No. 13, July 1994

VIRUSES, AND HOW TO FIGHT THEM

I decided it was time to start numbering the articles in this series, since we have now gone over a dozen. Last time I told you about the $5.00 computer purchased at Friendly Fest in November 1993. That machine is still ticking away, doing service at the Ozaukee County Justice Center on a packet station. You can talk to it if you like - just C N9VBJ (leave me a hello, and please tell me what you think about this series).

This time I would like to make some suggestions to help prevent a virus attack. Actually, I had another article in this spot, but decided on the virus topic because one hit one of our Ozaukee Radio Club members. It made a mess of his files, and made his hard drive practically inaccessible. It took me six hours at the keyboard to rescue one critical file, and even then the file was damaged.

What is a computer virus? Nothing more or less than a nasty little program, which is designed to do you damage. It resides on a floppy, inside another program or, more commonly, in the floppy boot sector. When you put the floppy in your machine, it transfers itself to your hard drive, and waits. Some do their damage next time you boot up your computer. If it is the Michelangelo virus, it waits until your system date is 5 March, then it does it's dirty work. As of April 1994, there were 2,885 different viruses or strains known (a strain is a virus that has been modified somewhat from the original version).

There are two basic ways to protect yourself from a virus. The first is to use a good virus scan program to test each and every floppy before you run any programs on it or transfer any to your hard drive. The best known such program is SCAN.EXE by McAfee Associates:

McAfee Associates, Inc.	(408) 988-3832 office
2710 Walsh Avenue, Suite 200	(408) 970-9727 fax
Santa Clara, CA 95051-0963	(408) 988-4004 BBS (25 lines)
	USR HST/v.32/v.42bis/MNP1-5
Latest version: 9.25V114	CompuServe GO MCAFEE
(17Apr94)	InterNet support@mcafee.COM
	America Online MCAFEE

You can get a shareware copy from Exec-PC (right in Milwaukee). Once you have it, write protect the disk it resides on and check your hard drive by giving the command: SCAN C:. It will check every file on your hard drive that has program code in it (EXE, COM, OVL and so on). If it finds a virus, it will tell you so and the name. The DOC file that comes with the program will tell you how to eliminate the virus. Once you have a clean hard drive, copy the SCAN files to it, and check EVERY floppy you get from someone else, by putting it in your A: drive for example, and giving the command SCAN A:.

The second way to protect yourself is even better, and it does not require the use of any additional programs, provided you have DOS 6.xx (xx = version 00 or above). DOS 6.xx contains an excellent program that can actually immunize your machine, called VSAFE.COM. The presence of VSAFE.COM in the latest version of DOS (6.20) is really good reason to upgrade, if you are using DOS 5 or below. DOS 6.20 is generally an excellent operating system.

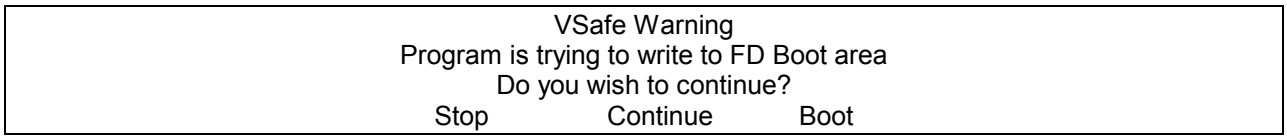
VSAFE is a TSR (Terminate and Stay Resident) program that you should call from your AUTOEXEC.BAT file each time you boot up. It will use about 23k of memory, but that can be high memory if you have a 386 or above. VSAFE sits in the background, and pops up on your screen to warn you of anything that might smack of a virus trying to infect your machine. Here is how I load it on my 386 machines:

```
loadhigh c:\dos\VSAFE.COM /1+ /2- /3- /4- /5+ /6+ /7+ /8-
```

If you have an XT or a 286, the "loadhigh" should be changed to "load" (without the quotes).

What are all those switches after the VSAFE.COM above? /1+ tells the program to warn you if anything tries to format the hard drive. /2- turns off the warning if anything tries to become resident in memory. /3- turns off the warning when anything tries to write to any disk drive. /4- means don't check each executable file when it is run. /5+ tells VSAFE to check the boot sector of any floppy you put in your machine. /6+ tells the program to warn you if anything tries to write to your hard drive's partition table. /7+ turns on a warning if anything tries to write to a floppy's boot sector. /8- tells VSAFE not to warn you if anything tries to modify an executable file.

As you might have guessed by now, a + after a number turns that feature on, while a - turns it off. The loadhigh command line above reflects my particular desires, but you might try turning all switches on when first trying the program out. The warnings will pop right up on your screen. Here is what will happen if the /7+ switch is on, and you format a floppy disk:



Pressing S will stop the process, C will let it occur, and B will reboot your computer. Now that's control! Go upgrade to DOS 6.20. Safe computing!