Title:
Several Common Ways That Viruses Spread

Word Count:
652

Summary:
In addition to the common methods of spreading through email attachments, boot infections and program infectors, there are other ways by which viruses spread to your computer. These include:

Infection by Disk(Floppy, Zip, CD's, Tapes, etc.)

Floppy disks, though not as commonly used as in the past, are still a very common way viruses being spread from machine to machine. Anyone with an infected machine, using a floppy disk to copy and save files, can also copy and transf...

Keywords:
blackworm virus, antivirus, computer security

Article Body:
In addition to the common methods of spreading through email attachments, boot infections and program infectors, there are other ways by which viruses spread to your computer. These include:

Infection by Disk(Floppy, Zip, CD's, Tapes, etc.)

Floppy disks, though not as commonly used as in the past, are still a very common way viruses being spread from machine to machine. Anyone with an infected machine, using a floppy disk to copy and save files, can also copy and transfer the virus. Any use of that same removable disk, by any user, at any time in the future, will most likely contaminate, or re-contaminate the any computer it is used with. The only way to properly clean an infected floppy disk is to perform a low-level format. The normal Windows(tm) "format disk" is often not enough.

With CD's, all the above holds true with the exception that an infected CD can never be cleaned. To get rid of an infected CD, you need to put it in the trash and never use it again.

Infection from Networks

Peer-to-Peer network, Local Area Networks (LAN), a Wide Area Network (WAN),

Wireless Networks, and the Internet, are all computer networks. They all have the same basic purpose; to share software, and information resources between two or more computers. As with anything else that is shared between computers, networks let users share files, and wherever files are shared, viruses can be shared and spread.

Most network virus/worm/Trojan activity is like what we described earlier, although more and more examples of automatic mass mailing attacks, system resource attacks are being found.

Recently many attacks are designed to specifically target major corporate interests (Microsoft, eBay, Amazon, major Banks etc.) in an attempt to disrupt their online services. Very generally these are called DOS (denial of service) attacks. The way they most commonly work is by secretly infecting thousands of local user computers (like the one you are using right now), and then at a specific time, launching a combined attack from all the infected machines against the primary target.

As you can see, your computer can be hijacked without your knowledge and then used in a major attack against an unsuspecting company. However with up-to-date virus/firewall protection, your computer will be immune to such hijacking.

Other ways by which virus spreads

Other sources of viruses have been found to be the result of software downloads available over the Internet. Software patches, drivers, demonstration software, from reputable companies, generally carries little risk. However, the Internet is also filled with "unofficial" software, pirated programs, and low-budget software from questionable sources that may be intentionally or unintentionally infected with viruses. Files downloaded directly from the Internet (either through file-sharing programs or direct download from websites), are among the fastest growing sources of computer virus infections.

Email, with its nearly universal availability and ease of use; chat rooms and messenger systems, not only make communication simple and quick, also make the transmission and re-transmission of infection simple and alarmingly fast. Creators of newer viruses, and internet worms specifically target these systems because they are widely used, and are often built right into the operating system and used with default settings making them much easier to attack and exploit.

As a point of reference, Internet Explorer, and Outlook/Outlook express email clients are two of the applications most targeted by Internet viruses and worms.

Why? Because they are installed on more computers around the world than any other software, and they are installed 99% of the time with default settings (which means virus programmers have an easy blueprint to follow).

If you use an email system or instant message system that is installed automatically with your computer's operating system you need to install and use current antivirus software. You also need to learn how to turn off certain default settings that can leave your system open to very easy attack.