Behavior Research Methods, Instruments, & Computers
1989, 21 (2), 334-340

SESSION XIII
TUTORIAL: COMPUTER VIRUSES

Walter Schneider, *Presider*
University of Pittsburgh

Computer viruses: What they are, how they work, how they might get you, and how to control them in academic institutions

WALTER SCHNEIDER
University of Pittsburgh, Pittsburgh, Pennsylvania

A computer virus is a program that replicates itself and spreads to computers with the goal of disrupting or destroying normal computer use. In academic computing, viruses represent a serious problem that costs millions of dollars in losses annually and hinders the free exchange of information so critical to education. Viruses operate in incubation, infection, and destroy phases. The nature, mechanisms, and preventive measures for personal-computer viruses are reviewed. Different procedures are recommended to protect research laboratories, instructional laboratories, and software lending libraries. Tradeoffs between providing adequate protection and not having the security become too burdensome are considered.

Computer viruses are programs that replicate themselves to spread to other computers; they have the potential of altering the behavior of their computer hosts. They can destroy research and instructional data and computer equipment, and they can easily be spread by honest, unknowing individuals, who are themselves using the host computers appropriately. Researchers need to take basic steps in order to prevent any catastrophic loss of data due to computer viruses, because universities, which typically encourage free exchange of information among many individuals, unfortunately thus make it very easy for computer viruses to do extensive damage. This paper provides a tutorial on what computer viruses are and how one can deal with them in academic settings. A complete description of computer viruses can be found in R. Roberts's (1988) book on the topic.

A computer virus can affect any laboratory in which honest individuals are using programs imported from other sources. Viruses can be spread through the normal use or installation of commercial software, as well as through malicious intent. It is important to remember that in most cases, viruses have been spread unintentionally by people who did not mean to harm the computer systems they operate.

One should always operate a computer with the assumption that a virus may infect one's computer if one does not take preventive action. Even a single individual tens of thousands of miles away from a university can destroy the data in an undergraduate laboratory. The University of Pittsburgh, for example, was hit by the "BRAIN" virus, which has spread to over 110 countries. It was originally written by two brothers in Pakistan, who felt that they were not making sufficient money in their software company because of the illegal copying of programs. Their virus began by making its way into some of the illegal software-copying stores in Pakistan.

I do not know with certainty just what this virus's path of spread was, but here is a likely scenario: The virus replicated itself and spread to many of the software distribution stores in Pakistan. It is thought that someone from the medical center at the University of Delaware then bought some software at one of them; the software is very cheap in these stores, because they pay no royalties to the manufacturer. This individual then brought the soft-

This work was supported in part by Office of Naval Research Contracts N00014-87-K-0397 and N00014-86-K-0678 and Army Research Institute Contract MDA903-86-C-0149. Reprint requests may be sent to Walter Schneider, Learning Research and Development Center, 3939 O'Hara St., University of Pittsburgh, Pittsburgh, PA 15260.

ware back to the University of Delaware, where the virus spread through the medical center and on to the University of Delaware in general.

It is also believed that someone from the University of Pittsburgh who used a computer at the University of Delaware imported the same virus back to the University of Pittsburgh, where it then replicated itself in the university's public laboratories. One of the students who was operating a computer in the psychology department's laboratory took a floppy disk from the undergraduate lab and ran it on one of the public sites (perhaps he was doing word processing both at the public sites and on the laboratory computer). This was, of course, a totally legitimate use of computers on campus. Unfortunately, while the student was word processing at the public site, the virus attached itself to the student's copy of the word-processing program. When the student returned his floppy disk to the psychology lab, the virus attached itself to the operating system on a lab computer.

The virus spread within our laboratory when data from all of the computers were merged on one master file in the main computer. After several days of replicating itself, the virus began to erase the disks of the computers in the undergraduate laboratory. With the exception of the very first activity that occurred in Pakistan, probably all of the other activities that enabled the virus to spread resulted from honest individuals' appropriate use of computers.

The net effect of the virus attack was the destruction of several months' worth of data collected in the undergraduate labs. When the virus destroyed the data from 120 students from my laboratory class, I was more infuriated than I have ever been in my academic career. It was as if someone had broken into my office and gone through my filing cabinets destroying all my data. Fortunately, because the data had been backed up, after several days of work the lab was functioning again. This type of spreading of a computer virus can and probably will occur in any laboratory that allows disks to come in from the outside.

It is important to take precautions to reduce the virus threat. One should think of controlling viruses as one thinks about the security of one's home. Almost any home can be broken into even when extreme security measures have been taken. Most people use basic security measures, such as locking their doors, to make it at least somewhat difficult for a would-be thief. Such basic measures inhibit robberies enough so that they are infrequent, and we can proceed with our lives relatively unincumbered by either robberies or extreme security measures. But if robberies become more of a problem, one may have to consider more extensive measures against intrusion (such as installing a security system that requires one to enter passwords whenever entering or leaving the premises). One must trade off ease of access against security. Fortunately, however, a few simple procedures can provide protection from most viruses. It is important not to become paranoid about the virus problem, but rather to choose an appropriate level of security that will allow computers to accomplish one's tasks while the virus problem is kept in check.

What Is a Computer Virus?

A computer virus is a program that installs itself upon a system to infect and/or destroy (or alter) other systems. It is very important to understand the characteristics of a virus so that one may reduce the likelihood of its spreading. A virus is an executable program that attaches itself to other programs in order to spread. A simple example would be a virus that alters a computer's operating system so that whenever the system is started up (booted), the virus code will be executed. The virus then examines other programs that can carry it (e.g., executable programs on any floppy disks inserted into the machine), and it will reinstall itself on floppy disks, which may travel to other computers. It can then install itself on other systems, whenever the infected programs on the disks are run at new installations.

The virus threat is very real. The National Security Agency of the United States has estimated that over 40% of the nation's college campuses have been hit by computer viruses. It does not take an exceptional ability at programming to write a new virus; only about three computer courses and some detailed reading will suffice. A single individual almost anywhere in the world can thus inflict damage in hundreds of countries. In the future, there will be more viruses, and they will be more dangerous. We may even find academic terrorists targeting academic departments (e.g., animal rights groups targeting programs that collect animal data). Disillusioned students may inject viruses to disrupt classes so that they do not have to turn in assignments (similar to the way "bomb scare" reports became a problem in the 1960s in the United States).

There are three phases to the operation of a computer virus; they reflect metaphorical similarities between computer science and biology. The first phase is *incubation*—staying dormant for a period of time. A computer virus can remain dormant, doing nothing, for an extended period. For example, it might only replicate itself after a certain number of starts of the operating system (e.g., every 50th reboot). An incubating virus is thus like a mole in a spy network. It sits there and operates normally for a long time, so that nobody suspects that it is there. Users are frequently suspicious of new programs that cause trouble on their computers, so that a virus that would immediately alter the operation of a computer might quickly be detected. A virus that would allow normal operation for several months, however, and only then begin to alter the operations of the system, would be more likely to go undetected. Note that *there is virtually no way to detect a virus while it is in its incubation phase*. Unless one has a copy of the program before a virus has hit it, or particular signature information for a specific virus, there is no way to detect a virus during this period.

The second phase of a virus is *infection*, during which the virus tries to replicate itself and spread to more computers. During the infection phase, the virus program tries to identify new host programs and install itself on them. A sophisticated virus will install itself on other programs without doing damage, so that it can spread before it is detected. Typically a virus will install itself on the boot block or operating system, or on executable programs (e.g., .COM, .EXE, .SYS, .BAT, or overlay files on IBM-compatible computers). Note that *a virus can only spread by installing itself on executable programs*. A virus cannot be spread by modifying text or data files. A virus may install itself on a boot block or the operating system (e.g., COMMAND.COM file). During the infection phase, a virus can be detected. For simple viruses, this is done by means of identifying the change in the date or the length of existing files. Complex viruses may alter a file without changing its date or length; these viruses can typically be detected if there are changes in the check sum of individual files. However, the check sum requires a signature file thar records the check sums of the files to be recorded.

In the third phase of a virus, the *destroy* phase, the virus destroys or modifies the operations of the host computer system. The destroy phase typically occurs after a period of time during which the virus has spread. For example, one virus might allow the system to be rebooted 20 times before it would shift from the infection to the destroy phase. The typical user might run a system for nearly a month of infecting other disks before the virus would go into the destroy phase.

Many different malicious activities have been carried out during the destroy phase. A benign virus might put up a scare message or lock the system. For example, a program might put on the screen "beware of the virus," and not allow any other actions by the user. Some viruses will destroy all data and programs (e.g., the BRAIN virus will erase the hard disk). Note that *a virus can destroy data passing through a machine, as well as destroy data on the system disk*. For example, a virus may destroy just a subset of data files and then only destroy those files on the backup floppy disks. Such a virus could destroy a person's complete dissertation work. The student, for example, might run an analysis and find that the data file can no longer be read by the analysis program. The student might then take the backup data, stick it into the disk, and copy that data file back onto the disk. However, at this point the virus could attack the original data file, destroying it while the copying takes place. In this way, both the original file and all backups of the data file could be lost.

One should remember that a virus can attack files even if they are not being read or written by the user. Some viruses consume computer resources. For example, a virus might execute a simple loop repetitively on each interrupt from the time-of-day clock, thereby consuming 50% of the computer's capacity. Another virus might create hidden files that use up disk space. At least one virus has been reported as destroying computer hardware. This virus could continuously move the disk back and forth from its minimum to its maximum travel. The hardware was not designed to withstand such continuous movement; it resulted in the heating up of the disk coil or motor, and it was claimed to have started fires within the computer. Viruses have also been known to alter the writable control store. Computers often contain a small amount of nonvolatile memory, which typically encodes information such as the kinds of disks or special devices that are attached to the computer. If a virus writes this writable control store, it can alter the machine so that it doesn't even recognize the hardware that exists in it, and the user must then reconfigure the system completely. Since the original configuration may have been made in the factory, most users can be at quite a loss when having to fix the writable control store.

Perhaps the most dangerous mode of destruction occurs when viruses alter data in a manner that is undetectable. Viruses can be written to seek out programs of a particular file type and alter the data, yet maintain the format of the data so that the programs using the data operate normally. For example, a virus could be written to locate all the spreadsheet files (which have a common extension file name such as ".wks") and randomly alter a few of the data cells on the spreadsheet (e.g., it might alter some of the summation formulas to add 10% to the total). The spreadsheet program would then operate normally but give bad results. In a research application, this could cause someone to falsely report a result as significant because practically no one calculates data by hand anymore.

To review: a virus infects a computer in three phases; only the third phase is detectable without special virus protection programs. In the first phase, incubation, the program typically waits until the user no longer suspects that a new applications program contains the virus. In the infection phase, the virus spreads to other programs that can be transported to other computers in a way that is not likely to become detected. In the destroy phase, the virus produces some sort of havoc within the host system.

How to Limit the Spread of a Virus

There are three approaches that can be taken in order to limit the spread of a virus. They involve: limiting access to the computer, installing virus protection programs, or installing disk-watch programs. Each method has its costs and benefits. No method is certain.

Since viruses come from other computers, the first approach is *to limit the number of foreign executable programs* that can be run on one's computer. Computer viruses cannot be spread through the air like some human viruses. A computer virus is more analogous to the human disease AIDS, which can be spread only through intimate physical contact or the exchange of blood. A computer will not pick up a virus unless one executes a program infected by another computer that has the virus. If executable programs are not imported from other sources, a computer cannot become infected. Viruses are particularly common on free computer bulletin boards, Christmas card programs, games, and some antivirus programs. One should be very cautious about importing entertainment programs. Any popular game program is likely to have been run on many machines, and hence it is a good target for viruses.

One should also be wary about using pirated software. Such software is more likely to have a virus because of its questionable history. The original manufacturers of software products will generally compile their programs from raw source code, which makes it very unlikely that a virus will be introduced by a manufacturer (although, there have been several instances in which commercial software houses have unintentionally spread viruses).

The first line of defense I use in my lab is to have all staff members sign an agreement that they will not bring any executable software into the laboratory without written permission from the lab director. I also have my staff read sections of this paper for background. Students can still do word processing of their homework on the machines, but they must use the word-processing programs that are already in the laboratory. I find the risk of having a virus incubate for several months and then begin to randomly alter data to be too great to offset the minor benefit of allowing people to use external programs in my laboratory.

The second method of limiting access is to use write-protection tabs on disks whenever possible. Write-protection tabs are usually small pieces of foil for 5.25-in. floppy disks, or a small tab on 3.5-in. diskettes, which can be flipped. The hardware in the disk drive checks to be sure that the disk is not write-protected before writing on it. By write-protecting a disk, one prevents a virus from altering the disk and also has the possibility of detecting a virus during its infection phase (e.g., if one gets a write-protection error on the disk that one was not trying to write to, the probable cause is a virus). When one takes a floppy disk to a public site, it is particularly important to install write protection. Remember, even if one does not intend to write on a disk, a virus may copy itself onto the disk. Write-protection tabs can prevent this problem.

The third method of limiting the access of viruses involves bringing copies of one's own operating system and any executable programs to external computers. In this way, one will be protected from being attacked by a virus at a public site. Note that it is critical that one boot off of one's own floppy disks rather than the public site's operating system, because the most likely source of the virus is the operating system itself. If it is necessary to execute programs at a public site, one should remove all executable files from any floppy disks to be operated there, and use write-protection tabs whenever possible.

The second approach to virus protection, the *installation of virus protection programs*, has both benefits and costs. The Appendix provides a list of commercially available antivirus programs. Of course, any virus protection program is limited. Such programs can only detect viruses during their infection or destroy phase, and they can substantially disrupt normal computer functioning.[1] The typical antivirus program installs itself on the operating system and monitors the likely locations where a virus would attack. For example, an antivirus program might monitor to determine if any program tries to do a direct write to the disk, or install itself on the clock interrupt (common behaviors of viruses). The problem is that many programs will appropriately do direct writes to the disk (it is often much more efficient) or alter the operating system. Most terminate and stay resident (TSR) programs, such as Borland's Sidekick or various spell checkers function thus (see Duncan, 1988). Some virus programs will do a check sum on every sector of the disk when it is read into the system. This can quickly detect when a virus goes into its infection phase, but, the check sum may consume 20-30% of one's computer time during disk input/output and substantially decrease the disk storage space.

A serious problem with antivirus programs is that they frequently "false alarm." I found this to be an acute problem with the public domain antivirus program called Flushot. The program detected and provided a warning every time a program did a direct write to the disk. However, the word-processing program that I use on my computer also does direct disk writing. Thus, every time I used the word processor I got many false alarms, warning me about potential virus writes. Just as the lamb that always cries wolf will be ignored, an antivirus program that reports many legitimate operations as potential viruses will come to be ignored too. I decided that the standard antivirus programs false alarm too frequently to be usable in my laboratory.

The third approach to limiting access of viruses is to install disk-watch programs to detect the results of the infection phase of a virus. A disk-watch program will maintain a check sum (i.e., a code for the specific bit pattern for all the bytes on the file) for every appropriate file on the system disk. The disk-watch program is run originally to make a fingerprint of all the executable files (typically the .EXE, .COM, .SYS, .BAT, driver, and overlay files, the boot block, and the operating-system overlay files). Whenever the disk-watch program checks the system, it checks the date, length, and check sum of all the files to see whether or not they have been altered. In most applications environments, users modify data but rarely modify the executable forms programs (the notable exception occurs when programmers use compilers to make new programs). For example, the user might utilize a word processor to modify many word-processing files in the system. The disk-watch program will verify that the word-processing executable program (e.g., WP.EXE) is not altered, and it will report any such alteration. However, it does not report when any of the word-processing files are altered. Since a virus cannot be spread via the word-processing files, it is not necessary that these be checked for viral infection. For the typical user of a computer system, the .EXE and .COM files are not altered except when new software is installed. Thus, a disk-watch program will rarely false alarm, and usually one can recognize the legitimate occurrences of false alarms (e.g., when a new version of the software has recently been installed).

The process of installing and using disk-watch programs is straightforward. On first installation, the disk-watch program scans all of the files creating a signature file with the date, length, and check sums of all the programs. Every time the computer is rebooted, all of the executable files are checked for their length and date of last modification. This is done by including the disk-watch program name in the "AUTOEXEC.BAT" file to automatically check the disks. It takes about 12 sec to do a date, time, and length check of all the critical files on a reboot. Every week I do an automatic check-sum test. This requires 5 min (on an AT computer with a 200 MB disk and 200 files to check). The program that I use allows one to set a check-sum verification interval, so it automatically does the check-sum test once a week and the fast length and date checks otherwise.[2] This eliminates the need to keep records on when to do the check-sum test, and it does not slow down the boot process substantially. If the system detects that a file has been altered, it reports the file name and the way in which the file has been altered (changed in length, date, check sum). The user must then respond by indicating that he or she has noticed this change and can tell the program to alter the signature file so that the new version of the file will be recognized in the future. The user may have to enter a password to change the signature file. Updating the signature file takes only a few seconds for each altered file.

A disk-watch program can be used on a "quarantine" computer to detect new viruses. One computer in my laboratory is designated as the quarantine computer, on which any new software is first run. On this computer, the disk-watch program checks not only the executable files but all files on the disk. In this way, any attack of the virus will be detected. I do check sums on the quarantine computer at both the beginning and the end of each day's running of the programs.

To be effective, antivirus procedures must be as automatic and as easy to execute as locking the door of a house. An antivirus program should be completely self-explanatory. It should be possible to create and update any signature files by means of the user's simply indicating "yes" or "no" to questions that require judgment (e.g., when a changed version of a program appears). If the program false alarms, or if it requires one to consult a manual, the antivirus procedures will probably not be used reliably.

Whether one limits access to a computer, installs virus protection programs, or installs disk-watch programs, users incur at least some type of inconvenience when they attempt to limit the spread of computer viruses. Any system can be broken into. In my own laboratory, I have found limited access in combination with a disk-watch program to be the best compromise. This combined approach has prevented further virus infection, and it required only minimal changes in the normal routine of the laboratory.

What to Do if Hit by a Virus

The typical first symptom of a virus attack is that the computer seems not to be operating normally. Once in the destroy phase, a message may appear and all the files may be lost. For an unsophisticated virus, the spreading of the virus either does nothing or programs exhibit some strange behavior. For example, with the BRAIN virus, when one executes a program, some random characters appear on the screen and the program appears to abort. During this period, the virus attaches itself to the operating system. Frequently, the length and date of some of the executable files will have been altered on the disk. Also, one may get write-protection errors on a floppy disk that has been protected, even if one does not intend to write on the disk. Getting write-protection errors is strong evidence that a virus exists on the computer. A complex virus may change executable files without necessarily altering the date or the length of the file. A complex virus, for example, may add new hidden files that do not appear when one executes normal directory commands.

The process of *disinfecting a computer from a virus* amounts to rebuilding the system from scratch. The first thing to do is to save any nonexecutable files (e.g., data files) on floppy disks and label the disks as potentially corrupted. One should do the copying after booting from a new copy of the operating system. The second step is to reformat the system, rebuilding the entire system from the originals. This means booting the system from an original operating-system floppy disk. One must reformat the disks (note that to delete all the files may not be enough) and reinstall the operating system. Then one copies all of the other files from original masters or backup copies.[3] Thereafter, one may copy any of the nonexecutable files that were backed up from the original system before it was reformatted. One should not copy any of the old executable files that may have been corrupted. Finally, one should label all disks that have passed through the machine as possibly infected. Also, any machines that ran disks which passed through the system should be labelled as potentially infected. One must be cautious in interpreting any data that has been potentially corrupted.

Once a virus has attacked a site, the virus may be expected to hit again. This is a particularly serious problem in public sites. Students will use infected software at a public site and transfer a virus to their own floppy disks. Several weeks later, the virus may be detected and corrected at the public site. Thereafter, the students may come back with their disks and reinfect the public site. Some viruses have continued to reappear for months after the original infection at public sites.

Once a virus has infected a site, users will blame almost any unreliable behavior on it. It is important to remember that hard disks often become unreliable with age, and that the loss of data does not imply that a virus must be acting. I have found in my laboratory that after a virus scare, users blame absolutely everything on the virus. I recommend running frequent disk-maintenance programs on a regular basis, or whenever someone complains about unreliability and there is no other evidence of a virus. I had one user who would turn off the computer while it was writing files, which produced problems in the file allocation table that we initially blamed on a computer virus.

How to Check New Software

It is very difficult to check new software in order to verify that it does not contain a virus. I have seen the following techniques reported on various bulletin boards on the topic: When using new software, it is useful to run the software on a quarantine computer. On the quarantine computer, one should use some type of disk-watch program to verify whether or not any program has tried to infect other programs. One should run new programs on several days with several executions, restarting the program numerous times. One should alter the system date, changing the month, day, and year between restarts of the program. One should check special dates (e.g., Friday the 13th). These procedures are likely to counteract the incubation time of a virus and increase the chances of its being detected.

Impact on Academic Exchange

The presence of computer viruses need have no direct impact on data transfer or text transfer between laboratories. Since a virus will not be spread by data files, no one should hesitate to send or request somebody else's data. However, researchers should be cautious about requesting or using someone else's executable programs.

Software lending libraries must alter their procedures to limit the spread of viruses. Some universities run software lending libraries, which are likely to become spreaders of computer viruses. The easiest way to protect a software lending library is to write the data on notchless disks that cannot be written on by standard equipment. A notchless disk is one on which write protection is always in effect. To write on such a disk requires specially ordered disks and modified disk drives. Such drives can be purchased or modified by an experienced technician. For any new software package, data should be copied from original disks to the notchless disks, which then may be loaned out without fear of any unintentional copying of a virus on to the disks. A second procedure involves running a disk-watch program to check the disks when they are returned. In this case, a signature file for each of the disks is maintained on a master disk within the library. When the loaned disks are returned, the date, length, and check sum are compared to the signature file, in order to verify that none of the files has been altered. This check is also useful for verifying that no one has unintentionally deleted any of the files from the loaned disk. Note that both the notch procedure and the disk-watch procedure work fine on disks when the user is not supposed to alter any of the files on the system. If the user must alter some of the files on the system (e.g., in using the disks on a two-disk system), only the disk-watch procedure can be used, and it can only check the system's nonaltered files.

Public sites require special precautions to limit virus spread. At a public site, many users operate computers and viruses can be introduced at any time. If the system at the public site employs floppy disks, each computer should have its own set of write-protected operating-system disks.[4] Between every use, the computer should be rebooted and the disk-watch program run. At the very least, the date and time of all of the files should be checked, and probably a check sum should be made as well. It is important that all changes to the executable files be reported to a laboratory supervisor. At a public site, a special password should be entered to update the signature file on disk-watch programs. In this way, a student who reboots a system will have to notify the supervisor when a critical file has been altered. Students might be encouraged to bring in their own operating systems and executable files when they are using a public site. When a user always executes only his or her own files, the user will neither pick up nor spread a virus. It is important that all users of the public site be aware of the seriousness of computer viruses and ready to report any behaviors that suggest a virus.

Summary

Laboratories should be run under the assumption that without precautions they will be hit by a computer virus. The virus will most likely be brought into the lab by somebody who is making legitimate use of the computer. Taking precautions to protect against viruses is not very difficult. Basically this involves the limitation of access to the computer and the installation of systems that will detect when a virus begins to spread. But one must remember that no system for detecting viruses is foolproof. Nevertheless, given a few precautions, one should be able to keep this very serious threat to scientific computing sufficiently in check in order to prevent serious loss of information.

REFERENCES

COMPUTER SECURITY INSTITUTE. (1988). *A manager's guide to computer viruses*. Northborough, MA: Author.

DUNCAN, R. (ED.). (1988). *The MS-DOS encyclopedia*. Redmond, WA: Microsoft Press.

ROBERTS, R. (1988). *Compute!'s computer viruses*. Radnor, PA: Compute! Publishing.

NOTES

[1] Some antivirus programs scan the disk for specific strings that have been found in viruses. This is not a general solution, but it will detect a few well-known unsophisticated viruses during the incubation phase.

[2] The program is named A-OK; it is distributed by Psychology Software Tools (see Appendix), and it can be purchased for single, departmental, and university site licenses.

[3] Note that, as a precaution, it is important to back up all files on a periodic basis and use write-protection tabs on floppy disks when one is restoring the files.

[4] If there is one set of boot floppy disks that are not write-protected and used for all the computers in a laboratory, an infection on any one computer will very rapidly be spread to all of the computers.

APPENDIX
Antivirus Protection Products

A-OK ($49 single,
$149 department,
$499 university)
Psychology Software Tools,
Inc.
511 Bevington
Pittsburgh, PA 15221
(412) 244-1908

Antidote ($60)
Quaid Software
45 Charles St., E.,
Third Floor
Toronto, Ontario
Canada M4Y 1S2

Antigen, No Virus ($199)
Digital Dispatch, Inc.
1580 Rice Creek Road
Minneapolis, MN 55432
(612) 571-7400

C4, Tracer ($40)
Interpath Corp.
4423 Cheeney St.
Santa Clara, CA 95054
(408) 988-3832

Composec-II ($400)
American Computer Security
112 Blue Hills Court
Nashville, TN 37214
(615) 883-6741

Corporate Vaccine ($189)
Foundation Ware
2135 Renrock Rd.
Cleveland, OH 44118
(800) 722-8737
(216) 932-7717

CryptoLock II ($79)
Commcrypt Inc.
1105 Piney Meetinghouse
Road
Rockville, MD 20854
(301) 299-7337

Protec ($195)
Sophco Inc.
P.O. Box 7430
Boulder, CO 80306
(800) 922-3001
(393) 444-1542

Softlog, Reporter ($2400)
Asky Inc.
770 Sycamore Drive
Milpitas, CA 95035
(408) 943-1940

Vaccinate Plus ($70)
Computer Integrity Corp.
P. O. Box 17721
Boulder, CO 80308
(393) 449-7377

Vaccine ($80)
World Wide Data Corp.
17 Battery Pl.
New York, NY 10004
(212) 422-4100

Vir Alarm, Vir Alert,
Vir a LAN ($100)
Integrity Technologies Inc.
395 Main St.
Metuchen, NJ 08840
(201) 906-1901

Vir-Pro ($50)
International Security
Technology Inc.
515 Madison Ave.,
Suite 3200
New York, NY 10022
(212) 288-3101

Virusafe ($150)
Com Net Co.
29 Olcott Square
Bernardsville, NJ 07925
(201) 953-0322

Data Physician ($200)
Digital Dispatch
55 Lakeland Shores
St. Paul. MN 55042
(800) 221-8091
(612) 436-1000

DiskManagerPC ($100)
Cooke Publications
Box 4448
Ithaca, NY 14852
(607) 277-6287

Disk Watcher ($100)
RG Software Systems Inc.
2300 Computer Ave.,
Suite I-51
I-51 Willow Grove, PA 19090
(215) 659-5300

Dr. Panda Utilities ($80)
Panda Systems
801 Wilson Rd.
Wilmington, DE 19803
(302) 764-4722

Flushot Plus ($10)
Software Concepts Design
594 Third Ave.
New York, NY 10016
(212) 889-6431

LAN Investigator ($3,000)
Absolute Security Inc.
63 Great Road
P.O. Box 399
Maynard, MA 01724
(508) 897-1991

Mace Vaccine ($20)
Paul Mace Software
400 Williamson Way
Ashland, OR 97520
(800) 523-0258
(503) 488-2322

Xficheck ($15)
Gilmore Systems
P.O. Box 3831
Beverley Hills, CA 90212
(213) 275-8006

For the MacIntosh:

Empower ($395)
Magna 2540 N. First St.,
Suite 302
San Jose, CA 95131
(408) 433-5467

Symantec Utilities for
Macintosh (SUM) ($100)
Symantec Corp.
10201 Torre Ave.
Cupertino, CA 95014
(408) 253-9600

Virex ($100)
HJC Software
P.O. Box 51816
Durham, NC 27717
(919) 490-1277

Free and Shareware
Programs:

Agar (Bill Krimmel)
CRC (Raymond Lau)
Ferret (Larry Nedry)
Interferon (Robert Woodhead)
Killscores (Mac Pack/
Apple corps of Dallas)
Rez Search (Wade Blomgren)
Vaccination (Mike Scanlin)
Vaccine (CE Software)
V-Check (Albert Lunde)
Virus Detective
(Jeffrey Shulman)
Virus RX (Apple Computer)

Note—This list includes programs listed in *PC Magazine*, 6/28/88, p. 36; *Datamation*, 10/15/88, p. 30; *Infoworld*, 1/9/89, p. S8; *A Manager's Guide to Computer Viruses* (1988).