

Avoiding Computer Viruses

The number of viruses being developed each day is astounding, and with the advent of the Internet, the ability of these new viruses to spread to your system is causing great concern. Computer viruses can range from simply annoying ones to downright deadly ones. They can infect your system and destroy programs, data, and even hardware on your computer workstations. Knowing what type of damage viruses can do to your systems and how to protect your systems from these attacks is important.

Types of viruses

The thousands of computer viruses that can infect your workstations fall into several major categories:

- Executable viruses
- Boot-sector viruses
- Partition-table viruses
- Memory-resident viruses
- Macro viruses

Executable Viruses

An executable virus infects your files by attaching itself to your EXE and COM files when you launch them. The virus finds information in the executable file's header, which indicates the length of the file and other vital information. (The file header is located at the end of an EXE file and at the beginning of a COM file.) Once attached, executable viruses corrupt the header, preventing the file from working or redirecting it to run another command.

Because these viruses destroy the executable code of the infected program, you can easily identify them, delete the infected code, and reinstall the necessary program files. Some executable viruses seek out only EXE files, while others seek out only COM files. Common executable viruses are Vaccina; Troi; Yankee Doodle; Black Monday Leprosy; Stealth and Spyder etc.

Boot-sector viruses

Boot-sector viruses corrupt the boot sector by overwriting the sector with bad information, thus preventing your workstation from booting (or starting up). These viruses usually activate when you read or write to an infected disk.

Some boot-sector viruses copy the boot-sector information to another part of your hard disk and then overwrite the boot sector with their own bad code. When you reboot your workstation, the system BIOS executes the virus code from the boot sector, which in turn executes the boot-sector information it copied elsewhere on your drive. This means that you may not even notice you have a boot-sector virus until it's too late. Common boot-sector viruses include Lezop; Spanish Trojan; Anthrax; SVC60; Trackswap Filler etc.

Partition-table viruses

A partition-table virus takes aim at your hard disk's partition table. These viruses can either move or destroy (or delete altogether) your hard disk's partition-table information. They copy the partition-table information to another location on your hard disk and then copy their bad code into the area normally containing the partition table.

After the workstation's BIOS loads and executes the virus during the boot sequence, the virus executes the partition information it saved elsewhere. A virus that infects only the partition table probably won't spread from one computer to another. It spreads by infecting your boot sector and/or the executable files on your hard disk. Some common partition-table viruses include LastDirSect; NOINT; Michelangelo; Stoned III; Bloomington and Music Bug etc.

Memory-resident viruses

Memory-resident viruses avoid detection by loading into different areas of your workstation's memory. The virus waits there until you launch an application; then, it infects your workstation.

A few viruses place their memory-resident code in memory normally allocated for the command processor, either in its stack space or in the command data region of your workstation's memory. Because these viruses tamper with the command processor, they frequently cause your workstation to crash.

Many such viruses simply allocate memory through a DOS call and assume you won't notice the loss of a few kilobytes of RAM. This keeps the viruses from being overwritten while in memory. A few viruses place their code into unallocated memory. This approach doesn't decrease the amount of available memory on your workstation, thereby making detection less likely. However, these viruses are more vulnerable since another application can overwrite their code.

Some viruses intercept any memory allocation calls to the 21h interrupt, thus preventing the operating system from allocating the memory block in which the viruses stores their information. Other viruses do nothing about this problem, and your workstation crashes whenever it attempts to overwrite these areas.

A large number of viruses place themselves in the top portion of resident memory, just below the 640KB boundary. Then, they redirect BIOS interrupt 21h, which reports the total amount of conventional memory available in your workstation. This approach reduces the apparent amount of total memory, preventing function calls from overwriting the virus.

Viruses may also incorporate their code into the video-card buffers between 640KB and 768KB (A0000h and C0000h). The amount of total memory won't change, but your workstation may crash.

Macro viruses

While most viruses infect program files, macro viruses can infect data files. Macro viruses infect Microsoft Word documents in particular, but newer versions of macro viruses can also infect Microsoft Excel spreadsheets. Because Microsoft controls most of the application market, their programs have become favourite targets of virus makers. Common macro viruses include Concept; Boom; Goldfish; KillDLL; Laroux and Sofa etc.

Macro viruses take advantage of an application's built-in programming language. Application vendors now include powerful programming languages in their programs so users can perform complex tasks, and the people who create macro viruses turn this feature against software owners. Virus makers can hide a complex macro virus in any document or spreadsheet. When you load the infected file, your application will then spread it to any other file you open.

Macro viruses can destroy data on your hard disk.

Protecting your systems

The first line of defence in the war against viruses begins with protecting your systems with an antivirus software package. Below are examples of a few antivirus packages – there are many more. Your computer supplier will advise on the packages that are compatible with your operating systems and other software.

Product	Company	Website
Vet	Computer Associates	www.vet.com.au/
Norton AntiVirus	Symantec	www.symantec.com
McAfee VirusScan	McAfee/Network Associates	www.nai.com
ThunderBYTE Anti-Virus	Authentex/NovaStor	www.authentex.com
F-Prot Professional	Command Software Systems	www.commandcom.com
IBM AntiVirus Enterprise	IBM	www.ibm.com/IBMAntiVirus
InocuLAN	Cheyenne Software	www.cheyenne.com
Sweep	Sophos	www.sophos.com
Office Scan	Trend Micro	www.trendmicro.com
e-Trust	Computer Associates	www.my-etrust.com

Corporate versions or business versions should be used rather than home versions for practices as the incorrect choice can crash systems and slow down clinical and billing package operation.

Updating virus definitions/signatures

According to IBM researchers, computer hackers create new viruses at the rate of about three per day-over a thousand new viruses per year. So, a virus scanner that's two or three months old won't detect and eradicate the newer computer viruses cropping up every day. That's why it's extremely important that you regularly update your antivirus package's virus definition file or virus signature file. Many antivirus packages allow PCs to be set up so they check the manufacturer's website at regular intervals for updates and download these to an administration PC. Client PCs on the network then look to this PC for their updates. It is recommended that your administration PC for antivirus purposes is not the main server as sometimes this PC requires a reboot to fully update all components before redistribution to the other PCs on the network.

Update Service Packs and Patches

Another line of defence is by updating service packs and patches for operating systems and application software (eg. Windows, Internet Explorer and Outlook in particular). These are released regularly from Microsoft and can be automatically be downloaded using the Windows Update feature on a PC.

Use a Firewall

Viruses can also enter a PC via an open port, examples include the Sasser worm which caused so much damage in May 2004. Ports are open when surfing the Internet or when an Internet connection is active. There are a huge range of ports and many are used for malicious activity. Having a firewall *and having it properly configured*, protects against viruses of this kind. Most ports do not need to be open, the notable exceptions for practices are port 25 for SMTP mailserver connections and port 389 UDP for HIC's PKI healthcare directory. If you use Outlook Web Access this would mean port 80 being opened too. Depending on your requirements and configurations, some of these can be closed too. Firewalls should only be installed and configured by competent IT Professional who is skilled in this kind of work. If you are unsure whether your firewall is protecting your system, check it out using ShieldsUp! a free, quick and easy way to see if your files are effectively being published on the Internet. www.grc.com.

Upgrading software

It is recommended that you disable any antivirus automatic/background scanning during a software installation. This is because antivirus software checks files on opening and may slow down or interrupt the installation but more importantly installations can mimic virus-like behaviour, which may mean the installation is stopped or prevented from running.

If you are planning to convert a disk from FAT32 format to NTFS format, apart from backing up your data, always completely uninstall your antivirus software and reboot the PC before proceeding. This is because antivirus software also protects the boot sector and can mean the conversion cannot take place. The drive is left in a state where it cannot be recovered if the conversion process fails. Following a successful conversion, reinstall the antivirus software.

Conclusion

Computer viruses are a big problem these days, and prevention is far better and cheaper than cure. Protecting patient security, privacy and confidentiality involves having appropriate antivirus software installed, updating service packs and patches for operating system and application software and having a properly configured firewall.