

Understanding Viruses

Wednesday, 26 September 2007

The first tenet of warfare is this: know thy enemy. So what exactly are computer viruses? Computer viruses are devious little computer programs that attach themselves to legitimate program hosts and then engage in rampant self-replication. It's easy to be fooled by their small size. Don't be. They're never small for long. Computer viruses propagate like rabbits -- and by the time you first recognize their presence, your data may be permanently damaged or erased.

On this point, however, an important clarification must be made. Like biological viruses, computer viruses are not inherently destructive. You're probably harboring a fugitive cold virus in your body right now, even if you're not actually sick. With both biological and computer viruses, you can be infected without being affected. Your computer can be a veritable hive of viruses without exhibiting any visible symptoms or actual damage. If not instructed to do otherwise, viruses will quietly, unobtrusively and perpetually replicate. They're only destructive if intentionally engineered to be so.

Malicious computer viruses contain a "payload" -- a programming element separate from the self-replication code that executes its objectives. For example, a payload might display a personalized message on your monitor. It might erase critical data or program files, reformat your hard drive, or infiltrate your messaging software and overload the local network with authorless e-mail. But not all computer viruses are created equal. Some are full of sound and fury, yet signify nothing. Others are silent but deadly. In general, though, computer viruses are of three main types:

Macro Viruses: These are the most prevalent type of virus today. Unlike conventional viruses which can attach to virtually any program, macro viruses prey on specific programs. A macro itself is an instruction code that automatically executes other program commands. Many popular and prominent software applications utilize macros extensively. Essentially, macro viruses are macros that embed within a program and self-replicate.

Macro viruses that run on Microsoft applications like Word and Excel are particularly common -- chiefly because certain programming strategies employed by these applications make them particularly susceptible. Macro viruses work like this: when an infected document is initially opened, the macro virus embeds itself in the associated application and then proceeds to attach itself to every subsequent document created. In this way, the macro virus is unwittingly disseminated whenever the user transfers a document.

Parasitic Viruses: These are the most infectious type of virus. Parasitic viruses attach themselves to executable programs like .com or .exe files. Once an infected file is launched, the virus is free to replicate itself, embed in primary memory, or release its payload. Further, it can corrupt not just specific programs, but virtually any program being processed in RAM.

Boot Sector Viruses: The boot sector is essential software that resides on hard, floppy or optical disk, and is responsible for loading your operating system into memory at the start of a computing session. Boot sector viruses penetrate this vital boot sector and alter its contents. As opposed to macro viruses, boot sector viruses are spread not by sharing documents, but diskettes. Whenever new diskettes are introduced to a previously infected computer, the boot sector virus is transferred to the healthy diskette, which then conveys the virus to other computers, and so on.

These are all considered true computer viruses. Another commonly observed form of computer pestilence (though not literally a virus) is the worm. Worms differ from viruses in that they do not require a host to wreak their havoc. Other viruses are referred to as Trojan Horses. Trojan Horses are viruses that masquerade as legitimate programs, documents or other software, only to reveal their true function later. Trojan Horse viruses are often spread through e-mail or online bulletin boards.

Certainly no one would knowingly expose their computer to a virus. Unknowingly, however, thousands daily place their machines in peril. Ignorance is no excuse, though -- an ounce of prevention is worth a pound of cure. The following are some common troubleshooting techniques for keeping your computer virus-free:

- Always rely on a reputable anti-virus software application like Norton or McAfee.
- Always scan new files, diskettes or software before loading them on your machine.
- Always back-up critical software or files to avoid permanent loss due to infection or deletion.
- Always be wary of strange operating tics or unusual graphics.
- Always ensure vigilance from the other members on your computer or network.
- Always write-protect your system and program disks.
- Always enable Macro Virus Protection in all Microsoft applications.
- Never share diskettes or software without assuring their integrity.
- Never download e-mail or Internet files/programs without scanning them first.
- Never act on an e-mail virus alert without confirmation from an IT professional or trustworthy resource.
- Never boot your system with a diskette other than the original.