Bureau of Mineral Resources, Geology & Geophysics

R E C O R D

RECORD 1991/18

Anti-Virus Software and its Implementation in BMR

Part 1: The IBM-Compatible PC Environment

Prame N. Chopra
Information Systems Branch

RECORD 1991/18

Anti-Virus Software and its Implementation in BMR

Part 1: The IBM-Compatible PC Environment

Prame N. Chopra
Information Systems Branch

TABLE OF CONTENTS

Abstract

BMR is beginning to depend heavily on desktop personal computers (PCs) for much of the data manipulation, numeric analysis and presentation work being done by its scientists. Numerous databases are being established in the PC-arena, often as a developmental aid for refinements to the main BMR corporate databases. Client-server applications are also being developed to facilitate the efficient use of BMR databases by BMR scientists working from PCs (e.g. Ryburn, 1990). Other uses of PCs in BMR are legion but include image processing, GIS (e.g. Williams, 1991), accounting, word processing, data acquisition, ethernet network management and point of sale administration.

There has at present been no concerted effort by BMR to protect the enormous investment that the organisation has in terms of data, programs and other scientific output that resides on its PCs (Sharp, 1990). The protection of such valuable resources in an organisation like BMR which makes such widespread use of PCs is greatly compounded by the large number of PCs, the wide spectrum of users and the general commerce that goes on in floppy discs. If a malignant PC virus were to gain a foothold in BMR, its containment and total eradication could be a difficult proposition. Clearly, a well-thought out plan to deal with such an infestation needs to be developed before damage is done. The essential element in any such plan is an effective anti-virus software package.

I have examined the anti-virus packages offered by 3 different companies in order to assess their relative merits and their possible usefulness to BMR. These packages are:

McAfee Associates anti-computer virus products
McAfee Associates, California, USA

Dr Solomon's Anti-virus Toolkit
S & S International, Chesham, UK

The Calmer Utilities
Calmer Utilities, Sydney, Australia

Each of these packages claims to be able to detect and remove 220+ known viruses and their variants and each claims to provide frequent upgrades to registered users of their products. These packages are amongst the more popular of the many anti-virus packages available commercially for the IBM-PC compatible environment. This is far from an exhaustive list however because of the sheer number of packages available and the rapidity with which they must be updated in order to keep up with the appearance of new viruses.

I summarise the claimed capabilities of these anti-virus packages and have assessed their relative performance in scanning and monitoring executable files for signs of virus attack. I have also examined the ability of these anti-virus products to detect and remove real viruses by setting up a carefully quarantined BMR computer to which I have introduced a 'cocktail' of 227 computer viruses.

Finally, I present what I believe could be workable anti-virus measures that could be used by many of BMR's PC users.

What is a Computer Virus

A computer virus is a malicious piece of code which acts to impair the operation of a computer and to spread itself from computer to computer. The virus is generally hidden somewhere within the system and may lie dormant for an extended period before actively damaging the computer system's software and/or data. The trigger for the activation of the virus may be the reaching of a particular date (e.g. Friday the 13th) or the attainment of a particular condition (e.g. the number of files on a disc exceeding a certain number). There have been numerous articles written in the computer press in the last few years on the subject of viruses, worms and trojans (see the text that follows for definitions). Some of these articles are listed in the reference section of this Record.

Viruses may be "benign" or "malignant." Benign viruses replicate, but they do not attempt to do anything hostile. For example, they may beep, display messages on the screen, or do something else innocuous, but they do not intentionally try to do any damage. On the other hand, malignant viruses, in addition to replicating, do attempt to do damage. For example, in the IBM PC world the "Israeli" virus was programmed to wake up and erase hard drives on Israel's Independence day.

It is very important to realize, however, that even benign viruses can be damaging, even if this is unintentional. Viruses occupy memory and disk space, and this is enough to cause problems. They reside at very low levels in the operating system and can interfere in unexpected ways with other parts of the system. Furthermore, some benign viruses contain apparently inadvertent bugs that can cause unexplained crashes and strange behaviour and in some cases, loss of data (e.g. the Stoned virus overwrites the directory entries for files 33 to 48 on 1.2 Mbyte floppy discs).

Viruses should not be confused with other types of destructive software such as "worms" and "Trojan horses." The media seem to have incorrectly appropriated the term "virus" to describe all types of destructive software. A "worm" is a program that replicates and spreads, but does not attach itself to other programs. Worms usually spread within a single computer or over a network of computers. They are not spread through the sharing of programs. The most well-known example is the Fall 1988 internet worm, which infected and disabled several thousand US government and university UNIX computers in a single day. A "Trojan horse" is a program that appears to do something useful, yet additionally does something destructive. A poignant example is the Macintosh "Sexy Ladies" HyperCard stack, which erases the hard drive while the user ogles the images. Trojan horses do not replicate.

Where they hide

All known viruses infect one of the following areas: The hard disk partition table; the DOS boot sector of hard disks or floppies; or one or more executable files within the system. These files can be .EXE or .COM files which are part of commercially produced software (e.g. a word processor) or they may be files of the same type produced by a user with a computer language compiler and a linker. Some of the more advanced viruses attach themselves to auxiliary files such as .OVL and .OVR overlay files and .SYS system files in an attempt to avoid detection.

How they replicate

The essential symptom of a virus attack is an unexplained increase in the size of executable files. Whatever the file type, the purpose is the same. The virus is programmed to load itself into the memory of the infected computer when the contaminated file is executed. Once in memory, the virus seeks to attach itself to all other programs that are subsequently run, or alternatively to copy its code to the boot sector of all floppy discs that are subsequently used. Viruses copy themselves in this way either by using DOS interrupts and functions or by writing directly to the disc controller.

Programs can access a disc and the data on it by directly communicating with the disc drive's controller rather than using DOS's services or that of the BIOS (basic input output system). Access of this type would be impossible to detect without the use of specialised hardware interposed between the CPU and the disc controller. Fortunately, the degree of variation that exists in hard disc controllers makes it unlikely that viruses could use this method to replicate successfully. Floppy disc controllers on the other hand tend to be more standard and thus floppy discs could be vulnerable to a virus attack via direct I/O.

Irrespective of how viruses replicate, they spread from computer to computer through the exchange of floppy discs carrying viruses either in executable files or on the boot sector. Viruses may also reach other computers over a network, particularly if they can enter the file server or servers on the network.

Symptoms of a Virus Attack

The presence of a virus in a computer can result in a wide range of symptoms being displayed and these symptoms may intensify as the infestation worsens. These symptoms may include any of the following:

- unfamiliar graphics or messages appearing on the screen
- programs taking longer to execute than normal
- excessive disc accessing &/or processing time for simple tasks
- unusual error messages occurring frequently
- less memory available than usual
- mysterious disappearances of programs or files
- increases in the sizes of executable files
- unaccountable changes in file dates and time stamps
- unaccountable changes in disc volume IDs

Source: Price Waterhouse, 1990

Examples: (from Dr Solomon's Anti-virus Toolkit)

Cascade (1701) Virus

What it does:

"At apparently random times the virus triggers the 'crumble'. The crumble is quite entertaining to watch, although if you weren't expecting it, it would be very alarming. Characters detach themselves from the screen, and fall to the bottom of the display. If they hit a character on the way down, then that character falls instead. Characters speed up as they fall. As each character starts to fall the speaker is clicked, so the whole effect is rather like a hailstorm of characters. Eventually all the characters end up at the bottom of the screen in a heap, in the correct columns, but the wrong rows."

How it replicates:

"Cascade is very infectious. If you run an infected .COM program the virus installs itself into memory. Once it is installed in memory it will infect any program that is run as a .COM file, including COMMAND.COM. It will spread with .COM files as they are passed around; these could be parts of DOS such as MODE or FORMAT; most people would see nothing wrong in copying these programs from one computer to another, as almost every computer already has a legal copy of DOS.

The virus does not go memory resident via the DOS interrupts, so some programs which try to detect viruses going memory-resident may not detect it."

Ogre

What it does:

When the virus triggers "it clears the screen and puts up 'Disk Killer - Version 1.00 by COMPUTER OGRE 04/01/1989' in black characters on a white background. Then in yellow on green it says 'Warning!!' and two lines down, 'Don't turn off the power or remove the diskette while Disk Killer is Processing!' Then in bright red, and blinking, on black it says 'PROCESSING.'

By the time you see that and react to it, it is too late as the disc will be inaccessible. You might decide to switch off in spite of what Ogre has told you, but even if you do, the disc will have been made unreadable by then..."

How it replicates:

"When you boot from an infected diskette, the virus goes memory-resident; this is true whether the diskette is a boot disc or not.... While it is in memory, any disc you access is liable to be infected. If you access the diskette (whether a read or a write) and the diskette is write enabled then Ogre will replace the boot sector with its own code, move the boot sector further up the disc, add the rest of the Ogre code, and mark these sectors as bad in the File Allocation Table. But there is a bug (or perhaps it is deliberate) in the virus; instead of marking the sectors it has used as bad, it marks a different group. Ogre also infects hard discs."

Anti-Virus Software

McAfee Associates anti-virus software

This package provides eight main programs for the detection and eradication of viruses. These programs are:

SCAN — This program scans a disc for recognisable fragments of the viruses which it knows about. In version 67 of January 1991, it includes information about 223 viruses. SCAN searches the boot sector and all executable files for recognisable virus fragments. SCAN can also attach a checksum value to each executable file which can be used by the VSHIELD programs to detect any virus attack which alters program size. With the /D switch enabled, SCAN will overwrite and then delete any files found to contain viruses. The overwriting step ensures that the infected file cannot be undeleted by programs such as NORTON UTILITIES. This protects the user from accidentally re-activating the virus. SCAN is user initiated or can be run from the autoexec.bat file at boot time. It is not memory resident.

NETSCAN — This program is a network version of SCAN which permits viruses present on file servers to be detected and the infected files to be deleted.

VSHIELD1 — This program checks program validation codes that have been attached to executable files by SCAN. It will not allow any program to execute if the validation codes have changed. VSHIELD1 is a memory resident program which requires 6Kb of RAM.

VSHIELD — This program will scan for specific virus signatures and identify the virus if one exists in addition to providing validation code checking. VSHIELD is also a memory resident program. It requires 34Kb of RAM and typically adds approx 4 seconds to the execution time of every program and it adds approx 6 seconds to the boot up time. It can be run in a disc swapping mode to reduce its RAM requirements (it then requires only 3Kb) but this can result in interrupt conflicts with other TSR programs and also adds further delays to program executions and bootup.

SENTRY — This program employs a checksum technique on the initial instructions and branch addresses for each executable program in the system (including the code in the boot and partition sectors) and logs this checksum information in a file. Because it only examines part of each executable file, it is able to scan an entire system for a virus much more quickly than global checksum techniques. It normally takes less than 20 seconds for the average system. Once the log file has been created, SENTRY will check each executable file against its log information whenever it is run. Any change in file size will be reported as a possible virus attack. SENTRY is not a memory resident program.

CLEAN-UP kills and removes computer viruses, and in most instances repairs infected files, re-constructs damaged programs and returns the system to normal operation. CLEAN-UP works for all viruses identified by the current version of SCAN.

FSHIELD This program shields executable files so that virus infections are instantly detected and automatically removed. Programs shielded in this manner will not remain infected and will not propagate a virus.

VCOPY This program duplicates the functionality of the DOS COPY command but includes a virus checking routine to prevent the copying of any infected program files. This is most useful as a means of preventing infected programs from getting onto the PC from floppy discs.

CENTRAL This is a 3rd-party package which provides a WIMP interface for the McAfee SCAN and CLEAN-UP programs. It requires a separate US$25 licence.

Anti-Virus Software (Continued)

Dr Solomon's Anti-virus Toolkit

This package provides four main programs for the detection and eradication of viruses. In addition to these, a suite of utility programs is provided to help with the detection, removal and containment of unknown viruses.

FINDVIRU — This program scans for any of 245 known viruses and their variants. It searches computer memory, the boot and partition sectors of discs and all executable files and their overlays. It is relatively quick, taking only 48 seconds to scan a 80 Mb hard disc containing 598 executable files compared with the McAfee SCAN program which took 255 seconds. This program is not memory resident.

NETFV — A network version of FINDVIRU without boot sector checking (which is impossible over a network).

CHKVIRUS — This program uses a checksum approach to monitor the integrity of executable files. When CHKVIRUS is first run on a disc it creates a log file containing "the signatures" of all the discs executable files (including operating system files). Subsequent runs of CHKVIRUS cause it to check all executable files against the list it had compiled. This program is not memory resident.

QCV — This program is a quick version of CHKVIRUS and again is not memory resident. It is less secure because it does not use a checksum for the executable files. Rather it compares the file sizes, dates and times against a reference list it compiles. This scheme will catch many viruses but not ones which overwrite code such as 405.

Utility Programs

PEEKA — A hexadecimal viewer for examining disc sectors for virus traces.

HEXDUMP — A hexadecimal viewer for examining files for virus traces.

RUN — A shell program to run others. RUN acts as a 'sacrificial lamb' for the real program being run. The virus attaches to RUN.EXE and not to the user's program. The size of RUN.EXE can be continually monitored for signs of virus attack.

UNVIRUS — This program removes most boot sector viruses (e.g. DENZUK) from diskettes.

UNSTONE — This program removes the STONED virus from hard discs.

NOHARD This program write protects a hard disc to prevent unauthorised writing to it. Its operation is the equivalent of putting a write protect tab on a floppy disc.

NOFLOPPY This program write protects a floppy drive so that all floppy discs put into that drive are treated as if they have write protect tabs on them.

INOCULAT This program can be used to inoculate an executable file against attack from a single specified virus. This ability is useful during clean-up operations after a virus attack when executable files need to be protected against re-infection.

INOCMEM This program inoculates a computer's memory against the Icelandic virus which is also known as Saratoga and Disk Eater. INOCMEM prevents this specific virus from going memory resident.

CHECKMEM This program produces a map of RAM usage showing the way in which RAM is currently assigned to system and application programs. Periodic checking of memory with this utility could reveal the presence of unknown programs in RAM such as viruses.

WATCH21 This program monitors the status of DOS Interrupt 21 which can be taken over by some viruses.

TRYOUT This program tests the correct operation of memory resident anti-virus software. TRYOUT writes code to the boot sector of a disc in four ways that are commonly used by viruses. Memory resident anti-virus programs should act to prevent these write operations.

CHKV1, CHKV2, CHKV3 These are DOS batch files intended to make the regular running of CHKVIRUS easier for the PC user.

WEEKDAY, MONTHDAY These programs interrogate the DOS clock and return the day of the week and the day number in the month respectively. They can be used to build semi-intelligent batch files for the regular running of anti-virus (and other) software.

LASTRUN This program reports on when it was last run. When used in conjunction with anti-virus (and other programs) in a batch file, it can be used to help users to keep track of their back-up and anti-virus system maintenance.

SHRED This program overwrites a specified existing file prior to deleting it. In this way, the file cannot be undeleted. This would be a desirable procedure to use when purging virus-infected files from a computer's discs.

Anti-Virus Software (Continued)

The Calmer Utilities

This package comprises 2 Mb of utility programs including the following 3 virus detection and eradication programs.

NBY — This program is available for the MSDOS, OS/2 and Unix operating systems. NBY is an acronym which stands for "Not Born Yesterday". It scans boot sectors, partition sectors and all files (executable and data) for 234 known viruses. It also calculates and logs checksum data for all the files on the disc when it is first run and subsequently checks all files against this log whenever it (NBY) is run. Infected files can be deleted.
NBY has a very useful message file capability which allows it to put customised instructions for the user on the screen if a virus is detected (e.g. the user could be instructed to immediately contact the Information Systems Branch help-desk on extension 9402 if a virus were found). It is not a memory resident program.

FASTNBY — This is a fast version of NBY which, like the McAfee SENTRY program, only checks the start-up code of executable files for known viruses. FASTNBY also calculates and stores the checksum for all executable files in a log file.

FIM — This program scans computer memory for a user specified text string. This can be used to look for a suspected virus provided that the virus message code isn't encrypted (e.g. DATACRIME II).

Virus Detection Results

An 80286 Data General IBM-PC compatible computer with a 40 Mbyte hard disc was used as a quarantined environment in which to test the effectiveness of the virus scanning products. The hard disc of the computer was loaded with 227 files known to be infected with at least 140 different viruses. Some files carried multiple infections. The names of the identified viruses are listed in Appendix A.

Each of the anti-virus packages (SCAN, FINDVIRU and NBY) were used to scan the hard disc. In each case, the scanning program was run from a write-protected floppy disc in order to prevent viruses escaping from the hard disc. The results of these tests are listed in Table 1 and Appendices B, C and D for the 3 virus scanning programs.

TABLE 1

Effectiveness of the Virus Scanning Programs

Program	Package	Version	Number of virus infected files present	Number of virus infected files found
SCAN	McAfee	67	227	158
		75	227	201
FINDVIRU	S & S	4.22	227	183
		4.26	227	190
NBY	Calmer	2.77	227	168

The results of Table 1 illustrate the limitations of the virus scanning approach. None of the scanning programs were able to detect all the viruses present presumably due to the inevitable lag that occurs between the creation of a new virus or variant and the implementation of effective scanning measures to detect it. This lag is well illustrated by the observation that the McAfee SCAN program (version 75) did the best job of locating virus code, while its earlier version, 67 was the least effective.

Inspection of the results in Appendices B, C and D illustrates a worrying shortcoming of all the packages. **No single scanning program located all the viruses.** For example, the file VIRUS101.EXE was correctly identified as being infected by the VIRUS-101 virus by FINDVIRU but went undetected by SCAN (version 67) and NBY. Similarly, the SCOTT'S VALLEY virus was detected correctly by SCAN and NBY in the file SCOTSVAL.COM but was not identified by FINDVIRU. The VIRUS-B virus which was carried by the file VIRUS-B.COM went undetected by all three scanning programs.

Performance Test Results

The speed with which an anti-virus package goes about its task is just as important as its technical merits in virus detection because users are only going to use such programs if they are fast and painless to use.

Virus Scanning Programs

The scanning speeds of the 3 scanning programs were assessed by running each of them on an Osborne 80386 personal computer running at a clock speed of 25 MHz. The 80 Mbyte hard disc on this machine contained a mix of off-the-shelf applications software, data and executable files built with FORTRAN and C compilers. This collection of programs and data is probably broadly typical of what would be found on many of the PCs used in BMR. The test results with the virus scanning programs are therefore likely to be of relevance to many BMR PC users.

There are very substantial differences in the speed with which the scanning programs operate as indicated in Table 2 and Figure 1.

TABLE 2

Performance Data for 3 Virus Scanning Programs

Program	Package	Version	Number of viruses scanned	Time+ Taken (seconds)
SCAN	McAfee	67	223	255
FINDVIRU	S & S	4.22	245	48
NBY	Calmer	2.77	234	1740

+These times are for a scan of an 80 Mb hard disc containing 598 .EXE and .COM files. The test PC was an Osborne 80386 running at a clock speed of 25 MHz.

The results in Table 2 and Figure 1 highlight very large differences in the performance between the 3 programs. Each of these programs scanned all 598 executable files, in addition to the boot and partition sectors on the disc for > 220 known viruses. The FINDVIRU program from the Dr Solomon's Anti-Virus Toolkit was by far the fastest to execute of the 3 programs. The elapsed time of 48 seconds implies a data transfer rate off the 80 Mb hard disc of 480 Kbs^{-1} if all of the 23 Mb of executable files were scanned in their entirety. The NBY program of the Calmer Utilities was extremely slow, taking 29 minutes to complete the scanning task.

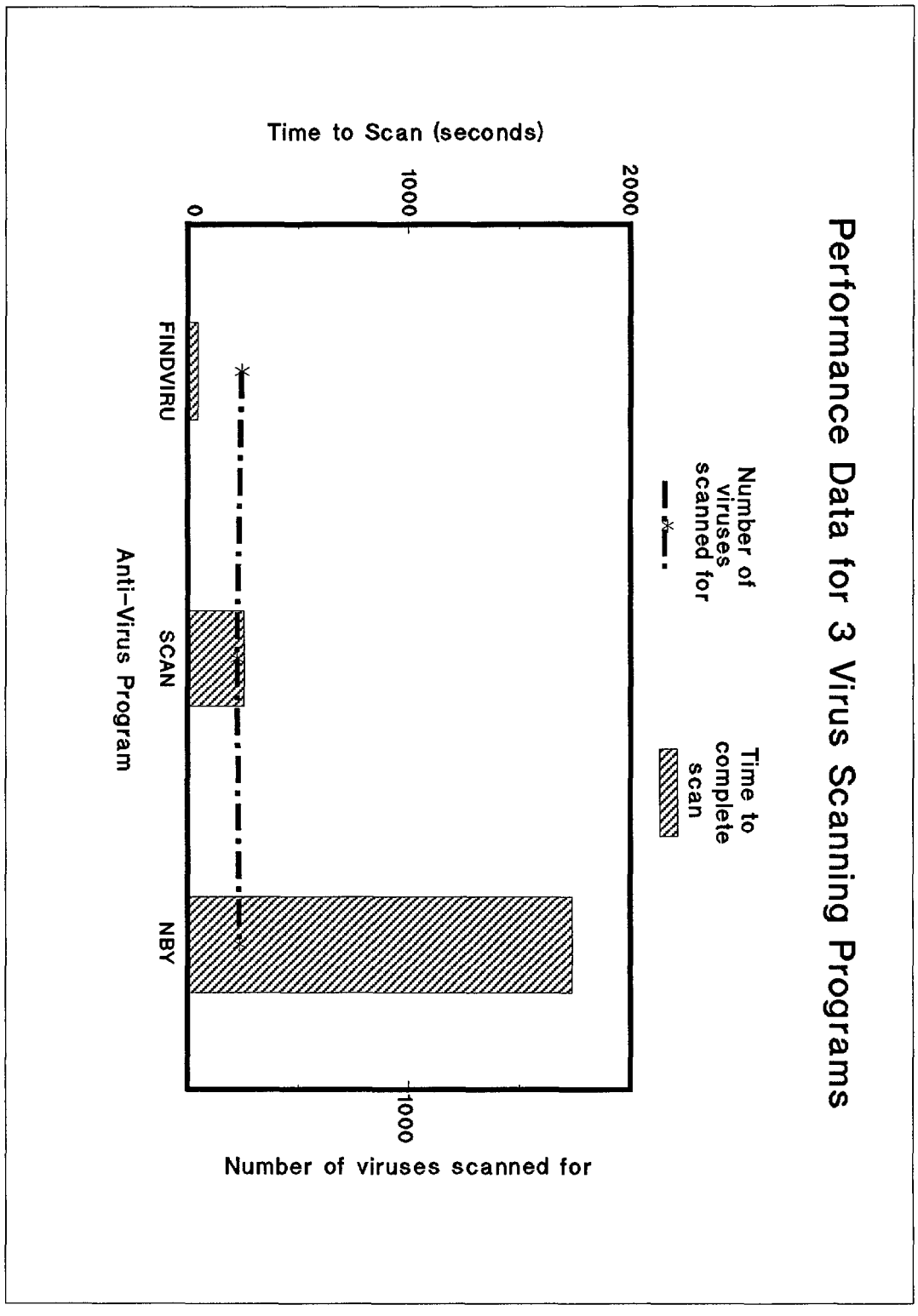

Figure 1 Performance data for 3 Virus Scanning Programs and a plot of the number of viruses they can detect (see text).

Checksum Anti-Virus Scanning Programs

All 3 software packages reviewed here also provide checksum programs to monitor the unexpected growth in executable file sizes that accompany an infestation by most viruses. Each program keeps data on a different mix of files. The McAfee SENTRY program monitors the size of .EXE and .COM files, most executable device drivers and the boot sector. CHKVIRUS from S & S International monitors the size of .EXE and .COM files, all executable device drivers and the boot sector. FASTNBY is the most thorough. In its normal mode it monitors not only all .EXE, .COM and .SYS, but also .BAT DOS batch files and .LIB library files.

In all these checksum programs, there is an initial install phase in which the program goes through the target disc and calculates signatures for each file and writes these data to a log file. Subsequent running of the program sees it check each file's signature against the recorded data (see the individual program descriptions above for more information on how they operate).
The performance results for each program are given in Table 3 and Figure 2.

TABLE 3

Performance Data for 3 Checksum Anti-Virus Programs

Program	Package	File types checked	Number of files checked	Time to build signature file (seconds)	Time to check files (seconds)
SENTRY	McAfee	.EXE, .COM, .SYS	436	82	26
CHKVIRUS	S & S Int.	.EXE, .COM, .SYS	438	198	167
FASTNBY	Calmer	.EXE, .COM, .SYS, .LIB, .BAT	490	25	36

The results in Table 3 show that the Calmer Utilities FASTNBY program is the best of the programs in this group. FASTNBY checks more file types than the other two programs and it creates the file signatures more quickly than the others. It checks its larger number of files against the recorded signatures much more quickly than CHKVIRUS and only a little more slowly than SENTRY.

All these programs are run either by the user directly invoking them, or more usually by a command or commands in the autoexec.bat file. FASTNBY and CHKVIRUS both come with utility programs which make it possible to run them regularly from autoexec.bat without the necessity to have them execute with every reboot. The provision of such a utility is a striking omission from the McAfee software because few, if any, users are likely to endure a check of their system which adds half a minute or more to every re-boot.

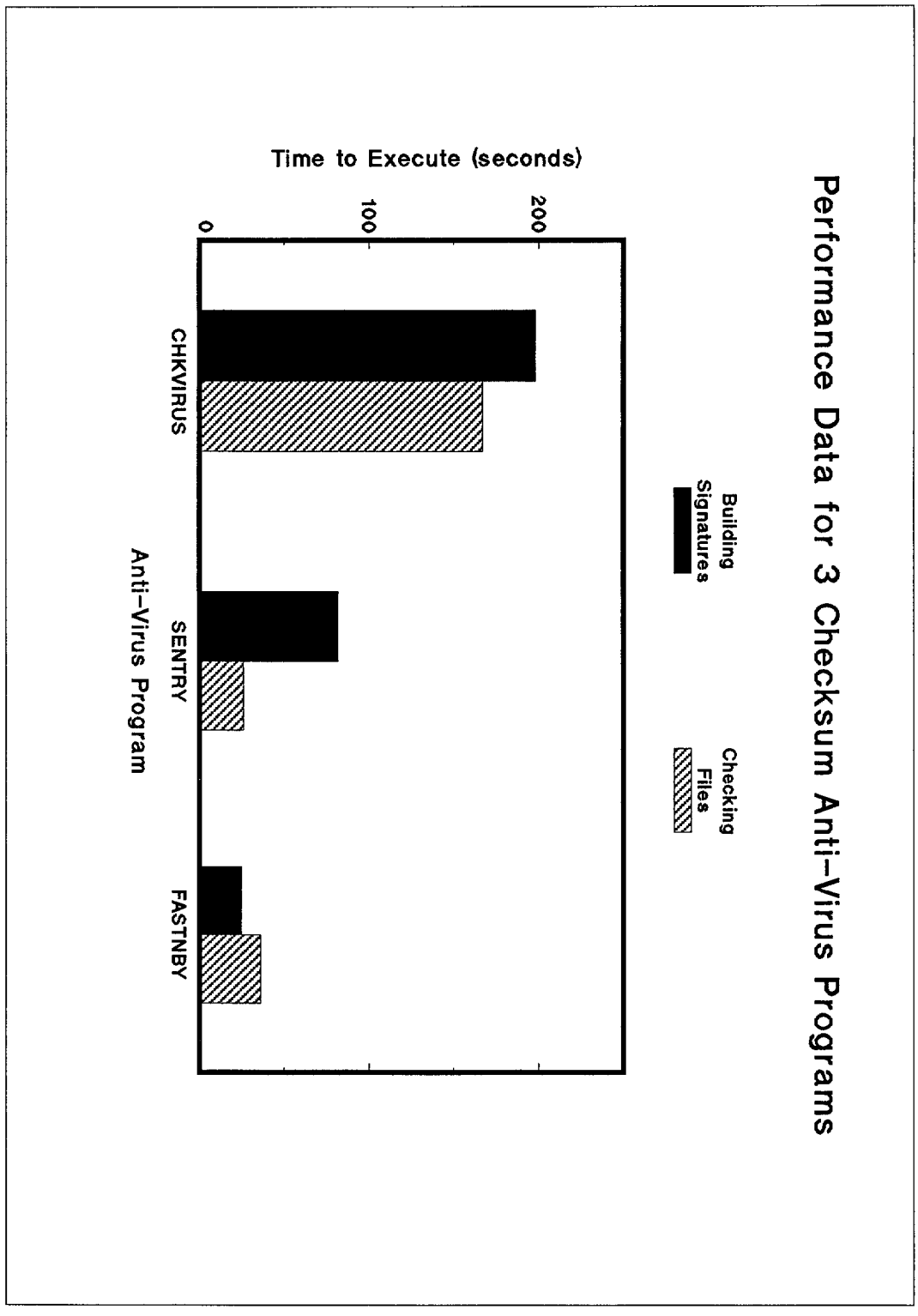

Figure 2 Performance data for 3 Checksum Anti-Virus Programs (see text).

Discussion

Implementing a Virus Protection Scheme

There are 3 ways in which a user can implement a virus protection scheme with the software packages reviewed here.

1) Regular scanning for viruses. The user can regularly run programs which identify and remove viruses from memory, and discs. This is probably best done with some sort of smart autoexec.bat file which allows scanning daily &/or weekly (irrespective of the number of times the system is rebooted). All 3 of the anti-virus packages reviewed provide one or more scanning programs for this purpose (e.g. SCAN, FINDVIRU and NBY). The effective use of this approach is dependent upon the software house keeping up-to-date with virus developments and upon the user obtaining regular updates of the anti-virus software.

2) Checksum monitoring of executable files. In this scheme anti-virus programs first create a log file containing checksum information on all the executable files on the disc. Subsequent runs of the program, initiated either by the user or by the autoexec.bat file at bootup, recheck all the executable files against the log file information. Any variation in an executable file will trigger a warning of a possible virus attack. This approach does not require any prior knowledge of virus structures and methods and so is not dependent on regular updates of the anti-virus software. All 3 packages provide software of this type (SENTRY, CHKVIRUS, QCV, NBY & FASTNBY).

3) Memory resident scanning for known viruses and checksum variations. This method is provided by the McAfee VSHIELD and VSHIELD1 programs. This approach provides the most secure protection against virus attack but it is also the most intrusive on the user. The VSHIELD program, the more comprehensive of the two, uses 34 Kb of RAM and adds approx 4 seconds to the run time of every executable file. This overhead would probably only be acceptable to users who need highly secure systems.

As BMR has yet to suffer any serious virus attack on its IBM-type PCs, it is very unlikely that many BMR PC users will opt for the McAfee memory resident virus scanning programs at the moment. If some other less obtrusive product was available, then it might find some use.

The bulk of BMR's IBM-type PC users are therefore likely to opt for one of 3 anti-virus strategies:

1) regular or irregular backups of important files and no anti-virus strategy
2) occasional scanning of their systems and unknown floppy discs together with backups of important files.
3)regular use of a checksum anti-virus program through a command in autoexec.bat, regular scanning of hard discs, occasional scanning of unknown floppy discs and regular backups.

Most, if not all, of BMR's PC users currently use strategy 1) above (i.e. no explicit anti-virus strategy other than backing up of important files). This is clearly not a very good practice given the inevitability of BMR eventually suffering a virus attack on its IBM-type PCs similar to that which affected BMR's Macintosh computers several years ago. The sooner a strategy like 3) above is widely adopted the better.

Implementation in BMR

The need for effective anti-virus strategies for BMR's computing systems is quite apparent from even a cursory examination of the capabilities of computer viruses, worms and trojans and the havoc they have caused elsewhere (e.g. Alexander, 1988 and 1990). Effective strategies to safeguard BMR data and software systems are also required by the Secretary of the Department of Primary Industries and Energy (who will soon be releasing a Secretary's Instruction on "Safeguarding Computer Equipment and Resources") and by the Department of Finance (Department of Finance Direction Section 34 - "Safeguarding Departmental Operations, Computer Records and Installations").

BMR needs to develop an action plan to use in the event of an infectious virus attack in the future. This plan needs to address how a major virus infestation should be contained and eradicated. It may not be enough to rely upon individual users to eradicate such a virus because, particularly with the increasing degree of PC networking going on in BMR, re-infections will be all too easy. Information Systems Branch (ISB) needs to take a lead in developing this action plan and in disseminating appropriate anti-virus software within BMR. Site licencing of this software would probably be the most cost-effective way in which to distribute it to BMR's PCs.

BMR's PC users also need to be educated with regard to the risks that a virus attack poses to their PC dependent projects. These users need to be assisted with the tailoring of suitable anti-virus software to their needs. Most of the anti-virus software programs described here can be invoked in an advanced user mode with switches set to customise the program to the PC environment it is running on. Information Systems Branch could take a lead in this work but effective consultation with the users would be essential if the anti-virus measures are to be useful and used. For example, some BMR PCs only run commercial software applications like spreadsheets and word processors. These PCs may be able to use checksum-type anti-virus software successfully. On the other hand, PC users involved with extensive program development, are likely to find these checksum routines very irritating and quite possibly unusable.

The choice of package must obviously be based on perceived suitability (number of viruses scanned for, time to scan, time to calculate and monitor checksum signatures, RAM used by memory resident programs) and on price. The prices of the 3 packages reviewed here are given in Table 4.

TABLE 4

Costs of the Anti-Virus Packages

Package	Single User licence	100 User licence	200 User licence
McAfee			
SCAN	-	$1891.	$3192.
VSHIELD	-	$2276.	$3987.
CLEAN-UP	-	$2276.	$3987.
NETSCAN		------- $2564. flat fee -------	
All 4 programs	$141.	$4167.	$6538.
Dr Solomon			
Package 1[a]	$35.	$3000.	$6000.
Package 2[b]	$50.	$4000.	$8000.
Package 3[c]	$65.	$5500.	$11000.
Calmer	$40.	$499. $899.[d]	$499. $899.[d]

[a] Includes: CHKVIRUS, QCV, WEEKDAY, MONTHDAY, LASTRUN
[b] Includes: FINDVIRU, NETFV, WEEKDAY, MONTHDAY, LASTRUN
[c] Includes: FINDVIRU, NETFV, CHKVIRUS, WEEKDAY, MONTHDAY, LASTRUN
[d] with automatic upgrade for one year

Conclusions

Any effective effort to protect BMR's PCs from virus attack needs to be based on knowledge of the anti-virus products that are available, and just as importantly, it needs to be based on cognizance of how BMR's PC users will respond to the measures. It is not much use purchasing a site licence for a technically preferred anti-virus package if nobody will use it.

The spectrum of usage of BMR's PCs is very wide and this makes it difficult to provide virus protection to all users with a single software solution. Ideally two functions need to be provided. The first scans hard and floppy discs for known viruses and neutralises them when they are detected. This type of virus protection is likely to be most widely used in BMR. The second virus protection function that is needed is an efficient checksum program which can be used on PCs which have stable software configurations (e.g. PCs used principally for word processing, spreadsheets, etc). This needs to be fast to operate so that it is not too intrusive.

Of the three anti-virus packages reviewed here, the Dr Solomon's Anti-Virus Toolkit would appear to provide the best virus scanning program (FINDVIRU). This program ran 5 times faster than McAfee's SCAN program and 36 times faster than the Calmer Utilities' NBY. FINDVIRU version 4.26 detected almost as many virus infected files on the quarantined 80286 PC as did McAfee's SCAN version 75. It is salutary to note however that none of the scanning programs detected all the viruses on the quarantined machine.

FINDVIRU's scanning speed must be balanced however against its higher price. The McAfee SCAN program costs less than half that of FINDVIRU and provides equivalent or better functionality at what may still be an acceptable speed.

With regard to the checksum anti-virus programs, the Calmer Utilities' FASTNBY program is a clear winner. It checks a wider range of executable and related files and builds its signature log file appreciably faster than either CHKVIRUS (which takes 8 times as long) or SENTRY (3 times as long). FASTNBY performs its subsequent checks 5 times faster than CHKVIRUS and only marginally slower than SENTRY in spite of the fact that it checks more files.

BMR needs to develop an action plan to use in the event of an infectious virus attack in the future. This plan needs to address how a major virus infestation should be contained and eradicated. Information Systems Branch (ISB) needs to take a lead in developing this action plan and in disseminating appropriate anti-virus software within BMR. Site licencing of this software would probably be the most cost-effective way in which to distribute it to BMR's PCs.

Acknowledgments

I wish to thank Rod Ryburn of Information Systems Branch for drawing my attention to the anti-virus programs in The Calmer Utilities and for loaning me his copy. I also wish to thank Dave Downie of Information Systems Branch for loaning me his evaluation copy of the Dr Solomon's Anti-Virus Toolkit.

The manuscript benefited from thoughtful reviews by Sonja Lenz and David Berman of Information Systems Branch.

References

Alexander, M. (1988). Virus ravages thousands of systems, *Computerworld*, v22 n45 p1-2.

Alexander, M. (1989). It's the flu season for micros. Expected autumn virus strains breed apprehension among PC users, *Computerworld*, v23 n38 p39,41.

Alexander, M. (1990). Morris: worm spiraled out of control, *Computerworld*, v24 n4 p8

Bates, J. (1989). All about viruses, *Practical Computing*, v12 n3 p87.

Bates, J. (1990). High speed action defeats rogue disks within 24 hours, an antidote had been found to the PC "AIDS" bug, *Practical Computing*, v13, n2, p14-15.

Bornstein, H. (1989). Beyond the hype. After all the furor over viruses dies down, the real question remains - what's being done to control them and what should be done?, *InfoWorld*, v11 n43 p57-61.

Brownstein, M. (1990) Security, anti-virus program upgraded Certus 2.0 controls access to, provides usage monitoring of LANs, *InfoWorld*, v12 n17 p28.

Chaffin, E. (1989). Computer viruses: an epidemic real or imagined? Viruses have been around as long as the computer--why the sudden attention? How can users combat them?, *Electronic Learning*, v8 n6 p36-37.

Davis, M. (1989). Terminal illness Inoculating yourself against the myth, mystery, and dangers of computer viruses, *A+*, v7 n4 p48-52.

Foster, E. (1990). Virus stories can sell papers, but may contain a Trojan horse *InfoWorld*, v12 n14 p41.

Gantz, John (1990). Evil, dreaded viruses! Coming soon to a screen near you, *InfoWorld*, v12 n6 p46.

References (Continued)

Greenstein, I. and M. Neubarth (1988). Virus plagues DOS network, *MIS Week*, v9 n45 p51-52.

Grossman, E.O. (1989). Experts warn of Datacrime virus, plan prevention, *PC WEEK*, v6 n36 p11.

Honan, Patrick (1989). Avoiding virus hysteria. Virus programs are after your computer. Plan a strategy to prevent an attack now, before losing data, time, and money, *Personal Computing*, v13 n5 p84-92.

Howard, B. (1990). Virus protection, *PC Magazine*, v9 n12 p181.

Kenner, H. (1990). Stomping the nasties - A field guide through the jungle of computer invaders, *BYTE*, v15 n12 p466-467.

Littman, J. (1990). The shockwave rider. Why did Robert Morris unleash his paralyzing worm?, *PC Computing*, v3 n6 p142-159.

Palmore, T.B. (1989). Computer bytes, viruses and vaccines, *TechTrends*, v34 n2 p26-28.

Perez, E. (1988). Computer viruses: preventive medicine, *LINK-UP*, v5 n5 p21-26.

Price Waterhouse (1990). *The Computer Virus Handbook.*

Rubenking, N. J. (1990). Vi-Spy finds and destroys known viruses, *PC Magazine*, v9, n11, p49.

Ryburn R.J. (1990). GetSeq, A PC Program for Extracting Data from a Remote SQL Database - An Example of Client-Server Programming, *Bureau of Mineral Resources, Geology and Geophysics, Australia,Record* 1990/39.

Sharp N. (1990). *Computer Security in BMR - a Crucial Issue*, Information Systems Branch occasional paper, *Bureau of Mineral Resources, Geology and Geophysics, Australia.*

Stephens, M. (1989). DOS virus will erase disks on Columbus Day, *InfoWorld*, v11 n37 p5

Wilder, C. (1988). Cashing in on virus anxieties, *Computerworld*, v22 n47 p1-2.

Williams P.R. (1991). Structural Geology Information: Collection Techniques and Data Transfer Between DG_ORACLE and Arc/Info, *Bureau of Mineral Resources, Geology and Geophysics, Australia,Record* 1991/6.

Worms + Viruses. *LAN Times*, December 1, 1989 , v6 n12 p71-97.

Appendix A

140 Viruses used to Test the Scanning Programs

333
353
367
403
435 (Vienna 435)
507
512 (Number of the Beast)
623
648
1008
1024
1253 (Thanksgiving)
1381
1554 (Ten bytes)
1559
1701 (Cascade)
1704 (Vienna 353)
1720
2930
3551 (Syslock, Macho)
4096
5120
8 Tunes
12 Tricks (Trojan)
100 years
Aids
Aids 2
Alabama
Amoeba 1392
Anarkia
Anthrax
AntiCad 1
AntiCad 2
April 1st
Barcelona
Black Monday
Burger 1
Burger 405
Cookie
Choinka
Dark Avenger
Dark Avenger 3
DataCrime B
DataCrime 2B
DBASE
Devils Dance
Diamond
Do Nothing
Doodle 25
Doodle 41
Doodle 44
Doodle B1
Durban
E_C_46 (RK)
Eddie 2
Fellowship
Fish
Flash
Frere Jacque
Friday 13th
Jerusalem
JoJo 1
Kennedy
Keypress
KHETAPUNK
Lehigh
Leprosy
Leprosy-B
Mixer 1A
Murphy 1
Fu-Manchu
Ghost
Halloechen
Hahaha
Icelandic
Icelandic 2
Icelandic 3
Internal
ItaVir
Japan XMAS
Mystic 1
Nomenklatura
Nothing
Oropax
Paris
Pascal 1
Pascal 2
Peace
Perfume (765)
Pixel 3
Plastique
Plastique 2
Pretoria
Recovery 382
Red Cross
Saratoga
Saturday 14th
Scott's Valley
Shake
Slow
Sorry
St Leos
Subliminal
Sunday
SVIR
Sylvia
Syslock
Taiwan
Taiwan 2
TCC
Tiny 1
Traceback
TypoCOM
V-1L
V2000
V2100
Vacsina V5
Vbasic
VCOM
VHP
VHP-2
Victor
Vienna 62A
Vienna 62C
Vienna 627
Vienna X1
VP
Violator
Virdem
Virus-90
Virus-101
W13-a
W13-b
W-13
Westwood
Whale
Whale 22
Wisconsin
Wolfman
Zero-Bug

Appendix B

Virus Scanning Results for SCAN version 67

```
Scanning C:\!3012.COM                   Found Plastique Related Virus
                                                Found Jerusalem Related Virus
Scanning C:\!3012.EXE                   Found Plastique Related Virus
                                                Found Jerusalem Related Virus
Scanning C:\!382.COM                    Found 382 Virus
Scanning C:\!DOOM2.EXE                  Found Doom2 Virus
Scanning C:\!PLAS451.EXE    Found Plastique Related Virus
                                                Found Jerusalem Related Virus
Scanning C:\!PLAS521.COM    Found Invader Virus
                                                Found Plastique Related Virus
                                                Found Jerusalem Related Virus
Scanning C:\!PLASTQ.EXE                 Found Plastique Related Virus
                                                Found Jerusalem Related Virus
Scanning C:\!WOLFMAN.EXE    Found Wolfman Virus
Scanning C:\1008.COM                    Found 1008 Virus
Scanning C:\1024-B.COM                  Found Nomenclature Virus
Scanning C:\1024.COM                    Found 1024 Virus
Scanning C:\1253.COM                    Found 1253 Virus
Scanning C:\1280.COM
Scanning C:\12TRICKS.COM    Found 12 Tricks Trojan
Scanning C:\1392.COM                    Found 1392 (Amoeba) Virus
Scanning C:\1559.COM                    Found 1554 Virus
Scanning C:\1701.COM                    Found 1701/1704 Virus - Version B
Scanning C:\1701CHIC.COM    Found 1701/1704 Virus - Version B
Scanning C:\1704-B.COM                  Found 1701/1704 Virus - Version B
                                                Found Vienna (DOS 62) Virus
Scanning C:\1704-C.COM                  Found 1701/1704 Virus - Version B
Scanning C:\1704.COM                    Found VHP Virus
                                                Found 1701/1704 Virus - Version B
Scanning C:\1704FRMT.COM    Found 1701/1704 Virus - Version B
Scanning C:\1704MULT.COM    Found 1701/1704 Virus - Version B
Scanning C:\17Y4.COM                    Found 1701/1704 Virus - Version B
Scanning C:\1971.COM                    Found 1971 Virus
Scanning C:\2000.COM                    Found V2000 Virus
Scanning C:\2930.COM
Scanning C:\3551.COM                    Found 3551 (Syslock) Virus
Scanning C:\403.COM
Scanning C:\405.COM
Scanning C:\4096.COM                    Found 4096 Virus
Scanning C:\4096E.EXE                   Found 4096 Virus
Scanning C:\435.COM                     Found VHP Virus
Scanning C:\512.COM                     Found 512 Virus
Scanning C:\5120.COM
Scanning C:\623.COM                     Found VHP-2 Virus
Scanning C:\AIDS.COM
Scanning C:\ALABAMA.EXE
Scanning C:\AMSTRAD.COM
Scanning C:\ANAR2.COM                   Found Jerusalem Related Virus
Scanning C:\ANARKIA.COM                 Found Jerusalem Related Virus
Scanning C:\ANTHRAX.COM                 Found Anthrax Virus
Scanning C:\ANTICAD1.EXE    Found Jerusalem Related Virus
Scanning C:\ANTISCAN.COM    Found 1605 Virus
                                                Found Jerusalem Related Virus
Scanning C:\AP-400.COM
Scanning C:\AP-440.COM
Scanning C:\AP-480.COM
Scanning C:\AP-529.COM
Scanning C:\AP-605.COM
Scanning C:\APRILEXE.EXE
Scanning C:\ARMAGEDO.COM    Found Armagedon Virus
Scanning C:\BENNY.EXE                   Found 1381 Virus
Scanning C:\BMONDAY.COM                 Found Black Monday Virus
Scanning C:\BMONDAY.EXE      Found Black Monday Virus
Scanning C:\BUGS.COM
Scanning C:\BURGER.COM
Scanning C:\CASPER.COM                  Found Casper Virus
Scanning C:\CHKDSK.COM                  Found Whale Virus
Scanning C:\CUNNING.COM                 Found 1701/1704 Virus - Version B
Scanning C:\D-DANCE.COM                 Found Devil's Dance Virus
Scanning C:\DARK-A.COM                  Found Dark Avenger virus
Scanning C:\DARK3.COM                   Found Dark Avenger virus
Scanning C:\DARKAV-1.EXE    Found Dark Avenger virus
Scanning C:\DARKAV-2.COM
Scanning C:\DARKAV-3.COM    Found Dark Avenger virus
Scanning C:\DARKAV-4.EXE    Found Dark Avenger virus
Scanning C:\DATCRM2B.EXE
Scanning C:\DBASE.COM
Scanning C:\DOODLE.EXE                  Found Yankee Doodle Virus
Scanning C:\DOODLE41.COM    Found Yankee Doodle Virus
Scanning C:\DOODLE44.COM    Found Yankee Doodle Virus
Scanning C:\DOS62.COM                   Found Vienna (DOS 62) -B Virus
Scanning C:\DRKAVNGR.COM    Found Dark Avenger virus
Scanning C:\FELLOW.EXE                  Found Fellowship Virus
Scanning C:\FISH.COM                    Found Fish Virus
```

Appendix B (Continued)

Virus Scanning Results for SCAN version 67

```
Scanning C:\FISH.EXE
Scanning C:\FLASH.COM                   Found Flash Virus
Scanning C:\FRERE.COM                   Found Jerusalem Related Virus
Scanning C:\FREREC.COM
Scanning C:\FREREE.EXE                  Found Jerusalem Related Virus
Scanning C:\FRIDAY13.EXE    Found Jerusalem Related Virus
Scanning C:\FUMANCHU.COM    Found Jerusalem Related Virus
Scanning C:\GHOST.COM                   Found Vienna (DOS 62) Virus - Version B
Scanning C:\GRAB.EXE
Scanning C:\GUPPY.COM
Scanning C:\H1701.COM                   Found 1701/1704 Virus - Version B
Scanning C:\H1704.COM                   Found 1701/1704 Virus - Version B
Scanning C:\HALLOE.EXE                  Found Halloechen Virus
Scanning C:\HM2.EXE                     Found Invader Virus
                                                Found Plastique Related Virus
                                                Found Jerusalem Related Virus
Scanning C:\ICE-3.EXE
Scanning C:\ICE2.EXE
Scanning C:\ICELANDI.EXE
Scanning C:\INFECTED.EXE
Scanning C:\INVADER.COM                 Found Invader Virus
Scanning C:\ISRAEL-C.COM    Found Jerusalem Related Virus
Scanning C:\ISRAELI.COM
Scanning C:\ITAVIR.EXE                  Found ItaVir Virus
Scanning C:\JAP-XMAS.COM    Found Christmas in Japan Virus
Scanning C:\JB-A204.COM
Scanning C:\JER-204.COM
Scanning C:\JER-B.EXE                   Found Jerusalem Related Virus
Scanning C:\JERSPAIN.COM    Found Jerusalem Related Virus
Scanning C:\JOJO.COM                    Found JoJo Virus
Scanning C:\JUNE16.COM                  Found June 16th Virus
Scanning C:\KENNEDY.COM                 Found Kennedy Virus
Scanning C:\KEYPRESS.COM
Scanning C:\KEYPRESS.EXE
Scanning C:\LEHIGH.COM
Scanning C:\LEHIGH2.COM
Scanning C:\LEPR-B.COM
Scanning C:\LEPR-B.EXE
Scanning C:\LEPR-BA.COM
Scanning C:\LEPROSY.COM
Scanning C:\LIBERTY.COM                 Found Liberty Virus
Scanning C:\LIBERTYE.EXE    Found Liberty Virus
Scanning C:\LISBON-B.COM    Found Lisbon Virus
Scanning C:\LISBON.COM                  Found Lisbon Virus
Scanning C:\MINI.COM                    Found Whale Virus
Scanning C:\MIX1.EXE
Scanning C:\MONDAC.COM                  Found Black Monday Virus
Scanning C:\MONDAY.EXE                  Found Black Monday Virus
Scanning C:\MURPHY-1.COM    Found Murphy Virus
Scanning C:\MYSTIC-2.COM    Found Liberty Virus
Scanning C:\MYSTIC1.EXE                 Found Liberty Virus
Scanning C:\NOTHING.COM
Scanning C:\ONTARIO.COM                 Found Ontario Virus
Scanning C:\OROPAX.COM                  Found Oropax Virus
Scanning C:\PAYDAY.EXE                  Found Jerusalem Related Virus
Scanning C:\PCOM.EXE
Scanning C:\PCOPY.EXE
Scanning C:\PCSETUP.EXE
Scanning C:\PEACE.EXE                   Found Fellowship Virus
Scanning C:\PERFUME.COM
Scanning C:\PHOENIX.COM                 Found P1 Related Virus
Scanning C:\PHOENIXD.COM    Found P1 Related Virus
                                                Found Nomenclature Virus
Scanning C:\PLASTIQU.COM    Found Plastique Related Virus
                                                Found Jerusalem Related Virus
Scanning C:\PLASTIQU.EXE    Found Plastique Related Virus
                                                Found Jerusalem Related Virus
Scanning C:\POLAND1.EXE                 Found Vcomm Virus
Scanning C:\POLAND3.COM                 Found W-13 Virus
Scanning C:\PRUD.EXE                    Found 1210 Virus
Scanning C:\PRUDENTS.EXE    Found 1210 Virus
Scanning C:\PSQR.COM                    Found 1720 Virus
                                                Found Jerusalem Related Virus
Scanning C:\PUERTO.COM                  Found Jerusalem Related Virus
Scanning C:\REALDCHK.COM
Scanning C:\REALMINI.COM
Scanning C:\REALTINY.COM
Scanning C:\REDX.COM                    Found RedX Virus
Scanning C:\SARATOGA.EXE
Scanning C:\SAT14.COM                   Found Saturday 14th Virus
Scanning C:\SCOTSVAL.COM    Found Scott's Valley Virus
Scanning C:\SCUD.COM
Scanning C:\SHAKE.COM                   Found Shake Virus
Scanning C:\SHAKE.EXE                   Found Shake Virus
```

Appendix B (Continued)

Virus Scanning Results for SCAN version 67

```
Scanning C:\SLOW.COM                    Found Slow Virus
Scanning C:\SOLANO.COM                  Found Solano Virus
Scanning C:\SUBLIMNL.COM
Scanning C:\SUNDAY.COM                  Found Sunday Virus
OScanning C:\SURIV01.COM
Scanning C:\SURIV02.EXE
Scanning C:\SURIV03.COM                 Found Jerusalem Related Virus
Scanning C:\SVIR.EXE
Scanning C:\SYLVIA.COM                  Found Holland Girl (Sylvia) Virus
Scanning C:\TAIWAN.COM                  Found Taiwan Virus
Scanning C:\TAIWAN2.COM                 Found Taiwan Virus
Scanning C:\TAIWAN3.COM                 Found Jerusalem Related Virus
Scanning C:\TCC.EXE                     Found Paris Virus
Scanning C:\TCFISH6.COM                 Found Fish Virus
Scanning C:\TCVP.COM                    Found VP Virus
Scanning C:\TERROR.EXE
Scanning C:\TETRIS.COM                  Found Sorry Virus
Scanning C:\TINY-158.COM   Found Tiny Virus or Related Virus
Scanning C:\TINY-159.COM   Found Tiny Virus or Related Virus
Scanning C:\TINY-160.COM   Found Tiny Virus or Related Virus
Scanning C:\TINY-167.COM   Found Tiny Virus or Related Virus
Scanning C:\TINY-198.COM   Found Tiny Virus or related
Scanning C:\TINY.COM                    Found Whale Virus
Scanning C:\TRACEBCK.COM
Scanning C:\TSTVIRB.COM
Scanning C:\TYPO.COM
Scanning C:\USCAN.EXE
Scanning C:\V-277.COM
Scanning C:\V1226.COM                   Found 1226 Related Virus
Scanning C:\V1226D.COM                  Found 1226 Related Virus
Scanning C:\V1226M.COM                  Found 1226 Related Virus
Scanning C:\V1701NEW.COM   Found P1 Related Virus
Scanning C:\V1721.COM                   Found Slow Virus
Scanning C:\V2100.COM                   Found 2100 Virus
Scanning C:\V2P2.COM                    Found V2P2 Virus
Scanning C:\V2P6.COM                    Found V2P6 Virus
Scanning C:\V2P6Z.COM
Scanning C:\V512.COM                    Found 512 Virus
Scanning C:\V651.COM                    Found 651 Virus
Scanning C:\V800.COM                    Found V800 Virus
Scanning C:\VACSINA.COM                 Found Vacsina virus
Scanning C:\VCOMM.EXE                   Found Vcomm Virus
Scanning C:\VHP-348.COM                 Found VHP Virus
Scanning C:\VHP-353.COM                 Found VHP Virus
Scanning C:\VHP-367.COM                 Found VHP Virus
Scanning C:\VHP-435.COM                 Found VHP Virus
Scanning C:\VHP-623.COM                 Found VHP-2 Virus
Scanning C:\VHP-627.COM                 Found Vienna (DOS 62) -B Virus
Scanning C:\VICTOR.COM                  Found Victor Virus
Scanning C:\VIEN6.COM                   Found Violator Virus
                                                Found Vienna (DOS 62) -B Virus
Scanning C:\VIENNA.COM                  Found Vienna (DOS 62) -B Virus
Scanning C:\VIENNA62.COM   Found Vienna (DOS 62) -B Virus
Scanning C:\VIOLATR.COM                 Found Violator Virus
Scanning C:\VIR13J.EXE                  Found July 13th Virus
Scanning C:\VIRDEM.COM
Scanning C:\VIRUS-90.COM
Scanning C:\VIRUS-B.COM
Scanning C:\VIRUS101.EXE
Scanning C:\VTINY.COM                   Found Tiny Virus
Scanning C:\W13-A.COM                   Found W-13 Virus
Scanning C:\W13.COM                     Found W-13 Virus
Scanning C:\WESTWOOD.COM   Found Jerusalem Related Virus
Scanning C:\WISCON.COM                  Found Wisconsin Virus
Scanning C:\YANKEE.COM                  Found Yankee Doodle Virus
Scanning C:\YANKEE.EXE                  Found Yankee Doodle Virus
Scanning C:\YANKEE19.COM   Found Yankee Doodle Virus
Scanning C:\YD-1961.EXE                 Found Yankee Two Virus
Scanning C:\YDOODLE.COM                 Found Yankee Doodle Virus
Scanning C:\YDOODLE.EXE                 Found Yankee Doodle Virus
Scanning C:\ZEROBUG.COM

          Disk C: contains 2 directories and 227 files.
                    Found 158 files containing viruses.
```

Appendix C

Virus Scanning Results for FINDVIRU version 4.22

C:\!3012.COM could have Anticad 3 virus
C:\!3012.EXE could have Anticad 3 virus
C:\!PLAS451.EXE could have Anticad 3 virus
C:\!PLAS521.COM could have Anticad 1 virus
C:\!PLASTQ.EXE could have Anticad 3 virus
C:\1008.COM could have Suomi virus
C:\1024-B.COM could have Nomenklatura virus
C:\1024.COM could have Diamond virus
C:\1253.COM could have Thanksgiving virus
C:\1280.COM could have Datacrime-1b virus
C:\12TRICKS.COM could have Twelve tricks trojan
C:\1392.COM could have Amoeba virus
C:\1559.COM could have Tenbytes virus
C:\1701.COM could have Cascade.1701 virus
C:\1701CHIC.COM could have Cascade.1701 virus
C:\1704-B.COM could have Vienna virus
C:\1704-C.COM could have Cascade.1704 virus
C:\1704.COM could have Vienna-353 virus
C:\1704FRMT.COM could have Cascade.1704 virus
C:\1704MULT.COM could have Cascade.1704 virus
C:\17Y4.COM could have Cascade.1704 virus
C:\1971.COM could have Eight tunes virus
C:\2000.COM could have Dark Avenger 3 virus
C:\2930.COM could have Traceback-2930 virus
C:\3551.COM could have Syslock virus
C:\405.COM could have 405 virus
C:\4096.COM could have Frodo virus
C:\4096E.EXE could have Frodo virus
C:\435.COM could have Vienna-435 virus
C:\512.COM could have No. of the beast-a virus
C:\5120.COM could have Vbasic virus
C:\623.COM could have Vienna-623 virus
C:\AIDS.COM could have Aids virus
C:\AIDS2.COM could have Aids 2 virus
C:\ALABAMA.EXE could have Alabama virus
C:\AMSTRAD.COM could have Pixel virus
C:\ANAR2.COM could have Jerusalem virus
C:\ANARKIA.COM could have Anarkia virus
C:\ANTHRAX.COM could have Anthrax virus
C:\ANTICAD1.EXE could have Anticad 2 virus
C:\AP-400.COM could have Anti Pascal 400 virus
C:\AP-440.COM could have Anti Pascal 440 virus
C:\AP-480.COM could have Anti Pascal 480 virus
C:\AP-529.COM could have Anti Pascal 529 virus
C:\AP-605.COM could have Anti Pascal 605 virus
C:\APRILEXE.EXE could have Suriv-2 virus
C:\ARMAGEDO.COM could have Armagedon virus
C:\BMONDAY.COM could have Black Monday virus
C:\BMONDAY.EXE could have Black Monday virus
C:\BURGER.COM could have Burger virus
C:\CASPER.COM could have Chameleon virus
C:\CUNNING.COM could have Cascade.1701 virus
C:\D-DANCE.COM could have Devil's dance virus
C:\DARK-A.COM could have Dark Avenger 1 virus
C:\DARK3.COM could have Dark Avenger 1 virus
C:\DARKAV-1.EXE could have Dark Avenger 1 virus
C:\DARKAV-2.COM could have Dark Avenger 1 virus
C:\DARKAV-3.COM could have Dark Avenger 1 virus
C:\DARKAV-4.EXE could have Dark Avenger 1 virus
C:\DATCRM2B.EXE could have Datacrime-2b virus
C:\DBASE.COM could have Dbase virus
C:\DOODLE.EXE could have Vacsina-44 virus
C:\DOODLE41.COM could have Vacsina-41 virus
C:\DOODLE44.COM could have Vacsina-44 virus
C:\DOS62.COM could have Vienna virus
C:\DRKAVNGR.COM could have Dark Avenger 1 virus
C:\FELLOW.EXE could have Better world virus
C:\FISH.COM could have Fish6 virus
C:\FLASH.COM could have Blink virus
C:\FRERE.COM could have Jerusalem virus
C:\FREREE.EXE could have Jerusalem virus
C:\FRIDAY13.EXE could have Jerusalem virus
C:\FUMANCHU.COM could have Fu Manchu virus
C:\GHOST.COM could have Ghostballs virus
C:\H1701.COM could have Cascade.1701 virus
C:\H1704.COM could have Cascade.1704 virus
C:\HALLOE.EXE could have Halloechen virus
C:\HM2.EXE could have Anticad 1 virus
C:\ICE-3.EXE could have December 24 virus
C:\ICE2.EXE could have Icelandic-2 virus
C:\ICELANDI.EXE could have Icelandic-1b virus
C:\INVADER.COM could have Anticad 4 virus
C:\ISRAEL-C.COM could have Jerusalem virus
C:\ITAVIR.EXE could have Itavir virus
C:\JB-A204.COM could have Jerusalem virus
C:\JER-204.COM could have Jerusalem virus
C:\JER-B.EXE could have Jerusalem virus
C:\JERSPAIN.COM could have Jerusalem.Spanish virus
C:\JOJO.COM could have Jojo virus
C:\JUNE16.COM could have June 16 virus
C:\KENNEDY.COM could have Kennedy virus
C:\LEHIGH.COM could have Lehigh virus
C:\LEHIGH2.COM could have Lehigh virus
C:\LIBERTY.COM could have Liberty virus
C:\LIBERTYE.EXE could have Liberty virus
C:\LISBON-B.COM could have Lisbon virus
C:\LISBON.COM could have Lisbon virus
C:\MIX1.EXE could have Mix1 virus
C:\MONDAC.COM could have Black Monday virus
C:\MONDAY.EXE could have Black Monday virus
C:\MURPHY-1.COM could have Murphy-1 virus
C:\MYSTIC-2.COM could have Liberty virus
C:\MYSTIC1.EXE could have Liberty virus
C:\NOTHING.COM could have Stupid virus
C:\OROPAX.COM could have Oropax virus
C:\PAYDAY.EXE could have Jerusalem virus
C:\PEACE.EXE could have Better world virus
C:\PERFUME.COM could have Perfume virus
C:\PHOENIX.COM could have Phoenix virus
C:\PHOENIXD.COM could have Phoenix virus
C:\PLASTIQU.COM could have Anticad 3 virus
C:\PLASTIQU.EXE could have Anticad 3 virus
C:\POLAND1.EXE could have Vcomm virus
C:\POLAND3.COM could have W13-b virus
C:\PRUD.EXE could have Prudents virus
C:\PRUDENTS.EXE could have Prudents virus
C:\PSQR.COM could have PSQR virus
C:\PUERTO.COM could have Jerusalem virus
C:\REDX.COM could have Ambulance virus
C:\SARATOGA.EXE could have Icelandic-1a virus
C:\SAT14.COM could have Saturday 14 virus
C:\SHAKE.COM could have Shake virus
C:\SLOW.COM could have Zerotime virus
C:\SOLANO.COM could have Solano virus
C:\SUBLIMNL.COM could have Subliminal virus
C:\SUNDAY.COM could have Anarkia virus
C:\SUNDAY.COM could have Jerusalem.Sunday virus
C:\SURIV01.COM could have Suriv-1 virus
C:\SURIV02.EXE could have Suriv-2 virus
C:\SURIV03.COM could have Suriv-3 virus
C:\SVIR.EXE could have Svir-0 virus
C:\SYLVIA.COM could have Sylvia virus
C:\TAIWAN.COM could have Taiwan virus
C:\TAIWAN2.COM could have Taiwan-2 virus
C:\TAIWAN3.COM could have Anticad 2 virus
C:\TCFISH6.COM could have Fish6 virus
C:\TCVP.COM could have VP virus
C:\TERROR.EXE could have Terror virus
C:\TINY-158.COM could have Tiny virus
C:\TINY-159.COM could have Tiny virus
C:\TINY-160.COM could have Tiny virus
C:\TINY-167.COM could have Tiny virus
C:\TINY-198.COM could have Tiny virus
C:\TRACEBCK.COM could have Traceback-3066 virus
C:\TYPO.COM could have Fumble virus
C:\V-277.COM could have Pixel.277 virus
C:\V1226.COM could have Live after Death-2 virus
C:\V1226D.COM could have Live after Death-2 virus
C:\V1226M.COM could have Live after Death-2 virus
C:\V1701NEW.COM could have Live after Death-3 virus
C:\V1721.COM could have Zerotime virus
C:\V2100.COM could have Dark Avenger 4 virus
C:\V2P2.COM could have Chameleon virus
C:\V512.COM could have No. of the beast-a virus
C:\V651.COM could have Dark Avenger 2 virus
C:\V800.COM could have Live after Death-1 virus
C:\VACSINA.COM could have Vacsina-05 virus
C:\VCOMM.EXE could have Vcomm virus
C:\VHP-348.COM could have Vienna-348 virus
C:\VHP-353.COM could have Vienna-353 virus
C:\VHP-367.COM could have Vienna-367 virus
C:\VHP-435.COM could have Vienna-435 virus
C:\VHP-623.COM could have Vienna-623 virus
C:\VHP-627.COM could have Vienna-627 virus
C:\VICTOR.COM could have Victor virus
C:\VIEN6.COM could have Vienna virus
C:\VIENNA.COM could have Vienna virus
C:\VIENNA62.COM could have Vienna virus
C:\VIOLATR.COM could have Violator virus
C:\VIR13J.EXE could have July13 virus
C:\VIRDEM.COM could have Virdem virus
C:\VIRUS-90.COM could have Virus-90 virus
C:\VIRUS-B.COM could have Virus-B virus
C:\VIRUS101.EXE could have Virus-101 virus

Appendix C (continued)

Virus Scanning Results for FINDVIRU version 4.22

```
C:\YANKEE19.COM could have Vacsina-25 virus
C:\YD-1961.EXE could have Old Yankee-1 virus
C:\YDOODLE.COM could have Vacsina-44 virus
C:\YDOODLE.EXE could have Vacsina-44 virus
C:\ZEROBUG.COM could have Zero bug virus

        227 files were on the disk.
        8 files were not checked.
        36 files were checked and are clean.
        183 files appear to have a virus.
        No boot sector viruses were found.
        No partition sector viruses were found.
-------------------------------------------------------------
     1889 kb of files took     94 seconds.
```

Appendix D

Virus Scanning Results for NBY version 2.77

```
C:\!3012.EXE            no known virus found.
C:\!DOOM2.EXE           infected by the Doom Two Virus
C:\!PLAS451.EXE                 no known virus found.
C:\!PLASTQ.EXE                  no known virus found.
C:\!WOLFMAN.EXE                 infected by the Wolfman Virus
C:\4096E.EXE            infected by the 4096 Virus
C:\ALABAMA.EXE                  infected by the Alabama Virus
C:\ANTICAD1.EXE                 infected by the Taiwan 3 Virus
C:\APRILEXE.EXE                 infected by the April Fool Virus
                                (also  Jerusalem-Version E Virus)
                                (also  Suriv201/Israeli/1488 Virus)
                                (also  Suriv A Virus)
C:\BENNY.EXE            infected by the 1381 Virus
                                (also  1381 Virus)
C:\BMONDAY.EXE                  infected by the Black Monday Virus
C:\DARKAV-1.EXE                 infected by the Dark Avenger Virus
C:\DARKAV-4.EXE                 infected by the Dark Avenger Virus
C:\DATCRM2B.EXE                 infected by the Datacrime II-B Virus
C:\DOODLE.EXE           infected by the Yankee Doodle Virus
C:\FELLOW.EXE           infected by the 1022 Virus
                                (also  Fellowship Virus)
C:\FISH.EXE             no known virus found.
C:\FREREE.EXE           no known virus found.
C:\FRIDAY13.EXE                 infected by the Jerusalem-Version B Virus
                                (also  Friday 13th Virus)
                                (also  Suriv 300 Virus)
                                (also  Jerusalem Version B Virus)
C:\GRAB.EXE             no known virus found.
C:\HALLOE.EXE           no known virus found.
C:\HM2.EXE              infected by the Invader Virus
C:\ICE-3.EXE            infected by the Icelandic-3 Virus
                                (also  December 24th Virus)
C:\ICE2.EXE             infected by the Icelandic-Version B Virus
                                (also  Saratoga/Icelandic Virus)
                                (also  MIX 1-Icelandic Virus)
C:\ICELANDI.EXE                 infected by the Saratoga (2)/656 Virus
                                (also  Saratoga/Icelandic Virus)
                                (also  MIX 1-Icelandic Virus)
C:\INFECTED.EXE                 no known virus found.
C:\ITAVIR.EXE           infected by the ItaVir Virus
C:\JER-B.EXE            infected by the Jerusalem-Version B Virus
                                (also  Friday 13th Virus)
                                (also  Suriv 300 Virus)
                                (also  Jerusalem Version B Virus)
C:\KEYPRESS.EXE                 no known virus found.
C:\LEPR-B.EXE           infected by the Leprosy B Virus
C:\LIBERTYE.EXE                 infected by the Liberty Virus
                                (also  Liberty Virus)
C:\MIX1.EXE             infected by the MIX 1-Icelandic Virus
C:\MONDAY.EXE           infected by the Black Monday Virus
C:\MYSTIC1.EXE                  infected by the Liberty Virus
                                (also  Liberty Virus)
C:\PAYDAY.EXE           infected by the Jerusalem-Version B Virus
                                (also  Friday 13th Virus)
                                (also  Suriv 300 Virus)
                                (also  Jerusalem Version B Virus)
C:\PCOM.EXE             no known virus found.
C:\PCOPY.EXE            no known virus found.
C:\PCSETUP.EXE                  no known virus found.
C:\PEACE.EXE            infected by the 1022 Virus
                                     (also  Fellowship Virus)
C:\PLASTIQU.EXE                 no known virus found.
C:\POLAND1.EXE                  infected by the Vcomm Virus
C:\PRUD.EXE             infected by the 1210 Virus
                                (also  Prudent Virus)
C:\PRUDENTS.EXE                 infected by the 1210 Virus
                                (also  Prudent Virus)
C:\SARATOGA.EXE                 infected by the Saratoga (1)/Icelandic/642 Virus
                                (also  Saratoga/Icelandic Virus)
                                (also  MIX 1-Icelandic Virus)
C:\SHAKE.EXE            infected by the Shake Virus
C:\SURIV02.EXE                  infected by the April Fool Virus
                                (also  Jerusalem-Version D Virus)
                                (also  Suriv201/Israeli/1488 Virus)
                                (also  Suriv A Virus)
C:\SVIR.EXE             infected by the stupid Virus
C:\TCC.EXE              infected by the TCC Virus
                                (also  Paris Virus)
C:\TERROR.EXE           no known virus found.
C:\USCAN.EXE            no known virus found.
C:\VCOMM.EXE            infected by the Vcomm Virus
C:\VIR13J.EXE           no known virus found.
C:\VIRUS101.EXE                 no known virus found.
C:\YANKEE.EXE           infected by the Yankee Doodle Virus
C:\YD-1961.EXE                  infected by the Yankee 2 Virus
                                (also  Yankee Doodle Two Virus)
C:\YDOODLE.EXE                  infected by the Yankee Doodle Virus
```

Appendix D (Continued)

Virus Scanning Results for NBY version 2.77

```
C:\NBY1.EXE             no known virus found.
C:\COMMAND.COM                  no known virus found.
C:\LHARC.COM            no known virus found.
C:\!3012.COM            no known virus found.
C:\!382.COM             infected by the 382 Virus
C:\!PLAS521.COM                 infected by the Invader Virus
C:\1008.COM             no known virus found.
C:\1024-B.COM           infected by the Nomenclature Virus
C:\1024.COM             infected by the 1024 Virus
C:\1253.COM             infected by the 1253 Virus
C:\1280.COM             infected by the 1280 Virus
                                (also  Datacrime/1280/1168 Virus)
                                (also  1280 Virus)
C:\12TRICKS.COM                 infected by the 12 Tricks Dropper Virus
                                (also  12 Tricks Trojan (53) Virus)
C:\1392.COM             infected by the Amoeba (1392) Virus
                                (also  KHETAPUNK Virus)
C:\1559.COM             infected by the 1559 Virus
                                (also  1554 Virus)
C:\1701.COM             infected by the Cascade (1)/Fall/1701 Virus
                                (also  1701/1704-Version B Virus)
                                (also  1701/1704-Version B Virus)
C:\1701CHIC.COM                 infected by the Cascade (1)/Fall/1701 Virus
                                (also  1701/1704-Version B Virus)
                                (also  1701/1704-Version B Virus)
C:\1704-B.COM           infected by the Cascade (1)/Fall/1701 Virus
                                (also  1701/1704-Version B Virus)
                                (also  Vienna (2)/Unesco  /648 Virus)
                                (also  Vienna (DOS 62)-Version A Virus)
                                (also  1701/1704-Version B Virus)
C:\1704-C.COM           infected by the 1701/1704-Version C Virus
                                (also  Cascade (2)/1704 Virus)
                                (also  1701/1704-Version B Virus)
C:\1704.COM             infected by the Cascade (1)/Fall/1701 Virus
                                (also  1701/1704-Version B Virus)
                                (also  1701/1704-Version B Virus)
                                (also  VHP Virus)
C:\1704FRMT.COM                 infected by the 1701/1704-Version C Virus
                                (also  Cascade (2)/1704 Virus)
                                (also  1701/1704-Version B Virus)
C:\1704MULT.COM                 infected by the Cascade (1)/Fall/1701 Virus
                                (also  1701/1704-Version B Virus)
                                (also  1701/1704-Version B Virus)
C:\17Y4.COM             infected by the Cascade (1)/Fall/1701 Virus
                                (also  1701/1704-Version B Virus)
                                (also  1701/1704-Version B Virus)
C:\1971.COM             infected by the 1971 Virus
C:\2000.COM             infected by the V2000 Virus
C:\2930.COM             infected by the 2930 Virus
                                (also  3066/2930 Traceback Virus)
C:\3551.COM             infected by the Syslock Virus
                                (also  Syslock 3551 Virus)
C:\403.COM              no known virus found.
C:\405.COM              infected by the 405 Virus
                                (also  405 Virus)
C:\4096.COM             infected by the 4096 Virus
C:\435.COM              infected by the VHP Virus
C:\512.COM              infected by the 512 Virus
C:\5120.COM             infected by the 5120 Virus
C:\623.COM              infected by the VHP-2 Virus
C:\AIDS.COM             infected by the AIDS Virus
                                (also  Hahaha Virus)
C:\AIDS2.COM            infected by the AIDS II Virus
C:\AMSTRAD.COM                  infected by the Amstrad Virus
                                (also  847 Virus)
C:\ANAR2.COM            infected by the Jerusalem-Version B Virus
                                (also  Fu Manchu Virus)
C:\ANARKIA.COM                  infected by the Jerusalem-Version B Virus
                                (also  Jerusalem Version B Virus)
                                (also  Anarkia Virus)
C:\ANTHRAX.COM                  infected by the ANTHRAX Virus
C:\ANTISCAN.COM                 infected by the Friday 13th Virus
                                (also  Suriv 300 Virus)
                                (also  1605 Virus)
C:\AP-400.COM           infected by the 400 Virus
                                (also  Anti-Pascal Virus)
C:\AP-440.COM           infected by the 400 Virus
                                (also  Anti-Pascal Virus)
C:\AP-480.COM           infected by the 400 Virus
                                (also  Anti-Pascal Virus)
C:\AP-529.COM           no known virus found.
C:\AP-605.COM           no known virus found.
C:\ARMAGEDO.COM                 infected by the Armagedon Virus
C:\BMONDAY.COM                  infected by the Black Monday Virus
C:\BUGS.COM             no known virus found.
C:\BURGER.COM           no known virus found.
C:\CASPER.COM           no known virus found.
```

Appendix D (Continued)

Virus Scanning Results for NBY version 2.77

```
C:\CHKDSK.COM              no known virus found.
C:\CUNNING.COM                      infected by the Cascade (1)/Fall/1701 Virus
                                    (also  1701/1704-Version B Virus)
                                    (also  1701/1704-Version B Virus)
C:\D-DANCE.COM                      infected by the Devil's Dance Virus
C:\DARK-A.COM              infected by the Dark Avenger Virus
C:\DARK3.COM               infected by the Dark Avenger Virus
C:\DARKAV-2.COM                     no known virus found.
C:\DARKAV-3.COM                     infected by the Dark Avenger Virus
C:\DBASE.COM               infected by the DBASE Virus
C:\DOODLE41.COM                     infected by the Yankee Doodle Virus
C:\DOODLE44.COM                     infected by the Yankee Doodle Virus
C:\DOS62.COM               infected by the Vienna (2)/Unesco  /648 Virus
                                       (also  Vienna (DOS 62)-Version A Virus)
C:\DRKAVNGR.COM                     infected by the Dark Avenger Virus
C:\FISH.COM                infected by the Fish Virus
C:\FLASH.COM               infected by the FLASH Virus
                                    (also  Flash variant Virus)
C:\FRERE.COM               no known virus found.
C:\FREREC.COM              no known virus found.
C:\FUMANCHU.COM                     infected by the Fu Manchu-Version A Virus
                                    (also  Fu Manchu Virus)
                                    (also  Fu Manchu-Version A Virus)
C:\GHOST.COM               infected by the Vienna (2)/Unesco  /648 Virus
                                    (also  Vienna (DOS 62)-Version A Virus)
                                    (also  Ghost Virus)
C:\GUPPY.COM               no known virus found.
C:\H1701.COM               infected by the Cascade (1)/Fall/1701 Virus
                                    (also  1701/1704-Version B Virus)
                                    (also  1701/1704-Version B Virus)
C:\H1704.COM               infected by the Cascade (1)/Fall/1701 Virus
                                    (also  1701/1704-Version B Virus)
                                    (also  1701/1704-Version B Virus)
C:\INVADER.COM                      infected by the Invader Virus
C:\ISRAEL-C.COM                     infected by the Jerusalem-Version B Virus
                                    (also  Jerusalem-Version B-2 Virus)
                                    (also  Jerusalem-Version B-2 Virus)
                                    (also  Friday 13th Virus)
                                    (also  Suriv 300 Virus)
                                    (also  Jerusalem Version B Virus)
C:\ISRAELI.COM                      no known virus found.
C:\JAP-XMAS.COM                     infected by the XMas (Japanese) Virus
C:\JB-A204.COM                      infected by the Jerusalem-Version B Virus
                                    (also  Friday 13th Virus)
                                    (also  Suriv 300 Virus)
                                    (also  Jerusalem Version B Virus)
C:\JER-204.COM                      infected by the Jerusalem-Version B Virus
                                    (also  Friday 13th Virus)
                                    (also  Suriv 300 Virus)
                                    (also  Jerusalem Version B Virus)
C:\JERSPAIN.COM                     infected by the Jerusalem-Version B Virus
                                    (also  Friday 13th Virus)
                                    (also  Suriv 300 Virus)
                                    (also  Jerusalem Version B Virus)
C:\JOJO.COM                no known virus found.
C:\JUNE16.COM              infected by the June 16th Virus
                                    (also  Pretoria Virus)
C:\KENNEDY.COM                      infected by the Kennedy Virus
                                    (also  333 Virus)
C:\KEYPRESS.COM                     no known virus found.
C:\LEHIGH.COM              infected by the Lehigh Virus
                                    (also  Lehigh V B Virus)
                                    (also  Lehigh Virus)
C:\LEHIGH2.COM                      infected by the Lehigh Virus
                                    (also  Lehigh V B Virus)
                                    (also  Lehigh Virus)
C:\LEPR-B.COM              infected by the Leprosy B Virus
C:\LEPR-BA.COM                      infected by the Leprosy B Virus
C:\LEPROSY.COM                      infected by the Leprosy Virus
C:\LIBERTY.COM                      infected by the Liberty Virus
                                    (also  Liberty Virus)
C:\LISBON-B.COM                     no known virus found.
C:\LISBON.COM              infected by the Lisbon Virus
C:\MINI.COM                no known virus found.
C:\MONDAC.COM              infected by the Black Monday Virus
C:\MURPHY-1.COM                     infected by the Murphy Virus
C:\MYSTIC-2.COM                     infected by the Liberty Virus
                                    (also  Liberty Virus)
C:\NOTHING.COM                      infected by the Do Nothing Virus
                                    (also  Do Nothing 2 Virus)
C:\ONTARIO.COM                      infected by the Ontario Virus
C:\OROPAX.COM              infected by the Oropax Virus
C:\PERFUME.COM                      infected by the Perfume Virus
                                    (also  765 Virus)
C:\PHOENIX.COM                      no known virus found.
C:\PHOENIXD.COM                     infected by the Nomenclature Virus
C:\PLASTIQU.COM                     no known virus found.
```

Appendix D (Continued)

Virus Scanning Results for NBY version 2.77

```
C:\POLAND3.COM                  infected by the W-13 Virus
                                (also  W-13 Virus)
                                (also  W13 Virus)
C:\PSQR.COM             infected by the 1720 Virus
                                (also  PSQR Virus)
C:\PUERTO.COM           infected by the Jerusalem-Version B Virus
                                (also  Friday 13th Virus)
                                (also  Suriv 300 Virus)
                                (also  Jerusalem Version B Virus)
C:\REALDCHK.COM                 no known virus found.
C:\REALMINI.COM                 no known virus found.
C:\REALTINY.COM                 no known virus found.
C:\REDX.COM             infected by the Red X Virus
C:\SAT14.COM            infected by the Saturday 14th Virus
                                (also  Durban Virus)
C:\SCOTSVAL.COM                 infected by the Scott's Valley Virus
C:\SCUD.COM             no known virus found.
C:\SHAKE.COM            infected by the Shake Virus
C:\SLOW.COM             infected by the E_C_46 (RK) Virus
                                (also  Slow Virus)
C:\SOLANO.COM           infected by the Solano Virus
                                (also  Subliminal Virus)
                                (also  Solano Virus)
C:\SUBLIMNL.COM                 infected by the Subliminal Virus
                                (also  Solano Virus)
C:\SUNDAY.COM           infected by the Sunday Virus
C:\SURIV01.COM                  infected by the April First-Version C Virus
                                (also  Suriv101/Israeli/897 Virus)
                                (also  Suriv A Virus)
C:\SURIV03.COM                  infected by the Jerusalem-Version E Virus
                                (also  Friday 13th Virus)
                                (also  Suriv 300 Virus)
                                (also  Jerusalem Version B Virus)
                                (also  Suriv B Virus)
C:\SYLVIA.COM           infected by the Holland Girl Virus
                                (also  Sylvia Virus)
C:\TAIWAN.COM           infected by the Taiwan Virus
C:\TAIWAN2.COM                  infected by the Taiwan Virus
                                (also  Taiwan 2 Virus)
C:\TAIWAN3.COM                  infected by the Taiwan 3 Virus
C:\TCFISH6.COM                  infected by the Fish Virus
C:\TCVP.COM             infected by the VP Virus
                                (also  VP Virus)
C:\TETRIS.COM           infected by the Sorry Virus
C:\TINY-158.COM                 no known virus found.
C:\TINY-159.COM                 no known virus found.
C:\TINY-160.COM                 no known virus found.
C:\TINY-167.COM                 no known virus found.
C:\TINY-198.COM                 no known virus found.
C:\TINY.COM             no known virus found.
C:\TRACEBCK.COM                 infected by the Traceback/3066 Virus
                                (also  3066 (Traceback) Virus)
                                (also  3066/2930 Traceback Virus)
C:\TSTVIRB.COM                  no known virus found.
C:\TYPO.COM             infected by the Typo COMVirus
C:\V-277.COM            no known virus found.
C:\V1226.COM            no known virus found.
C:\V1226D.COM           no known virus found.
C:\V1226M.COM           no known virus found.
C:\V1701NEW.COM                 no known virus found.
C:\V1721.COM            infected by the E_C_46 (RK) Virus
                                (also  Slow Virus)
C:\V2100.COM            infected by the V 2100 Virus
C:\V2P2.COM             no known virus found.
C:\V2P6.COM             no known virus found.
C:\V2P6Z.COM            no known virus found.
C:\V512.COM             infected by the 512 Virus
C:\V651.COM             infected by the 651 Virus
C:\V800.COM             infected by the V800 Virus
C:\VACSINA.COM                  infected by the Vacsina Virus
C:\VHP-348.COM                  infected by the VHP Virus
C:\VHP-353.COM                  infected by the VHP Virus
C:\VHP-367.COM                  infected by the VHP Virus
C:\VHP-435.COM                  infected by the VHP Virus
C:\VHP-623.COM                  infected by the VHP-2 Virus
C:\VHP-627.COM                  infected by the Vienna (2)/Unesco/648 Virus
                                (also  Vienna (DOS 62)-Version A Virus)
C:\VICTOR.COM           infected by the Victor Virus
C:\VIEN6.COM            infected by the Vienna (DOS 62)-Version A Virus
                                (also  Violator Virus)
C:\VIENNA.COM           infected by the Vienna (2)/Unesco  /648 Virus
                                (also  Vienna (DOS 62)-Version A Virus)
C:\VIENNA62.COM                 infected by the Vienna (2)/Unesco  /648 Virus
                                (also  Vienna (DOS 62)-Version A Virus)
C:\VIOLATR.COM                  infected by the Violator Virus
C:\VIRDEM.COM           no known virus found.
C:\VIRUS-90.COM                 infected by the Virus-90 Virus
```

Appendix D (Continued)

Virus Scanning Results for NBY version 2.77

```
C:\VIRUS-B.COM                    infected by the Friday 13th Virus
C:\VTINY.COM            infected by the Tiny Virus
C:\W13-A.COM            infected by the W-13 Virus
                                    (also  W-13 Virus)
                                    (also  W13 Virus)
C:\W13.COM              infected by the W-13 Virus
                                    (also  W-13 Virus)
                                    (also  W13 Virus)
C:\WESTWOOD.COM                   no known virus found.
C:\WISCON.COM           infected by the Wisconsin Virus
C:\YANKEE.COM           infected by the Yankee Doodle Virus
C:\YANKEE19.COM                   no known virus found.
C:\YDOODLE.COM                    infected by the Yankee Doodle Virus
C:\ZEROBUG.COM                    infected by the Zero Bug (1536) Virus
```