Information Techniques in Research

# Computer Viruses and Related Threats

THE TERM *COMPUTER VIRUS* is often used to refer to any software that is intended to damage computer systems or networks. More narrowly it is used to refer to a particular type of "terrorist" software—namely a program that performs some unwanted function while hiding within a legitimate program and that copies its hidden code to other programs, thereby infecting them. Other categories of malicious software include—

*Trojan horse*--a program that the user intentionally installs for some useful purpose but that contains hidden code that performs mischievous or harmful acts.

*network worm*--a program that uses network connections and network vehicles to spread from system to system. Once within a system, the worm can behave as a computer virus, implant Trojan horse programs, or perform other disruptive actions.

*macro virus*--a computer virus that resides within data files as one or more macros (which are mini-programs stored with data in the files created by such programs as *Word* and *Excel*).

*boot sector virus*--a virus that spreads when computers attempt to boot from infected floppy disks or when infected computers access floppy disks.

*polymorphic virus*--a virus that changes it characteristics with each infection, making its detection more difficult.

Some viruses do little harm; others delete files, change the order or digits in entries in a spreadsheet, or disable the computer's operating system. Viruses are often designed to remain undetected until they have infected other programs or other computers. A *time bomb* describes a virus that is activated on a certain date or after a certain period of time. A *logic bomb* is activated by a certain sequence of events, such as the virus having replicated a specified number of times, or the program that contains it having been run a specified number of times.

## What to do about viruses

*Brief summary:* (1) Use an antivirus program and keep it updated. (2) Back up your files regularly.

There are a number of *antivirus* programs that you can install on your computer to continually look for viruses and to help you remove those that it finds. UF's Center for Instructional and Research Computing Activities (CIRCA) has arranged a 3-year site license for one such program: McAfee's *VirusScan* software. The license includes a provision that allows UF faculty, staff and students to use *VirusScan* at home. *VirusScan* is among the programs on the UF Software CD, available for $3.18 at UF Bookstore's Technology Hub.

Anti-virus software works by scanning for *known* viruses. Because new viruses are continually created and set loose, antivirus programs cannot completely protect you from virus damage. To be completely safe, you would have to completely isolate your computer from direct or indirect access by other computers—thereby foregoing the advantages of networks, e-mail, and new software. Here are some ways to minimize the chances of infection:

- Install anti-virus software and update it periodically.

- Don't try to start your computer with a disk in the floppy drive. It won't start anyway until you remove the floppy, and, in its attempt to start, it may become infected with a boot sector virus that the disk picked up elsewhere.

  The normal boot sequence (i.e., the order in which drives are checked for the start-up files) is A:, C:. This allows you to start your computer with a "boot disk" even if something is wrong with the start-up files on the hard drive or with the hard drive itself.

- Be wary of free programs, especially if you do not know their origins (for instance, if they arrive as attachments to e-mail from unknown senders.)

You can never be sure that an undetected virus won't destroy your files or make them inaccessible. For that matter, you can lose your work in a variety of other ways (hard disk crash; sabotage by a spurned lover, loss of computer by fire or theft, etc.). *Therefore you should make regular backups of the files you value and, for especially important ones, you should keep one set of backups in a building other than the one that houses your computer.*

## *Some details*

The text below is copied (with deletions) from National Institute of Standards and Technology Special Publication 500-166: "Computer viruses and related threats: a management guide," by J. P. Wack and L. J. Carnahan, 1989. (http://csrc.nist.gov/nistpubs/sp500166.txt) [Being a U.S. government document, it is in the public domain.]

Computer viruses are the most widely recognized example of a class of programs written to cause some form of intentional damage to computer systems or networks. A computer virus performs two basic functions: it copies itself to other programs, thereby infecting them, and it executes the instructions the author has included in it. Depending on the author's motives, a program infected with a virus may cause damage immediately upon its execution, or it may wait until a certain event has occurred, such as a particular date and time. The damage can vary widely, and can be so extensive as to require the complete rebuilding of all system software and data. Because viruses can spread rapidly to other programs and systems, the damage can multiply geometrically.

Related threats include other forms of destructive programs such as Trojan horses and network worms. Collectively, they are sometimes referred to as malicious software. These programs are often written to masquerade as useful programs, so that users are induced into copying them and sharing them with friends and work colleagues. The malicious software phenomena is fundamentally a people problem, as it is authored and initially spread by individuals who use systems in an unauthorized manner. Thus, the threat of unauthorized use, by unauthorized and authorized users, must be addressed as a part of virus prevention.

The term *computer virus* is often used in a general sense to indicate any software that can cause harm to systems or networks. However, computer viruses are just one example of many different but related forms of software that can act with great speed and power to cause extensive damage -other important examples are Trojan horses and network worms. In this document, the term *malicious software* refers to such software.

**Trojan Horses**

A Trojan horse program is a useful or apparently useful program or command procedure containing hidden code that, when invoked, performs some unwanted

function. An author of a Trojan horse program might first create or gain access to the source code of a useful program that is attractive to other users, and then add code so that the program performs some harmful function in addition to its useful function. A simple example of a Trojan horse program might be a calculator program that performs functions similar to that of a pocket calculator. When a user invokes the program, it appears to be performing calculations and nothing more, however it may also be quietly deleting the user's files, or performing any number of harmful actions. An example of an even simpler Trojan horse program is one that performs only a harmful function, such as a program that does nothing but delete files. However, it may appear to be a useful program by having a name such as CALCULATOR or something similar to promote acceptability.

Trojan horse programs are introduced into systems in two ways: they are initially planted, and unsuspecting users copy and run them. They are planted in software repositories that many people can access, such as on personal computer network servers, publicly-accessible directories in a multi-user environment, and software bulletin boards. Users are then essentially duped into copying Trojan horse programs to their own systems or directories. If a Trojan horse program performs a useful function and causes no immediate or obvious damage, a user may continue to spread it by sharing the program with other friends and co-workers.

Trojan horse programs are named after the use of a hollow wooden horse filled with enemy soldiers used to gain entry into the city of Troy in ancient Greece.

**Computer Viruses**

Computer viruses, like Trojan horses, are programs that contain hidden code which performs some usually unwanted function. Whereas the hidden code in a Trojan horse program has been deliberately placed by the program's author, the hidden code in a computer virus program has been added by another program, that program itself being a computer virus or Trojan horse. Thus, computer viruses are programs that copy their hidden code to other programs, thereby infecting them. Once infected, a program may continue to infect even more programs. In due time, a computer could be completely overrun as the viruses spread in a geometric manner.

An example illustrating how a computer virus works might be an operating system program for a personal computer, in which an infected version of the operating system exists on a diskette that contains an attractive game. For the game to operate, the diskette must be used to boot the computer, regardless of whether the computer contains a hard disk with its own copy of the (uninfected) operating system program. When the computer is booted using the diskette, the infected program is loaded into memory and begins to run. It immediately searches for other copies of the operating system program, and finds one on the hard disk. It then copies its hidden code to the program on the hard disk. This happens so quickly that the user may not notice the slight delay before his game is run. Later, when the computer is booted using the hard disk, the newly infected version of the operating system will be loaded into memory. It will in turn look for copies to infect. However, it may also perform any number of very destructive actions, such as deleting or scrambling all the files on the disk.

A computer virus exhibits three characteristics: a replication mechanism, an activation mechanism, and an objective. The replication mechanism performs the following functions:

- searches for other programs to infect
- when it finds a program, possibly determines whether the program has been previously infected by checking a flag
- inserts the hidden instructions somewhere in the program
- modifies the execution sequence of the program's instructions such that the hidden code will be executed whenever the program is invoked
- possibly creates a flag to indicate that the program has been infected

The flag may be necessary because without it, programs could be repeatedly infected and grow noticeably large. The replication mechanism could also perform other functions to help disguise that the file has been infected, such as resetting the program file's modification date to its previous value, and storing the hidden code within the program so that the program's size remains the same.

The activation mechanism checks for the occurrence of some event. When the event occurs, the computer virus executes its objective, which is generally some unwanted, harmful action. If the activation mechanism checks for a specific date or time before executing its objective, it is said to contain a time bomb. If it checks for a certain action, such as if an infected program has been executed a preset number of times, it is said to contain a logic bomb. There may be any number of variations, or there may be no activation mechanism other than the initial execution of the infected program.

As mentioned, the objective is usually some unwanted, possibly destructive event. Previous examples of computer viruses have varied widely in their objectives, with some causing irritating but harmless displays to appear, whereas others have erased or modified files or caused system hardware to behave differently. Generally, the objective consists of whatever actions the author has designed into the virus.

As with Trojan horse programs, computer viruses can be introduced into systems deliberately and by unsuspecting users. For example, a Trojan horse program whose purpose is to infect other programs could be planted on a software bulletin board that permits users to upload and download programs. When a user downloads the program and then executes it, the program proceeds to infect other programs in the user's system. If the computer virus hides itself well, the user may continue to spread it by copying the infected program to other disks, by backing it up, and by sharing it with other users. Other examples of how computer viruses are introduced include situations where authorized users of systems deliberately plant viruses, often with a time bomb mechanism. The virus may then activate itself at some later point in time, perhaps when the user is not logged onto the system or perhaps after the user has left the organization.