



Connections

By David J. Buerger

A Specter Is Haunting Networks — The Specter of Viruses, Hidden in Horses

PC viruses are in the news. A spate of recent articles has left many users with the impression that a mysterious cancer is gobbling up computer data left and right.

It's time for network managers, bulletin board enthusiasts, and anyone who shares programs or data with other PC users to understand how viruses work and how to confront them.

A computer virus operates like a biological virus. It is a program file containing logic that replicates by attaching the viral code to another program file. Viruses are transmitted when infected files are copied to your computer disk. Each time the infected program executes, the virus can attach itself to other programs or perform whatever its designer intended it to do.

Benevolent viruses sometimes are deliberately used for friendly purposes: file security (encryption/decryption), file transfer and storage (compression/decryption), copy protection, and commercial program enhancement (third-party add-ons).

Malevolent viruses wreak computer system havoc without a user's consent. These intruders can randomly contaminate data or programs, erase files, and format disks. Their secret operation can even spread similar mischief to co-

workers' computers.

More insidious viruses lie dormant before spreading their destruction. Their trigger may be a predetermined date, time, or system configuration, or a preset number of executions of the infected program. Network viruses might look for the absence of a user ID or a security clearance change.

Motivations for spreading malevolent viruses may include taking revenge on an employer, espionage, or simply the thrill of vast destruction.

The apparent rise of computer terrorism requires everyone to consider exposure and devise protection strategies.

The first step is to consider how much you are at risk of exposure to malevolent viruses. Your risk is minimal if:

- Your computer is a stand-alone unit rather than networked.
- Your computer has no modem.
- Your computer and software are used only by yourself.
- Your computer and software are not accessible to other users.
- You never share programs or files with other users.
- You do not use unauthorized copies of commercial software or operating systems.
- You do not use public domain or shareware software.

Risk increases as more of these categories do not apply to you.

If you want your risk is high enough to warrant a protective strategy, there are many ways to decrease the chances of viral infection.

Nontechnical tactics include: limiting access to your computer by locking your computer or office and by logging off a network account when you step away from your desk; using only commercial software purchased in a sealed, shrink-wrapped package; using only known public domain or shareware software; and letting someone else be a guinea pig who runs suspected software on another system before you copy it to your own disk.

If you are a bulletin board addict who loves to download the newest utilities, you are at a high risk of exposure to infected "Trojan horse" software. Terrorist programmers like to hide viruses in popular utilities. I have recently seen reports of two well-known utilities, ARC and List, which were infected with a virus. Other potential carriers are public domain programs that break copy protection and unauthorized copies of commercial software or operating systems.

Don't be lulled into a false sense of security merely because you use a


"hidden" bulletin board. Despite system operators' best attempts to flag down Trojan horse software, a few programs do slip by. One recent example is the virus found in a Macintosh program on Compuserve's Hypercard forum. Although the virus was exterminated in one day, about 40 people unsuspectingly downloaded the virus.

The surest remedy is to download only source code files, examine every line of code to verify the absence of mischievous programmed logic, and then compile the code yourself.

If this tactic is not practical or possible, you still can take additional technical steps to protect your computer from viral contamination. "Anti-virus" software can be used to help prevent the intrusion of unknown viruses, along with "vaccine" software to eliminate known viruses. My next column will look at how several of these programs work to reduce the risk of destruction caused by virus software.

David J. Buerger is director of the Personal Computer Center at Santa Clara University, in California. E-Mail comments may be sent to: dbuerger@scu.bitnet or MCI Mail ID 304-0160; start the MCI "Subject" line with [DDB]DBJuerger. The views expressed are his own.

 <p>ATI 8T8/10 MHz</p> <ul style="list-style-type: none"> • 80286 processor selectable • 8 & 10 MHz keyboard • 640K RAM included • 1MB motherboard • 8 I/O expansion slots <ul style="list-style-type: none"> • Real time clock/calendar • 1.2MB floppy drive • Floppy/hard controller card • AT style keyboard • Setup software <p>\$999 Monitor Optional</p> <p>What the editor said... "Overall system performance is quite excellent."</p> <p>PROCESSOR OPTIONS: 16 MHz with 0 wait state, 8/12 MHz with 0 wait state available</p> <p>SPECIAL: ANI's 8T 640K, HDC/FDC, 12 floppy drive, 30MB hard disk monochrome graphic card with parallel port, high res mono monitor, MS-DOS 3.1/GW-Basic, AT style keyboard \$1795</p>	<p>MODEMS</p> <p>EVERETT 100% Hayes 300/1200</p> <p>Basic Internal Compatible features auto answer, send, redial with built-in speaker and software \$299 1200/3000 Basic \$229</p> <p>US ROBOTICS 300/1200/2400 \$199 300/1200 Internal \$120 300/1200 External \$120</p> <p>NEW 3.5" 1.44MB drive for XT/AT w/mounting kit (PS2 compatible) \$149</p>	 <p>ATI PC 2</p> <ul style="list-style-type: none"> • 640K, 8 slot motherboard with 4.77 MHz clock • Two 360 KB DS/DD drives • 150 watt switching power supply • FDC I/O card • (includes serial, parallel, game port, clock/calendar, battery backup) • IBM XT compatible • AT style keyboard <p>\$CALL</p> <p>• OPTIONAL: Turbo option 4.77/8MHz using NEC V-20/8088-2 available. All mono/color/EGA configurations available.</p> <p>SPECIAL: ANI PC2 20MB hard disk system with 640K, FDC, 1 drive, Hercules compatible monochrome graphics card with parallel port, high resolution monochrome monitor, AT style keyboard \$995 MS-DOS 3.1 with GW-Basic only \$99 (SOLD WITH SYSTEM)</p>
---	--	---



TOSHIBA AT1200

HARD DISK PERFORMANCE IN A BATTERY-OPERATED PORTABLE.

\$CALL

- 20MB hard disk, 1MB memory, 720KB 3.5" floppy, super-twist screen and removable, rechargeable battery pack
- All in a 10.9 pound portable that runs up to 7 hours on batteries (AC too!)
- Easy expansion with built-in ports and broad option choices
- Everything you want in a portable PC!

DON'T COME HOME WITHOUT IT!

TOSHIBA T3100/20

Standard Features:

Processor: 80286 CPU running at 8 or 4 MHz

Memory: 640KB Ram, extendable to 2.6 MB

Disk Drives:

- 35 MB hard disk
- 720 KB 3 1/2 inch PS2 compatible diskette drive

Display:

- High resolution 80 x 25 character gas plasma screen
- 640 x 480 bit mapped monochrome graphics capability
- IBM CGA compatible

Dimensions:

- 12"2" W x 3"1" H x 14"2" D
- and only 19 pounds!



THE ULTIMATE PRINTING MACHINE



P351 SX
by TOSHIBA of course

With print speed of 360 cps draft and 120 cps letter quality, it handles 120 column paper, built in tractor feed... **\$CALL**

ALL MODELS IN STOCK

Alphanumeric International **Call 213/921-8689** **TOSHIBA T3200 AND T5100 COMPUTERS IN STOCK**

13300 East Firestone Blvd., Suite F
Santa Fe Springs, California 90670