Computer Virus
by Douglas A. Turner, Esq.

With the recent events at home and abroad, we can do very well without any more threats to our security. The World Trade Center and Pentagon plane crashes, the Anthrax scare, and the wars in Afghanistan and Iraq are enough to put us all at the edge of our seats. And if our computers were alive, they'd probably feel the same way, too.

Of course, terrorism is nothing new. Neither are computer viruses. The concept of a computer virus can be traced all the way back to 1949 when the Hungarian-American mathematician John Von Neumann, at the Institute for Advanced Study in Princeton, New Jersey, proposed that it was theoretically possible for a computer program to replicate. In the 1950s, Bell Laboratories tested the theory by means of a game called Core Wars. The game involved players who created tiny computer programs that attacked, erased and tried to propagate on an opponent's system. The term virus was coined 33 years later by an American electrical engineer (Fred Cohen) to describe a self-replicating computer program.[1] The rest is, shall we say, history.

Today, there are more than 58,000 virus threats -- more than most of us would ever imagine could exist. Although a number so large is enough to cause the hairs on our backs to stand on end, we need not lose sleep over it. Proper knowledge and background information - and of course, preparation - are our best defense against this threat.

First things first, a virus is a **malicious code** but not all malicious codes are viruses. The major/common types of malicious codes are the Virus, the Trojan Horse, and the Worm. Each is described in brief below. With respect to each, however, it is important to bear in mind that a malicious code is merely a computer program crafted by another human being. He or she may be a researcher, a prankster, an outright vandal, a neophyte to the world of programming, a hobbyist, a complete loony or a genius. Regardless, he or she is still a human being who can (and eventually will) be outsmarted by other programmers. Many of these programmers work for anti-virus companies. Some of the most widely-known anti-virus companies are Symantec (Norton), McAfee, Trend Micro (PCcillin), AVG, and F-Secure.

Virus. A virus is a self-replicating computer program that interferes with a computer's hardware or operating system (the basic software that runs the computer). Viruses are designed to replicate and to elude detection. Like any other computer program, a virus must be executed to function—that is, it must be loaded from the computer's memory. After loading, the virus's instructions must then be followed by the computer. These instructions are called the payload of the virus. The payload may disrupt or change data files, display a message, or cause the operating system to malfunction.[2]

Trojan Horse. This harmful computer program was named after the popular wooden horse the Achaeans used to fool – and eventually destroy – the people of Troy. It usually appears to be innocent-looking and interesting, such as a game or screen-saver, but when runs, it can do many nasty things such as delete files, capture user-names and passwords (and send them to another person), or allow a hacker to control your system. It does not replicate itself, however, and it cannot execute itself unless a user actually runs or executes the code that triggers it.

Worm. A worm is a self-replicating program. It crawls and slithers through systems and eats up storage space, slowing the computer down. It doesn't alter or delete files, but it can cause significant trouble when systems get so filled up with the worm that they break down.

Other Types of Viruses. Another malicious program is called **Logic Bomb**. It is activated when certain conditions apply, such as when a particular date and time is reached, or when a specific order or combination of characters is typed.

False Threats. There are real threats and there are false threats. **Hoaxes** spread like wildfire in the internet via forwarded mails – courtesy of users who believe the virus warnings received from friends, relatives, or colleagues. Signs that a virus warning is probably a hoax would include a message with (1) a tone of urgency and even panic; (2) a claim that the government or an authoritative company has issued the warning; and (3) urgent advice to send it everyone you know. Not only do these forwarded mails cause unnecessary traffic in the information superhighway, they can also be carriers of some real viruses. In addition, hoaxes and chain letters may be used by spammers (bulk mailers of unsolicited mail) to harvest legitimate e-mail addresses for their use. Remember that, instead of believing and forwarding these messages, it is always safer to check out the anti-virus sites for latest updates on virus alerts and also hoax sites such as VMyths.com and Hoaxbusters for verification.

It is also very helpful to be vigilant in all respects. Be aware that the people who create viruses can use known hoaxes to their advantage. A good example is the AOL4FREE hoax. This began as a hoax warning about a nonexistent virus. Once it was known that this was a hoax, somebody began to distribute a destructive trojan horse (recall that a trojan horse differs from a virus in that it does not reproduce itself) in a file named AOL4FREE, which was attached to the original hoax virus warning!"

Avoiding Trouble. As computer users, we can avoid being terrorized by malicious codes by preparation and vigilance. Here are suggestions which offer a measure of protection:

?? Always create back-up files. Copies on your hard disk are recommended but having other back-up copies, such as on a CD-R is advisable.

?? Install anti-virus software and keep it updated. Update anti-virus software at least once a month if not more often.

?? If you are accepting submissions via e-mail (resumes, applications, etc.), specify that you only accept documents within the e-mail message. Do no accept attachments.

?? Delete e-mail attachments as much as possible. The only safe attachment is a deleted one. If you really need the attachment, save it first then have your anti-virus software scan it before you open the file.

?? If you receive an unexpected attachment from a name you recognize, you may try contacting or e-mailing that person and ask what it is and what it does before opening it.

?? It is also recommended that if your e-mail software has the ability to automatically run JavaScript, Macros or other executable code, it is better to disable this feature.

?? For those who like to chat, it is best not to accept any file sent through IRC.

?? Close the preview pane of your e-mail program because it opens the e-mail message automatically. Remember that some worms already have the capability to hide in the body of an e-mail (mostly html).

?? Have an emergency system boot disk on hand.

?? For Local Area Networks, it is safer to keep the write-access privileges to a bare minimum. Executable files written on one user's computer should not be readable on another user's.

?? Avoid swapping of disks. If it's unavoidable, make sure to scan the disk using your anti-virus software.

?? Obtain software only from trusted sources.

?? Install a firewall program, especially if on cable or DSL.

?? If you are running a company, it is good to specify to your employees the guidelines concerning computer viruses and security, and the risks involved if they are not careful.

?? Have an expert's phone number in hand and ready at all times so you know who to contact in case something untoward happens.

Finally, after all is said and done, we must remember Nick's First Law of Computer Virus Complaints: **Just because your computer is acting strangely**

or one of your programs doesn't work right, this does NOT mean that your computer has a virus.[3]

[1] Microsoft® Encarta® Encyclopedia 99. © 1993-1998 Microsoft Corporation.
[2] "Virus (computer)," Microsoft® Encarta® Encyclopedia 99. © 1993-1998 Microsoft Corporation.
[3] www.faqs.org