

An Introduction to Viruses and Malicious Code, Part One: Overview

Brad Griffin 2000-11-06

An Introduction to Viruses and Malicious Code, Part One: Overview

by Brad Griffin (gryphonn@austarnet.com.au)

last updated Nov. 6, 2000

You worked late last night, getting the final details together for a contract that could pull your business out of the red and generate plenty of new work. This could be the break that puts you in front of the big guys. Next morning you jump onto the workstation to print the tender so you can make the noon submission deadline, but something is wrong. Your system isn't responding. "Must be another computer lockup", you think as you push the 'reset'. However, the computer doesn't reboot. In fact, it doesn't 'do' anything.

You just became a victim of the 'Chernobyl' virus. Unfortunately, the trouble has just started. The [virus](#) has probably spread to the other computers on your network, rendering them useless. Depending on whether your systems maintenance people have spare BIOS chips or mainboards available, you could be offline for days. When you do get the computers up and running, the virus may have wiped out your crucial documents. One small computer virus has put your [network](#) out of commission. It may have wiped out your business at the same time.

An Introduction to Viruses

In this, the first of a two-part series, we will introduce you to [viruses](#) and other [malicious code](#) that can threaten your data and system security. We will discuss the different types of viruses and malicious code, what they are, how they infect your computer and what damage they can cause.

In the second part of this series, we will describe how you can protect yourself and your valuable information against malicious code and discuss a variety of recovery techniques in the event of a virus 'attack'.

What is a Virus?

Simply put, viruses are small programs designed with (usually) malicious intent that attach themselves to other programs or files. They are capable of copying themselves throughout a computer or computers. They are called viruses because of the way they emulate their

biological namesakes. A virus will infect healthy programs in a host computer and then spread to other healthy hosts, infecting them as well. Just as biological viruses range from being quite harmless to lethal, computer viruses may simply cause a harmless message to appear on your screen occasionally, or may render your system inoperable.

Types of Viruses

Viruses have been categorised into several different types according to the ways in which they infect a system, the part of the system they affect or their behaviours.

File Infector Viruses

File infector viruses are those that infect other files or programs on your system. They operate in a number of ways. Once the original 'host' program is run, the virus can stay resident or 'live' inside your systems memory (RAM) and infect programs as they are opened, or they can lay dormant inside another program. Each time that program is run, the virus will infect another program or file.

A second, more complex file infector is one that doesn't alter the program itself, but alters the route a computer takes to open a file. In this way, the virus is executed first, and then the original program is opened. If a program or file that is infected with a file infector virus is passed from one computer to another, over a network or via floppy disk for example, the virus will begin infecting the 'clean' computer as soon as the file or program is opened.

Boot Sector Viruses

Whereas file infector viruses infect programs on a computer's hard drive, boot sector viruses can infect hard drives and removable disks, such as floppy disks. The boot sector is an area at the beginning of a hard drive or other disk where information about the drive or disk structure is stored. Symptoms of a boot sector virus may be a computer that is unbootable or gives error messages upon booting. Frustratingly, boot sector viruses may be present with no noticeable problems.

One thing should be noted about floppy disks. It does not matter whether the floppy disk is a 'bootable' disk or not, if the disk is infected with a boot sector virus and you inadvertently leave the disk in the drive when you reboot the computer, the virus can still be executed. Ways of

preventing this will be discussed in part two of this series.

Macro Viruses

Macro viruses are by far the most common type of malicious code found today. This is due to the popularity of software such as Microsoft Office and others such as Corel Draw, which use the macro programming languages extensively in the products.

Macro viruses use an application's own macro programming language to distribute themselves. Macro viruses do not infect programs; they infect documents. Macro viruses typically arrive in an infected document, a price list written with MS Word for example. When the file is opened, the virus infects the base template on the victim computer, in this case Normal.dot. Normal.dot is the 'framework' that Word documents are created on. Once this template is infected, every document that is opened from then on will be infected as well, making all documents created or opened in Word a carrier of the macro virus. Macro viruses have been written for most Microsoft Office applications, including Excel, Access, PowerPoint and Word. They can also be found in Lotus AmiPro and Corel products to name a few.

One more warning about macro viruses is that they are not platform specific. They can be found and spread through Macintosh, DEC Alpha, Microsoft NT and Microsoft Windows. In other words, just because you received a Microsoft Word file from a colleague using a Macintosh, doesn't mean you will not be infected by a macro virus embedded in that document.

Worms

A [worm](#) is a piece of code that can make fully functional copies of itself and travel through a computer network and/or across the Internet through a number of means. A worm does not attach themselves to other programs like traditional viruses, but creates copies of itself, which in turn create even more copies. The computer 'worm' is so-called because of the way in which 'rogue' computer code was originally detected. Printouts of computer memory locations would show random 'wormhole' patterns, much like that of the patterns on worm-eaten wood. The term eventually became shortened and used to describe viruses that could 'worm' or propagate across networks and the Internet, leaving copies of themselves as they travelled.

Worms are prolific due to the fact that most are created using simple scripting languages that can be created with a text editor and become fully functional 'programs' under the right

conditions. For example, if you were to obtain a copy of the 'I Love You' worm and changed the files extension from vbs to txt, you could safely open the file in Notepad and view the structure of the worm. This makes the vbs script worm extremely popular among the '[script kiddy](#)' fraternity, as it takes no (or very little) programming knowledge to modify an existing worm and release it into the wild (when a virus is circulating in the computing community or throughout the Internet, it is said to be 'in the wild'.)

Trojan Horses

[Trojan horses](#) are named after the wooden horse from Greek mythology in which Greek soldiers snuck into the city of Troy. Accordingly Trojans are malicious programs that sneak into a victim computer disguised as harmless software. Trojans may also be 'wrapped' inside another program so that when the original innocent program is installed, the Trojan program is installed as well.

The most commonly described Trojan has a [payload](#) that will allow a user on another computer somewhere else in the world to gain full control and access to the files on your computer. In this way, they can be used to launch [denial of service](#) attacks such as those that brought down Yahoo! and E-bay early in 2000.

Trojan horses typically consist of two parts, the server and the client. The server is the part that is installed on the victim computer. When the server is installed, it allows the remote client to send commands to the computer as if the other person were sitting at the keyboard. The remote attacker can upload and download files, delete and create files on your system, play with the CD drive and generally control most aspects of the victim machine. Most of the approximately 550 known Trojans will send some sort of message to the attacker to let them know the server is running on the computer. Therefore, every time you connect to the Internet the person who sent the Trojan will know that the system is online and open for abuse.

Legal Risks Associated with Trojan Infections

In addition to the effects previously mentioned, a Trojan infection may affect you legally. If your network has been used surreptitiously by an attacker as a launching pad for a denial of service or other attack, you may be held responsible for any legal damages. Further, a Trojan on your system could be used to gain access to another network to steal sensitive information. If the intrusion is traced back to your computer, it may be difficult and expensive to defend

yourself against prosecution.

There is also the risk of losing your sensitive business information; contacts, blueprints, liabilities, etc to a competitor eager to gain an advantage over you. Imagine how easy it would be for a competitor to undercut you if they had access to all your customer accounts and contact details.

Hoax Viruses

There are hundreds of hoax viruses that spread like chain letters through e-mail. Although they cause little or no long-term damage, these hoaxes can be as disruptive as real malicious code. The standard response of most people when receiving a virus warning is to pass it on to all people in their organisation and most likely everyone else in their contacts lists. This sets up a chain reaction that not only wastes Internet bandwidth, but also wastes the valuable time of recipients.

Further, a hoax can be damaging to a company's reputation. For example, NVision Design Inc produced three small games prior to Christmas of 1999. A virus hoax was spread worldwide that these games (Frog-a-pult, Elf-Bowl and Y2K game) contained a delayed action virus that would wipe out the users hard-drive. Not only did this cause damage to the reputation of the games' developer Vectrix, it also caused a deluge of e-mails in peoples' mail servers and inboxes.

How Can a Virus, Worm or Trojan Infect Your System?

Malicious code can be spread through just about any computer medium. They can arrive on an infected floppy disk and infect your system when a file on the disk is opened. Worse still, a floppy disk could be inadvertently left in the computer when it is shut down. Upon reboot, if the floppy is infected with a boot sector virus, the infection will be transmitted to your system.

The most common methods employed to spread viruses and worms are either through e-mail as attachments or through IRC (Internet Relay Chat). Typically, in the case of e-mail, a message will arrive with an attachment, the user clicks on the message and the code is executed immediately. Viruses are capable of bringing down entire networks by clogging e-mail servers with copies of themselves. Some viruses will repeatedly extract addresses from e-mail 'address' books and send themselves to the recipients. Some contact lists can generate

potentially thousands of messages, causing massive network bandwidth problems.

Don't think that just because your new software program is in a shrink-wrapped box it is virus-free either. Viruses have been found on software disks distributed by major software companies, as well as on computer systems that have come fresh from the factory. In 1995, Microsoft inadvertently released a Compact Disc containing the 'Concept' macro virus and as late as last year, IBM shipped an undisclosed number of Aptiva computers infected with the CIH (Chernobyl) virus.

Potential Damage

Virus infection can have a variety of effects on an infected system. Some viruses may simply take up space on the computer hard drive until you receive 'low disk space' messages from the system. Others may pop-up messages on a particular date or change system icons. For example, the 4K virus will pop up a message on the screen, 'FRODO LIVES!' on the 22nd of September. The Tentacle2 virus will change your icons to that of a purple 'monster'.

Other viruses are potentially much more damaging. The CIH, or Chernobyl virus will, if not detected and removed, overwrite files on your hard disk and destroy the BIOS information on your computer. Chernobyl spreads easily and hides in an infected system until the 26th of a particular month depending on which variety it is. The BIOS chip is the 'heart' of your computer. If the information contained in this chip is overwritten by CIH, the system will become unusable, meaning the chip will have to be replaced. However, on some systems, the chip cannot be removed, which means the entire main-board of the computer will have to be replaced, an expensive, time consuming process.

Conclusion

This article, the first of a two-part series, has intended to serve as an introduction to the different types of malicious code: viruses, Trojan horses and worms. In the second part of this series, we will detail a number of procedures that can be implemented to minimise the threat of virus, worm and Trojan infections. Topics will include safe computing habits, policy implementation and e-mail security and safety.

To read **An Introduction to Viruses and Malicious Code Part Two: Protecting Your Computers and Data** , click [here](#).

Relevant Links

For more information on viruses, please visit the [Security Focus Virus Focus Area](#)

[All About Viruses](#)

From Dr.Solomon.com

[Computer Virus FAQ for New Users](#)

From FAQ.org

[Computer Virus Help](#)

By Henri Delger

[Privacy Statement](#)

Copyright 2006, SecurityFocus