SECUR IT

IT SECURITY CORNER

I've got a Monkey in my computer and it won't come out *or*

How I learned to stop worrying and deal with computer viruses

Computer viruses get a lot of press whenever there's another big, sensational media frenzy to be had. As a case in point, remember what happened three or four years ago when the Michelangelo virus was set to destroy every computer in the world? The purpose of this article is to provide you with a little bit of education about computer viruses (as they relate to the IBM PC clone computing world), some common-sense tips to help you either avoid or deal with them, and to help you demystify them to a large degree so that you can be freed of a lot of the FUD — fear, uncertainty and doubt - that surrounds them.

Computer viruses are a fact of computing life these days. You're going to get them. People you know are going to get them. You might even lose data because of them, and you might hear sensational stories about them (like the so-called Internet "Good Times" virus — it's a hoax).

Essentially, there are two kinds of computer viruses: boot sector viruses and file infector viruses. They are very similar in terms of what they do once you're infected, but they differ greatly in how they spread. To effectively deal with them, and prevent them, you have to know these differences. Don't let some of the medical terminology (virus, infection, vector, etc.) fool you into thinking they're more complicated than they really are.

Firstly, a computer virus is nothing more than a small computer program, written by a computer programmer. Computer viruses execute like computer programs, and have an expected function or outcome.

Boot sector viruses are by far and away the most common type of viruses at DFAIT. Every computer disk, whether a floppy diskette or a hard disk, has a "boot sector" at the very start of the disk. The phrase comes from the old mainframe terminology of "bootstrapping" a computer, which basically means a computer pulling itself up (or turning itself on) by its bootstraps. Computers usually contain just enough code in firmware to turn themselves on and perform some very basic self-diagnostics. The firmware then tells the computer to go and look at the boot sector of the first disk it finds to tell it what to do from there.

When you turn on your computer, that is exactly what happens. The firmware performs some initial diagnostics, then control passes to the boot sector of your hard disk (or C: drive) and your computer finishes the boot process. If you have a diskette in your A: drive, the computer will try to read the boot sector off that disk first. If the diskette is not a "system disk" (is not "bootable" because it has not had the appropriate code transferred to its boot sector), you will get a message similar to "Non-system disk or disk error, replace and press any key when ready." At that point, thwack yourself in the forehead, remove the diskette from drive A: and press a key. The system will then proceed to boot from the hard disk.

Boot sector viruses exploit this fact of computer life by living in the boot sectors of disks. When a computer reads the boot sector of a disk, the virus gets loaded into the computer's memory and is then "active," and able to wreak its own havoc. Examples of boot sector viruses are Stoned, Michelangelo, NYB, Monkey and Form — all of which are different in terms of what they do, but all of which exploit the boot sector reality of life.

File infector viruses are different in that they come attached to the executable files you run. An acquaintance hands you a diskette with the latest and greatest game on it. You put the diskette in your computer, being careful not to boot from it, and start up the game by typing GAME.EXE. The virus is hiding inside the program and gets executed first, then the game — so you see nothing untoward as you play. In the meantime, the virus is now busy probably infecting your system and doing whatever other damage it's been programmed to. The Jerusalem virus, for example, puts a moving and expanding black rectangle on your screen. The Cascade virus causes letters to fall from the top of your screen to a jumble at the bottom. Imagine that while you're playing your game and destroying the Evil Space Mutants who are trying to invade the Earth, the virus is working in the background destroying the Important Budget Report that you hoped would get you a raise. Other examples of file infector viruses are Dark Avenger and Friday the 13th.

Just to make things a little more interesting, there are newer viruses that are both boot sector and file infectors — viruses such as Natas and One-Half. In other words, you can get them either way.

So how can you prevent viruses? You can take reasonable precautions. **Firstly, get a good virus scanner.** DFAIT uses McAfee's VirusScan. **Make sure you scan each new program or diskette you want to use before you use it, and this includes off-the-shelf, shrinkwrapped software and new, preformatted floppy diskettes.** On SIGNET-D, an option to scan diskettes may be found from the Utilities folder in Windows' Program Manager. Scan files you get from electronic bulletin board systems (BBS's) and diskettes/programs you get from colleagues. For scanning your hard disk, or your computer at home, you'll want to ensure you have a clean, write-protected bootable diskette that contains some essential DOS files and the scanning program. If you're unsure of how to do these things or need assistance, please call your SIGNET Systems Administrator who can walk you through the procedures.

Make sure you don't leave floppy diskettes in your computer for any longer than absolutely necessary. If you always remember to check your A: drive before turning your computer off, you minimize the chance that you'll turn it back on with a diskette there — and perhaps wind up with a boot sector virus. If your computer reboots in the middle of your work because of a power spike or because you intentionally rebooted it because it was "hung," make sure to take out any diskette you might have been using at the time so that you don't accidentally try to boot from it.

Above all, if you find you have a virus, DON'T PANIC. Odds are that whatever bad is going to happen has already happened, so there's little point in worrying about it. If you know or suspect you have a computer virus, call your SIGNET Systems Administrator, who will help you to clean your system.

In short, if you take reasonable, sensible precautions and apply them to your daily work routine and interaction with computers, you greatly decrease your chance of losing data from a virus incident.

SIGNET News is published monthly by the SIGNET Client Services Division (STC) and distributed in Canada and at missions abroad to all employees of the Department of Foreign Affairs and International Trade.

Units wishing to have a notice published in *SIGNET News* should forward the text to STC with a memo signed at the director level. All readers are invited to send via ICONDESK (Suggestions) draft articles they wish to have published.