Computer Viruses: Can It Happen At IU?

Mark Sheehan

In the past few months, the popular press has been full of articles about "computer viruses." The New York Times, the Chicago Tribune, the Chronicle of Higher Education, and any number of university computer center newsletters have featured stories on these diseases and others. While there have been no reports of computer viruses breaking out on the Bloomington campus of IU, it's important that our computing community be aware of them and take as many practical steps as possible to protect itself from them. The probability that a serious computer disease will eventually break out on our campus is high.

What is a computer virus?

A computer virus is not really a microorganism, of course. It's a form of vandalism whose target is computer data, and whose perpetrator's motives are much less clear than those of a hard-reproducing microbe trying to make an honest living in someone's lungs. A few computer diseases can attack hardware, but the more common species concentrate on data.

Specifically, a virus is a computer program containing instructions that cause the program to be appended to other computer programs and to duplicate itself whenever the opportunity arises. Other types of computer disease programs include "time bombs," "worms," and "trojan horses" that don't replicate themselves, but do make mischief of one kind or another. Most of the viruses in the news lately affect IBM PCs, though nearly any computer is susceptible to one type of vandalism or another. Some viruses are perfectly harmless if they are coded properly. I imagine their authors are like the people who write their initials on dollar bills in hopes of some day seeing one come back to them.

Unfortunately, not all viruses are benign. If a virus program is poorly written, like one that appeared recently at Hebrew University in Jerusalem, it can keep appending itself to a given program until that program gets too big for its disk and crashes.

Sometimes viruses are written with malicious intent. One discovered at Lehigh University in Bethlehem, Pennsylvania, went through a period of reproduction, then erased all the files in the infected computers. The Hebrew University virus, apart from being so badly written that its symptoms could not be ignored, had an apparently "terrorist" purpose. It was a virus that is also a "time bomb" — set to delete files on Friday, May 13th, the 40th anniversary of Israel's declaration of independence.

The Lehigh virus caused about 100 students to lose the text and data files they had created on microcomputers in the university's public computing clusters. On larger computer systems, the effects of a destructive virus would involve more users at a stroke, and are completely out of the control of the average user. They may be a little more frightening. At the same time, though, larger machines are usually well monitored and protected. The individual microcomputer is more vulnerable.

This article won 1st place in the ACM-SIGUCCS Technical Writing Contest in the Reportage category. It originally appeared in BACSpace, *Indiana University at Bloomington.*

Who is at risk?

As with human diseases (AIDS is a disturbingly good example), some populations of computer users are more likely to run into viruses than others. Characteristics of a high risk computing style are:

- The use, even occasionally, of public computers, especially those with hard disks. (A virus program can very easily be placed — and replaced — on the hard disk of a public micro. From there it can infect every data disk inserted into the computer.)

- The "promiscuous" sharing of computer programs and system disks. (If you don't know where a program's been you probably shouldn't accept a copy of it. It's a little bit risky to trust any software whose shrink-wrap you didn't open yourself. There are lots of reasons not to use anyone else's DOS system disk in your PC — among them compatibility and conflicting disk usage. Viruses are the best reason, though.)

- The use of electronic bulletin boards as a source of software. (Downloading an interesting looking program from a bulletin board can save money and provide wonderful tools. It can also be just the same as welcoming that large wooden horse through the gates of Troy.)

- The use of microcomputers in semi-public areas, like open office complexes, or buildings in which office doors are not commonly locked. This applies especially to office PCs that are used by more than one person, especially if they have hard disks. (Any place a vandal can go when nobody's looking is a potential site for vandalism. Any PC with more than one user shields the vandal with even greater anonymity.)

- The angering, miffing, or affronting of any socially immature computer expert. (Many viruses take a high level of sophistication to produce and install. Infecting a perceived persecutor's computer with a virus program would be a tempting vent for the frustration of a certain kind of "hacker.")

How can a virus be detected?

The best virus is one that infects the computer's operating system. These are in the background at all times, seizing opportunities for deviltry. On an MS-DOS computer, IBM PCs and clones, three files are loaded into computer memory when the machine is booted. One, COMMAND.COM, appears in the directory of a system disk. The others, with names involving the character strings "DOS" and "BIOS," are "hidden files," and do not appear in the directory. Any one of these files could be infected with a virus that could be active whenever the computer was running. Currently, infected COMMAND.COM files are a few bytes larger than the original version. Comparing them with the size of the same file on the original (backup) DOS disk is a good way to detect them. Infected DOS and BIOS files can be detected in the same way, by using a program like the Norton Utilities (which reveals hidden files).

Other viruses infect application programs and can cause their size to increase by a few bytes. Again, you can reveal a virus by comparing the size of the file on the backup disk to the size of the file on the more frequently used disk. Note that the installation process can also add bytes to a program file, beyond the size of the original disk. This is a usual cause of differences in file sizes, and should be taken into account when probing for viruses.

A really well-written virus may have no symptoms, until it finally executes the vandal's plan. At least one expert, Professor Fred Cohen of the University of Cincinnati, quoted in the Chicago Tribune, regards it as impossible to defend against computer viruses.

An ounce, then, of prevention?

There are a few things you can do to protect your data (and your hardware, in the odd case) against disease.

- As always, the best advice for ANY computer user is BACK UP YOUR FILES! Never, ever, ever keep only a single copy of a file that has any importance to you.

- If you boot your computer from a floppy disk, you're more likely to guard against the effects of vandalism than if you boot from a hard disk. The world welcomed the first "bootable" hard disk for PCs back in the early '80s. Nowadays you might consider returning to the days when your hard disk was not a system disk, and you booted from a floppy. The advantage? The floppy can be write-protected so that it can't be infected by virus programs, and it an be locked up at night to thwart vandals. The program and data files on your hard disk are still vulnerable, but at least you will be protected from DOS-file viruses.

- If you compute in a public cluster, always use your own disks and keep your system disk write-protected. If the public PC has a hard disk, you will have to rely on the owner (BACS or an academic department) to keep the system and program files clean, but you can protect your own disks pretty well with a write-protect tab. Also, before inserting your floppy disk, turn the PC off, then on.

- If you have a hard disk, you can look into programs like "Disk Defender," that claim to protect hard disks from contamination. (BACS will evaluate such programs and make information available through the PC HelpLine, 335-6212.)

- A program called FLU_SHOT, available at the ACCESS MicroCenter, may offer your COMMAND.COM file some protection. At the same time, it is a public-domain program taken from a public bulletin board, so we advise you use the same caution as with any other public-domain program.

- Record the sizes of your most frequently used computer programs. (To get the size, get a directory listing of the .EXE or .COM files with the names you type to run the programs — WP.EXE for WordPerfect, WS.COM for WordStar, LOTUS.COM and others for Lotus 1-2-3, and so on. The size is the number to the right of the filename on the directory listing.) Check the sizes every week or so to be sure the programs aren't growing. If they are, make fresh copies from your original disks. NEVER use your original disks as your working disks, unless the manufacturer's copy-protection scheme makes that necessary.

- For computer users who want to continue to boot their PCs from the hard disk: if you haven't done so lately, you might refresh the system files on your PC's hard disk with copies from the floppy disks you got with the computer. Turn your computer off, then on, with the original floppy disk in drive A. Follow the instructions for the SYS command in your DOS manual, and re-SYS the hard disk. Copy COMMAND.COM from the A drive to the hard disk.

So — should you worry?

Professor Cohen's claim seems to be that if your computer is going to get a computer disease, there's little or nothing you can do to prevent it. If it's out of your hands, worrying might not be appropriate. But there are a few things you can do — some "safe computing" guidelines — listed above. A little attention — an ounce of prevention — to your computing lifestyle now, before viruses are common at IU, might be worthwhile. The price of a pound of cure these days is pretty steep.