CodeBreakers Magazine
Security & Anti-Security - Attack & Defense

Examining Viruses

by Giovanni Tropeano

Vol. 1, No. 2, 2006

Abstract:
Let's look at what viruses are, the different types of viruses, and how each of these types infects your computer.

Virus Attacks

By Giovanni Tropeano

Is it virii, or viruses? - Viruses. :) I have to admit, I am fascinated with virus programming. Not sure why, but I am always reading about them, reading up on how to defeat them, and even coding them for my own educational purposes. I decided to write this high-level overview of virii that may help to give you a better understanding of the different types of viruses out there. So, let's get started...

1 Introduction

A virus is a program that causes damage to the components of a computer or to the files stored on your computer. A computer can acquire a virus through e-mail, file downloads, virus-infected Compact Disks (CDs), and floppies. Viruses such as script viruses are designed to automatically spread on a network.

Virus attacks can destroy files, hard disk drives, or other hardware or software components of a computer. Viruses attach themselves to an existing file or replace an existing program. In order to protect your computer from viruses, you need to take certain precautions, such as disabling e-mail from unknown senders and installing antivirus software on your computer. The Internet security policy is of prime importance in organizations with a Local Area Network (LAN) to maintain data security and network security. Internet Security Policy depends on the organizational setup and differs from organization to organization.

In this article, I will discuss various types of viruses and the effects of virus attacks. Depending on how long this article turns out to be, I'll also possibly discuss prevention.

2 The Many Forms of a Virus

Viruses can be categorized based on whether or not they infect **operating systems**, **files**, or **disks**. Some of the commonly known viruses are:

- Boot sector virus
- File virus
- Macro and script virus
- Stealth virus
- Polymorphic virus

I will discuss each of these in moderate detail.

3 Boot Viruses

Whenever you switch on your computer, the boot process takes place. The first sector of the hard disk contains a program known as the Master Boot Record (MBR), which searches for the location of the operating system (OS) on the hard disk so that the OS can be loaded into the Random Access Memory (RAM). MBR performs this task with the help of a partition table that contains the addresses of all the hard disk partitions. As soon as you power on your system, the boot process takes place. The Master Boot Record (MBR) is a program located in the first sector of the hard disk. It searches for the location of the OS on the hard drive so the OS can be loaded into the RAM. MBR performs this task with the help of a partition table. That table contains the addresses of all the hard disk partitions. The boot sector virus does not allow the computer to start. *The Bastards*. The virus infects the boot sector or the MBR of a computer by replacing the MBR code with **virus code**.

There are two methods that I know of by which the boot sector virus replaces the MBR code. The virus either copies the MBR code to a different file and writes the virus program in MBR or overwrites MBR with the virus program. When the MBR code is replaced with the virus code, the virus spreads to all the disk partitions that MBR reads to find the OS. Since MBR copies the OS to the RAM, the virus infects the RAM also.

The boot sector virus is repaired using a Repair disk, which is a floppy disk that is used to repair and restart Windows when the operating system is damaged. The Repair disk has a copy of all the startup files that are used to boot the computer. When the Repair disk is run, the startup files in the disk overwrite the infected MBR. You can also resolve the boot sector virus by starting your computer from the installation disks and using the Recovery Console commands, such as FIXBOOT and FIXMBR.

4 File Virus

File viruses almost always attach themselves to executable files with diffetent extensions and corrupt the file when the file is opened. File viruses are classified depending on how the virus infects the files. The following are the various types of file viruses:

- Overwriting virus
- Parasitic virus
- Companion virus
- Link virus
- Worm virus
- OBJ/LIB viruses
- Source code virus

5 Overwriting Virus

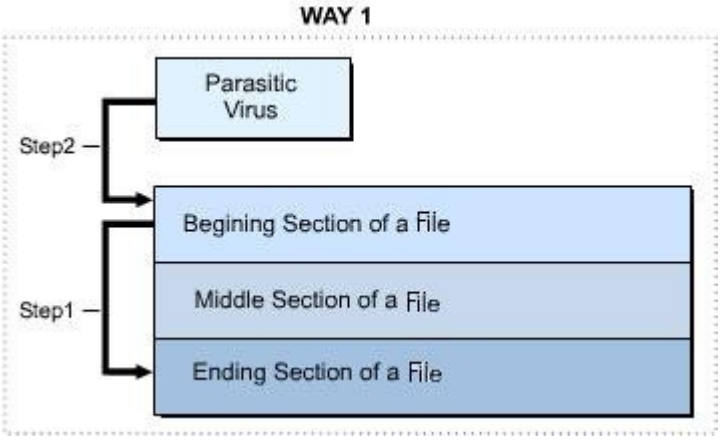
The overwriting virus overwrites the file to which the virus is attached. The contents of the file are replaced with virus code. Whenever an infected file is executed, the virus code replaces the original code and starts spreading to other programs running in the system.

An executable file has two parts, EXE-Header and EXE-Body. EXE-Header is placed at the beginning of an executable file and contains information about the executable file, such as information about the relocation tables and the status of the registers. EXE-Body contains the code of the executable file. A file virus can infect EXE-Header or EXE-Body. If the file virus infects EXE-Header, the executable file works properly but the header is destroyed. The infected header, in turn, infects the memory. When the file virus infects EXE-Body, the executable code is infected and the file does not function properly.

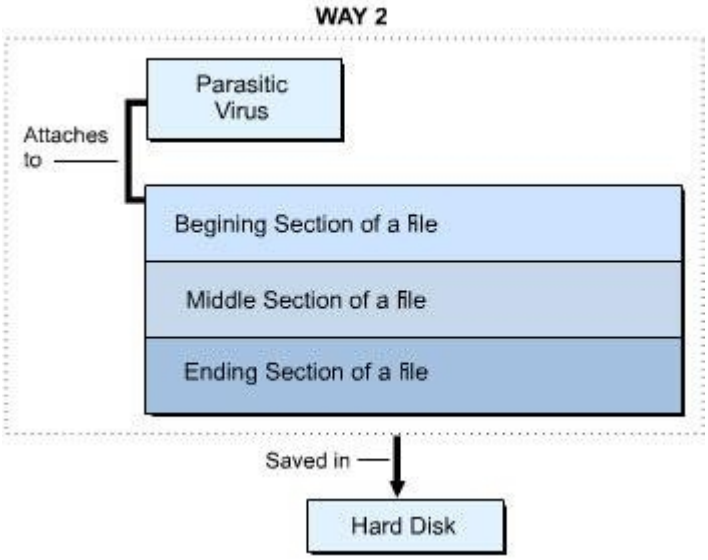
6 Parasitic Virus

A parasitic virus is a type of file virus that replaces the segments of a file by the virus code in several ways. A parasitic virus infects the .com and .exe files. Parasitic viruses attach themselves to a file in the following ways:

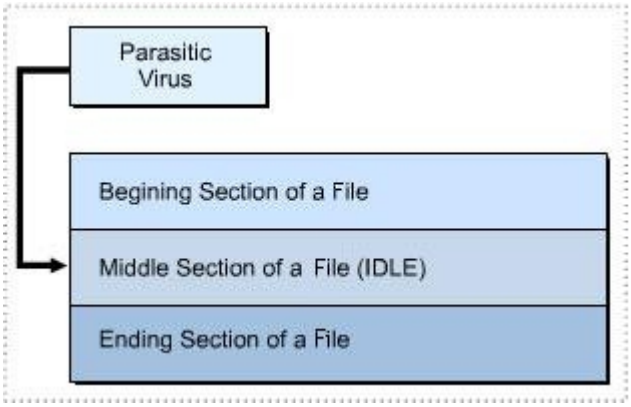
1. Virus attached to the beginning of a file: In this case, the parasitic virus transfers the contents at the beginning of the file to the end. The parasitic virus places itself at the beginning of the file, as shown in this picture:



2. Another method by which the parasitic virus works is by placing a copy of itself in the main memory of the computer and then attaching itself to a file, as shown in this picture:

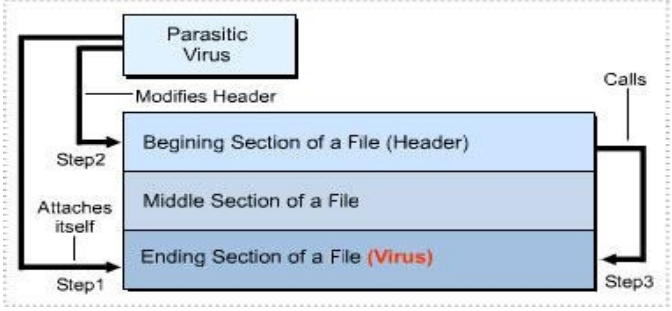


Virus attached to the middle of a file: In this case, the parasitic virus infects a file by attaching itself to the freed space at the middle of the file, as shown here:



Another method by which the parasitic virus attaches itself to a file is with the help of the relocation table. The parasitic virus determines the address of the idle or empty parts of a file and attaches itself to those parts.

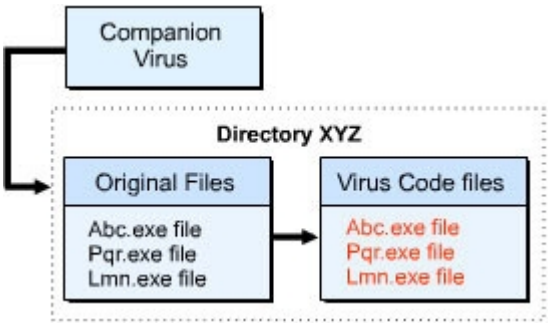
Virus attached to the end of a file: In this case, the parasitic virus attaches itself to the end of a file. The parasitic virus changes the first few bytes of the header of the file to force the header to call the virus code instead of the other sections of the file. My next picture shows how the parasitic virus is attached to the end of a file:



Note: The file here refers to an .exe file or a .com file.

7 Companion Virus

A companion virus infects a file in such a way that the original file is not disturbed or modified in any manner. The companion virus creates a copy of the original file and saves the copy with a different extension at the same location as that of the original file. The file that is newly created contains the virus code. The next picture shows the working of a companion virus:



The companion virus also uses other operating system properties to infect files. For example, the companion virus uses a property of the operating system by which the virus executes the batch files instead of the .com and .exe files. In this case, whenever you try to execute a .com file or an .exe file, MS-DOS executes the corresponding batch files that contain the virus.

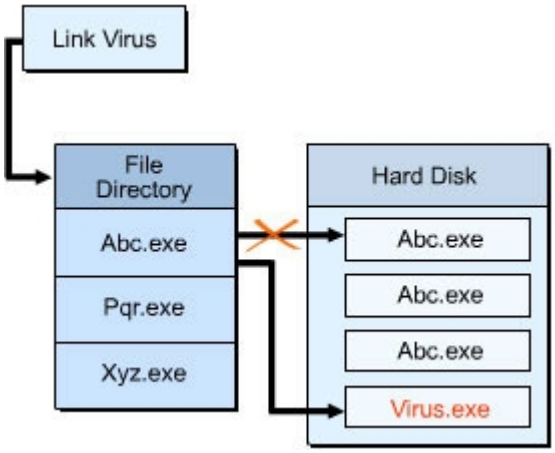
Companion viruses can also use the path property of MS-DOS to infect files. In this case, the companion virus creates a copy of the .exe files and places them at a higher level in the hierarchy. The file copies contain the virus code. As a result, whenever you try to execute the .exe file, MS-DOS encounters the copy of the file with the virus code first and executes the file.

Note: MS-DOS has a hierarchical file system structure with the root directory at the top of the hierarchy followed by the directories, subdirectories, and files. The path describes the route MS-DOS follows from the root through the hierarchical structure to locate a folder, directory, or file.

8 Link Virus

A link virus links itself to a file but does not modify the original file. Link viruses manipulate the structure of the file system and force the operating system to execute the virus file instead of the original file to which the virus is linked. The link virus is also known as cluster virus because the link virus places itself in a cluster of the file system. The link virus then replaces the cluster address of the original file with the address of the file with the link virus. As a result, whenever you try to execute the original file, the file system will point to the virus file and execute the file.

My next picture shows the working of link viruses:



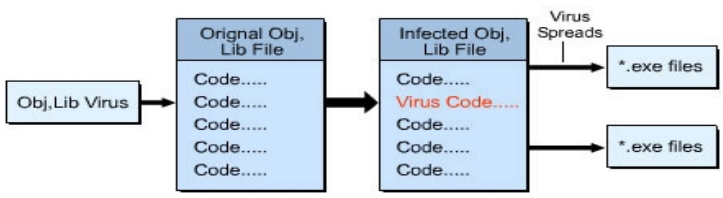
You can clean the files infected with link virus using antivirus software. You can also clean the link virus by changing the extension of all the .exe files to a different extension. You need to restart the computer and run the CHKDSK command. Now you can rename the executable files to their original names and run the CHKDSK command again.

9 Worm Virus

File worms can multiply at a very fast rate and spread the virus code to various disks on the directory. A worm virus gives a special name to the virus files so that you cannot detect that the file is a virus file. Worm viruses spread to various parts of a computer and wait for the execution of the virus file.

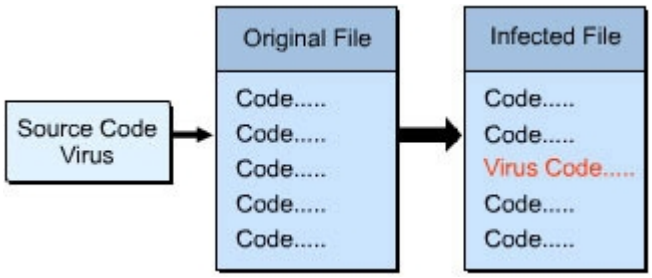
10 OBJ/LIB Viruses

The OBJ/LIB viruses modify the object module files and the complier library files, respectively, by inserting the virus code in the original files. The virus code that is inserted in the object or library files is in the format of the object or library files, respectively. When the virus code is inserted, the object or library files are infected but the virus does not spread directly. The virus spreads and activates itself when the .com or .exe files linked to the infected object or library files are executed. My nexy picture shows the working of the OBJ/LIB Viruses:



11 Source Code Virus

These viruses modify the source code of the original file by inserting the virus code in the original file. The virus executes when you execute the original file. You will notice the virus only after the infected file is compiled and executed. Next picture shows the working of the source code virus:



12 Macro and Script Viruses

Macro viruses are written in the form of a macro and are embedded in a document such as a Microsoft Word document. A macro is a collection of commands or keystrokes that is executed when a specific event occurs, such as opening the document or closing a document. A macro virus infects the applications that use macros, such as Microsoft Word or Microsoft Excel. A macro virus is an autoexecutable virus that can replicate and copy itself to other documents.

Macro viruses affect Word documents through the Word templates. There are three types of macro viruses that can infect Word documents:

- Auto-Execute Macro: AutoExec is an autoexecute macro of Word that macro resides in the startup directory of Word and executes whenever Word is started. The Auto-Execute macro virus works similar to the AutoExec macro. Auto-Execute macro viruses are stored in the global template of the startup directory of Word and are executed every time Word is started.
- Auto Macro: Auto macros are macro viruses that are executed in the following situations: opening a Word document, closing a Word document, creating a new document, or quitting a Word document. You can disable the auto macro by pressing the Shift key when opening Word documents or by executing the DisableAutoMAcros Word.Basic command in a macro.
- Macros with command names: Macros with command names are the most dangerous type of macro viruses because you cannot disable these macros. A macro with command name has the same name as that of an existing Word macro command. For example, a macro virus with the name, FileClose, stored in the global template of Word will replace the original Word macro command. Whenever you select File-> Close, the macro virus will be executed instead of the original Word command.

13 Script Virus

Script viruses are created using scripting languages, such as VBScript and JavaScript. A script virus reaches a computer through e-mail messages and e-mail attachments. Script viruses also spread through HTML pages that can have virus scripts embedded in their code. Script viruses can affect computer hardware components and file system. Some script viruses spread not only on your computer but also to all the e-mail addresses stored in your address book. If you have set your e-mail program to automatically open Word and Excel files, the virus will be activated. You may get virus alerts when you try to open an attached document. You need to close the browser window and scan your computer for viruses after receiving the virus alert.

14 Stealth Viruses

Stealth viruses hide their identity and infect your computer by manipulating the system functions used to read files and system sectors. When you request for the file that is infected by a stealth virus, you will view the original file if the virus is active in the memory. The stealth virus encrypts the original information and keeps it safe in the infected sector. It is very difficult to identify stealth viruses because the virus shows the original contents of the infected file.

Stealth viruses are of two types, File Stealth viruses and Full Stealth viruses. File Stealth viruses infect the .exe and .com files by changing the size of the original files. When you use CHKDSK to repair the files, the infected files are completely destroyed. Full Stealth viruses temporarily store the normal calls to the file locations and make the file appear virus-free by subtracting the size of the virus program from the file size.

You can repair the stealth virus by restarting your computer using a clean bootable diskette. You can also use antivirus software to identify and remove stealth viruses.

15 Polymorphic Virus

Polymorphic viruses manipulate their code frequently so that it becomes impossible to detect and disable them. Polymorohic viruses are of two types:

1. Polymorphic Viruses that can change their code whenever they infect a file or replicate themselves. Another method by which the virus code is changed is by adding some nonfunctional code to the virus file. As a result, the virus file changes and appears to be a new file. In this case, the scanning programs of antivirus software cannot detect a polymorphic virus easily.
2. Polymorphic Viruses that can encrypt their virus code and have a nonconstant key. The decryption routine is different for each changed copy of the polymorphic virus because the decryption routine is also modified whenever a new copy of the virus is created.

You can write a polymorphic virus program using a toolkit known as Mutation Engine that can also convert an existing virus into a polymorphic virus.

16 Summary

Well, that about covers all the basics. I hope you have come out of this article with a little more knowledge of virii and the different types there are. Unfortunately, I won't get to the prevention methods I wanted to, as this article was much longer than I intended.