

VirusScan Version 2.2
Copyright 1995 by McAfee, Inc.
All Rights Reserved.

McAfee, Inc. (408) 988-3832 office
2710 Walsh Avenue (408) 970-9727 fax
Santa Clara, CA 95051-0963 (408) 988-4004 BBS (25 lines)
U.S.A. USR HST/v.32/v.42bis/MNP1-5
CompuServe GO MCAFEE
InterNet support@mcafee.COM

Using VirusScan (Version 2.2)

TABLE OF CONTENTS

Chapter 1: Welcome to VirusScan / 1	
What VirusScan includes / 3	
System requirements / 5	
License and registration / 6	
Technical support / 6	
Chapter 2: Don't skip this chapter / 10	
Installing VirusScan / 11	
Scanning your system / 14	
If you detect a virus / 16	
Activating VShield / 19	
Making a clean start-up diskette / 21	
Running the VirusScan programs / 23	
When to rescan / 25	
Updating VirusScan regularly / 25	
Chapter 3: Scan Reference / 28	
Technical overview / 30	
Validating Scan / 31	
Running Scan from the command line / 31	
Scan command line option summary / 33	
Scan option descriptions / 36	
Cleaning viruses / 46	
Examples / 50	
Error levels / 51	
Application note 1: Updating validation codes / 53	
Application note 2: Reformatting infected diskettes with DOS 5.0 and later / 53	
Technical note 1: Creating an exception list file for the /EXCLUDE option / 54	
Chapter 4: VShield Reference / 55	
Four levels of protection / 58	
Running VShield / 60	
VShield option summary / 64	
VShield option descriptions / 66	
Deciding which options are for you / 73	
Examples / 75	
Error levels / 76	
Using VShieldCRC / 77	
VShieldCRC option summary / 78	
Using CheckVShield / 79	
Technical note 1: Creating an exception list for the /EXCLUDE option / 81	
Technical note 2: Sample NetWare login script and .BAT file / 82	
Chapter 5: Tips & troubleshooting / 83	
Appendix A: Retrieving McAfee programs with communications software / 91	
Appendix B: Options comparison between VirusScan versions 1.5 and 2.1.1 / 96	
Glossary / 106	

CHAPTER 1: WELCOME TO VIRUSSCAN

Thank you for purchasing McAfee(R)'s VirusScan(TM) software, a powerful and advanced system designed to detect, eradicate, and prevent computer viruses. VirusScan will help you protect one of your most important assets--the information on your personal computer or local area network.

VirusScan includes two main programs:

- o The Scan program detects known viruses in your computer's memory or on disks. It can also detect new and unknown viruses. Once viruses are detected, it can remove them and restore your system to normal operation. The Scan program comes in two forms:
 - o A graphical interface so that you can select commands and options using a mouse and keyboard, if you like. For instructions, see the on-line documentation.
 - o A command line interface, so you can run the program and select options by typing from a command prompt or from batch or script files, if you prefer.
- o The VShield(TM) memory-resident program continuously monitors and protects your system from viruses that might be introduced.

The VirusScan programs run on IBM-PC or 100% compatible personal computers (PCs) that use DOS, Windows, or OS/2.

VirusScan is an important element of a comprehensive security program that includes a variety of safety measures, such as regular backups, meaningful password protection, training, and awareness. We urge you to set up and comply with such a security program in your organization. For tips on how to do this, see "Other sources of information" in this chapter.

HOW TO USE THIS MANUAL

This manual will help you get VirusScan running quickly and properly on DOS, Windows, and OS/2 systems.

All the key information is in Chapter 2, "Don't skip this chapter." Please don't install VirusScan before reading it, even if you are a PC power user or already familiar with Scan. Installing and using VirusScan is not like using other software.

The rest of Chapter 1, "Welcome to VirusScan," describes the programs and files on your VirusScan disk, system requirements, how to register, and how to get help.

Chapter 3, "Scan Reference," and Chapter 4, "VShield Reference," contain reference information for Scan and VShield, respectively. Many users will not need to read these chapters, because basic operation of VirusScan, as described in Chapter 2, will detect and remove most viruses from your system. The options described in Chapters 3 and 4 offer additional power and control, and are most useful in vulnerable environments and to network administrators and information services staff.

Chapter 5, "Tips & troubleshooting," explains how to get the most out of VirusScan, and how to cope with some common problems.

Appendix A describes how to retrieve new versions of McAfee programs using your communications software.

Appendix B describes differences in command line options between VirusScan version 1.5 and version 2.1.1.

In this manual, we use several conventions to distinguish particular kinds of text.

Upper-case in ³ <ENTER> ³ Key to press
brackets ³ ³ on the
³ ³ keyboard.

In addition to Scan and VShield, your VirusScan diskette contains another program that will help you use VirusScan. The Validate program ensures that new versions of VirusScan software you've obtained are authentic and unmodified.

Your VirusScan diskette also contains several useful text files, which you can view and print with a text editor, word processor, or print command. You'll find version-specific information in the README.1ST file.

VIRUSSCAN FILES AFTER UNPACKING

After unpacking VirusScan you should have appropriate program files on your system for the version you have obtained (DOS, Windows, or OS/2). Several useful text files are also included.

VirusScan for DOS Files

AGENTS.TXT - lists McAfee authorized agents.
CLEAN.DAT - virus removal data file required by SCAN.EXE
COMPUSER.NOT - explains how to obtain CompuServe membership
FILE_ID.DIZ - description of VirusScan used by some BBS software
FILENAME.TXT - explains ZIP file naming conventions
LICENSE.TXT - explains how to license VirusScan
NAMES.DAT - virus name data file required by SCAN.EXE
PACKING.LST - contains a list of all files, including validation information
README.TXT - late-breaking information and new instructions not contained in this manual
REGISTER.TXT - explains how to register VirusScan for your use
SCAN.DAT - virus string data file required by SCAN.EXE
SCAN.EXE - the VirusScan program
VIRUSCAN.TXT - on-line manual for VirusScan
VIRUSCAN.DOC - on-line manual for VirusScan (MS Word 6.0)
VALIDATE.EXE - check VirusScan programs for authenticity
VALIDATE.TXT - explains how to run VALIDATE.EXE

VShield Files

AGENTS.TXT - lists McAfee authorized agents
CHKVSHLD.EXE - checks for presence of VShield and VShieldCRC in memory
COMPUSER.NOT - explains how to obtain CompuServe membership
FILENAME.TXT - explains ZIP file naming conventions
FILE_ID.DIZ - description of VShield used by some BBS software
LICENSE.TXT - explains how to license VShield
NAMES.DAT - virus name data file
PACKING.LST - contains a list of all files, including validation information
README.TXT - late-breaking information and new instructions not contained in this manual
REGISTER.TXT - explains how to register VirusScan for your use
SCAN.DAT - virus string data file
VALIDATE.EXE - check VirusScan programs for authenticity
VALIDATE.TXT - explains how to run VALIDATE.EXE
VIRUSCAN.TXT - on-line manual for VirusScan
VIRUSCAN.DOC - on-line manual for VirusScan (MS Word 6.0)
VSHLDCRC.EXE - internal program for VShield
VSHIELD.DAT - virus string data file required by VSHIELD.EXE
VSHIELD.EXE - the VShield program
VSHINST.EXE - creates program group, icon for VSHLDWIN.EXE
VSHLDCRC.EXE - the VShieldCRC program
VSHLDWIN.EXE - used by VShield and VShieldCRC to display messages within Windows

VirusScan for OS/2

AGENTS.TXT - lists McAfee authorized agents

CLEAN.DAT - virus removal data file required by
OS2SCAN.EXE

COMPUSER.NOT - explains how to obtain CompuServe membership

FILE_ID.DIZ - description of VirusScan used by some BBS
software

FILENAME.TXT - explains ZIP file naming conventions

LICENSE.TXT - explains how to license VirusScan

NAMES.DAT - virus name data file required by OS2SCAN.EXE

PACKING.LST - contains a list of all files, including
validation information

README.TXT - late-breaking information and new
instructions not contained in this manual

REGISTER.TXT - explains how to register VirusScan for your
use

OS2SCAN.EXE - the VirusScan program

SCAN.DAT - virus string data file required by
OS2SCAN.EXE

VALIDATE.EXE - used to check VirusScan programs for
authenticity

VALIDATE.TXT - explains how to run VALIDATE.EXE

VIRUSCAN.TXT - on-line manual for VirusScan

VIRUSCAN.DOC - on-line manual for VirusScan (MS Word 6.0)

SYSTEM REQUIREMENTS

The VirusScan programs require an IBM-compatible personal computer and any of the following operating systems:

- o DOS 3.1 or later

- o Windows 3.1 or later

- o IBM OS/2 2.1 or later

VShield is a terminate-and-stay-resident (TSR) program. VShield attempts to minimize the use of conventional memory by loading into expanded, extended, or upper memory. For more information, see "VShield Reference" in Chapter 4.

You'll need a high-density 3.5" diskette drive to use the VirusScan diskette in this package. Contact McAfee for other media, or download the software from the McAfee bulletin board system (BBS).

LICENSE AND REGISTRATION

The VirusScan software is provided under license from McAfee, Inc., a copy of which is provided with this manual. Please read it and comply with it.

Also, please fill out and return the registration form in your VirusScan package. Registration entitles you to upgrades at no charge from McAfee's bulletin board system and other sources, as well as technical support, for one year from your date of purchase.

TECHNICAL SUPPORT

For help in using this product, we invite you to contact McAfee technical support. You can contact us:

- o On-line 24 hours a day, through our bulletin board system, CompuServe, or Internet (see "On-line access to updates and technical support" below);
- o By fax, at (408) 970-9727; or
- o By telephone at (408) 988-3832, Monday through Friday, 6:00 am to 5:00 pm Pacific Standard Time.

For fast and accurate help, please have the following information ready when you contact McAfee:

- o Program name and version number.
- o Type and brand of computer, hard disk, and any peripherals.
- o Version of DOS, along with any TSRs or device drivers in use.
- o Printouts of your AUTOEXEC.BAT and CONFIG.SYS files.
- o A printout of the contents of memory, from the MEM command (provided in DOS 4.0 and later) or a similar utility.

- o A description of the exact problem you are having. Please be as specific as possible. If you can't be at your computer when you call, a printout of the screen will be helpful.

If you are overseas, you can contact a McAfee authorized agent. Agents are located in more than 50 countries around the world and provide local sales and support for our software. Please refer to the AGENTS.TXT file for a complete list of McAfee agents.

ON-LINE ACCESS TO UPDATES AND TECHNICAL SUPPORT

McAfee updates VirusScan approximately once a month to add new virus detectors, new options, and fix reported bugs. To distribute these new versions, we run a multi-line bulletin board system, a forum on CompuServe, and an Internet node.

MCAFEE BULLETIN BOARD SYSTEM (BBS)

Our multi-line BBS is accessible 24 hours a day, 365 days a year, except for scheduled downtime and maintenance. All lines run high-performance modems operating from 1,200 bps to 28,800 bps with line settings of 8 data bits, no parity, and 1 stop bit. The McAfee BBS phone number is (408) 988-4004.

Appendix A, "Retrieving McAfee programs with communications software" explains how to dial up the McAfee BBS. Both technical support and software updates are available on the bulletin board.

MCAFEE FORUM ON COMPUSERVE

We sponsor the McAfee Virus Help Forum on CompuServe. To reach it, type GO MCAFEE at any CompuServe prompt. A free introductory membership is available. For more information, please read the enclosed COMPUSER.TXT file.

INTERNET ACCESS

The latest versions of McAfee's anti-virus software are available by anonymous ftp (file transfer protocol) over the Internet from the site [ftp.mcafee.com](ftp://ftp.mcafee.com). If your domain resolver does not support names, use the IP address 192.187.128.3. Enter anonymous or ftp as your user ID and your own e-mail address as the password. Programs are located in the pub/antivirus directory. If you have questions, please send e-mail to support@mcafee.com.

You can also find McAfee's anti-virus software at the SimTel Software Repository at Oak.Oakland.EDU in the simtel/msdos/virus directory and its associated mirror sites:

- o wuarchive.wustl.edu (US).
- o ftp.switch.ch (Switzerland).
- o ftp.funet.fi (Finland).
- o src.doc.ic.ac (UK).
- o archie.au (Australia).

MCAFEE PRODUCTS AND SERVICES

Founded in 1989, McAfee, Inc. is the leading provider of tools for productive computing for the DOS, OS/2, and Windows environments. Our anti-virus products are used by more than 16,000 corporations worldwide. Our utility products provide data security, automated version updating, and system inspection and editing. McAfee is also the pioneer and leading provider of electronically distributed software. All of McAfee's products can be purchased through dealers or downloaded from bulletin board systems and on-line services around the world.

McAfee doesn't stop at developing the world's best anti-virus and utility products. We back them with the industry's best service and technical support. Product support is provided by a full-time staff of virus researchers, programmers, and support professionals, and delivered directly by McAfee or our network of more than 150 Authorized Agent offices in more than 50 countries worldwide.

OTHER SOURCES OF INFORMATION

The McAfee BBS and CompuServe Virus Help Forum are excellent sources of information on virus protection. Batch files and utilities to help you use VirusScan software are often available, along with helpful advice.

Independent publishers, colleges, training centers, and vendors also offer information and training about virus protection and computer security.

We especially recommend the following books:

- o Ferbrache, David. A Pathology of Computer Viruses. London: Springer-Verlag, 1992. (ISBN 0-387-19610-2)
- o Hoffman, Lance J. Rogue Programs: Viruses, Worms, and Trojan Horses. Van Nostrand Reinhold, 1990. (ISBN 0-442-00454-0)
- o Jacobson, Robert V. The PC Virus Control Handbook, 2nd Ed. San Francisco: Miller Freeman Publications, 1990. (ISBN 0-87930-194-0)
- o Jacobson, Robert V. Using McAfee Associates Software for Safe Computing. New York: International Security Technology, 1992. (ISBN 0-9627374-1-0)

In addition, the following sources can provide useful information about viruses:

- o National Computer Security Association (NCSA)
10 South Courthouse Avenue
Carlisle, PA 17013
- o CompuServe VIRUSFORUM
- o Internet comp.virus newsgroup

CHAPTER 2: DON'T SKIP THIS CHAPTER or, What You Really Need to Know About VirusScan.

We're serious about this. Installing and running the VirusScan(TM) programs is not like using other software. Even if you are a personal computer power user, use the VirusScan installation procedure and follow the tasks in this chapter.

The reason is to avoid spreading a computer virus infection. Viruses spread when you start your computer (sometimes called booting) from an infected disk, or when you run an infected program. If your computer is infected, installing and running VirusScan on your hard disk may spread the infection, even to the VirusScan programs themselves. The tasks in this chapter will ensure that you have a clean environment to detect, eradicate, and prevent viruses.

This is like a surgical team establishing a "sterile field" before performing surgery. Once it is established, they make sure that everything brought into the field has already been sterilized. In this procedure, you will create a clean anti-viral start-up diskette with which you can always re-establish the sterile field.

Your VirusScan diskette is write-protected to ensure that no virus can alter the programs and information stored there. Under no circumstances should you remove the write protection.

Here's a summary of the tasks you'll follow in this chapter:

- o Installing VirusScan
- o Scanning your system.
- o If you detect a virus.
- o Activating VShield(TM).
- o Making a clean start-up (boot) diskette.
- o Running the VirusScan programs.
- o When to scan for viruses.
- o Updating VirusScan regularly.

INSTALLING VIRUSSCAN

This task explains how to check your system and install the VirusScan software under DOS, Windows, or OS/2 using the install program. For instructions on installing downloaded software, see Appendix A.

Don't use any other method to install VirusScan, or you risk spreading a virus.

INSTALLATION STEPS

Start from the system prompt (C:\> or [C:\]). If you are running Windows or an application program, exit from it to display the prompt. If you are running OS/2, close all DOS and Win-OS/2 sessions. Open the Command Prompts folder in the OS/2 System folder, and click on either the OS/2 Full Screen or OS/2 Window icon.

NOTE: See Appendix A for additional instructions for setting up WScan and VShield under Windows.

1. Create a directory to contain the VirusScan files, as in the following example:

```
C:\> mkdir c:\mcafee
```

and press <ENTER>.

If you have an earlier version of VirusScan already installed, create a separate directory (such as c:\newvscan) for the new version. (You should test the new version before removing the earlier version.)

2. Copy the VirusScan archived (.ZIP) file to this directory, as in the following example:

```
C:\> copy c:\download\*.zip c:\mcafee
```

and press <ENTER>.

3. Change to the VirusScan directory you just created, as in the following example:

```
C:\> cd c:\mcafee
```

and press <ENTER>.

4. Unzip the file using PKUNZIP.EXE, as in the following example:

```
C:\mcafee> PKUNZIP *.ZIP
```

and press <ENTER>.

5. Run VirusScan to check your local hard disk(s) by typing:

```
c:\mcafee> scan /adl
```

and pressing <ENTER>. It may take several minutes for the Scan program to check for viruses in memory, then on the system and user portions of your drives. Scan keeps you informed of its progress. Read the information carefully, and write down the name of any viruses Scan reports.

6. If Scan reports no virus found, congratulations--most likely your system is currently virus-free. Continue with "Making a Clean Start-Up Diskette" in this chapter.

If Scan finds one or more viruses, you'll see a message like:

```
Found the Jerusalem Virus
```

and installation will stop. Don't panic, even if the virus has infected many files. At the same time, don't run any other programs, especially if the virus is found in memory. Go directly to "If you detect a virus" later in this chapter for further instructions.

7. Create a directory on your hard disk to store the VirusScan files in by typing:

```
C:\> mkdir mcafee
```

and pressing <ENTER>.

8. Copy the VirusScan files from the 'VirusScan Program Diskette' in drive A: to your hard disk by typing:

```
C:\> copy a:\*.* c:\mcafee
```

and pressing <ENTER>. VirusScan has now been installed onto your hard disk. Now your system's startup files must be modified to find VirusScan on your system.

9. DOS and Windows users: Using a text editor program, load your AUTOEXEC.BAT file. Locate the path statement, which typically begins with a 'PATH' or 'SET PATH =' statement. Place your cursor at the end of this line and type:

```
;C:\MCAFEE
```

and press <ENTER>. Now save your AUTOEXEC.BAT file and exit the editor.

NOTE: If a semi-colon ";" is already present at the end of the line, do not add one to the path statement.

OS/2 users: Make the same change listed above to the 'SET PATH=' and 'SET LIBPATH=' statements in your CONFIG.SYS file. Now save your CONFIG.SYS file and exit the editor.

Congratulations! You've successfully installed VirusScan. Restart your computer now and continue with this chapter to see how you can use VirusScan to keep your computer virus-free. We recommend looking over the following sections in this chapter:

- o "Scanning Your System"
- o "If You Detect A Virus"
- o "Activating VShield"
- o "Making A Clean Start-Up Diskette"

Continue with the remaining tasks in this chapter, beginning with "Running the VirusScan Programs" to find out how and when to run and update the VirusScan programs.

SCANNING YOUR SYSTEM

VirusScan's Scan program examines your PC and disks to detect viruses there. The first time you run Scan, do so from the original, write-protected diskette so that the programs themselves cannot be infected.

Start from the system prompt (C> or [C:\]). If you are running Windows or an application program, exit from it to display the prompt. If you are running OS/2, close all DOS and Win-OS/2 sessions; then open the Command Prompts folder in the OS/2 system folder, and click the OS/2 Full Screen or OS/2 Window icon.

After typing each entry on the command line, press [Enter]. If you include the /REPORT option, Scan saves a report of infected files and any system errors to a log file that you specify.

1. Insert the VirusScan program diskette in drive A.
2. Scan your C drive for known viruses by typing:

DOS or Windows

```
C> a:scan c: /report c:\virus.log
```

OS/2

```
[C:\] a:os2scan c: /report c:\virus.log
```

Or, if you have more than one hard drive, scan them in the same way. For example, if you have C and D drives:

DOS or Windows

```
C> a:scan c: d: /report c:\virus.log
```

OS/2

```
[C:\] a:os2scan c: d: /report c:\virus.log
```

You can also scan all local drives using the /ADL option. For example:

DOS or Windows

```
C> a:scan /adl /report c:\virus.log
```

OS/2

```
[C:\] a:os2scan /adl /report c:\virus.log
```

It may take several minutes for the Scan program to check for viruses in memory, then on the system and user portions of your drives. Scan keeps you informed of its progress. Read the information on the screen carefully. Below is a sample of what Scan reports when checking a drive for viruses.

```

UAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA;
^ Virus data file V2.1.204 created Thu Jun 02      ^
^ 12:17:53 1994                                   ^
^                                                  ^
^ No viruses found in memory.                      ^
^                                                  ^
^ Scanning C:                                     ^
^ Summary report on C:                          ^
^ File(s)                                       ^
^ Analyzed:..... 1500                        ^
^ Scanned:..... 750                          ^
^ Possibly Infected:..... 0                   ^
^ Master Boot Record(s):.. 1                  ^
^ Possibly Infected:..... 0                   ^
^ Boot Sector(s):..... 1                      ^
^ Possibly Infected:..... 0                   ^
^                                                  ^
^ Time: 60.00 sec.                             ^
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAU

```

3. If Scan reports No viruses found, congratulations--most likely your system is currently virus-free. Skip to "Activating VShield" later in this chapter.

If Scan finds one or more viruses, you'll see a message like:

```

UAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA;
^ Scanning C:                                     ^
^ Scanning file C:\DOS\ATTRIB.EXE                ^
^ Found the Jerusalem Virus                       ^
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAU

```

DON'T PANIC, even if the virus has infected many files. At the same time, don't run any other programs, especially if the virus is found in memory. Turn to "If you detect a virus" later in this chapter, where VirusScan will help you eradicate it.

NOTE: Scan has many options to control and fine-tune the scope, validation, and operation of its scan. For details, see Chapter 3 and "Detecting new and unknown viruses" in Chapter 5.

IF YOU DETECT A VIRUS

In this task, you will run Scan with the /CLEAN option to eradicate most known viruses from your disks.

NOTE: If you are at all unsure about how to proceed once you've found a virus, contact McAfee for assistance (see "Technical support" in Chapter 1).

We strongly recommend that you get experienced help in dealing with viruses if you are unfamiliar with anti-virus software and methods. This is especially true for "critical" viruses and master boot record (MBR or so-called "partition table")/boot sector infections, because improper removal of these viruses can result in the loss of all data and use of the infected disks.

RESTART FROM A CLEAN ENVIRONMENT

You must run Scan from a clean, virus-free environment. With DOS or Windows, restart from a clean diskette. With OS/2, simply close all DOS and Win-OS/2 sessions.

DOS OR WINDOWS

With DOS or Windows, the only way to ensure a clean environment is to turn your computer off to eliminate any viruses in memory, then restart from a virus-free diskette, preferably the original, write-protected DOS installation diskette that came with your computer. If you don't have one, borrow or buy one; don't use a diskette that might be infected. (See "Making a clean start-up diskette" later in this chapter for instructions. Create this diskette after you clean your system.)

1. Turn off your computer. (Don't just reset or reboot, which may leave some viruses intact in the computer's memory.)

2. Make sure your clean boot (start-up) diskette is write-protected.

- o For a 3.5" diskette, slide its corner tab so that the square hole is open.

- o For a 5.25" diskette, cover its corner notch with a write-protect tab. Be sure to use the write-protect stickers provided with your diskettes, not tape.

3. Insert your start-up diskette in drive A.

4. Turn on your computer and wait until you see the system prompt (probably A>). Don't run any programs on your hard disk, or you may reactivate the virus.

OS/2

With OS/2, you can eliminate viruses from memory by closing all DOS, Win-OS/2, and virtual DOS machine (VDM) sessions.

BACK UP YOUR HARD DISK

Some viruses may leave certain disks or files unusable when cleaned up. To increase your chance of recovery, boot from a clean copy of the operating system, then copy all the files on all of your hard disks onto fresh diskettes or a backup tape. You can use a commercial backup program, or the one included with DOS or OS/2. Scan the program disk first to make sure that the backup program itself is not infected. Do not run the backup program if it is infected. Instead, reload it from your original installation diskettes.

Although some of the backed-up files may be infected, it is better to have current copies than not. However, don't overwrite previous backup disks or tapes, which may or may not be infected.

RUN SCAN WITH THE /CLEAN OPTION

Start from the system prompt (probably A> or [A:\]). If you are running OS/2, open the Command Prompts folder in the OS/2 system folder, and click the OS/2 Full Screen or OS/2 Window icon.

After typing each entry on the command line, press [Enter].

1. Insert the VirusScan program diskette in drive A.
2. Eliminate the first known virus on your hard drive(s) by typing:

DOS or Windows
A> scan /adl /clean

OS/2
[A:\] os2scan /adl /clean

Scan keeps you informed of its progress and generally reports virus removed successfully. If Scan reports that the virus could not safely be removed, see the next section, "If viruses were not removed."

NOTE: Scan has options to control and fine-tune the scope, validation, and operation of its disinfection. For details, see "Scan option descriptions" in Chapter 3.

IF VIRUSES WERE NOT REMOVED

If Scan can't remove a virus, it will tell you:

Virus cannot be removed from this file.

Make sure to take note of the filename, because you will need to restore it from backups. Run Scan again, this time using the /CLEAN and /DEL options to delete the remaining infected files, as described in Chapter 3. If you have any questions, contact McAfee (see "Technical support" in Chapter 1).

IF VIRUSES WERE SAFELY REMOVED, RESCAN AND CHECK DISKETTES

If Scan has successfully removed all the viruses, restart your computer. Restart installation as described in "Installing VirusScan" earlier in this chapter. Thereafter, you can proceed to "Making a clean start-up diskette" and "Running the VirusScan programs" later in this chapter.

One common source of virus infection is floppy diskettes. Once you've finished installing VirusScan on your hard disk, use Scan again to examine and disinfect the diskettes you use, as described in "When to rescan" later in this chapter.

FALSE ALARMS

Due to the nature of anti-virus software, there is a possibility that Scan may report a virus in a file that is not infected. This can be more likely if you are using more than one brand of virus protection software, especially if the virus is reported in memory and not anywhere on the disk when you boot.

If Scan reports a virus infection that you suspect may be in error, contact McAfee (see "Technical support" in Chapter 1). You can upload the file to our bulletin board system at (408) 988-4004, along with your name, address, daytime telephone number, and electronic mail address (if any).

ACTIVATING VSHIELD

VirusScan's VShield program can help prevent viruses from infecting your system. It runs as a "terminate-and-stay-resident" (TSR) program, remaining in memory and scanning and intercepting programs as they are executed.

To activate VShield at any time:

o DOS or Windows

Restart your computer by pressing [Ctrl]+[Alt]+[Del], or by turning it off and then on again, or any other reset method.

- o OS/2

Restart all DOS and Win-OS/2 windows. If you have difficulties running VShield, it may be due to conflicts with other TSR programs in your system, or with other programs that monitor disk access. See "VShield option summary" in Chapter 4 and "Troubleshooting VShield" in Chapter 5 for more information. Contact McAfee technical support if you need help (see "Technical support" in Chapter 1).

VShield minimizes the use of conventional memory by attempting to load into extended, expanded, upper memory, or a combination of them, before using conventional memory. For extreme memory limitations, you can use VShield's /SWAP option to reduce memory requirements to 8Kb, although this decreases VShield's speed. For details, see Chapter 4.

NOTE: VShield has options to control and fine-tune the scope, validation, and operation of its virus prevention. For details, see Chapter 4.

When used in conjunction with some Scan options, VShield can help protect your system from new and unknown viruses. At a minimum, consider checking floppy disk (/ANYACCESS, /FILEACCESS, or /BOOTACCESS). For details, see "Detecting new and unknown viruses" in Chapter 5.

In OS/2, VShield runs in DOS and Win-OS/2 sessions only, because viruses can operate only in those sessions.

In Windows, you can use the VShield icon to turn messages from VShield on and off. (VShield itself, however, remains active.) For details, see Chapter 4.

MAKING A CLEAN START-UP DISKETTE

In DOS or Windows, create a clean anti-viral start-up (boot) diskette that you can use to regain your "sterile field" if your system becomes infected. This is not necessary in OS/2, although it will be helpful to make backup copies of your OS/2 installation diskettes.

NOTE: Your system must be virus-free before starting these steps.

DOS OR WINDOWS

In DOS, start from the system prompt (C>). In Windows, you may open a DOS window, or duplicate these steps with the Windows File Manager.

1. Insert a blank or dispensable diskette in drive A. Make sure the diskette contains no important information, as this procedure will overwrite it.
2. Format it as a start-up diskette with the system files by typing:

```
C> format a: /s/v/u
```

NOTE: If you are using a version of DOS before DOS 5.0, do not type the /U option. The /U option in recent DOS versions ensures that the system portions of the diskette are overwritten.

When prompted for a volume label, enter virusfree01 or another name of up to 11 characters.

3. Copy the Scan program to the diskette. Here's one way to do this, assuming that your VirusScan files are stored in C:\MCAFEE\VIRUSCAN:

```
C> copy c:\mcafee\viruscan\scan.exe a:
C> copy c:\mcafee\viruscan\scan.dat a:
C> copy c:\mcafee\viruscan\clean.dat a:
C> copy c:\mcafee\viruscan\names.dat a:
```

4. Copy useful DOS programs to the diskette.
Here's one way to do this, assuming that your DOS files are stored in C:\DOS:

```
C> copy c:\dos\chkdsk.* a:  
C> copy c:\dos\debug.* a:  
C> copy c:\dos\diskcopy.* a:  
C> copy c:\dos\fdisk.* a:  
C> copy c:\dos\format.* a:  
C> copy c:\dos\label.* a:  
C> copy c:\dos\mem.* a:  
C> copy c:\dos\syst.* a:  
C> copy c:\dos\unerase.* a:  
C> copy c:\dos\xcopy.* a:
```

In the same way, copy other DOS programs that you think might be useful.

NOTE: If you use a disk compression utility, be sure to copy the drivers required to access the compressed disks onto the clean start-up diskette.

5. Remove the diskette from the drive and write-protect it so that it cannot become infected.
- o For a 3.5" diskette, slide its corner tab so that the square hole is open.
 - o For a 5.25" diskette, cover its corner notch with a write-protect tab. Be sure to use the write-protect stickers provided with your diskettes, not tape.
6. Label the diskette "Virus-Free start-up" and put it away in a secure place in case you need to reestablish a virus-free environment in the future. You may want to note the date and versions of DOS and VirusScan on the label.

OS/2

With OS/2, you don't need a virus-free start-up disk. However, it will be helpful to keep a clean copy of important files. Copy the VirusScan OS/2 program and data files and your CONFIG.SYS, STARTUP.CMD and AUTOEXEC.BAT files onto a clean start-up diskette. Write-protect the diskette, label it, and put it away in a secure place.

RUNNING THE VIRUSSCAN PROGRAMS

DOS

To run the VirusScan programs from the DOS command prompt, type the program name (SCAN or VSHIELD) on the command line. Follow the program name with the drive (if applicable to the program) and whatever options you want.

NOTE: If you have not changed the path statement in your AUTOEXEC.BAT file, you will need to include its location (usually C:\MCAFEE\VIRUSCAN) in the command, or change to that directory.

For example, to examine a diskette in drive A:

```
C> c:\mcafee\viruscan\scan a:
```

EXCEPTION: If Scan detects a virus in memory or on your hard disk, don't run Scan with the /CLEAN option from C:\MCAFEE\VIRUSCAN. Instead, restart your computer and run Scan from your clean start-up diskette as described in "If you detect a virus" earlier in this chapter.

VirusScan can list the viruses it detects. To view this list, run Scan with the /VIRLIST option, as described in Chapter 3.

WINDOWS

If you used the installation procedure earlier in this chapter or installed downloaded files using the instructions in Appendix A, the WScan and VShield icons appear in the McAfee group. To use them, open the folder and double-click the program icon. See Chapter 3 for instructions on using Scan for Windows.

NOTE: If a virus is active in memory, do not use interactive Scan to remove it, because Windows or other system files might be infected and you risk spreading the virus.

If you've detected such a virus, restart your computer and run Scan from your clean start-up diskette, as described in "If you detect a virus" earlier in this chapter.

VSHIELD AND WINDOWS

The install program adds a line to your AUTOEXEC.BAT file that automatically activates VShield whenever you start or restart your computer. In Windows, it also gives you a VShield icon that you can click to see VShield status. (See Appendix A for instructions for downloaded software.)

NOTE: You can change VShield options from the DOS command line by removing VShield from memory and rerunning it, by editing the VSHIELD command in your AUTOEXEC.BAT file, or by editing the default configuration file. See Chapter 4 for details.

OS/2

To run Scan from OS/2, open the Command Prompts folder in the OS/2 system folder and click the OS/2 Full Screen or OS/2 Window icon. Next, type the program name (os2scan) on the command line. Follow the program name with the drive, directory, or file(s) you want to scan and the options you want to use.

NOTE: If you have not changed the PATH and LIBPATH statements in your CONFIG.SYS file, you will need to include its location (usually C:\MCAFEE\VIRUSCAN) on the command line, or change to that directory.

For example, to examine a diskette in drive A:

```
[C:\] c:\mcafee\viruscan\os2scan a:
```

NOTE: VShield does not run in OS/2 sessions, only under DOS and Win-OS/2 sessions inside of OS/2. You can place the VShield command in your AUTOEXEC.BAT file, where it will run automatically when you start a DOS or Win-OS/2 session. You can also run it from the DOS command line, as described earlier in this section.

WHEN TO RESCAN

Although VShield will monitor your software for viruses, it's wise to scan your disks when you introduce new programs, or disks that may be infected. New programs and files are generally introduced in two ways: by inserting a diskette and booting from it, and by installing new programs. It is also possible to download a virus inadvertently via a modem, but this is very rare.

You can use VShield with the /ANYACCESS option to scan diskettes automatically. For more information, see "/ANYACCESS" in "VShield option descriptions" in Chapter 4.

For instructions on running VirusScan, see "Running the VirusScan programs" earlier in this chapter.

WHEN YOU INSERT AN UNCHECKED DISKETTE

Every time you insert a new diskette in your drive, run Scan on it before executing, installing, or copying its files. If you have several diskettes to scan, you can scan them consecutively using the /MANY option described in Chapter 3. In fact, we recommend doing this now with all the diskettes you normally use, as well as diskettes received from friends, coworkers, salespeople, and even your own diskettes if they have been in another PC.

WHEN YOU INSTALL OR DOWNLOAD NEW FILES

Every time you install new software on your hard drive, or download executable files from a network server, bulletin board, or on-line service, run Scan on the directory in which the files were placed before you execute the files.

UPDATING VIRUSSCAN REGULARLY

Unfortunately, new viruses (and variants of old ones) appear and circulate often in the personal computer community. Fortunately, McAfee updates the VirusScan programs regularly--usually monthly, but sooner if many new viruses have appeared. Each new version may detect and eradicate as many as 60-100 new viruses or more, and may add new features. To find out what's new, review the README.1ST text file.

DOWNLOAD NEW VERSIONS

As a VirusScan licensee, you may download new versions without charge for one year from your date of purchase. Use your communications software to download new versions from the McAfee bulletin board, CompuServe, or the Internet. See Chapter 1 and Appendix A for more information.

New versions of McAfee software are stored in compressed form to reduce transmission time.

NOTE: Always download and decompress the files in a separate directory from your current files. That way, if you discover a problem with the new files, you'll still have the old ones.

VALIDATE VIRUSSCAN

When you download a program file from any source other than the McAfee bulletin board or other McAfee service, it's important to verify that it is authentic, unaltered, and uninfected. McAfee anti-virus software includes a program called Validate that helps you do this. When you receive a new version of VirusScan, run Validate on all of the program files.

To do this for Scan, start from the system prompt (C> or [C:\]):

1. Navigate to the directory to which you've downloaded the files. For example, if you've stored the files in C:\MCAFEE\DOWNLD\VIRUSCAN:

```
C> c:  
C> cd \mcafee\downld\viruscan
```

2. Type the command:

```
DOS or Windows  
C> validate scan.exe
```

```
OS/2  
[C:\] os2val os2scan.exe
```

3. Compare the results with the information in the PACKING.LST file or other text file for the program you validated. If the validation results match what's in the file, it is highly unlikely that the program has been modified.

UPDATE YOUR CLEAN START-UP DISKETTE

Once you have validated the new version, copy it into your C:\MCAFEE\VIRUSCAN directory. In addition, copy the Scan program onto your clean start-up diskette. Below is one way to do this; you may also use the Windows File Manager or the OS/2 environment.

Note any changes you've made to default options, because you may want to select and save them again. Start from the system prompt (C> or [C:\]).

1. Navigate to the directory to which you've retrieved the files, such as C:\MCAFEE\DOWNLD\VIRUSCAN:

```
C> c:  
C> cd \mcafee\downld\viruscan
```

2. Copy the contents of the directory to C:\MCAFEE\VIRUSCAN:

```
C> copy *.* c:\mcafee\viruscan
```

3. Temporarily remove write-protection from your clean start-up diskette and insert it in drive A.

- o For a 3.5" diskette, slide its corner tab so that the square hole is closed.

- o For a 5.25" diskette, remove the tab from its corner notch.

4. Copy the Scan program to the diskette.

DOS or Windows

```
C> copy SCAN.EXE a:  
copy SCAN.DAT a:  
copy CLEAN.DAT a:  
copy NAMES.DAT a:
```

OS/2

```
[C:\] copy OS2SCAN.EXE a:
```

5. Remove the diskette from the drive and write-protect it again.

CHAPTER 3: SCAN REFERENCE

The Scan program detects, identifies, and disinfects known DOS computer viruses. Scan checks memory as well as the system and data areas of disks for virus infections. If Scan finds a known virus, in most cases it will eliminate the virus and fully restore infected programs or system areas to normal operation.

To obtain a list of all the viruses that Scan detects, run Scan with the /VIRLIST option.

In addition, Scan can also assign validation and recovery codes to files, and use those codes to detect and treat infection by new and unknown viruses. If Scan has stored validation or recovery data for files, it may detect file changes and warn that infection by an unknown virus may have occurred. Scan can also use the recovery codes to remove new or unknown viruses and restore infected files.

Scan runs on DOS, Windows, and OS/2. The program files are SCAN.EXE (DOS), WSCAN.EXE (Windows), and OS2SCAN.EXE (OS/2), respectively. This chapter describes them all.

NOTE: Because OS/2 operates in a protected mode environment, Scan for OS/2 does not check memory. To protect against viruses in OS/2 DOS and Win-OS/2 sessions, use the VShield (for DOS) virus prevention program.

Scan is designed so that basic operation, as described in "Scanning your system" and "When to rescan" in Chapter 2, will detect most viruses. The command line options described here offer additional power and control over virus detection. They enable you to run Scan from batch or script files. Network administrators, information services staff, and computer systems with vulnerable environments will benefit from this feature.

SYSTEM REQUIREMENTS AND SUPPORT

Scan requires DOS 3.1 or later, Windows 3.1 or later, or IBM OS/2 Version 2.1 or later.

Scan works with 3Com 3/Share and 3/Open, Artisoft LanTastic, AT&T StarLAN, Banyan VINES, DEC Pathworks, IBM LAN Server, Microsoft LAN Manager, Novell NetWare, and any other IBMNET- or NETBIOS-compatible network operating systems. Contact McAfee or your local authorized agent if you do not see your network listed (see "Technical support" in Chapter 1).

Scan is designed to check for pre-existing infections of known and unknown viruses on floppy, hard, CD-ROM, and compressed disks (SuperStor, Stacker, DoubleSpace, and so on) on both stand-alone and networked personal computers, as well as network file servers. If you have a Novell NetWare/386 V3.1X or 4.01 file server, you may want to use the NETShield(TM) virus prevention NetWare Loadable Module (NLM) in conjunction with Scan.

NOTE: To use Scan to clean up (disinfect) virus-infected files, the CLEAN.DAT file must be present in the same subdirectory as SCAN.EXE. If you don't have the CLEAN.DAT file, first verify whether you should contact your system administrator or information systems staff directly for virus clean-up. Otherwise, you can contact McAfee (see "Technical support" in Chapter 1).

TECHNICAL OVERVIEW

KNOWN VIRUS DETECTION

Scan detects known viruses by searching the system for characteristics (sequences of code) unique to each computer virus and reporting their presence if found. For viruses that encrypt or cipher their code so that every infection is different, Scan uses detection algorithms that work by statistical analysis, heuristics, and code disassembly.

NEW AND UNKNOWN VIRUS DETECTION

Scan can also check for new or unknown viruses by comparing files against previously recorded validation data. If a file has been modified, it will no longer match the validation data, and Scan will report that the file may have become infected. With certain options, SCAN /CLEAN can use the validation and recovery data to restore infected files. Refer to the /AF, /AV, /CF, /CV, /RF, and /RV options in Chapter 4.

NOTE TO NETWORK USERS

To use Scan on a network drive (or directory), you must be connected to that drive and have read access to it. Some command line options described in this chapter attempt to create, change, and delete files. To use these options, you must have sufficient access rights. If you have questions about access rights, contact your network administrator.

VALIDATING SCAN

The Scan program in your VirusScan package is supplied on a write-protected diskette that should be secure from infection. We recommend that you update your copy of the VirusScan programs regularly. You can obtain an upgrade from several sources, as described in "Updating VirusScan regularly" in Chapter 2.

Before using a new version of Scan for the first time, verify that it has not been tampered with or infected by using the Validate program, as described in "Validate VirusScan" in Chapter 2. If your new copy of Scan differs from the validation data in the on-line documentation file, it may have been damaged. Don't use it, and obtain a clean copy of Scan from a known source.

Scan performs an integrity test when run. This self-check allows Scan to determine if it has been modified. If Scan fails its integrity test, a warning message appears, and Scan refuses to run and returns to the command line prompt. You must obtain an undamaged copy before continuing.

RUNNING SCAN FROM THE COMMAND LINE

Scan checks files and other areas of the system that can contain computer viruses. When a virus is found, Scan identifies the virus and the system area or file where it was found.

By default, Scan examines only executable files (.EXE, .COM, .SYS, .BIN, .OVL, and .DLL files). These are the files most likely to be infected with a virus. Use the /ALL option to scan all files on your system. Refer to "Scan option descriptions" later in this chapter for more information about the /ALL option.

From DOS or OS/2, you can run Scan from the system prompt. (From OS/2, open the Command Prompts folder in the OS/2 system folder, then click either the OS/2 Full Screen icon or the OS/2 Window icon to see the system prompt. Once you see the prompt,

For DOS, type:

```
C> scan {drives} [options]
```

For OS/2, type:

```
[C:\] os2scan {drives} [options]
```

{drives} indicates one or more drives to be scanned. You must specify one or more drives to scan. If you list a drive like c:, all of its subdirectories will be scanned. If you list \, only the root directory of the current disk will be scanned. If you list \ or a directory, its subdirectories will not be scanned unless you use the /SUB option.

[options] indicates one or more of the Scan options listed in the next section, "Scan command line option summary."

SCAN COMMAND LINE OPTION SUMMARY

/? or /HELP

Display help screen (not available in Windows, use Help menu instead).

/ADL

Scan all local drives (including CD-ROM and PCMCIA drives, but not floppy drives).

/ADN

Scan all network drives.

/AF {filename}

Store validation/recovery codes in {filename}.

/ALL

Scan all files, not just standard executables.

/APPEND

Append to, rather than overwrite, the file (used with the /REPORT option).

/AV

Add validation/recovery data to program files.

/BOOT

Scan boot sector and master boot record only.

/CF {filename}

Check validation/recovery codes in {filename}.

/CLEAN

Clean up infections in boot sector, master boot record, and files when possible.

/CV

Check validation/recovery data in files.

/DEL

Overwrite and delete infected files.

/EXCLUDE {filename}

Exclude from scan any files listed in {filename} (used with the /AV option).

/FAST

Speed up VirusScan's scanning; may detect fewer viruses.

/FREQUENCY {hours}

Set the time frequency with which to scan your system.

/LOAD {filename}

Use Scan settings stored in {filename}.

/LOG

Save date and time that Scan was last run in a hidden file (SCAN.LOG).

/MANY

Scan multiple diskettes on a single drive.

/MOVE {directory}

Move infected files to {directory}.

/NOCOMP

Skip checking compressed executables created with the LZEXE or PKLITE file compression programs.

/NOMEM

Skip memory checking (not applicable to OS/2).

/PAUSE

Enable screen pause.

/PLAD

Preserve last access dates on Novell drives.

/REPORT {filename}

Create report of infected files found during scan in {filename}.

/RF {filename}

Remove validation/recovery codes in {filename}.

/RPTCOR

Add list of corrupted files to the report file (used with the /REPORT option).

/RPTERR

Add list of system errors to the report file (used with the /REPORT option).

/RPTMOD

Add list of modified files to the report file. (used with the /REPORT option in conjunction with either /CF or /CV).

/RV

Remove validation/recovery data from files.

/SHOWLOG

Display information in SCAN.LOG.

/SUB

Scan subdirectories inside a directory.

/VIRLIST

Display list of viruses detected by VirusScan.

SCAN OPTION DESCRIPTIONS

Here is a detailed description of Scan's options.

`/?` or `/HELP`

Display list of Scan options.

Does not scan. Instead, displays a list of Scan command line options with a brief description of each. No scanning is performed when these options are specified. Use either of these options alone on the command line.

`/ADL`

Scan all local drives (except floppy drives).

Scans all local drives for viruses, in addition to those specified on the command line. In DOS, use `/ADL` to check all local drives (including compressed drives, CD-ROMs, and PCMCIA drives, but not floppy drives). To scan both local and network drives, use `/ADL` and `/ADN` together in the same command line.

`/ADN`

Scan all network drives.

Scans all network drives for viruses, in addition to those specified on the command line. To scan both local and network drives, use `/ADL` and `/ADN` together in the same command line.

`/AF {filename}`

Store validation/recovery codes in {filename}.

Helps you detect and recover from new or unknown viruses. `/AF` logs validation and recovery data for executable files (but not the boot sector or the master boot record) of a disk in the file you specify. The log file is about 95 bytes per file validated. You must specify a {filename}, which can include the target drive and directory (such as `D:\VSVALID\VALCODES.VSC`). If the target path is a network drive, you must have rights to create and delete files on that drive. If {filename} exists, Scan updates it. `/AF` adds about 300% more time to scanning.

To recover from a virus using the /AF information, use the /CF and /CLEAN options together in the same command line. Using any of the /AF, /CF, or /RF options together in the same command line returns an error.

NOTE: /AF performs the same function as /AV, but stores its data in a separate file rather than changing the executable files themselves. For more information, see "Detecting new and unknown viruses" in Chapter 5.

/ALL

Check all files, not just standard executable files.

Increases system security by performing a more thorough scan. Otherwise, Scan checks only standard executable files (with .COM, .EXE, .SYS, .BIN, .OVL, and .DLL extensions), which are the files most likely to be infected by a virus. If /ALL is specified, Scan checks all files on the specified drive, which increases Scan's ability to detect viruses in overlay files but substantially increases the scanning time required. Use this option if you have found a virus or suspect one. (Note that the list of extensions for standard executables, above, has changed from previous releases of VirusScan.)

/APPEND

Append to the report file.

Used in conjunction with /REPORT, appends the report message text to the specified report file, if it exists. Otherwise, the /REPORT option overwrites the specified report file, if it exists.

/AV

Add validation/recovery data to files.

Helps you detect and recover from new or unknown viruses. /AV adds recovery and validation data to each standard executable file (.EXE, .COM, .SYS, .BIN, .OVL, and .DLL), increasing the size of each file by 98 bytes. To update files on a shared network drive, you must have update access rights. The /AV option adds about 100% more time to scanning.

To exclude self-modifying or self-checking files that might cause false alarms, use the /EXCLUDE option. To recover from a virus using the /AV information, use the /CV and /CLEAN options together in the same command line. Using any of the /AV, /CV, or /RV options together in the same command line returns an error.

NOTE: The /AV option does not store any information about the master boot record (MBR) or boot sector of the drive being scanned.

/BOOT

Scan boot sector and master boot record only.

Scans the boot sector and master boot record on the specified drive(s), but not files or directories on those drives.

/CF {filename}

Check validation/recovery codes in {filename}.

Helps you detect new or unknown viruses. Checks validation data stored by the /AF option in {filename}. If a file or system area has changed, Scan reports that a viral infection may have occurred. The /CF option adds about 250% more time to scanning. For more information, see "Detecting new and unknown viruses" in Chapter 5. You can use /CF and /CLEAN in the same command line to check validation/recovery codes and remove any viruses found. Using any of the /AF, /CF, or /RF options together in a command line returns an error.

NOTE: Some older Hewlett-Packard and Zenith PCs modify the boot sector each time the system is booted. If you use /CF or /CV, Scan continuously reports that the boot sector has been modified even though no virus may be present. Check your system's reference manual to determine whether your PC has self-modifying boot code, or contact McAfee for help (see "Technical support" in Chapter 1).

NOTE OS/2 dual boot systems change the boot sector between DOS and OS/2 depending on which operating system is active. This causes Scan to report that the boot sector has been modified.

/CLEAN

Remove viruses from boot sector, master boot record, and infected files.

Attempts to restore the boot sector, if infected, and any infected files. Usually, between 10% and 20% of all viruses are not removable; they damage the file they infect beyond repair. If the infected file resides on a network drive, you must have rights to modify files on that drive to clean it. If it cannot restore a file, you'll see a message that identifies the name of the unrecoverable file. To use /CLEAN, the CLEAN.DAT file must reside in the Scan directory. For more information, see "Cleaning viruses" later in this chapter.

Use /CLEAN instead of /DEL when you want to restore infected files, not just delete or overwrite them. The /CLEAN option can remove master boot record (MBR) and boot sector viruses, but the /DEL option cannot. If you use /CLEAN and /DEL in the same command line, Scan first attempts to disinfect an infected file, then deletes it only if it cannot be repaired. Similarly, if you use /CLEAN and /MOVE in the same command line, Scan first attempts to clean an infected file, then moves it to the specified subdirectory if the file is unrecoverable.

You can use /CLEAN and /CF or /CV in the same command line to check validation/recovery codes and remove any viruses found. We strongly recommend that you get experienced help in dealing with viruses if you are unfamiliar with anti-virus software and methods. This is especially true for "critical" viruses and master boot record (MBR)/boot sector infections, because improper removal of these viruses can result in the loss of all data on the infected disks.

NOTE: When scanning a network drive using /CLEAN, you must have sufficient rights to update files on that drive.

/CV

Check validation/recovery data in files.

Helps you detect new or unknown viruses. Checks validation data added by the /AV option. If a file is modified, Scan reports that a viral infection may have occurred. The /CV option adds about 50% more time to scanning. You can use /CLEAN and /CV in the same command line to check validation/recovery codes and restore infected files. Using any of the /AV, /CV, or /RV options together in the same command line returns an error.

For more information, see "Detecting new and unknown viruses" in Chapter 5. See also the note under /CF in this section.

/DEL

Overwrite and delete infected files.

Deletes and overwrites each infected file. Files erased by the /DEL option cannot be recovered (you should generate a report so that you can restore them from backups). Instead of /DEL alone, we recommend using it in combination with the /CLEAN option to attempt to disinfect an infected file first, then delete it only if the file is unrecoverable. The /CLEAN option can remove master boot record and boot sector viruses, but the /DEL option cannot.

NOTE: When scanning a network drive using /DEL, you must have sufficient access rights to delete files on that drive.

/EXCLUDE {filename}

Scan using exception list file called {filename}.

Allows you to exclude files from /AV validation and /CV checking. Self-modifying or self-checking files can cause a false alarm during a scan. To create {filename}, see "Technical note 1: Creating an exception list file for the /EXCLUDE option" in this chapter.

/FAST

Speed up Scan's scanning.

Reduces scanning time by about 15%. Using the /FAST option, Scan examines a smaller portion of each file for viruses, although it examines more files overall. Using /FAST might miss some infections found in a more comprehensive (but slower) scan. Do not use this option if you have found a virus or suspect one.

/FREQUENCY {hours}

Set the time frequency with which to scan your system.

In environments where the risk of viral infection is very low, use this option to prevent unnecessary or too-frequent scans. The lower the number of {hours} specified, the greater the scan frequency and the greater your protection against infection.

The first time this option is used on a workstation, Scan creates a hidden file named MCAFEE.FRC in the root directory of drive C. In it, Scan stores the date and time that the system was scanned. Thereafter, whenever this option is used, Scan checks this file and compares the time elapsed from the last scan with the specified number of {hours}. If {hours} exceeds the elapsed time, Scan exits without scanning the system. Otherwise, Scan proceeds as usual to scan the system and, when finished, updates MCAFEE.FRC with the system date and time.

/LOAD {filename}

Use Scan settings stored in {filename}.

By default, Scan loads its internal default settings plus any options specified on the command line. You can store all custom settings in a separate ASCII text file, then use /LOAD to load those settings from that file.

Use a text editor to create the file. You can put all options on the same command line or put each option (with its parameter) on its own line, separated by a hard carriage return and line feed, as shown in the following examples.

Sample load file with all options on the same command line:

```
m: /report a:infectn.rpt /rptcor /rpterr
```

Sample load file with each option on a separate command line:

```
m:  
/report a:infectn.rpt  
/rptcor  
/rpterr
```

/LOG

Save date and time of last scan.

Stores the time and date Scan is being run by updating or creating a file called SCAN.LOG in the current directory.

/MANY

Scan multiple floppies.

Scans multiple diskettes consecutively in a single drive. Scan will prompt you for each diskette. Once you have established a virus-free system, use this option to check multiple diskettes quickly.

/MOVE {directory}

Move infected files to {directory}.

Moves all infected files found during a scan to the specified directory. If you use /MOVE in conjunction with /CLEAN, Scan attempts to restore an infected file first, then moves it to the specified directory only if the file cannot be restored. Using /MOVE and /DEL in the same command line returns an error message.

/NOCOMP

Skip checking compressed executable files.

Reduces scanning time when a full scan is not needed. Otherwise, by default, Scan checks inside executable, or self-decompressing, files that have been created using the LZEXE or PKLITE file compression programs. Scan decompresses each file in memory and checks for virus signatures, which takes time but results in a more thorough scan. If you use /NOCOMP, Scan does not check inside compressed files for viruses, although it can check for modifications to those files if they have been validated using validation/recovery codes.

/NOMEM

Skip memory checking.

Reduces scan time by omitting all memory checks for viruses. Use /NOMEM only when you are absolutely certain that your system is virus-free.

By default, Scan checks system memory for critical known computer viruses that can inhabit memory. In addition to main memory from 0Kb to 640Kb, Scan checks system memory from 640Kb to 1088Kb that can be used by computer viruses on 286 and later systems. Memory above 1088Kb is not addressed directly by the processor and is presently not susceptible to viruses.

NOTE: /NOMEM is not applicable to OS/2.

/PAUSE

Enable screen pause.

If you specify /PAUSE, the More? (H = Help) prompt appears when Scan fills up a screen with messages, such as when using the /SHOWLOG or /VIRLIST options. Otherwise, by default, Scan fills and scrolls a screen continuously without stopping, which allows Scan to run on PCs with many drives or that have severe infections without requiring you to attend. We recommend that you omit /PAUSE when keeping a record of Scan's messages using the report options (/REPORT, /RPTCOR, /RPTMOD, and /RPTERR).

/PLAD

Preserve last access dates (NetWare drives only).

Prevents changing the last access date attribute for files stored on a network drive in a Novell network. Normally, NetWare updates the last access date when Scan opens and examines a file. However, some tape backup systems use this last access date to decide whether to back up the file. Use /PLAD to ensure that the last access date does not change as the result of scanning.

/REPORT {filename}

Create report of infected files and system errors.

Saves the output of Scan to {filename} in ASCII text file format. If {filename} exists, /REPORT erases and replaces it. You can use /APPEND to append the current scan report to the end of {filename}. You can include the destination drive and directory (such as D:\VSREPRT\ALL.TXT), but if the destination is a network drive, you must have rights to create and delete files on that drive. You can also use /RPTCOR, /RPTMOD, and /RPTERR to add corrupted files, modified files, and system errors to the report.

/RF {filename}

Remove validation/recovery codes in {filename}.

Removes recovery and validation data from {filename} created by the /AF option. If {filename} resides on a shared network drive, you must be able to delete files on that drive. Using any of the /AF, /CF, or /RF options together in the same command line returns an error.

/RPTCOR

Add corrupted files to Scan report.

Used in conjunction with /REPORT, adds the names of corrupted files to the report file. A corrupted file is a file that a virus has damaged beyond repair, which typically occurs in 10% to 20% of all viral infections. You can use /RPTCOR with /RPTMOD and /RPTERR on the same command line.

/RPTERR

Add errors to Scan report.

Used in conjunction with /REPORT, adds system errors to the report file.

System errors include problems reading or writing to a diskette or hard disk, file system or network problems, problems creating reports, and other system-related problems. You can use /RPTERR with /RPTCOR and /RPTMOD on the same command line.

/RPTMOD

Add modified files to the Scan report.

Used in conjunction with /REPORT, adds the names of modified files to the report file. Scan identifies modified files when the validation/recovery codes do not match (using the /CF or /CV options). You can use /RPTMOD with /RPTCOR and /RPTERR on the same command line.

/RV

Remove validation/recovery from files.

Removes validation and recovery data from files validated with the /AV option, along with the SCAN.LOG file on the specified drive. To update files on a shared network drive, you must have access rights to update them. Using any of the /AV, /CV, or /RV options together in the same command line returns an error.

/SHOWLOG

Update and display the contents of SCAN.LOG.

Stores the time and date Scan is being run by updating or creating a file called SCAN.LOG in the current directory, and shows you the date and time of previous scans that have been recorded in the SCAN.LOG file using the /LOG switch. The SCAN.LOG file contains text and some special formatting. To pause when the screen fills with messages, specify the /PAUSE option.

/SUB

Scan subdirectories.

By default, when you specify a directory to scan rather than a drive, Scan will examine only the files it contains, not its subdirectories. Use /SUB to scan all subdirectories inside any directories you've specified. Do not use /SUB if you are scanning an entire drive.

/VIRLIST

Display the contents of SCAN.DAT.

Shows you the name and a brief description of the viruses that VirusScan detects. To pause when the screen fills with messages, specify the /PAUSE option. Use /VIRLIST alone or with /PAUSE on the command line.

You can save the list of virus names and descriptions to a file by redirecting the output of the command. For example, in DOS:

```
scan /virlist > filename.txt
```

CLEANING VIRUSES

Although /CLEAN removes many viruses and restores normal operation, viruses can be harmful and insidious, and no anti-virus program can undo all their damage. Usually, between 10% and 20% of all viruses corrupt the files they infect, making them unrecoverable. If the file is infected with an uncommon virus that /CLEAN can't remove, Scan notifies you and identifies the filename. Note this filename so that you know what to restore from a backup diskette or tape. If you use both the /CLEAN and the /DEL options, Scan will first attempt to repair an infected file and, if the file is damaged beyond repair, Scan will delete it. Deleted files are not recoverable except from backups.

Some viruses damage or overwrite program (.EXE) files or overlay files. Removing the virus can truncate the file or otherwise render it inoperable. Others, like the common virus Stoned, infect the master boot record (MBR). On systems partitioned with programs other than DOS (such as Disk Manager and SpeedStor), removing the virus can cause loss of the master boot record (MBR) and all data on the disk, if done improperly.

BASIC PRINCIPLES TO MINIMIZE DAMAGE

These considerations lead to the three important principles:

NOTE: Before running Scan with the /CLEAN option, back up all of your programs and data.

Of course, this works best if you back up your files regularly, so that you can restore your files from a backup made before your system was infected. But even a backup from an infected system can be useful for restoring data, because most viruses do not corrupt data. If a program no longer runs after being cleaned, replace it from the original disk or from a virus-free backup.

1. When disinfecting an infected system, it is important to start from a "sterile field," as described in Chapter 2.
2. Before running Scan with the /CLEAN option for DOS, restart your computer from a clean, write-protected diskette; before running it for OS/2, close all DOS and Win-OS/2 sessions.

Preferably, use the clean anti-virus start-up diskette you created in "Making a clean start-up diskette" in Chapter 2. And, because running any program can spread the infection:

3. Do not run any programs, including Windows, before running Scan /CLEAN.

Run Scan /CLEAN from DOS instead of Windows. Exit completely from Windows. Do not run Scan /CLEAN from within a DOS window.

IMPORTANT: If you are at all unsure about how to proceed once you've found a virus, contact McAfee technical support, or your local authorized agent, for assistance (see "Technical support" in Chapter 1).

We strongly recommend that you get experienced help in dealing with viruses if you are unfamiliar with anti-virus software and methods. This is especially true for "critical" viruses and master boot record (MBR) /boot sector infections, because improper removal of these viruses can result in the loss of all data and use of the infected disks.

RUNNING SCAN TO CLEAN UP INFECTIONS

PREPARATION

Before running Scan to clean up infections:

1. Clear the virus from system memory and prevent reinfection:
 - o With DOS or Windows, turn off your PC, then restart from a clean start-up diskette, preferably the anti-virus diskette you prepared in "Making a clean start-up diskette" in Chapter 2.
 - o With OS/2, close all DOS and Win-OS/2 sessions.
 - o With an OS/2 dual-boot system infected by a boot sector virus (like Form, or others identified by Scan), boot (start up) OS/2 first, delete the BOOT.DOS file from the \OS2 directory, and then boot DOS to create a new, virus-free DOS boot sector file.
2. Run the Scan program to locate and identify the infections.
3. Back up the files on the infected disks (be sure not to overwrite any previous backups).
4. Repeat Step 1.
5. Run the Scan program with the /CLEAN option to remove infections.

NOTE: Don't run any programs, including Windows, before running Scan /CLEAN.

If you have Windows, run Scan /CLEAN from DOS.

NOTE: When disinfecting a hard disk, always run Scan /CLEAN from a write-protected diskette to prevent infection of the Scan program. When disinfecting diskettes, make sure there is no active virus in memory before running Scan from your hard disk.

SUCCESSFUL AND UNSUCCESSFUL RESULTS

Scan /CLEAN reports the results of its attempt to remove the virus from each infected file. If a file has several infections, it will report on each.

IF VIRUSES WERE NOT REMOVED

If Scan can't remove a virus, you'll see a message like:

Virus cannot be safely removed from this file.

Make sure to take note of the file name, because you will need to restore it from backups. If you have any questions about how to proceed, contact McAfee technical support or your local authorized agent (see "Technical support" in Chapter 1).

IF VIRUSES WERE SAFELY REMOVED, RESCAN AND CHECK DISKETTES

If Scan /CLEAN has successfully removed all the viruses, turn your computer off again and restart from the system disk. Scan your hard disks again to make sure they are virus-free. If you suspect that your system was infected from a diskette, run Scan from your hard disk to examine and disinfect the diskettes you use.

These examples show different option settings.
In OS/2, remember to use OS2SCAN instead of SCAN.

scan c:

Scan all executable files on drive C.

scan f:

Scan all standard executable files on drive F, a network drive.

scan c: /adl /adn

Scan all local and network drives (including CD-ROM and PCMCIA drives but not diskettes).

scan f: g: h: /del /all

Scan all files on drives F, G, and H, and delete any infected files found.

scan c: d: e: /av /all

Scan for viruses in all files and add validation codes to executable files on drives C, D, and E.

scan m: /report c:infectn.rpt /rptcor /rpterr /append

Scan for viruses on network drive M: and create a log file of infections, corruptions, and errors in the file INFECTN.RPT on drive C. This will overwrite C:INFECTN.RPT, if it exists.

scan e:\user\jake e:\user\daisy e:\user\nick /sub

Scan all subdirectories inside the directories USER\JAKE, USER\DAISY, and USER\NICK on drive E.

scan c: d: e: /fast /cv

Quickly scan drives C, D, and E, and report any executable files that have associated validation codes and have been modified.

scan c:\command.com

Scan a single file.

scan c: d: /clean

Scan drives C and D and remove infections.

ERROR LEVELS

After Scan has finished running, it sets the ERRORLEVEL. You can use the ERRORLEVEL in batch files to take different actions based on the results of the scan. See your DOS operating system documentation for more information. Scan returns the following ERRORLEVELs:

ERRORLEVEL Description

- 0 No errors occurred and no viruses were found.
- 1 Error occurred while accessing a file (reading or writing).
- 2 A VirusScan database (*.DAT) file is corrupted.
- 3 An error occurred while accessing a disk (reading or writing).
- 4 An error occurred while accessing the file created with the /AF option; the file has been damaged.
- 5 Insufficient memory to load program or complete operation.
- 6 An internal program error occurred.
- 7 An error in accessing an international message file (MCAFEE.MSG).
- 8 A file required to run VirusScan, such as SCAN.DAT, is missing.
- 9 Incompatible or unrecognized option(s) or option argument(s) were specified in the command line.
- 10 A virus was found in memory.
- 11 An internal program error occurred.
- 12 An error occurred while attempting to remove a virus, such as no CLEAN.DAT file found, or VirusScan was unable to remove the virus.
- 13 One or more viruses was found in the master boot record, boot sector, or file(s).
- 14 The SCAN.DAT file is out of date; upgrade VirusScan data files.

Using VirusScan (Version 2.2) 52

- 15 VirusScan self-check failed. It may be infected or damaged.
- 16 An error occurred while accessing a specified drive or file.
- 17 No drive, directory or file was specified; nothing to scan.
- 18 A validated file has been modified (/CF or /CV options).
- 20 /FREQUENCY option in use
- 21-99 Reserved.
- 100+ Operating system error; Scan adds 100 to the original error number.

APPLICATION NOTE 1 UPDATING VALIDATION CODES

If you install any new software or programs on your system, including a new version of DOS, and are running Scan or VShield with the /CF (preferred) or /CV validation options, you need to install validation codes for the new files with Scan's /AF (preferred) or /AV options.

The quickest way to update the validation codes is to remove all validation codes from the hard disk and then add them back. In other words, first run Scan with the /RF or /RV option, then run it again with the /AF or /AV option.

APPLICATION NOTE 2 REFORMATTING INFECTED DISKETTES WITH DOS 5.0 AND LATER

When reformatting infected diskettes using DOS 5.0 and later versions, be sure to add the /U switch to the FORMAT command. This tells DOS to do an unconditional format of the diskette, without saving the original infected boot sector. This is necessary to erase certain infections, and will prevent reinfection by unformatting the diskette.

TECHNICAL NOTE 1

CREATING AN EXCEPTION LIST FILE FOR THE /EXCLUDE OPTION

If you set up validation codes using Scan's /AV option, subsequent scans using the /CV option will detect changes in executable files.

This can generate false alarms if the executable files are self-modifying or self-checking (most programs that do this will tell you to turn off your anti-virus software before running them; some of these files are listed below). Therefore, use the /EXCLUDE option in conjunction with /AV to identify such files and exclude them from the validation.

The exception list is an ASCII or DOS text file. If you use a word processor to create it, be sure to save the file as ASCII or DOS Text. Each line in the file contains the path and file name of one file that should not be validated. Here is an example:

```
c:\clipper\bin\clipper.exe
c:\123\123.com
c:\fox\foxprolx.exe
c:\dos\setver.exe
c:\pkware\pklite.exe
c:\pkware\pkzip.exe
c:\pkware\pkunzip.exe
c:\semware\q.exe
c:\swapvol.com
c:\wordstar\ws.exe
```

CHAPTER 4: VSHIELD REFERENCE

VirusScan's VShield(TM) is a memory-resident program that helps to prevent virus infection. It complements the Scan virus detection program as part of your computer security plan. While Scan lets you check areas on disks for viruses, the VShield program checks these areas automatically as they load into your computer's memory. This ensures that you don't "catch" any new viruses while you're working on your computer.

VShield does this by remaining in memory and:

- o Checking master boot records (MBRs), boot sectors, system files, and itself for viruses when you turn on or reset ([Ctrl]+[Alt]+[Del]) your machine.
- o Checking program files for viruses as your computer executes them.
- o Checking files for viruses as you copy them (optional).
- o Checking for viruses whenever your computer accesses a disk (optional).

Follow the instructions in Chapter 2 or Appendix A to install VShield. You can modify your AUTOEXEC.BAT file so that VShield loads into memory every time you turn on your computer.

If VShield finds a virus, you will hear three beeps and see a message like:

Found the Jerusalem Virus in memory

If that happens, don't panic. Turn to Chapter 3 to find out how to use the Scan program to get rid of the virus. If you need additional help, contact McAfee (see "Technical support" in Chapter 1).

NOTE: There is one way to infect your computer that VShield cannot prevent--only you can. Never accidentally start your computer from an unknown diskette. That's how 80% of all viruses are passed! VShield checks diskettes if you warm boot, but cannot check them when you cold boot. Always make sure your diskette drives are empty before you turn your computer on.

VShield runs under DOS, Windows, and OS/2 Virtual DOS Machine and WIN-OS/2 sessions. The program file is VSHIELD.EXE. The file called VSHLDWIN.EXE allows VShield to display messages from within Windows. The install program adds this icon to your WIN.INI file automatically, or you add it manually using the instructions in Appendix A. If you need to conserve memory on your system, you can use VShieldCRC, a version of VShield that offers fewer protection options but requires less memory. The program file is VSHLDCRC.EXE.

A companion program called CheckVShield checks whether either VShield or VShieldCRC is loaded in memory. The program file is CHKVSHLD.EXE. CheckVShield is especially useful for network administrators who want to ensure that everyone who logs on to the network is running VShield. All of these related programs are included in your VirusScan disk and described in this chapter.

DO YOU NEED TO READ THIS CHAPTER?

Many users will not need the VShield options described in this chapter. We have designed VShield so that basic operation--achieved by simply installing it in memory as described in Chapter 2--provides a high degree of protection for most users. The options here offer additional power and control for virus detection, and are most useful in vulnerable or memory-scarce environments and to network administrators and information systems staff. See "Four levels of protection" and the table "Deciding which options are for you" later in this chapter for help in deciding how to use VShield.

SYSTEM REQUIREMENTS AND PERFORMANCE

VShield is a terminate-and-stay-resident (TSR) program, which remains in memory while you run other programs. VShield tries to optimize memory usage and minimize conflicts with other TSRs. By default, VShield tries to conserve as much conventional memory as possible.

If you have only 640Kb or less memory in your system, VShield requires minimal conventional memory. By using the /SWAP option, you can reduce this to only 8Kb of conventional memory, although this will decrease VShield's speed.

If you have more than 640Kb, VShield tries to load as much of itself as possible above conventional memory: first into expanded memory (EMS), into extended memory (XMS), then into upper memory blocks (640Kb to 1024Kb, or UMB). If you have sufficient high memory available, VShield or VShieldCRC use no conventional memory.

After VShield loads, you'll see a message that describes where VShield loaded into memory and how much memory it uses. You can control how VShield loads by using the /NOUMB, /NOEMS, and /NOXMS options, as described later in this chapter.

NOTE: VShield might require slightly more memory as SCAN.DAT and NAMES.DAT grow to include more viruses.

VShield adds a small amount of time to program loads and reboots. Performance will vary, depending on your system. The /SWAP option adds more time, because VShield must reload from disk to check files. VShieldCRC adds an average of one second to each program load.

Once programs have been loaded, VShield does not degrade the performance of your system. Programs that load other files may run more slowly when you use the /FILEACCESS or /ANYACCESS options, because these options cause VShield to scan files whenever they are accessed, not just when they are executed.

You can think of VShield as providing four levels of protection. You can use VShield's options to customize it for the level of protection you need. Level II meets the protection needs of most systems.

Level I protection is appropriate for users who have very little memory available on their systems. It provides only minimal protection.

For Level I protection, first use Scan with the /AF or /AV option to add validation codes. Then, install VShieldCRC instead of VShield. VShieldCRC can inform you that a file has not been certified, a file has been modified, a file size has changed, or a file has not been added to the validation file. VShieldCRC will not prevent infection, nor will it tell you when you have a known virus. Use Scan instead to detect viruses, as described in Chapter 3. See "Using VShieldCRC" later in this chapter for instructions.

Level II protection is appropriate for most users. It will protect you from most viruses whether you have run Scan or not.

For Level II protection, install VShield according to "Running VShield" later in this chapter. When loading, VShield checks memory automatically for viruses. Once resident in memory, VShield checks master boot records (MBRs), boot sectors, and program files (when executed) for virus signatures.

Level III protection is appropriate for computers that are used by many people, as in an open-use computer lab, or onto which you frequently load files from public sources. Level III protection checks for both validation codes and virus signatures, incorporating both Level I and Level II protection.

For Level III protection, first use Scan with the /AF {filename} option, then use VShield with the /CF {filename} option. The /AF option logs recovery and validation data for program files (but not the boot sector or the master boot record) to a file you specify. The /CF option tells VShield to check against that log. See "Scan Reference" in Chapter 3 for instructions.

Level IV protection is for environments where security is extremely important and new software is seldom introduced. It combines Level III protection with access control, specifying that only programs known to be safe can be run.

For Level IV protection, run VShield with the /CERTIFY option. See the "VShield option descriptions" later in this chapter for details about /CERTIFY.

NOTE: VShield has many optional features that you might use at any protection level. See the table "VShield option summary" later in this chapter to see these options.

RUNNING VSHIELD

VShield checks programs, the master boot record (MBR), boot sector, system files, and itself for virus signatures, the pattern of code unique to each virus. If VShield finds an infection, it prevents programs from running. It also prevents warm boots ([Ctrl]+[Alt]+[Del]) from infected disks.

You can use options to control and fine-tune the scope, validation parameters, and operation of the VShield's checks. To use VShield with options, use the following syntax:

```
vshield [options]
```

[options] indicates one or more options described in the table in the next section.

NOTE: Don't enter the square braces, which indicate that what's within them is optional.

Because systems and environments differ, VShield gives you a choice of options. Consider the mixture of safety, performance, and maintenance that meets your needs, then choose the combination of options that works best.

When you run VShield for the first time, VShield uses the virus information contained in SCAN.DAT and NAMES.DAT to create a new file, VSHIELD.DAT, in the program directory. The VSHIELD.DAT file contains virus information in a format that is optimized for VShield operation. Thereafter, when you install an updated version of SCAN.DAT, VShield updates VSHIELD.DAT automatically with any new virus information it finds in SCAN.DAT.

DOS

You can add VShield to your AUTOEXEC.BAT file so it is activated every time you turn on your computer.

You can put VShield at the end of AUTOEXEC.BAT. In most cases this is OK. However, using a text editor,

1. Check the placement of the VShield command line in the AUTOEXEC.BAT file.
 - o VShield must be run before any menu programs, such as Windows, MS-DOS's DOSSHELL or Norton Commander, or it will not be loaded.
 - o If AUTOEXEC.BAT loads any network drivers, keyboard drivers, disk caching programs, drive compression programs, or custom disk drivers, VShield must be run both before and after them. These kinds of programs disable VShield. The second time VShield is loaded, use only the /RECONNECT option, as described later in this chapter.
2. If necessary, move the line that loads VShield.
3. Add the VShield options of your choice to the command line.

WINDOWS

When you install VShield, you can add the VShield command line to your AUTOEXEC.BAT file. If you used the install program or the instructions in Appendix A, your WIN.INI file was modified to include VSHLDWIN.EXE, which allows VShield to display messages under Windows.

However, you may need to change your Windows configuration for VShield to run properly.

To do so, follow these steps. If you need help with this procedure, see your Windows documentation, or you can contact McAfee (see "Technical support" in Chapter 1).

1. Follow the instructions for DOS users in the previous section.
2. Start Windows.
3. In the Control Panel, configure Windows to run in 386 enhanced mode.
4. Load Windows. You will see the VShield icon on your desktop.

If VShield finds or suspects a virus, you'll see a warning message. Choose OK to close the message dialog.

Double-clicking the VShield icon only displays a message confirming whether VShield is loaded.

OS/2

Because OS/2 is a protected environment, you need VShield only during Virtual DOS Machine (VDM) and WIN-OS2 sessions. When you install it, you can add VShield to AUTOEXEC.BAT so it is activated every time you start a VDM or WIN-OS/2 session.

If your start-up batch file is not AUTOEXEC.BAT, edit your start-up batch file to include VShield. For example:

```
[C:\] vshield /fileaccess
```

NOTE: See "/FILEACCESS," an option we recommend using with OS/2, later in this chapter.

SPECIAL INSTRUCTIONS FOR NETWORK ADMINISTRATORS

You have many options for setting up VShield on a network. The table "Deciding which options are for you" later in this chapter lists options that apply in network environments. If you need assistance in choosing the best configuration for your network, contact McAfee (see "Technical support" in Chapter 1).

If you run VShield from a network drive, flag VSHIELD.EXE as EXECUTE ONLY, READ ONLY, and SHAREABLE.

If you run VShield from clients' local drives (optimal):

- o Edit all clients' AUTOEXEC.BAT files to load VShield, with the options that are appropriate for your environment, before any other drivers are loaded.
- o Add VShield with the /RECONNECT option to the AUTOEXEC.BAT or the network login script, after the network drivers are loaded. See /RECONNECT, later in this chapter, for more information.
- o Run CheckVShield from the login script. CheckVShield returns a

DOS ERRORLEVEL that you can use in batch files to check and update VShield. For an example of using CheckVShield, see "Technical note 2: Sample NetWare login script and .BAT file" later in this chapter.

VSHIELD OPTION SUMMARY

DOS-OS/2 option Description

/? or /HELP

Display a list of valid VShield command line options.

/ANYACCESS

Scan the boot sector whenever a diskette is accessed (read and write); scan executables; scan any newly created files.

/BOOTACCESS

Scan the boot sector for viruses whenever a diskette is accessed (including read and write).

/CERTIFY

Prevent files without validation codes from running.

/CF {filename}

Check for viruses using recovery and validation data stored by Scan /AF in the specified {filename}.

/CONTACT {message}

Display specified message when a virus is found.

/CONTACTFILE {filename}

Display message stored in {filename} when a virus is found.

/CV

Check validation codes added to files by Scan.

/EXCLUDE {filename}

Don't check files listed in {filename} for validation codes (used with /CV).

/FILEACCESS

Scan executable files when they are accessed on a diskette, but don't check the boot sector.

/IGNORE {drive(s)}

Don't check programs loaded from the specified drive(s).

/LOCK

Halt the system when a file that is infected loads and attempts to execute.

/NOEMS

Prevent VShield from loading into expanded memory (EMS).

/NOMEM

Don't check memory for viruses.

/NOREMOVE

Prevent VShield from being removed from memory with the /REMOVE switch.

/NOUMB

Prevent VShield from loading into upper memory blocks (UMB).

/NOWARMBOOT

Don't check the diskette boot sector for viruses during warm boot ([Ctrl]+[Alt]+[Del]).

/NOXMS

Prevent VShield from using extended memory (XMS) when it loads.

/ONLY {drive(s)}

Check programs loaded only from the specified drive(s).

/POLY

Check for polymorphic viruses.

/RECONNECT

Restore VShield after certain drivers or TSRs have disabled it.

/REMOVE

Unload VShield from memory.

/SAVE

Save the command line options to the VSHIELD.INI file.

/SWAP [pathname]

Load VShield kernel (8Kb) only; swap the rest to pathname.

VSHIELD OPTION DESCRIPTIONS

/? or /HELP

Use this option to display a brief description of valid VShield command line options.

/ANYACCESS

Checks the diskette boot sector and all files for viruses whenever a diskette is accessed by a read or write operation, such as a DIR or COPY command, and when a program on the diskette is opened, read, updated, or executed.

/ANYACCESS prevents execution if a program file is infected. It also checks any new files created, such as with a copy command, regardless of the file's extension.

This is the highest level of protection against viruses that infect boot sectors. Using /ANYACCESS with either /BOOTACCESS or /FILEACCESS in the same command line returns an error message.

NOTE: The /ANYACCESS switch is not recommended for use with DOS and WIN-OS/2 sessions under OS/2 due to certain low-level operating system incompatibilities between OS/2 and DOS. Use the /FILEACCESS switch instead.

/BOOTACCESS

Checks the boot sector of a diskette for viruses whenever a diskette is accessed by a read or write operation, such as the DIR or copy commands. By default, VShield checks programs when they execute, but does not check the boot sector of the diskette for viruses. Using /BOOTACCESS with /ANYACCESS in the same command line returns an error message.

NOTE: This option does not work from within Windows File Manager. For virus-checking within Windows, use the /FILEACCESS or /ANYACCESS switch instead.

/CERTIFY

Prevents programs from running if they do not have Scan validation codes. Use it in high-security environments to prevent clients from running programs that have not been scanned. To use /CERTIFY, first run Scan with the /AF or /AV option, as described in Chapter 3. Then, use VShield with the /CERTIFY option and either the /CF or /CV option (either is required), such as:

```
vshield /certify /cf c:\mcafee\recvalch.sav
```

Some programs, such as Lotus 1-2-3, contain self-modifying code and do not work correctly with validation codes attached. You may create an exception list of files to exclude from validation. For instructions, refer to "Technical note 1: Creating an exception list for the /EXCLUDE option" later in this chapter.

/CF {filename}

Checks validation data stored by Scan's /AF {filename} option, where {filename} is the name of the validation data file created by Scan. If a file or system area has changed, VShield reports that a viral infection may have occurred.

In this example:

```
vshield /cf c:\mcafee\valcodes.dat /noems
```

VShield looks in the VALCODES.DAT file for validation data. For instructions on using Scan /AF to add validation codes, see "Scan option descriptions" in Chapter 3, and "Detecting new and unknown viruses" in Chapter 5.

`/CONTACT {message}`

Displays a custom message when a virus is found. This message is displayed in addition to all other VShield messages. Use `/CONTACT` to let network users know what to do if VShield finds a virus. The message can be up to 50 characters long, and can contain any character except a backslash " \ ". Place messages starting with a hyphen " - " or slash " / " in quotation marks.

If your message is longer than 50 characters or you want to store the message text in a file, use `/CONTACTFILE` instead. Using `/CONTACT` and `/CONTACTFILE` in the same command line returns an error message.

`/CONTACTFILE {filename}`

An alternative to the `/CONTACT` option, `/CONTACTFILE` identifies a file that contains the message string to display when a virus is found. This option is especially useful in network environments, because you can easily maintain the message text in a central file rather than changing the command line in the `AUTOEXEC.BAT` file on each workstation.

If your message is 50 characters or fewer, you can use `/CONTACT` instead. Using `/CONTACT` and `/CONTACTFILE` in the same command line returns an error message.

`/CV`

Checks validation codes added by Scan with the `/AV` option. If a file has changed, VShield reports that the file has been modified and a viral infection may have occurred. You can specify the `/EXCLUDE` option to exclude a list of files from validation checking. For instructions on using Scan to add validation codes, see "Scan option descriptions" in Chapter 3, and "Detecting new and unknown viruses" in Chapter 5.

`/EXCLUDE {filename}`

Excludes files listed in {filename} from validation when using /CV. For more information on this, see "Technical note 1: Creating an exception list for the /EXCLUDE option" later in this chapter.

`/FILEACCESS`

Checks standard executable files whenever the file is accessed or executed, and prevents execution of infected programs. Checks all files when accessed by a read or write operation. Using /ANYACCESS in the same command line with /FILEACCESS returns an error message.

NOTE: We recommend always using /FILEACCESS with OS/2. 1 For VShieldCRC, /FILEACCESS checks files only if they have been validated with the /AF or /AV options.

`/IGNORE {drives}`

Omits checking program loads from the specified drives, as shown in the following example:

```
vshield /ignore t: y: w:
```

Use /IGNORE or /ONLY to speed up VShield by excluding secure, virus-free network drives from virus checking. You can specify up to 26 drives. See also /ONLY, described later in this section. Using /IGNORE and /ONLY in the same command line returns an error message.

`/LOCK`

Halts the system to stop further infection if VShield finds a virus. /LOCK is appropriate in highly vulnerable network environments, such as open-use computer labs. If you use /LOCK, use /CONTACT or /CONTACTFILE to tell users what to do or whom to contact if a virus is found and the system locks up.

/NOEMS

Prevents VShield from using expanded memory (LIM EMS 3.2) when it loads. This ensures that EMS is available exclusively to other programs.

/NOMEM

Skips the memory check for viruses when VShield loads. Using /NOMEM improves performance slightly, but use it only if you are absolutely sure that your system is virus-free.

/NOREMOVE

Prevents VShield from being removed from memory with the /REMOVE option in a subsequent VShield command. When you load VShield with the /NOREMOVE option, subsequent loads with the /REMOVE option will have no effect. Your network will be more secure if users cannot remove VShield, but this option may prevent users from solving memory limitations or conflicts.

/NOUMB

Prevents VShield from loading into the upper memory block (UMB, 640Kb to 1024Kb). This ensures that the UMB is available exclusively to other programs.

/NOWARMBOOT

Omits checking the diskette boot sector during a warm boot ([Ctrl]+[Alt]+[Del]).

/NOXMS

Prevents VShield from using extended memory when it loads. This ensures that XMS is available exclusively to other programs.

`/ONLY {drive(s)}`

Checks program loads only from the specified drive(s), ignoring all other drives, as shown in the following example:

```
vshield /only c: f: k:
```

Use `/IGNORE` or `/ONLY` to speed up VShield by excluding secure, virus-free network drives from virus checking. You can specify up to 26 drives. See also `/IGNORE`, earlier in this chapter. Using `/ONLY` and `/IGNORE` in the same command line returns an error message.

`/POLY`

Checks for polymorphic viruses, which are viruses that attempt to evade detection by changing their internal structure or encryption techniques. Otherwise, VShield does not check for polymorphic viruses. Using `/POLY` on the same command line as `/FILEACCESS`, `/ANYACCESS`, `/BOOTACCESS`, or `/SWAP` returns an error.

`/RECONNECT`

Restores VShield's links into DOS after another program has disabled it, such as a network driver, keyboard driver, custom disk driver, drive compression program, or disk caching program. These types of programs replace the normal DOS system interrupts so that VShield no longer recognizes program loads. After the lines in your `AUTOEXEC.BAT` file (or network login script) that load these programs, add this command line to restore VShield:

```
vshield /reconnect
```

`/REMOVE`

Unloads VShield from memory. You may want to do this temporarily if you are running out of memory for programs. For best results, try using VShield with the `/SWAP` option first. Use `/REMOVE` only as a last resort.

NOTE: /REMOVE will not work if other memory-resident programs were loaded after VShield, or if VShield was loaded previously with the /NOREMOVE option.

/SAVE

Stores the VShield options you specify as the defaults in VSHIELD.INI. In the following example, /SAVE saves the /CONTACTFILE N:\MSGFILE as the default setting:

```
vshield /contactfile n:\msgfile /save
```

To remove custom options and return to VShield's original defaults, use the /SAVE option alone:

```
vshield /save
```

/SWAP [pathname]

Installs a small (8Kb) kernel of VShield in memory that loads the rest of VShield from disk on demand. Specify a pathname only if you want VShield to swap to a path other than the directory where VShield resides.

Use /SWAP only if you have very little memory available, but require a high assurance of safety. /SWAP will slow down your system and may cause conflicts with programs that fail to allocate memory properly. If you don't have enough memory to load VShield without swapping, consider using VShieldCRC instead. We do not recommend storing the swap file on a network path because, if the workstation disconnects from the network, the workstation will lock.

DECIDING WHICH OPTIONS ARE FOR YOU

Because systems and environments differ, VShield gives you a choice of options. Consider the mixture of safety, performance, and maintenance that meets your needs, then choose the combination of options that works best.

REQUIREMENT	OPTION	COMMENTS
More complete protection, any environment	³ /ANYACCESS	³ Highest protection against infected diskettes; checks for viruses whenever a diskette or files are accessed.
	³ /FILEACCESS	³ Next highest protection against infected diskettes; checks for viruses whenever a standard file is accessed.
	³ /BOOTACCESS	³ Of the three, lowest protection against infected diskettes; checks for viruses in boot sector when a diskette is accessed.
	³ /POLY	³ Used to check for polymorphic viruses.
More complete protection, stable software environment	³ /CERTIFY	³ Use with /CF {filename} or /CV and an exception list.
	³ /CF	³ Use /CF or /CV. Of the two, /CF is recommended.
	³ /CV	³ Use /CF or /CV.
Network or multi-user environments	³ /CONTACT	³ Use this (or /CONTACTFILE) to tell users what to do when a virus is found.
	³ /CONTACTFILE	³ Use this (or /CONTACT) to tell users what to do when a virus is found.
	³ /IGNORE	³ Use this (or /ONLY) to skip virus-free drives.
	³ /LOCK	³ Use with /CONTACT or /CONTACTFILE {filename}.

[illegible]

For network environments (continued)

³ /NOREMOVE ³ Prevents VShield from being removed from memory.

³ /ONLY ³ Use this (or IGNORE) to check only vulnerable drives.

³ /RECONNECT ³ Required if network drivers are loaded after VShield.

Faster performance any environment ³ /NOMEM ³ Only use on a virus-free computer.

³ /NOWARMBOOT ³ Omits checking the boot
³ ³ sector after a warm boot.

Manage memory, ³ /NOEMS ³ Use when other programs need
any environment ³ ³ exclusive use of EMS memory.
~~~~~  
<sup>3</sup> /NOUMB <sup>3</sup> Use when other programs need  
<sup>3</sup> <sup>3</sup> exclusive use of UMB memory.  
~~~~~  
³ /NOXMS ³ Use when other programs need
³ ³ exclusive use of XMS memory.
~~~~~  
<sup>3</sup> /NOREMOVE <sup>3</sup> Use to ensure that VShield  
<sup>3</sup> <sup>3</sup> remains in memory.  
~~~~~  
³ /REMOVE ³ May temporarily solve memory
³ ³ conflicts.
~~~~~  
<sup>3</sup> /SWAP <sup>3</sup> Use in environments with very  
<sup>3</sup> <sup>3</sup> limited memory.

|||||



## EXAMPLES

The following examples show different option settings:

```
vshield
```

Activates VShield (Level II protection).

```
vshield /cv
```

Activates VShield (Level III protection), if you have previously run SCAN /AV.

```
vshield /certify /cf c:\valcodes.dat
```

Activates VShield (Level IV protection) and checks a recovery and validation data file created when running Scan with the /AF option.

```
vshield /swap
```

Activates VShield kernel in memory and swaps from the directory in which VShield resides.

```
vshield /cv /exclude c:\exception.lst /contact  
"Call the PC Help Desk!"
```

Activates VShield (Level III protection), ignores checking files in the EXCEPTION.LST files, and displays a message if a virus is found.

```
vshield /reconnect
```

Re-enables VShield after it has been disconnected by network device drivers.

## ERROR LEVELS

When VShield loads, it sets the DOS ERRORLEVEL. You can use the returned ERRORLEVEL in AUTOEXEC.BAT or other batch files to take different actions based on whether VShield has loaded in memory. See your DOS manual for more information.

VShield returns these ERRORLEVELs:

### ERRORLEVEL/Description

- 0 VShield successfully loaded in memory with all options operational.
- 9 VShield not loaded correctly. Abnormal termination (program error).

VShield alerts you to problems by beeping once for system errors, twice for validation errors (/CF or /CF checking), or three times if a virus is found.

## USING VSHIELDCRC

For Level I protection on systems with limited memory, use VShieldCRC instead of VShield. VShieldCRC is a separate program that consumes little system overhead, but is not recommended for normal use because it provides only minimal protection. VShieldCRC can inform you that you have been infected with a virus, but it does not check for virus signatures nor does it prevent infection.

To use VShieldCRC, first use Scan with the /AF or /AV option. VShieldCRC checks the validation codes added by Scan. It also checks the master boot record (MBR) and boot sector validation codes, if present. See Chapter 3 for instructions on using Scan.

To load VShieldCRC with options, use the following syntax:

```
vshldcrc [options]
```

[options] include the options listed in the table "VShieldCRC option summary" later in this chapter. For more information on all options except /LOGFILE, see "VShield option descriptions" earlier in this chapter.

## EXAMPLES

```
vshldcrc
```

Activates VShieldCRC (Level I protection).

```
vshldcrc /cf valcodes.dat
```

Activates VShieldCRC and checks validation data stored in VALCODES.DAT, a file that was created using Scan with the /AF option.

## VSHIELDCRC OPTION SUMMARY

## /? or /HELP

Display a list of valid VShieldCRC command line options.

## /CERTIFY

Prevent files without validation codes from running.

## /CF {filename}

Check for viruses using recovery and validation data stored by Scan /AF in the specified {filename}.

## /CONTACT {message}

Display specified message when a virus is found.

## /CONTACTFILE {filename}

Display message stored in specified {filename} when a virus is found.

## /CV

Check validation codes added to files by Scan.

## /EXCLUDE {filename}

Don't check files listed in {filename} for validation codes (used with /CV).

## /FILEACCESS

Scan only validated executable files when accessed, but don't check boot sector. Prevent infected programs from running.

## /IGNORE {drive(s)}

Don't check programs loaded from specified drive(s).

## /LOCK

Halt the system when a file that is not certified attempts to load and execute.

## /LOGFILE {filename}

Write error information to {filename}.

## /NOREMOVE

Prevent VShieldCRC from being removed from memory with a subsequent VShieldCRC command using /REMOVE.

## /NOUMB

Prevent VShieldCRC from using upper memory blocks (UMB) when it loads.

## /ONLY {drive(s)}

Check programs loaded only from the specified drive(s).

## /REMOVE

Unload VShieldCRC from memory.

## USING CHECKVSHIELD

CheckVShield allows network administrators to make sure that workstations are running VShield or VShieldCRC before users can log onto a network. See "Technical note 2: Sample NetWare login script and .BAT file" later in this chapter for a sample Novell NetWare login script using CheckVShield.

To load CheckVShield with options, use the following syntax:

```
chkvshld [option(s)]
```

[option(s)] include:

**/?** and **/HELP**

Display a list of valid CheckVShield command line options.

**/DEBUG**

Displays the version of VShield or VShieldCRC resident in memory and the DOS ERRORLEVEL on the screen.

**/QUIET**

Suppresses CheckVShield messages (quiet mode) so users don't see the messages.

**/V "xxxxx"**

Tells CheckVShield to look for a specific version (2.00 or higher) of VShield or VShieldCRC in memory. For example, **/v "2.00"** for VShield 2.00.

## EXAMPLE

```
chkvshld /quiet
```

Checks for VShield or VShieldCRC in memory and suppresses messages.

## ERROR LEVELS

When CheckVShield runs, it sets the DOS ERRORLEVEL. Use the ERRORLEVEL in batch files to take different actions based on the results of CheckVShield's check. The ERRORLEVELs returned by CheckVShield are:

### ERRORLEVEL/Description

- 0 VShield or VShieldCRC is resident or, if /V is used, the version specified is resident in memory.
- 1 VShield or VShieldCRC is resident but does not match the version specified in the /V option.
- 2 VShield or VShieldCRC is not resident in memory.
- 3 Abnormal termination (program error).

TECHNICAL NOTE 1:  
CREATING AN EXCEPTION LIST FOR THE /EXCLUDE OPTION

VShield /CERTIFY permits a file to load only if:

- o It has been validated by Scan, or
- o It appears in the exception list file specified with the /EXCLUDE option, used in conjunction with /CV.

If you do not validate any files and do not use an exception list, /CERTIFY will disable all programs other than DOS internal commands.

The exception list file is an ASCII or DOS text file containing up to 1,024 characters. If you use a word processor to create it, be sure to save the file as ASCII or DOS Text. Each line in the file contains the path and filename of one file that should not be validated. Here is an example:

```
c:\clipper\bin\clipper.exe
c:\123\123.com
c:\fox\foxprolx.exe
c:\dos\setver.exe
c:\pkware\pklite.exe
c:\pkware\pkzip.exe
c:\pkware\pkunzip.exe
c:\semware\q.exe
c:\swapvol.com
c:\norton\ncache.exe
c:\wordstar\ws.exe
```

## TECHNICAL NOTE 2

### SAMPLE NETWARE LOGIN SCRIPT AND .BAT FILE

Here is a sample system login script for use by Novell NetWare system administrators. The login script gets the ERRORLEVEL from CheckVShield and displays messages on the user's screen. If VShield is not loaded correctly, there is an internal error with CheckVShield, either VShield or VShieldCRC is not installed, or an older version of VShield is present, the script exits the user to a NOLOGIN.BAT file that logs him or her out.

```
#REM REPLACE "XXX" WITH CURRENT VERSION NUMBER
CHKVSHLD /V "VXXX"
IF ERROR_LEVEL = "3" THEN
  FIRE PHASERS 5 TIMES
  WRITE "A CHKVSHLD internal error has occurred."
  WRITE "Please contact the Help Desk."
  #COMMAND /C NOLOGIN.BAT
  EXIT
ELSE
IF ERROR_LEVEL = "2" THEN
  FIRE PHASERS 5 TIMES
  WRITE "VShield has not been installed on your PC."
  WRITE "Access Denied. Please contact the Help Desk."
  #COMMAND /C NOLOGIN.BAT
  EXIT
ELSE
IF ERROR_LEVEL = "1" THEN
  FIRE PHASERS 5 TIMES
  WRITE "An old version of VShield has been installed."
  WRITE "Access to the network has been denied. Please"
  WRITE "contact the Help Desk to have a new version"
  WRITE "installed."
  #COMMAND /C NOLOGIN.BAT
  EXIT
END
END
END
```

You can create more complex login scripts to send a message to the supervisor if an error has occurred, update the user's VSHIELD.EXE as he or she logs in to the network, and so forth.

Here is a sample of the NOLOGIN.BAT file called by the login script.

```
ECHO OFF
REM Log the user off of the network
LOGOUT
```

## CHAPTER 5: TIPS & TROUBLESHOOTING

The other chapters in this manual are meant to tell you clearly and concisely how to use the VirusScan software. Still, you may have questions or encounter confusing situations. This chapter contains two kinds of advice:

- o Tips for getting the most out of VirusScan.
- o Common problems and how to solve or avoid them.

If this information doesn't help resolve your question or problem, contact McAfee (see "Technical support" in Chapter 1).

### TIPS

#### DETECTING NEW AND UNKNOWN VIRUSES

There are two ways of dealing with new and unknown viruses that may infect your system:

- o Update VirusScan regularly.
- o Store and check validation and recovery information about your files.

#### UPDATE VIRUSSCAN REGULARLY

Most likely, McAfee will see new viruses long before you do. We update the VirusScan programs often--usually monthly, but more often if many new viruses have appeared. Each new version may detect and eradicate as many as 60 to 100 new viruses or more, and may fix bugs that have been reported.

Updating VirusScan regularly is probably all you need to do to protect against new viruses. See the instructions for obtaining new versions in "Updating VirusScan regularly" in Chapter 2.

## USE THE VALIDATION AND RECOVERY OPTIONS

If your environment is highly vulnerable to viruses, or you require unusual security against them, you can use VirusScan's validation and recovery options. Scan checks for new or unknown viruses by comparing files against previously recorded validation data. If a file has been modified, it no longer matches the validation data, and Scan reports that the file may have become infected. Scan has two levels of validation, which are stored in two separate ways:

- o It can store the enhanced code in a separate recovery file, which can be stored off-line (for example, on a diskette) for recovery purposes (/AF, /CF, and /RF switches). This is the preferred method because it stores the data for files (but not the boot sector or the master boot record) in a separate recovery file.
- o It can append a simple 98-byte validation code to .COM and .EXE files (/AV, /CV, and /RV switches). This method applies to the files you specified only. It does not store data for the boot sector and master boot record (MBR).

Once the validation codes are stored, both Scan and VShield can use the /CV and /CF options to detect changes to the files. More importantly, if you have stored the recovery information with /AF, Scan can use it to restore infected files.

All of these options require continuing effort to store and maintain the codes. For example, if you install new programs or upgrade old ones, you should use the /RV or /RF options to remove all codes, then /AV or /AF to restore them.

If you want to use one of these methods, which should you use? We recommend the "F" options--/AF, /CF, and /RF--over the "V" options. /AF stores the validation and recovery information in a separate file, instead of modifying the program files themselves. This has three advantages:

- o You can store the recovery file off-line (on your clean anti-viral startup diskette, for example, or on a network drive or tape drive) and access it on demand to check for, and recover from, infection by unknown viruses. Use the procedure below to create a recovery diskette.
- o This method keeps self-checking files (usually copy-protected programs) from reporting that they have been tampered with.
- o If you use this method, you don't need an exception list. However, it's important that you run Scan with the /RF option on individual self-modifying files, such as Lotus 1-2-3, to remove the validation codes for those programs from the validation file.

The "V" options are primarily useful for companies that distribute software to their customers or employees, and want to incorporate an additional level of virus protection.

**Creating a recovery diskette** To store the recovery file on the clean startup diskette you created in "Making a clean start-up diskette" in Chapter 2, temporarily remove write-protection from the diskette and insert it in drive A. Run Scan on your hard disks with the /AF option. For example:

```
scan /adl /af a:\scanrc.crc
```

scans the local hard disk drives for known viruses and creates SCANCRC.CRC, a file containing recovery data and validation codes, on the diskette. After Scan finishes, write-protect the diskette.

To check for virus infection, turn your computer off, insert the recovery diskette in drive A, and turn the power back on. The PC will now start from the diskette. At the DOS prompt, type:

```
scan /adl /cf a:\scanrc.crc
```

to compare the local hard disk drives against the recovery data stored on the diskette in the SCANCRC.CRC file.

If you detect an unknown virus, to disinfect your system, turn your PC off, insert the recovery diskette, and turn the power back on. The PC will start from the floppy disk. At the DOS prompt, type:

```
scan /adl /cf a:\scanrc.crc /clean
```

to restore local hard disk drives with the recovery data stored in SCANCRC.CRC on the diskette.

If you install new software, or upgrade your DOS version, remember to update your recovery file. See "Application note 1: Updating validation codes" in Chapter 3.

## INTERACTING WITH YOUR NETWORK

Many personal computers are interconnected through a local area network (LAN). VirusScan is highly compatible with most networks. Here are some ways of using the VirusScan software with your network:

- o Run Scan on network drives Run from a workstation (PC) on the network, Scan checks network drives for viruses just as it does local drives. For convenience, the /ADN option scans all network drives to which the workstation is connected.
- o Use VShield and CheckVShield By activating VShield as part of every workstation's AUTOEXEC.BAT file, you can prevent the workstations from introducing viruses into the network. Network administrators can ensure that VShield is active on each workstation by running CheckVShield as part of the network login script, before actual login.
- o Use NetShield provides continuous virus protection on a NetWare server. NetWare network administrators can use it to check for both known and unknown viruses and to monitor all network activities. On other kinds of networks, you can use Scan to check network servers.
- o Develop a network security program, as described in the next tip.

## DEVELOP A SECURITY PROGRAM

VirusScan has been shown to be an effective virus-preventive measure when used in a conscientiously applied program of network security and regular professional care.

VirusScan is one important element of a comprehensive computing security program that includes a variety of safety measures, such as regular backups, meaningful password protection, user training, and awareness. Even with VirusScan, some viruses--not to mention theft or fire--can render a disk unrecoverable without a recent backup. Although outlining such a security program is beyond the scope of this manual, see "Other sources of information" in Chapter 1 for suggestions.

If you are a network administrator, we urge you to implement a security program to safeguard your organization's data and productivity. If you are a network user, please support and comply with such a program.

## TROUBLESHOOTING

### GENERAL ABNORMALITIES

#### Using VirusScan with other anti-virus software

When you run more than one anti-virus program, you risk strange results and false alarms. For example, some anti-virus programs store their "virus signature strings" unprotected in memory. Running VirusScan may "detect" them falsely as a virus.

### TSR CONFLICTS

Some "terminate-and-stay-resident" (TSR) software may conflict with VirusScan programs, especially VShield (which is itself a TSR). To check whether this is the problem, "comment out" the other TSR files in your AUTOEXEC.BAT file and restart your system. If the errors disappear, the TSR conflict caused them.

### SLOW DISK ACCESS, PROGRAM LOCKS

Running VShield will slow your system slightly as described in Chapter 4, especially if you use either the /ANYACCESS or /SWAP options. If you experience very slow disk access, or if programs lock or freeze while using Windows 3.1, you may be using a disk cache program that interferes with program operation, or you may need to increase the number of BUFFERS in your CONFIG.SYS file.

## TROUBLESHOOTING SCAN

### FALSE ALARMS

Scan may incorrectly report viruses in the boot sector or master boot record (MBR) of certain copy-protected diskettes. Contact technical support if you're unsure (see "Technical support" in Chapter 1).

## TROUBLESHOOTING VSHIELD

### PROGRAM LOCKS WITH /SWAP

When VShield is running with the /SWAP option, certain programs may lock up the computer. These programs may use memory without allocating it first, including older versions Lotus 1-2-3, pfs:Write and Professional Write, OfficeWrite, and DisplayWrite4. To correct, restart your computer and run VShield without the /SWAP option.

### UNABLE TO REMOVE VSHIELD

If the /REMOVE option doesn't successfully remove VShield from memory, you have probably loaded other terminate-and-stay-resident (TSR) programs after VShield. VShield can't be removed until the other TSRs are removed. If you need to unload VShield often, load it last.

## APPENDIX A: RETRIEVING MCAFEE PROGRAMS WITH COMMUNICATIONS SOFTWARE

You can use your communications software to dial up the McAfee bulletin board system (BBS) and retrieve (download) McAfee software by following these steps.

### DIAL UP

- o The McAfee BBS phone number is (408) 988-4004.
- o The BBS operates at up to 28,800 bps (baud).  
Set your communications parameters to 8 data bits, 1 stop bit, no parity, and your terminal emulation to ANSI or TTY.
- o The BBS is Bell- and ITU- (formerly CCITT) compatible.

### LOG ON

After receiving the CONNECT message from your modem, enter your name, geographic location, and password.

To retrieve VirusScan programs, type

guest (for first name)  
user (for last name)

Or, if you want personal answers or feedback, create your own account by entering your first and last name and a password. Passwords should be 3-8 characters long and are case-sensitive.

### THE MAIN MENU

Here are some of the important functions on the main menu:

- F File transfer area (download McAfee updates)
- M Message area (read and write messages in all sections and e-mail)
- G Goodbye (hang up and leave the BBS)

## DOWNLOADING MCAFEE PROGRAMS

1. Select F from the Main Menu to go to the File transfer area. This is the area from which you can download McAfee programs.
2. Select 1 for the McAfee Antivirus Files. A sorted directory listing of files available for download will be displayed.
3. Type D for download, then type in the filename as found in the directory.
4. The BBS will prompt you to select a protocol. If possible, use an error-correcting protocol such as ZMODEM, YMODEM or XMODEM.
5. You'll see the message Awaiting start signal. Tell your software to receive files. With PROCOMM for DOS or TELIX, press the [Page Down] key, with BITCOM, press the [F2] key. For other communications programs, check your manual.
6. Your software will prompt you to select a protocol and file name to receive the file. Select the same protocol and name.

## UNPACKING YOUR FILES

Once you have downloaded software, you need to unpack the downloaded files before you can use them for virus detection.

## ABOUT COMPRESSED FILES

Compressed files take less space on the disk and require less time to transfer electronically. McAfee uses a shareware program, PKZIP (produced by PKWare of Brown Deer, WI, and not a McAfee product), to compress updated software. PKUNZIP (also from PKWare) is the utility used to decompress file previously compressed with PKZIP. Once a file is decompressed, it can be used normally.

Note: Since McAfee's products are zipped using PKZIP version 2.04g, you must also have version 2.04g. This is available on our BBS in area one (1) as PKZ204.EXE. This is a self-extracting zip file. Simply download the file and, at the DOS prompt, run it by typing PKZ204 and pressing ENTER. It self-extracts several files, including PKUNZIP.EXE.

#### HOW TO UNPACK

Once you have downloaded the McAfee software, quit to DOS, and change to the directory where you downloaded the software to. (If you used QMODEM, TELIX, PROCOMM or CROSSTALK it will be in that directory, or a subdirectory of it usually named DOWNLOAD). If you used Windows Terminal, this may be the Windows directory). Then, enter the following command:

```
PKUNZIP zipfile destination
```

where

- o `zipfile` is the name of the file you downloaded.
- o `destination` is the target directory to store the McAfee software.

For example,

```
PKUNZIP SCN216.ZIP C:\MCAFEE
```

unpacks the SCN216.ZIP file and stores it in the C:\MCAFEE directory.

- o If you are updating an older version of McAfee software, you may get a message similar to the following example while decompressing:

```
PKUNZIP: (W18) Warning! AGENTS.TXT  
already exists. Overwrite (y/n/a/r)?
```

If this happens, type A for ALL and press ENTER. PKUNZIP will replace all files with the updated versions contained in the zip file.

- o The last lines after all of the files are decompressed should be similar to:

Authentic files Verified! #FZW807  
McAFEE Inc.

If you do not see this message, you might have files that have been tampered with. Be sure that you obtain them from a valid source before using them.

- o If you run VSHIELD after updating, you might get the following message:

WARNING: VSHIELD data file has been damaged.

This occurs because VSHIELD continually accesses its data file and it has detected a change. Simply restart your machine. VSHIELD will load with the new version.

## IF YOU ARE INSTALLING SOFTWARE FOR WINDOWS

If you downloaded WScan or VShield for the first time, you need to perform several additional configuration steps to complete your installation. You can skip this section if you are not running VirusScan under Windows.

### INSTALLING WSCAN

For WScan, you need to add the icon to your McAfee program group.

1. Create a McAfee program group, if one does not already exist. In the Windows Program Manager, choose File | New. In the New Program Object dialog box, select Program Group and choose OK. Enter a description (such as "McAfee") and a group filename (such as MCAFEE.GRP).

If a McAfee program group already exists, select it.

2. Create the WScan icon. In the Windows Program Manager, choose File | New. In the New Program Object dialog box, select Program Item and choose OK. Click Browse, locate the WSCAN.EXE file in the McAfee software directory, then double-click it. Choose OK to add the icon.

3. Double-click the icon to verify that it works.

Note: You do not need to make any changes to the WIN.INI file because WScan stores its startup settings in WSCAN.INI.

#### INSTALLING VSHIELD UNDER WINDOWS

The VSHLDWIN.EXE program allows VShield to display warning messages in a Windows message dialog box. For VShield, you need to add the VShield icon to the McAfee program group and modify WIN.INI so that VSHLDWIN.EXE loads automatically when you start Windows.

1. Within Windows, use the File Manager to locate the VSHINST.EXE program in your McAfee software directory and double-click it. The program creates a McAfee program group (if one does not already exist) and adds the icon for VSHLDWIN.EXE.
2. Edit your WIN.INI file using any ASCII text editor. Add the following line to the [windows] section of your WIN.INI file:

```
run=VSHLDWIN.EXE
```

Restart Windows for your changes to take effect.

#### UPDATING YOUR AUTOEXEC.BAT FILE

Finally, you might need to edit the AUTOEXEC.BAT file to:

- o Automatically load VShield. For more information, see "Running Vshield" in Chapter 5.
- o Add the McAfee software directory to your PATH statement.

Restart your system for the changes to take effect.

## APPENDIX B:

## OPTIONS COMPARISON BETWEEN VIRUSSCAN VERSIONS 1.5 AND 2.1.1

## COMPARISON OF SCAN VERSIONS 1.5 and 2.1.1

| Scan<br>Version 1.5 | Scan<br>Version 2.1.1 | Option Description   |
|---------------------|-----------------------|----------------------|
| /? /H or<br>/HELP   | /? or /HELP           | Display help screen. |

|    |      |                                          |
|----|------|------------------------------------------|
| /A | /ALL | Scan all files,<br>including data files. |
|----|------|------------------------------------------|

|         |         |                                             |
|---------|---------|---------------------------------------------|
| /AD {x} | /AD {x} | Scan all drives<br>{L=Local, N=Network}.    |
|         |         | Leave blank for both<br>(version 1.5 only). |

|                   |                   |                                                      |
|-------------------|-------------------|------------------------------------------------------|
| /AF<br>{filename} | /AF<br>{filename} | Store<br>validation/recovery<br>codes in {filename}. |
|-------------------|-------------------|------------------------------------------------------|

|                   |  |                                                                                |
|-------------------|--|--------------------------------------------------------------------------------|
| /AG<br>{filename} |  | Add recovery/validation<br>data to files except<br>those listed in {filename}. |
|-------------------|--|--------------------------------------------------------------------------------|

|                   |                   |                                                                                                                                  |
|-------------------|-------------------|----------------------------------------------------------------------------------------------------------------------------------|
| /AV<br>{filename} | /AV<br>{filename} | Add validation/recovery<br>data to program files.                                                                                |
|                   |                   | Exclude those listed in<br>{filename} (version 1.5<br>only); exclude those<br>listed in /EXCLUDE<br>option (version 2.1.1 only). |

|       |  |                                            |
|-------|--|--------------------------------------------|
| /BELL |  | default Beep whenever a virus<br>is found. |
|-------|--|--------------------------------------------|

|      |  |                                                   |
|------|--|---------------------------------------------------|
| /BMP |  | default Scan OS/2 Boot Manager<br>partition only. |
|------|--|---------------------------------------------------|

|       |  |                                                  |
|-------|--|--------------------------------------------------|
| /BOOT |  | Scan master boot record<br>and boot sector only. |
|-------|--|--------------------------------------------------|

|          |  |                         |
|----------|--|-------------------------|
| /CERTIFY |  | List files not having a |
|----------|--|-------------------------|

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
/CF           <sup>3</sup>/CF           <sup>3</sup> Check  
{filename}   <sup>3</sup>{filename}   <sup>3</sup> validation/recovery  
               <sup>3</sup>               <sup>3</sup> codes in {filename}.

## VERSION COMPARISON OF SCAN OPTIONS (continued)

| Scan<br>Version 1.5 | Scan<br>Version 2.1.1 | Option Description  |
|---------------------|-----------------------|---------------------|
| /CG                 |                       | Check               |
|                     |                       | recovery/validation |
|                     |                       | data in files.      |

|        |  |                       |
|--------|--|-----------------------|
| /CHKHI |  | Check memory from 0Kb |
|        |  | to 1,088Kb (not       |
|        |  | applicable to OS/2).  |

|                    |  |                         |
|--------------------|--|-------------------------|
| (CLEAN.EXE) /CLEAN |  | Clean up infections in  |
|                    |  | master boot records,    |
|                    |  | boot sectors, and files |
|                    |  | when possible.          |

|     |     |                     |
|-----|-----|---------------------|
| /CV | /CV | Check               |
|     |     | validation/recovery |
|     |     | data in files.      |

|    |      |                        |
|----|------|------------------------|
| /D | /DEL | Overwrite and delete   |
|    |      | infected files.        |
|    |      | Save date and time     |
|    |      | VirusScan was last run |
|    |      | in SCAN.LOG.           |

|       |      |                         |
|-------|------|-------------------------|
| /DATE | /LOG | Save date and time      |
|       |      | VirusScan was last run. |
|       |      | Save in SCAN.LOG file   |
|       |      | (version 2.1.1 only).   |

|            |  |                       |
|------------|--|-----------------------|
| /EXCLUDE   |  | Exclude from scan any |
| {filename} |  | files listed in       |
|            |  | {filename}. Typically |
|            |  | used in conjunction   |
|            |  | with the /AV option.  |

|            |  |                        |
|------------|--|------------------------|
| EXT        |  | Scan using external    |
| {filename} |  | virus information from |
|            |  | {filename}.            |

|       |       |                      |
|-------|-------|----------------------|
| /FAST | /FAST | Speed up VirusScan's |
|       |       | scanning; may detect |
|       |       | fewer viruses.       |

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

/HISTORY   <sup>3</sup> /APPEND   <sup>3</sup> Append Scan report to  
{filename}   <sup>3</sup>           <sup>3</sup> {filename} (version 1.5).  
                  <sup>3</sup>           <sup>3</sup> Append to, rather than  
                  <sup>3</sup>           <sup>3</sup> overwrite, the report  
                  <sup>3</sup>           <sup>3</sup> file (/REPORT, version 2.1.1)

## VERSION COMPARISON OF SCAN OPTIONS (continued)

| Scan<br>Version 1.5 | Scan<br>Version 2.1.1 | Option Description                                                                    |
|---------------------|-----------------------|---------------------------------------------------------------------------------------|
| /M                  |                       | Scan memory for all viruses (not applicable to OS/2).                                 |
| /MANY               | /MANY                 | Scan multiple floppy disks (diskettes).                                               |
| /MOVE               |                       | Move infected files to {directory} directory.                                         |
| /NLZ                | /NOCOMP               | Skip internal scan of LZEXE compressed files.                                         |
| /NOBREAK            | /NOBREAK              | Disable Ctrl-C and Ctrl-Break during scan.                                            |
| /NOEXPIRE           |                       | Do not display expiration notice.                                                     |
| /NOMEM              | /NOMEM                | Skip memory checking (not applicable to OS/2).                                        |
| /NOPAUSE            | /PAUSE                | Disable screen pause (version 1.5 only).<br>Enable screen pause (version 2.1.1 only). |
| /NPKL               | /NOCOMP               | Skip internal scan of PKLITE compressed files.                                        |
| /PLAD               |                       | Preserve Last-Access date of scanned files on Novell drives.                          |
| /REPORT             | /REPORT               | Create report of {filename} infected files found during scan in {filename}.           |

[illegible][illegible]

## VERSION COMPARISON OF SCAN OPTIONS (continued)

| Scan<br>Version 1.5 | Scan<br>Version 2.1.1 | Option Description                                                                                       |
|---------------------|-----------------------|----------------------------------------------------------------------------------------------------------|
| /RPTCOR             |                       | Add list of corrupted files to the report file (/REPORT).                                                |
| /RPTERR             |                       | Add list of system errors to the report file (/REPORT).                                                  |
| /RPTMOD             |                       | Add list of modified files to the report file (/REPORT).                                                 |
| /RV                 | /RV                   | Remove validation/recovery data from files.                                                              |
| /SAVE               | /SAVE                 | Save specified options as new defaults (not available in Windows).                                       |
| /SHOWDATE           | /SHOWLOG              | Show date and time of last scan (version 1.5 only). Display information in SCAN.LOG (version 2.1.1 only) |
| /SUB                | /SUB                  | Scan subdirectories inside a directory.                                                                  |
| /VIRLIST            |                       | Display list of viruses detected by VirusScan.                                                           |
| @{filename}         | /LOAD                 | Use Scan settings {filename} stored in {filename}.                                                       |



## COMPARISON OF VSHIELD VERSIONS 1.5 and 2.1.1

| VShield     | VShield       |                         |
|-------------|---------------|-------------------------|
| Version 1.5 | Version 2.1.1 | Option Description      |
| /?          | /HELP         | Display a list of valid |
|             |               | VShield command line    |
|             |               | options.                |

|         |  |                         |
|---------|--|-------------------------|
| /ACCESS |  | Check for viruses when  |
|         |  | files are opened and    |
|         |  | diskettes are accessed. |

|            |  |                          |
|------------|--|--------------------------|
| /ANYACCESS |  | Scan the diskette boot   |
|            |  | sector for viruses       |
|            |  | whenever a diskette is   |
|            |  | accessed (including any  |
|            |  | read and write           |
|            |  | operations); scan .EXE,  |
|            |  | .COM, .DLL, .OVL, .BIN,  |
|            |  | and .SYS files whenever  |
|            |  | the file is opened,      |
|            |  | read, or updated; scan   |
|            |  | .EXE and .COM files      |
|            |  | upon execution; scan     |
|            |  | any newly created file,  |
|            |  | regardless of extension. |

|       |             |                         |
|-------|-------------|-------------------------|
| /BOOT | /BOOTACCESS | Scan the diskette boot  |
|       |             | sector for viruses      |
|       |             | whenever a diskette is  |
|       |             | accessed (including any |
|       |             | read and write          |
|       |             | operations); individual |
|       |             | files on a diskette are |
|       |             | not scanned when a      |
|       |             | diskette is accessed.   |

|            |          |                         |
|------------|----------|-------------------------|
| /CERTIFY   | /CERTIFY | Prevent files without   |
| {filename} |          | validation codes from   |
|            |          | running. {filename} is  |
|            |          | an optional exception   |
|            |          | list (version 1.5 only) |

|            |            |                          |
|------------|------------|--------------------------|
| /CF        | /CF        | Check for viruses using  |
| {filename} | {filename} | validation and recovery  |
|            |            | data stored by Scan /AF  |
|            |            | in specified {filename}. |

/CG<sup>3</sup> Check for viruses using  
 {filename}<sup>3</sup> validation and recovery  
<sup>3</sup> data stored by Scan /AG  
<sup>3</sup>

## VERSION COMPARISON OF VSHIELD OPTIONS (continued)

| VShield | Version 1.5 | VShield | Version 2.1.1 | Option Description         |
|---------|-------------|---------|---------------|----------------------------|
| /CHKHI  |             |         |               |                            |
|         | 3           | 3       | 3             | 3                          |
|         |             | default |               | Check memory from 0Kb-     |
|         |             |         | 3             | 1088Kb when VShield loads. |

|                                                                  |   |           |   |                         |
|------------------------------------------------------------------|---|-----------|---|-------------------------|
| AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA |   |           |   |                         |
| /CONTACT                                                         | 3 | /CONTACT  | 3 | Display specified       |
| {message}                                                        | 3 | {message} | 3 | message when a virus is |
|                                                                  |   |           | 3 | found.                  |

|                                                                  |   |              |   |                        |
|------------------------------------------------------------------|---|--------------|---|------------------------|
| AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA |   |              |   |                        |
| found.                                                           |   |              |   |                        |
|                                                                  | 3 | /CONTACTFILE | 3 | Display message stored |
|                                                                  | 3 | {filename}   | 3 | in {filename} when a   |
|                                                                  | 3 |              | 3 | virus is found.        |

|                                                                  |   |     |   |                         |
|------------------------------------------------------------------|---|-----|---|-------------------------|
| AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA |   |     |   |                         |
| /CV                                                              | 3 | /CV | 3 | Check validation codes  |
|                                                                  |   |     | 3 | added to files by Scan. |

|                                                                  |   |            |   |                          |
|------------------------------------------------------------------|---|------------|---|--------------------------|
| AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA |   |            |   |                          |
|                                                                  | 3 | /EXCLUDE   | 3 | Don't check files        |
|                                                                  | 3 | {filename} | 3 | listed in {filename} for |
|                                                                  | 3 |            | 3 | validation codes         |
|                                                                  | 3 |            | 3 | (/CV option).            |

|                                                                  |   |  |   |                        |
|------------------------------------------------------------------|---|--|---|------------------------|
| AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA |   |  |   |                        |
| /F                                                               | 3 |  | 3 | Use with /SWAP for DOS |
| {pathname}                                                       | 3 |  | 3 | 2.0 systems ONLY.      |

|                                                                  |   |             |   |                         |
|------------------------------------------------------------------|---|-------------|---|-------------------------|
| AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA |   |             |   |                         |
|                                                                  | 3 | /FILEACCESS | 3 | Scan .EXE, .COM, .DLL,  |
|                                                                  | 3 |             | 3 | .OVL, .BIN, and .SYS    |
|                                                                  | 3 |             | 3 | files whenever the file |
|                                                                  | 3 |             | 3 | is opened, read, or     |
|                                                                  | 3 |             | 3 | updated; scan .EXE and  |
|                                                                  | 3 |             | 3 | .COM files upon         |
|                                                                  | 3 |             | 3 | execution; the diskette |
|                                                                  | 3 |             | 3 | boot sector is not      |
|                                                                  | 3 |             | 3 | checked when a diskette |
|                                                                  | 3 |             | 3 | is accessed.            |

|                                                                  |   |            |   |                      |
|------------------------------------------------------------------|---|------------|---|----------------------|
| AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA |   |            |   |                      |
| /IGNORE                                                          | 3 | /IGNORE    | 3 | Don't check programs |
| {drive(s)}                                                       | 3 | {drive(s)} | 3 | loaded from the      |
|                                                                  |   |            | 3 | specified drive(s).  |

|                                                                  |   |  |   |                         |
|------------------------------------------------------------------|---|--|---|-------------------------|
| AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA |   |  |   |                         |
| /LH                                                              | 3 |  | 3 | Load VShield into upper |
|                                                                  | 3 |  | 3 | memory area.            |

[illegible]

/LOCK      <sup>3</sup> /LOCK      <sup>3</sup> Halt the system when a

<sup>3</sup> file that is infected

<sup>3</sup> or not certified loads

<sup>3</sup> and attempts to execute.

## VERSION COMPARISON OF VSHIELD OPTIONS (continued)

| VShield<br>Version 1.5 | VShield<br>Version 2.1.1 | Option Description                                                      |
|------------------------|--------------------------|-------------------------------------------------------------------------|
| /M                     |                          | Scan base memory for viruses when VShield loads.                        |
| /NB                    | /NOWARMBOOT              | Disable boot sector check during install and reboot.                    |
| /NI6510                |                          | Fixes Rascal Datacomm NI6510 conflict.                                  |
| /NOBREAK               |                          | Prevent [Ctrl]+[C] / [Ctrl]+[Break] from working during install.        |
| /NOCONT                |                          | Prevent non-certified programs from running.                            |
| /NODISK                |                          | Turn off the boot sector check when VShield is loading.                 |
| /NOEMS                 | /NOEMS                   | Prevent VShield from using expanded memory (EMS) when it loads.         |
| /NOFLOPPY              |                          | Turn off the boot sector check for floppy drives.                       |
| /NOMEM                 | /NOMEM                   | Do not check memory for viruses upon running.                           |
| /NOREMOVE              | /NOREMOVE                | Prevent VShield from being removed from memory with the /REMOVE switch. |
| /NOUMB                 |                          | Prevent VShield from using upper memory blocks (UMB) when it            |

<sup>3</sup> <sup>3</sup> loads.

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

<sup>3</sup> /NOXMS <sup>3</sup> Prevent VShield from

<sup>3</sup> <sup>3</sup> using extended memory

<sup>3</sup> <sup>3</sup> (XMS) when it loads.

## VERSION COMPARISON OF VSHIELD OPTIONS (continued)

| VShield     | <sup>3</sup> VShield       | <sup>3</sup> Option Description      |
|-------------|----------------------------|--------------------------------------|
| Version 1.5 | <sup>3</sup> Version 2.1.1 |                                      |
| /ONLY       | <sup>3</sup> /ONLY         | <sup>3</sup> Check programs loaded   |
| {drive(s)}  | <sup>3</sup> {drive(s)}    | <sup>3</sup> only from the specified |
|             | <sup>3</sup>               | <sup>3</sup> drive(s).               |

|        |                    |                                    |
|--------|--------------------|------------------------------------|
| AAAAAA | <sup>3</sup> /POLY | <sup>3</sup> Check for polymorphic |
|        | <sup>3</sup>       | <sup>3</sup> viruses.              |

|        |              |                         |                                      |
|--------|--------------|-------------------------|--------------------------------------|
| AAAAAA | /RECONNECT   | <sup>3</sup> /RECONNECT | <sup>3</sup> Restore VShield after   |
|        | <sup>3</sup> | <sup>3</sup>            | <sup>3</sup> certain drivers or TSRs |
|        | <sup>3</sup> | <sup>3</sup>            | <sup>3</sup> have disabled it.       |

|        |              |                      |                                  |
|--------|--------------|----------------------|----------------------------------|
| AAAAAA | /REMOVE      | <sup>3</sup> /REMOVE | <sup>3</sup> Unload VShield from |
|        | <sup>3</sup> | <sup>3</sup>         | <sup>3</sup> memory.             |

|        |              |                    |                                         |
|--------|--------------|--------------------|-----------------------------------------|
| AAAAAA | /SAVE        | <sup>3</sup> /SAVE | <sup>3</sup> Save specified options     |
|        | <sup>3</sup> | <sup>3</sup>       | <sup>3</sup> as new defaults            |
|        | <sup>3</sup> | <sup>3</sup>       | <sup>3</sup> (version 1.5 only).        |
|        | <sup>3</sup> | <sup>3</sup>       | <sup>3</sup> Save the command line      |
|        | <sup>3</sup> | <sup>3</sup>       | <sup>3</sup> options to the VSHIELD.INI |
|        | <sup>3</sup> | <sup>3</sup>       | <sup>3</sup> file (version 2.1.1 only). |

|        |              |                         |                                    |
|--------|--------------|-------------------------|------------------------------------|
| AAAAAA | /SWAP        | <sup>3</sup> /SWAP      | <sup>3</sup> Load VShield kernel   |
|        | [pathname]   | <sup>3</sup> [pathname] | <sup>3</sup> only (5Kb in version  |
|        | <sup>3</sup> | <sup>3</sup>            | <sup>3</sup> 1.5; 8Kb in version   |
|        | <sup>3</sup> | <sup>3</sup>            | <sup>3</sup> 2.1.1); swap the rest |
|        | <sup>3</sup> | <sup>3</sup>            | <sup>3</sup> from pathname.        |



[illegible]

```
3 /FILEACCESS 3 Checks validated files
3           3 whenever the file is
3           3 accessed or executed.
3           3 Whenever a validated
3           3 .EXE, .COM, .DLL, .OVL,
3           3 .BIN, or .SYS file is
3           3 opened, read, or
3           3 updated, Scan checks
3           3 the accessed file.
3           3 Whenever a validated
3           3 .EXE or .COM file
3           3 executes, Scan checks
3           3 the file for viruses as
3           3 it loads and prevents
```

<sup>3</sup>           <sup>3</sup> execution if the file  
<sup>3</sup>           <sup>3</sup> is infected.

## VERSION COMPARISON OF VSHIELD1/VSHIELDCRC OPTIONS (continued)

VShield1   <sup>3</sup> VShieldCRC   <sup>3</sup>  
 Version 1.5   <sup>3</sup> Version 2.1.1   <sup>3</sup> Option Description  
 |||||0|||||0|||||

<sup>3</sup> /IGNORE   <sup>3</sup> Don't check programs  
<sup>3</sup> {drive(s)}   <sup>3</sup> loaded from specified  
<sup>3</sup>   <sup>3</sup> drive(s).

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

<sup>3</sup> /LOCK   <sup>3</sup> Halt the system when a  
<sup>3</sup>   <sup>3</sup> file that is not  
<sup>3</sup>   <sup>3</sup> certified attempts to  
<sup>3</sup>   <sup>3</sup> load and execute.

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

<sup>3</sup> /LOGFILE   <sup>3</sup> Write error information  
<sup>3</sup> {filename}   <sup>3</sup> to {filename}.

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

/NB   <sup>3</sup>   <sup>3</sup> Disable boot sector  
<sup>3</sup>   <sup>3</sup> checking during install  
<sup>3</sup>   <sup>3</sup> and reboot.

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

and reboot.

<sup>3</sup> /NOREMOVE   <sup>3</sup> Prevent VShieldCRC from  
<sup>3</sup>   <sup>3</sup> being removed from memory  
<sup>3</sup>   <sup>3</sup> with a subsequent VShieldCRC  
<sup>3</sup>   <sup>3</sup> command using /REMOVE.

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

<sup>3</sup> /NOUMB   <sup>3</sup> Prevent VShieldCRC from  
<sup>3</sup>   <sup>3</sup> using upper memory  
<sup>3</sup>   <sup>3</sup> blocks (UMB) when it loads.

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

<sup>3</sup> /ONLY   <sup>3</sup> Check programs loaded  
<sup>3</sup> {drive(s)}   <sup>3</sup> only from the specified  
<sup>3</sup>   <sup>3</sup> drive(s).

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

/REMOVE   <sup>3</sup> /REMOVE   <sup>3</sup> Unload VShieldCRC from  
<sup>3</sup>   <sup>3</sup> memory.



**ARCHIVED FILE** A file that has been archived using either LZEXE or PKLITE, file compression utilities.

**BOOT** To start a computer. The first step is to load startup instructions from the boot ROM or boot sector of a disk.

**BIOS** A read-only memory chip that contains the coded instructions for the operating system to start the computer. Always present in portable computers, a BIOS (boot ROM) is not susceptible to infection (unlike the boot sector on a disk). However, it is harder to update.

**BOOT SECTOR** A portion of a disk that contains the coded instructions for the operating system to start the computer.

**BOOT SECTOR INFECTIONS** Contamination of the boot sector by a virus. Particularly serious because information in the boot sector is loaded into memory first, before virus protection code can be executed. The only certain way to eliminate boot sector infections is to restart from a disk known to be uninfected, then clean up the infection.

**CLEAN STARTUP DISKETTE** A diskette known to be uninfected, that contains the coded instructions from which the computer can be started. See Chapter 2 for instructions on preparing one.

**COLD BOOT** To start a computer from power-off state.

**COMPRESSED FILE** A file (usually with a .ZIP extension) that has been compressed using the PKZIP file compression utility.

**CONVENTIONAL MEMORY** Up to 640Kb of main memory in which DOS executes programs.

**CORRUPTED FILE** A file that has been damaged. About 10% to 20% of viral infections involve viruses that damage files beyond repair.

**DETECTION** Scanning memory and disks for telltale marks or changes indicating that a virus might be present.

**DISINFECT** To eradicate a virus so that it can no longer spread or cause damage to a system.

**EXCEPTION LIST** List of files to which validation codes should not be added because they are immunized against viruses or contain self-modifying code. Scans /AV option uses the list to avoid adding codes to inappropriate files; VShield's /CERTIFY option can use it to allow certain unvalidated files to be run.

**EXECUTABLE (FILE)** A file containing coded instructions to be executed by the computer. Executable files include programs and overlays.

**EXPANDED MEMORY** Memory above the DOS 640Kb limit of conventional memory that is accessed by memory paging. You need special software, conforming to an expanded memory specification, to take advantage of expanded memory.

**EXTENDED MEMORY** Linear memory above the DOS 640Kb limit of conventional memory. Often used for RAM disks and print spoolers.

**FALSE ALARM** Detecting a virus when none is present.

**INFECTED FILE** A file contaminated by a virus.

**MASTER BOOT RECORD (MBR)** A portion of a hard disk that contains a partition table that divides the drive into chunks, some of which may be assigned to operating systems other than DOS.

**MEMORY** A storage medium where data or program code are kept temporarily while being used by the computer. DOS supports up to 640Kb of conventional memory. Beyond that limit may be accessed as expanded memory, extended memory, or an upper memory block (UMB).

**MEMORY INFECTION** Contamination of memory by a virus. The only certain way to eliminate memory infections is to restart from a disk known to be uninfected, then clean up the source of infection.

**MODIFIED FILE** A file that has changed after validation/recovery codes have been added.

**OVERLAY INFECTION** Virus contamination of a file containing auxiliary program code that is loaded by the main program.

**PARTITION TABLE** See MASTER BOOT RECORD.

**POLYMORPHIC VIRUS** A virus that attempts to evade detection by changing its internal structure or its encryption techniques.

**PROGRAM** Software that performs a defined function on a computer. See executable.

**READ OPERATION** Any operation in which information is read from a disk. DOS commands that perform read operations include dir (directory listing), type (display contents of a file), and copy (copy files). See also write operation.

**RECOVERY CODES** Information that Scan records about an executable file in order to recover if it is infected by a virus. See also validation codes.

**SELF-MODIFYING PROGRAM** Software that deliberately changes its own program file, often to protect against viruses or illegal copying, and is therefore difficult to validate in conventional ways.

**STANDARD EXTENSIONS** Filename extensions (suffixes) that signify executable files--EXE, .COM, .SYS, .DLL, .BIN, and .OVL--which Scan checks by default.

**SYSTEM ERRORS** Errors that can prevent Scan from completing its job successfully. System error conditions include disk format errors (such as unformatted disks), media errors (bad sectors), file system errors (unreadable files), network errors (unable to log in), file access errors (access permission denied), device access errors (printer out of paper), and report failures.

**TERMINATE-AND-STAY-RESIDENT (TSR)** A program, like VShield, that remains active in memory while you run other programs.

**TURBO** A scanning option that is faster than normal but less comprehensive (because it checks a smaller portion of each file).

**UNKNOWN VIRUS** A virus not yet identified and listed in SCAN.DAT. VirusScan can detect unknown viruses by observing changes in files that could result from infection.

**UPPER MEMORY BLOCK (UMB)** Memory in the range 640-1024Kb, just above the DOS 640Kb limit of conventional memory.

**VALIDATE** To check that a file is authentic and has not been altered. Most validation methods rely on computing a statistic based on all the data in the file, which is unlikely to remain constant if the file itself is changed.

**VALIDATION CODES** Information that Scan records about an executable file in order to detect subsequent infection by a virus. See also recovery codes.

**VIRUS** A software program that attaches itself to another program in computer memory or on a disk, and spreads from one program to another. Viruses may damage data, cause the computer to crash, display messages, or lie dormant.

**WARM BOOT** To restart (reset) a running computer, in DOS by pressing [Ctrl]+[Alt]+[Del].

**WRITE OPERATION** Any operation in which information is recorded on a disk. Commands that perform write operations include those that save, move, and copy files. Most write operations are also read operations because the system verifies that the data have been written correctly. See also read operation.

**WRITE PROTECTION** A mechanism to protect files or disks from being changed. A 3.5" diskette may be write-protected by sliding its corner tab so that the square hole is open; a 5.25" diskette by covering its corner notch with a write-protect tab. A file may be write-protected by changing its system attributes.