No. 44, July 1997

A FORMULA FOR DEALING WITH VIRUSES

A few months ago, a memo came to me at my office at the medical school saying that personal software could no longer be mounted on computers at the school. Admirably, the school was trying to institute a new software accounting procedure to thwart piracy. In order to cleanly implement it, they wanted only school software on the hundreds of machines on site. OK, I thought. No sweat. I made arrangements to get a school copy of Microsoft Word for my machine, and later installed it in place of my personal copy.

A few days later, I was virus scanning a student disk containing some software I had written. The student had sent me a note saying the disk was infected when she received it from another student. Sure enough, it was infected with "Ripper", a nasty stealth virus that infects floppy boot sectors and the Master Boot Record (MBR) of hard drives. It then messes things up by swapping information in the write buffer, about once in a thousand writes. The occasional scrambling of data makes it particularly hard to spot, often corrupting data on both the hard disk and in backups before it is discovered. Another characteristic that makes it tough to spot is its "stealth" nature. Stealth viruses can "sense" the efforts of a virus scanner to look at a particular place on a hard or floppy drive such as the boot sector, and then present the scanner with what is supposed to be there even though the virus itself is actually occupying that spot. For this reason, some virus scanners are unable to detect the presence of a stealth virus. Talk about sneaky!

I filed the infected floppy in my collection of infected disks and prepared a new, virus-free disk for student use. Then, as is my habit each time I finish working with a virus (even though I take certain precautions to prevent transfer to my machine), I proceeded to check my machine thoroughly to confirm that the infection had not spread to it. The boot sector was fine, but my virus detection software said that Microsoft Word's global document template called NORMAL.DOT was infected with the Concept virus! After a bit of investigation, I confirmed that this was indeed the case. The school's disks containing MS-Word had themselves been infected, which promptly spread to my machine when I installed the program.

"How can that be", you might ask. Only files with an EXE or COM extension can be infected with a virus, right? Wrong. Overlay files (*.OVL or *.OVR), dynamic link libraries (*.DLL) and several other file types can contain viruses. In the case of Microsoft Word word processing files, when you open your letter or other document, macros stored in NORMAL.DOT will automatically load and execute. If a macro is infected, your work and even the remainder of the data on your hard drive can be damaged.

The results of this relatively new type of virus found in files associated with word processing documents are far reaching. A single mouse click while on the World Wide Web can download an email file with it's infected MS-Word attachments, invoke the word processing program, read in the file and infect your machine. And don't think that just because you don't use Microsoft Word that you are immune. As the writers of viruses continue to experiment and explore, there will be other programs that will serve as vectors (carriers) of infection. There is no way to stop the process. More and more ways will be found to damage the data on your machine.

Gloomy Gus? Nope, just a realist. Anything that can be done will be done, somewhere, by some deranged person who wants to get some "kicks". Fortunately, you can take some positive steps that can prevent an infection or reduce the impact. That's the aim of this month's article.

1. Regularly use at least 2 (two, dos, zwei, duo; read that as **more than one**) virus scanners. None are perfect, and you decrease your chance of missing a virus to well under 1% if you use two.

2. Unlike fine wine, these software packages should be not more than 3 months old. That means that you must download or otherwise obtain a new copy every three months. No, that McAfee SCAN disk dated January 1989 will simply not do! SCAN and F-PROT are my personal preferences, but there are other good ones, too. I regularly download free copies of SCAN and F-PROT from Exec-PC. As of this writing (20Apr97), the latest versions are: SCAN, v. 3.00, 20Feb97 and F-PROT, v2.26, 24Feb97. New versions of both are issued about every three months, so a higher number version of each will be out and available when you read this. Make sure at least one of the scanners will detect macro viruses (both SCAN and F-PROT will). You can update SCAN or F-PROT at the following web sites:

   SCAN: http:/www/mcafee.com
   F-PROT: http://www/simtel.net/pub/simtelnet/msdos/virus/fp-xxx.zip
   (the xxx in the line above is the version number; try 227 for version 2.27)

3. Scan your entire hard drive whenever you put new programs on it (instances of virus infections in brand-new shrink-wrapped disks or CDs coming directly from the software manufacturer are **not** rare). Also do a scan just before each backup, and whenever you have downloaded files or had a friend's disk in your drive (the most frequent source of viral infections are disks obtained from a friend). Even if you have not added new software or had strange disks in your machine in three months, do a complete scan whenever you update your scanner software. A relatively new virus may be lurking on your machine, undetectable until the updated scanner software comes out with its new abilities.

4. Back up your hard drive often. What does often mean? Three months, maximum. More often if you use it heavily. For critical items like that 60-page manual you just finished, back it up on floppies, as you complete each session. The most painless viral infection (or hard disk crash) is the one that happens right after a complete backup.

5. Make sure you have a bootable floppy disk on hand, in addition to your backups. This applies no matter what operating system you use, including (especially!) Windows 95. You cannot restore files to a drive if you cannot boot it.

6. If you do become infected (and, sorry to say, the chances are you will), don't panic. Be positive; view the infection as a learning experience (this is a lot easier to do if you have a fresh backup on the shelf). Both hard drives and floppy disks can easily be disinfected, restoring them to perfect order without damage to your files. F-PROT and SCAN will disinfect, as well as detect. If you don't know how, don't do anything until you get competent help; don't even turn off your machine! If you want to learn how, do it **before** you become infected. Read the DOC files that come with the scanner software, and print them out (you may not be able to print or even access these files once the machine becomes infected).

7. Finally, do not curtail your activities because of viruses. Enjoy your machine; enjoy surfing the web. Share goodies with friends. If you pull back and become isolationist in an attempt to prevent infection, you have done exactly what the virus authors want. Do not make concessions to terrorists. Happy computing!