on the screen:

```
Non system-disk or disk error.
Replace and strike any key when ready.
```

Unstated Viruses

The Macintosh and Unix present their own strange variants of viruses and trouble programs due to their unique capabilities. Similarly, because the Macintosh and many Unix machines do not share the same file structure nor startup sequences as IBM PC Compatibles these other systems generally do not have the same virus problems as described earlier.

Just because it is not mentioned here doesn't mean it doesn't exist. Programs are created by humans so any creative human who can develop a useful program for fellow earthlings usually indicates that another creative human can develop a program totally destructive to fellow inmates.

The War Against Viruses

Doom and Gloom, but there are means for combatting virus infections and viruses.

Viruses are a big problem, but they are not unsurmountable and a number of good practises, common-sense behaviours can resolve a number of the problems.

Commercial products also exist to help you detect (find) and remove virus infections. The use of effective tools and good computing practises will minimise problems with virus infections.

Prevention

Combating Boot Sector Viruses

Since boot sector viruses are most commonly spread by letting the virus start from the System Boot Sector on floppy diskettes, the greatest prevention technique is to **always remove floppy diskettes before starting up a machine.**

It is wise to check any new floppy diskette to be used in your computer, before you start using the diskette. Most anti-virus programs allow you to check whether a disk or diskette contains any known viruses.

Combating Macro Viruses

Macro Viruses spread by sharing documents with other people.

If you must use somebody else's document, it is always wise to use a current anti-virus product to check the document for any known viruses before using it.

To combat virus infections, the applications programs (such as Microsoft Word) now offer the user the opportunity to disable any macros within a document before opening the document. It is recommended that you 'disable' any macros within a document.

Combating File Based Viruses

In a corporate environment, or in our school context, the best preventative medicine against File Based viruses is to **never run unauthorised programs.** If your system administrator has not installed a program on the machine, it probably means that program has not been tested for viruses (among other things.)

If you want to install a program you like onto a machine, or just want to try it out, take the time to learn how to use the anti-virus programs to test the programs and disks for any known viruses before you use them.

The Cure

Cures are solutions after the fact, and commercial anti-virus products spend as much effort in preventing virus infections as well as in removing, cleaning virus infections.

There are a number of these anti-virus tools on the market, but for our purposes the key features we should look for in an anti-virus product is listed below.

- Detect and Clean Boot Viruses
- Monitor the system to prevent Boot Virus infections
- Detect and Remove Macro Viruses
- Monitor the system to prevent Macro Virus infections
- Detect and Remove File Based Viruses
- Monitor the system to prevent File Based virus infections

The better an anti-virus product is in providing the above services, the better they are for our purposes. The use of fancy terms to describe what they are doing adds little to whether they can prevent the virus infections we have discussed so far.

Actions speak louder than words.

A note on anti-virus packages

Between 1993 - 1997 the anti-virus tools with the greatest ability to prevent virus infections, detect and remove existing virus infections have **never** been by the popular brands, marketed anti-virus packages.

Anti-virus suppliers can be the biggest misinformers about the true needs of the computer users and have in recent years been responsible for scare-mongering (creating fear to increase their product sales) of incredible proportions.

If you are ready to buy an anti-virus package and you are not willing to take the time to understand what they are for, and to check out the different not so popular packages then you are most likely to buy something in a glossy package that will also not give you near as good protection as lesser known products.

Conclusion

Remember, lost programs, lost data, and even damaged computers can either be repaired or somehow obtained. What cannot be retrieved is the time you and your computer staff lose when a virus infection causes you to reinstall programs, recreate data, test computers.

Anti-Virus Programs

Dr. Solomon
Thunderbyte http://www.tbav.com.au
McAfee Viruscan

Review Questions

Reference: Computer Viruses, Course Notes
Secondary Storage
MS-DOS A closer look Part II

To help you verify your understanding of this topic here are some self-examination questions.

- What is a virus
- Why are viruses potentially dangerous
- What is the difference between macro and file-based viruses

Give 4 methods that one can use to minimize viral attacks.

Give a reason why people should use several ways to counter virus attacks.

Sources and References

Norman Data Defense Systems, Norman Book on Viruses, (n/a,Norman Data Defense Systems, n/a)
Rosenberg, Rob, Michelangelo Fiasco: a Historical Timeline, (O'Fallon, n/a, 1992)
Stiller Research Virus News Page
Garfinkel, Simon and Gene Spafford, Practical Unix & Internet Security 2nd Ed., (Sebastopol, O'Reilly & Associates, Inc., 1996)

http://antivirus.cai.com - The InnoculateIT anti-virus package from CAI

http://www.tongatapu.net.to/compstud/ - Computer Studies Course Notes
http://www.tongatapu.net.to - **Tonga** on the **'NET**

Tonga on the **'NET** is available on all networked computers at Queen Salote College and participating schools.