



# Tech Talk

By Steve Gibson

## Effective and Inexpensive Methods Exist for Controlling Software Viruses

This is my final column, of four, on the topic of software viruses. The first three discussed fundamental technology, reproductive action, and anti-viral countermeasure issues. This column will discuss specific viruses and specific anti-viral countermeasures.

There's a terrific group of people in Santa Clara, California, who have dedicated themselves to catching, analyzing, and disseminating helpful and specific information about software viruses. This nonprofit organization, the National BBS Society (NBBSS), can be contacted at (408) 727-4559.

The NBBSS has identified 39 different strains of software viruses, and more are being found continually. For example, the latest virus, which the NBBSS has preliminarily named the "retro-virus," was just submitted by one of its members on April 19. This retro-virus infects and lives inside any one of three popular shareware programs. The virus reproduces by attaching passive carrier clones of itself to other executable files in the hope that the infected executable file will make its way to another system that contains one of its three target "infectable" host programs.

It was named the retro-virus because it continually communicates with its infected clone carrier executables via a

clever "flag" hidden within the system. When any of its viral clones executes, this flag is turned on. Then when one of the three internally infected hosts executes, this flag is checked, then turned off. If the flag was already off, the host determines that the system must have been swept clean of its viral carriers. Then, after quietly waiting for several months, the host *reinfests* several of the system's executable files. The system user thinks that the system was virus-free... but the same virus reemerges "from out of nowhere."

As you can see from this example, we are dealing with some extremely sophisticated programming that is specifically intended to defeat attempts at removing the viral code from the system.

So what measures can be taken to deal with and curtail the spread of software viruses? The good news is that there are several ways to approach the problem. Viruses can either be caught "in the act" of spreading their seed or located while they're lying dormant on a disk.

The "catch 'em in the act" approach provides the best protection currently available since the reproductive behavior of many viruses can be somewhat generalized and then readily spotted. Such solutions have the negative side effect of requiring continual RAM resi-

dency, with all the problems which that implies. Also, they can sometimes erroneously alert their owner to questionable but benign behavior of non-viral software. Even so, these programs are innocuous and are highly recommended when using new software submissions on any system that falls into a high-risk group for viral infection.

The two most effective virus detection monitors available today happen to be the least expensive of any available. Flushot+ is available as shareware, with a \$10 fee requested, and C-4 is a commercial product retailing for just \$29.95.

Flushot+ catches 22 of the 39 viruses that are known to the NBBSS, providing far greater protection than other currently available virus-fighting agents that retail for hundreds of dollars. Flushot+ can be downloaded from Compuserve (in the IBMSW Forum in DL0), from the IBM SIG on The Source, or from its author's bulletin board system in New York (1,200/2,400 baud: [212] 889-6438) under the name FSP12.ARC. Flushot+ can also be requested directly from its author, Ross Greenberg, at (212) 889-6431.

C-4, which derives its name from Cybernetic Xylene since Xylene inhibits the growth and spread of carbon-based






















viruses, is the best commercial viral inhibitor currently available. Though you might have trouble believing that \$29 could buy much, C-4's publisher is dedicated to stopping software viral spread and even intends to offer continual upgrades at near their cost. As a result of Interpath's association with the NBBSS, C-4 is the only product today that stops the spread of every one of the NBBSS' 39 known viral strains! It can be purchased from Interpath, 4423 Cheeney St., Santa Clara, CA 95054; (408) 988-3832.

Over the last four weeks it has been my goal to address this issue directly and frankly. Having looked closely at these viruses, I believe that the problem is less widespread than the popular press has indicated, but I also believe, based upon an analysis of the reproductive mechanisms involved, that it has far more potential for damage than is commonly believed.

Please exercise some form of self-protection, even if it's just altering some software trading habits. In the mean time, I'll keep you posted.

*Steve Gibson is the developer and publisher of Spin Rite and president of Gibson Research Corp. of Irvine, California. The views expressed are his own.*

# And choose.

 NBI, Inc. Model 908	 QMS-PS® 800 II, 810	 Linotype Company Linotronic™ 100, 300, 500	 Texas Instruments OmniLaser™ 2106	 Texas Instruments OmniLaser™ 2108, 2115	 The Laser Connection PS Jet/PS Jet™	 Dataproducts Corp. LZR™ 2665
 Qume Corporation ScriptTEN™	 Digital Equipment Corp. PrintServer 40™, ScriptPrinter™	 AST Turbo Laser®/PS	 IBM 4216-020 Personal Pageprinter™	 Vanityper VT-600	 Apple Computer Inc. LaserWriter® IIx, IIvX	 Quadram Quadlaser™ PS
 Agfa-Gevaert P400PS™	 General Computer Business LaserPrinter Plus™	 Wang LCS15™	 NEC Information Systems SilentWriter™ LC-890	 Diconix Diji® I/PS	 Apollo Computer Inc. Domain/Laser 26™	 QMS-PS® 2400, QMS® JetScript™