Text №9
Computer Viruses

What is a virus?

In 1983 researcher Fred Cohen defined a computer virus as “a program that can “infect” other programs by modifying them to include a ... version of itself.” This means that viruses copy themselves, usually by encryption or by mutating slightly each time they copy.

There are several types of viruses, but the ones that are the most dangerous are designed to corrupt your computer or software programs. Viruses can range from an irritating message flashing on your computer screen to eliminating data on your hard drive. Viruses often use your computer’s internal clock as a trigger. Some of the most popular dates used are Friday the13th and famous birthdays. It is important to remember that viruses are dangerous only if you execute (start) an infected program.

There are three main kinds of viruses. Each kind is based on the way the virus spreads.

1. **Boot Sector Viruses** - These viruses attach themselves to floppy disks and then copy themselves into the boot sector of your hard drive. (The boot sector is the set of instructions your computer uses when it starts up.) When you start your computer (or reboot it) your hard drive gets infected. You can get boot sector viruses only from an infected floppy disk. You cannot get one from sharing files or executing programs. This type of virus is becoming less common because today's computers do not require a boot disk to start, but they can still be found on disks that contain other types of files. One of the most common boot sector viruses is called "Monkey," also known as "Stoned."
2. **Program Viruses** - These viruses (also known as traditional File viruses) attach themselves to programs' executable files. Usually a program virus will attach to an .exe or .corn file. However, they can infect any file that your computer runs when it launches a program (including .sys, .dll, and others). When you start a program that contains a virus, the virus usually loads into your computers memory. When the virus is in your computer's memory, it can infect any other program that is started. Program viruses that have circulated recently are "SKA" (Happy99.exe) and "Loveletter."
3. **Macro Viruses -** These viruses attach themselves to templates (in PCs, usually the "normal.dot" file) that are used to create documents or spreadsheets. Once a template is infected, every document or spreadsheet you open using that program also will become infected. Macro viruses are widespread because they infect commonly used office applications and spread between PCs and Macintoshes. Macro viruses include "Concept," "Melissa," and "Have a Nice Day."

You cannot get a virus from...

- Opening an e-mail message. However, you can get a virus from opening a file attached to an e-mail message.
- Reading a Web page. You can get a virus only by downloading *and* running a program. Usually your Web browser will warn you when you begin to download a program from the Web.
- Downloading a file. Downloading a file will *not* infect your computer with a virus. However, installing or opening an infected document or a software program *will* infect your computer.

If you think you might have a virus, ask yourself these questions:

1) Are my software programs taking longer to load than they used to?
2) Are my software programs crashing for no apparent reason?
3) Is my computer checking my hard drive often?
4) Are my files disappearing for no apparent reason?
5) Am I experiencing frequent file corruption?
6) Are items that used to work no longer working (providing you haven't made any changes to your system)?
7) Have you recently used any floppy disks that were in someone else's computer?
8) Have you recently downloaded and executed any computer programs or games from the Internet?
9) Have you received e-mail from an unfamiliar source?
10) Have you received e-mail with an attachment?

Hoaxes

The truth about viruses

The majority of people believes that the most common source of viruses is the Internet through e-mail or downloaded files. The truth is, however, that the majority of viruses spread through shared floppy disks or shared files on an internal network.

Even if you are not connected to the Internet you should still be concerned about viruses. You should also be aware that there art-thousands of false rumors of viruses (virus hoaxes).

Three kinds of viruses

1. **Boot** Sector viruses attach to floppy disks and then copy into the boot sector of your hard drive.
2. **Program** viruses attach to a program's executable files.
3. **Macro** viruses attach to templates.

How can you get a virus?

Since 1988, thousands of virus hoaxes have appeared. Some of the more common hoaxes that have been circulating for years include "Good Times" and "Join the Crew." A "successful" virus hoax includes two factors:

1. **Technical sounding language** - For example, the "Good Times" virus hoax said the Federal Communications Commission (FCC) released a warning about the danger of the virus. In fact, the FCC did not issue the warning because virus warnings are not the FCC's responsibility.
2. **Credibility' by association** - Anyone from a company or organization can send out a warning under the e-mail identification of that company or organization. For example, if the e-mail address ends in @iastatc.edu you might think that a credible person from ISU's computer unit sent out the warning. However, it could be a student pulling a prank or a disgruntled employee. Check exactly who sent the warning and what his or her position is in the company.

There are many Web sites that specialize in virus hoaxes. Go to your favorite Internet search engine and type in "virus hoaxes" to get a listing of sites that you can review.

What to do when you receive a warning

- *Do **not*** pass on virus warnings without first checking with an authoritative source. Sources can include your computer system security administrator or one of the many virus Web sites on the Internet. Some government virus Web sites include <http:// csrc.ncsl.nist.gov/virus> and <http://www.fedcirc.gov/>. Warnings without the name of the person sending the original notice, or warnings with names, addresses, and phone numbers that do not exist probably are hoaxes.
- Make sure you have a current version of antivirus software, and run the software to check for viruses.
- If the warning refers to commercial software, verify the warning with the product's company. You can do this by calling the company or checking their Web site.

Antivirus software

Many choices exist for antivirus software, so determining what will work for you is important. Consider these points when looking at antivirus software:

- Does the company have NCSA/ICSA certification? The newest version of a company's antivirus software should be certified. To receive certification the software must detect 100 percent of the viruses that are in the "wild" and at least 90 percent of all other viruses.
- Check with virus testing centers. You can find such centers by searching the Internet.
- Make sure that you arc comfortable with the program you choose because you will want to access and update the program frequently.

Ask at your local computer store for antivirus software that meets the above standards.

You cannot get a virus from...

- opening an e-mail message,
- reading a Web page, or
- downloading a file.

You can get a virus from...

- opening a document or executable program that you received as an e-mail attachment or
- downloading *and* running a program from the Internet.

Viruses are multiplying

"According to one source, at the start of 1987, there were a total of six different viruses. Ten years later there were 'close to 12,000 '. During this 10 year period, the number of viruses doubled 11.5 times or every 10.5 months. Using these figures, there are now some 24,000 viruses and that number will double by next year."

—Thompson, Jim. "Fighting 'Vandals' with Virusweep Extra Strength." *Boardwatch Magazine,*www.boardwatch.corn (August 1998)

It is estimated that more than 42 percent of all computers suffered some sort of virus infection in 1999.

Hoaxes

*Do **not*** pass along a virus warning until verifying it with a reliable source. Many well intentioned people have forwarded virus hoax messages.

Virus hoaxes have been circulating since 1988. One of the first virus hoaxes appeared in October. 1988 and was called the "2400 baud modem virus."

If a virus warning asks you to pass the message on to everyone you know, think twice. Such a request usually is a sign the virus is a hoax.

There are thousands of Web sites that have information on hoaxes. A couple to check out include
http://ciac.llnl.gov/ciac/ ClACHoaxcs.html
http://www.icsa.nct/html/ communities,' antivirus/hoaxes

Antivirus software companies usually will have a Web page containing information on current viruses and hoaxes. Check the site often to keep abreast of the current viruses and hoaxes.