User’s Guide

VirusScan for DOS and OS/2
ScanPM

MCAFEE®
Network Security & Management

2805 Bowers Avenue
Santa Clara, CA 95051-0963

Phone: (408) 988-3832
Monday - Friday
6:00 A.M. - 6:00 P.M.

FAX: (408) 970-9727
BBS: (408) 988-4004

COPYRIGHT

TRADEMARK NOTICES

FEEDBACK

McAfee appreciates your comments and reserves the right to use any information you supply in any way it believes appropriate without incurring any obligations whatsoever. Please address your documentation feedback to: McAfee Associates, Inc., Documentation, 2805 Bowers Avenue, Santa Clara, CA 95051-0963, send e-mail to documentation@cc.mcafee.com, or send a fax to McAfee Documentation at (408) 970-9727.

Issued October 1997 / VirusScan v3.1.2 for DOS and OS/2, ScanPM

Table of Contents

Preface

The Bits and the Bytes

Computer viruses, most users know, can have a devastating impact on productivity. What many of those same users don't know is basic information that could help them protect themselves from infection—such as where viruses come from and how they operate.

In the beginning

The conceptual foundations for viruses have been around much longer than the virus threat itself. Although virus historians disagree on the specific whens and wheres, it is generally accepted that the ideas were born when computers were still huge and expensive—the domain of large corporations and the government, not the public. And while many of the viruses circulating today are malicious, destruction of data was not part of the original premise.

The idea was that if one could create a computer program that could make copies of itself, or self-replicate, it might also be possible for that program to evolve. If an error were to occur in the replication process, the resulting code (the bits of information that make up the program) would be mutant. Just as mutant genetic code is what disposes a biological virus to either be more or less able to survive and propagate, mutant digital code might dispose a computer virus to be more or less able to survive in the computer environment. Given enough time, the logical extension of the theory goes, a computer virus could evolve into something approaching artificial intelligence. Science fiction suddenly starts to look more like science and less like fiction.

What viruses really are

At its core, a virus is simply a program with one goal: self-replication. Part of achieving that goal is remaining undetected. If a virus is found by a user, it is likely to get deleted, which puts quite a damper on any self-replicating plans. Just like any other program, a virus has to be run to do its work. And since a user will not run a virus intentionally, the virus has to attach itself to a file that the user will run. That includes executable files and document files with embedded macros, as we will see in a couple of pages. For a virus to infect any other type of file—say, a plain text file—would be counter-productive: Remember, replication is its primary objective.

Computers with the sniffles?

Consider the similarities between computer and biological viruses. A computer virus infects a host program, just as a biological virus infects a host cell. It writes its own code in among the pieces of code that make up the host program. Then, in much the same way as a biological virus uses resources from its host organism to reproduce, a computer virus runs each time the infected host is run, and makes copies of itself. Those copies then infect other programs, and the cycle begins again.

Just as biological viruses have detrimental effects, so do their computer counterparts. The first computer viruses were simply experiments by research scientists to test the theory—to see if it could be done. They proved the theory, but also discovered that viruses had some unfortunate side effects. Viruses got in the way of some of the normal processes of the computer and caused erratic behavior. Many viruses are now specifically programmed to perform some function outside of self-replication. This function, called the payload, can be as innocuous as displaying a message on the computer's monitor or as harmful as destroying data on the system's hard disks. It is delivered when the trigger, an event such as a particular combination of keystrokes, a certain date or a pre-determined number of actions, occurs.

Who writes viruses?

The reason for this change in the behavior of viruses—from innocent experiment to malicious sneak attack—is a result of a change in the type of people who write them. Virus code is now developed by many people who are less interested in studying the possibility of artificial intelligence than in inflicting harm. Some do it out of spite, some because they aspire to be the underground "mad hacker” romanticized in much of pop culture as a freedom fighter of the digital age. The reasons people write virus code are probably as varied and strange as the reasons people perform other destructive acts.

Some virus writers actually choose to identify themselves, such as the Pakistani brothers who wrote the Brain virus. The brothers included the name, address, and telephone number of their software company in the viral code. When the payload was delivered, this information would be displayed for the user. Apparently, the brothers wrote the virus to show how widespread software pirating was. They put it on software leaving their office with the idea that wherever the virus spread, so had their software. Of course, what they overlooked was the fact that the virus spread by infecting programs other than the one it left their office in.

Other virus writers are disgruntled employees seeking revenge. Still others are schoolkids who write just to see if they can. The famous Stoned virus is said to have been written by such a youngster. Having written it, he feared the consequences of unleashing it, so he destroyed all copies of the virus except one, which he kept at his house. His younger brother and a couple of friends managed to lay their hands on it though, and infected some disks as a joke. But the infection spread quickly and soon was impossible to stop.

Whatever the motivation, the number of people capable of writing a virus is growing right alongside the computer industry. Those who stand to be affected by virus infection—anyone who uses a computer—should be alert and wary.

Only getting worse

In part, the fact that there are so many of us who need to be on the alert today is what makes virus proliferation possible. When the computer world was made up entirely of huge expensive machines, a virus did not have very far to go once it got started. But with the advent of the personal computer, viruses suddenly had a lot of places to go. The rapid growth of the Internet, the capability to attach files to e-mail messages, and the increasing degree to which the world depends on its computers all make conditions ever-better for the spread of computer viruses.

New developments

There are other reasons to be especially wary these days. Viruses get increasingly complex and advanced as computers on the whole do the same. Just in the last few years, sophisticated and dangerous new virus families have appeared, such as polymorphic viruses and macro viruses. Polymorphic viruses are especially tricky because they change each time they infect a new file. Where once anti-virus software could search for viruses by "signatures" (chunks of code unique to each virus), software must now be able to detect polymorphic viruses that change their signature each time they infect a file.

Macro viruses infect documents and document templates—new territory for viruses. Documents used to be safe from viral attack because until a few years ago, a document file didn’t have any executable code in it. Now that software applications like Microsoft Word and Microsoft Excel have embedded macro capabilities, viruses can infect documents created by that software through the macro language.

All that just in the last few years. And viruses as a serious threat have only been around for about ten years. To imagine what is in store as the computer becomes more complicated and more a part of everyday life is frightening. Luckily, you have purchased the best protection against infection available today. And with McAfee's outstanding support and worldwide anti-virus research teams, you can make sure your protection keeps up with the ever-changing computer world.

1

Introducing VirusScan

What is VirusScan?

VirusScan is McAfee's powerful anti-virus solution. Once installed, VirusScan continuously monitors your system for virus activity. If a virus is detected, you can respond by removing the virus, moving infected files to another location, or deleting the infected files. VirusScan can also be user-initiated to scan a file, folder, disk, or volume.

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 this type of security program as a preventive measure to protect against future infection. For tips on creating a secure environment, see Appendix A, "Preventing Virus Infection."

Main features

- NCSA-certified scanner assures detection of more than 90% of the viruses identified by the National Computer Security Association and 100% of the viruses found "in the wild." See the NCSA website, www.ncsa.com, for certification status.
- VShield, VirusScan's on-access scanner, provides real-time identification of both known and unknown viruses on file access, file creation, file copy, file rename, file execution, disk access, and system startup.
- On-demand scanning provides for user-initiated detection of known and unknown boot, file, mutation, multi-partite, stealth, encrypted, polymorphic, and macro viruses located within files, drives, and diskettes.

- Enhanced password sensitivity enables VirusScan to remove macro viruses that can set their own passwords, as well as remove macro viruses from password-protected Microsoft Excel 95 files without disturbing user passwords.
- Macro viruses are detected in password-protected Microsoft Word 95 (Word 7.0) files in at least six languages: Japanese, German, English, French, Italian, and Dutch. Even unknown macro viruses are detected by VirusScan's heuristic scanning technology.
- Code Trace™, Code Poly™, and Code Matrix™ scanning employ McAfee's proprietary technologies for pinpoint virus identification accuracy.
- Monthly updates of virus signatures are included with the purchase of a McAfee subscription license to assure the best detection and removal rates. See Appendix C, "McAfee Support Services," for details.

How virus detection works

VirusScan monitors your computer and searches for characteristics (sequences of code) unique to each known virus. If a virus is detected, VirusScan alerts you of its presence. For encrypted, mutated, and unknown macro viruses, VirusScan uses algorithms for detection that rely on statistical analysis, heuristics, and code disassembly.

When should I scan for viruses?

VirusScan's on-access scanner will perform automatic scans of your system every time you access a file, create a file, copy a file, rename a file, run a file, insert a diskette, or start up your system.

For maximum protection, use VirusScan's on-demand scanning feature to scan for viruses whenever files are added to your system. When copying files from a diskette or downloading files from an online service, run VirusScan to ensure that a virus has not been introduced.

Scan when you insert an unknown diskette

When inserting an unknown diskette in your drive, scan it before executing, installing, or copying its files.

Scan when you install or download new files

When installing new software on your hard drive or downloading executable files from an online service, run VirusScan to check the files.

Scan on a regular basis

Perform on-demand scans regularly. Depending on how susceptible your system is to virus infection, this may be as frequently as once a day to once a month.

How to Contact McAfee

Customer Service

To order products or obtain product information, we invite you to contact our Customer Care department at (408) 988-3832, or at the following address:

McAfee Associates, Inc.
2805 Bowers Avenue
Santa Clara, CA 95051-0963
U.S.A.

Technical Support

McAfee is famous for its dedication to customer satisfaction. We have continued this tradition by making our website a valuable resource for answers to technical support questions. We encourage you to make this your first stop for answers to frequently asked questions, for updates to McAfee software, and for access to McAfee news and virus information.

World Wide Web	http://www.mcafee.com

If you do not find what you need or do not have web access, try one of our automated services.

Automated Voice and Fax Response System	(408) 988-3034
Internet	support@mcafee.com
McAfee BBS	(408) 988-4004 1200 bps to 28,800 bps 8 bits, no parity, 1 stop bit 24 hours, 365 days a year

CompuServe	GO MCAFEE
America Online	keyword MCAFEE

If the automated services did not have the answers you need, contact McAfee technical support Monday through Friday between 6:00 A.M. and 6:00 P.M. Pacific time.

For corporate-licensed customers:

Phone	(408) 988-3832
Fax	(408) 970-9727

For retail-licensed customers:

Phone	(972) 278-6100
Fax	(408) 970-9727

To provide the answers you need quickly and efficiently, the McAfee technical support staff needs some information about your computer and your software. Please have this information ready before you call:

- Product name and version number
- Computer brand, model, and any additional hardware
- Operating system type and version
- Network type and version
- Contents of your AUTOEXEC.BAT, CONFIG.SYS, and system LOGIN script
- Specific steps to reproduce the problem

International Contact Information

To contact McAfee outside the United States, use the addresses and numbers below.

McAfee Canada
139 Main Street, Suite 201
Unionville, Ontario
L3R 2G6 CANADA
Phone: (905) 479-4189
Fax: (905) 479-4540

McAfee Europe B.V.
Gatwickstraat 25
1043 GL Amsterdam
THE NETHERLANDS
Phone: 31 20 586 6100
Fax: 31 20 586 6101

McAfee France
50 rue de Londres
75008 Paris
FRANCE
Phone: 33 1 44 90 87 37
Fax: 33 1 45 22 75 54

McAfee GmbH
Industriestrasse 1
82110 Germering
GERMANY
Phone: 49 89 894 356-0
Fax: 49 89 894 356-99

McAfee UK
Hayley House
London Road
Bracknell
RG12 2TH
UNITED KINGDOM
Phone: 44 1344 304 730
Fax: 44 1344 306 902

McAfee Japan KK
4F Toranomon Mori
Bldg. 33
3-8-21 Toranomon
Minato-Ku, Tokyo 105
JAPAN
Phone: 81 3 3435 8246
Fax: 81 3 3435 1349

2

Installing VirusScan

Before You Start

To prepare for installation and minimize the risk of spreading viruses that may already be present on your system, take the following steps:

Step	Action
1.	Review the system requirements below for VirusScan.
2.	Ensure that your system is virus-free. If you suspect your system is infected, see “If You Suspect You Have a Virus” on page 46 before installing the software.
3.	Confirm that your Date/Time settings are accurate.

System Requirements

- IBM-compatible personal computer running DOS
- 386 with at least 4MB of memory, 2.5MB of free hard drive space

✍ *For OS/2: 2.0GA or above*

✍ *For ScanPM: minimal conventional memory and at least 1.5MB of free hard drive space, running MS DOS version 3.3 or higher*

Installation Procedure

Follow the procedure outlined below to install VirusScan.

✍ *If you suspect the system is already infected by a virus, see "If You Suspect You Have a Virus" on page 46.*

Step	Action
1.	Start your computer.
2.	Do one of the following: ▪ If you are installing from diskette or compact disc, insert it into your floppy disk drive or CD-ROM drive. ▪ If you are installing from files downloaded from a BBS or the McAfee website, decompress the zipped files into a directory on the network or your local drive.
3.	At the command-line prompt, change to the directory where the installation files are located.
4.	Type `install` at the prompt, then press ENTER. **Response**: VirusScan begins scanning for viruses.
5.	Do one of the following: ▪ If VirusScan finds a virus and is unable to clean it, see "If You Suspect You Have a Virus" on page 46. ▪ If VirusScan does not find any viruses, the Welcome screen is displayed. Press ENTER.
6.	Select a target drive for the VirusScan program files and press ENTER.
7.	Enter a target directory path for the VirusScan program files and press ENTER.

8. Choose one of the following options:

   - To modify the AUTOEXEC.BAT file to load VShield on whenever you boot or start a DOS session in OS/2, select Yes and press ENTER. The installer will save a copy of the unmodified old file.

   - To leave the old AUTOEXEC.BAT file unmodified and save the new, modified version as MCAFEE.BAT, select No and press ENTER.

   Response: VirusScan begins copying the program files to the target directory.

9. When the installation is complete and the system returns to the command-line prompt, restart the system.

10. Make a clean start-up diskette. See "Making a Clean Start-up Diskette" on page 57 for more information.

Testing your installation

For information on how to use the Eicar Standard AntiVirus Test File to test your installation of VirusScan, see Appendix B, "Testing Your Installation."

3

On-access Scanning

What is On-access Scanning?

On-access scanning works through a memory-resident program, VShield, which provides real-time protection for your system. On-access scanning helps to prevent virus infection by automatically checking programs—such as files, directories, drives, and any media—as soon as you run them. To determine how VShield performs a scanning operation, start the version of the executable program that corresponds to your operating system and add configuration options to the command line. See “Selecting VShield options” on page 21 for a list of available options.

The VShield component does not run directly in the OS/2 environment, but you can use VShield features to scan DOS or FAT partitions on your hard disk by starting a DOS session in OS/2. If you have modified your AUTOEXEC.BAT file to load it at startup, VShield scans for viruses in memory and on disk using its default configuration options or the options you specified in your AUTOEXEC.BAT file. VShield terminates when you end your DOS session.

Note also that some of the configuration options do not function in an OS/2 environment—this manual notes these exceptions in the descriptions of each option. VShield detects only those viruses that can propagate in the OS/2 DOS environment; a virus in a file with a long filename, for example, will not be detected.

Starting VShield

VShield, VirusScan’s on-access scanner, is a memory resident program that, if configured to load at startup, remains active in the background when you start your system. To ensure VShield is active:

- Check your AUTOEXEC.BAT file for the VShield command line.
- Type `chkvshld` at the DOS prompt in the VirusScan directory. You will receive a message that tells you whether VShield is running and what options you have selected.

  ✍ *You cannot use* `chkvshld` *to verify whether VShield is running in OS/2. VShield does, however, beep when it finds a virus. (If used with OS/2, VirusScan will beep when it finds a virus, but will not display a message.)*

Configuring On-access Scanning

By default, VShield starts with the most common configuration options enabled. You can, however, use whichever options best suit your needs and your work environment. To customize VShield, follow these steps:

Step	Action
1.	Select VShield options. For more information, see "Selecting VShield options," below.
2.	Add the options to the VShield line in your AUTOEXEC.BAT file. For more information, see "Editing your AUTOEXEC.BAT file" on page 25.

Selecting VShield options

Before editing your AUTOEXEC.BAT to reconfigure VShield, you should first determine which parameters are necessary for your environment.

For an onscreen list of scanning options and their usage, use the `cd` command to change to the VirusScan directory, then type `vshield /?` at the command prompt. You'll see a list of available options similar to that shown in the tables on the following pages.

General

Command-line Option	Description
`/?` or `/HELP`	Displays a list of valid command-line options.
`/NOEXPIRE`	Disables the “expiration date” message if the VirusScan data files are out of date.
`/NOREMOVE`	Prevents VShield from being removed from memory with the /REMOVE switch.
`/RECONNECT`	Restores on-access scanning after certain drivers or TSRs have disabled it.
`/REMOVE`	Unloads VShield from memory.
`/SAVE`	Saves the command-line options to the VSHIELD.INI file.

Memory

Command-line Option	Description
`/NOEMS` Not valid for OS/2 or ScanPM	Does not use expanded memory (EMS).
`/MEMEXCL hhhh[-hhhh]` Not valid for OS/2	Does not allow Vshield to use UMB address specified.
`/NOUMB`	Does not use upper memory blocks (UMB).
`/NOXMS`	Does not use extended memory (XMS).
`/SWAP pathname`	Loads VShield kernel (9.2KB) only; swap the rest to [pathname].
`/XMSDATA`	Loads VShield data files into XMS memory.

Target

Command-line Option	**Description**
`/ANYACCESS` Scans only floppy disk files and executables in OS/2.	Scans the boot sector whenever a diskette is accessed (read and write); scans executables; scans any newly created files. ✍ `/ANYACCESS` *is incompatible with* `/POLY`. *They cannot be used together.*
`/BOOTACCESS`	Scans a diskette's boot sector for viruses whenever the diskette is accessed (including read/write operations).
`/FILEACCESS`	Scans executable files when they are accessed on a diskette, but does not check the boot sector.
`/IGNORE drive(s)`	Does not check programs loaded from the specified drive(s)
`/NODISK`	Does not scan boot sector while loading VShield.
`/NOMEM` Not valid for OS/2	Disables memory checking.
`/NOWARMBOOT`	Does not check the diskette boot sector for viruses during warm boot (system reset or CTRL+ALT+DEL).
`/ONLY drive(s)`	Checks only programs loaded from the specified drive(s).
`/POLY`	Checks for polymorphic viruses. ✍ `/POLY` *is incompatible with* `/ANYACCESS`. *They cannot be used together.*

Notification

Command-line Option	Description
`/CONTACT message`	Displays specified message when a virus is detected.
`/CONTACTFILE filename`	Displays message stored in [filename] if a virus is detected.
`/LOCK` Not valid for OS/2	Halts the system if a virus is detected.

Validation

Command-line Option	Description
`/CERTIFY`	Prevents running files that do not have VirusScan validation codes.
`/CF filename`	Checks validation codes stored by `scan /AF` in [filename]. For more information, see "Configuring Validation Options" on page 40.
`/CV`	Checks validation data stored in files by `scan /AV`. For more information, see "Configuring Validation Options" on page 40.
`/EXCLUDE filename(s)`or `directory`	Does not check files listed in [filename] for validation codes (/CV option). Also can be used to exclude directories and multiple files; e.g., `c:\dos` excludes all c:\dos directory files, and `c:\dos\fo` excudes all c:\dos\fo*.* files.

Editing your AUTOEXEC.BAT file

Before editing your AUTOEXEC.BAT file, decide which options are appropriate for your work environment and note which options function with your operating system. See “Selecting VShield options” on page 21.

To edit your AUTOEXEC.BAT file, follow these steps:

Step	Action
1.	Change to the root directory by typing `cd c:\` .
2.	Type the following: `edit autoexec.bat` **Response**: The program Edit starts.
3.	Locate the first VSHIELD line. Move the cursor to the end of the VShield line using the arrow keys. Press the spacebar to make sure one space is between VShield and the first option.
4.	Enter a scanning option (e.g., /ANYACCESS, /BOOTACCESS, etc.). ✍ *When running in a DOS session in OS/2, VShield scans files stored on floppy disks, but does not scan a disk’s boot sector. The /BOOTACCESS option, therefore, is not valid. The /ANYACCESS option, while functional, scans only floppy disk files.*
5.	Press the spacebar.
6.	Repeat steps 4 and 5 until you have entered all options.
7.	To save the file, press ALT+F to reveal the File menu then press S to save.
8.	To exit and return to the command prompt, press ALT+F to reveal the File menu then press X to exit.

4

On-demand Scanning

What is On-demand Scanning?

As described in the previous chapter, "On-access Scanning," VShield protects your system by constantly scanning for viruses whenever you open files or start programs. You can also tell VirusScan to conduct a scan operation at any time, on any target drive, directory or file, and using the scanning options you choose. This chapter describes explains how to use VirusScan's on-demand feature to detect known boot, file, multi-partite, stealth, encrypted, polymorphic, and macro viruses located within specific files, directories, or drives.

Basic Scanning

To perform basic scanning, start from the command-line prompt (C> or [C:\]).

✍ *Exit from Windows or any application programs.*

Complete the following procedure:

Step	**Action**
1.	Using the `cd` command, change to the directory where VirusScan is installed. ✍ *The default directory for DOS is* C:\MCAFEE\VIRUSCAN. *For OS/2 it is* C:\ MCAFEE\OS2SCAN. *For ScanPM it is* C:\MCAFEE\SCANPM.

2. Type the command to start the executable file for your operating system version, along with the options you choose. Use the examples shown below to run on-demand scan operations for various situations.

   ✍ *Each VirusScan version has its own executable file. To start the executable file in a DOS environment, type* `scan` *at the command line as shown. To start the executable file in an OS/2 environment, type* `os2scan` *at the command line. To start ScanPM, type* `scanpm` *at the command line. In each instance where this guide refers to* `scan`*, substitute the executable file that corresponds to your operating system, adding the options appropriate for your needs and operating system.*

   - To scan the C: drive for known viruses, type the following command:

     ```
     scan c: /all
     ```

   - To scan the C: and D: drive for known viruses, type the following command:

     ```
     scan c: d: /all
     ```

   - To scan all system drives (including compressed drives and PCMCIA drives—but not diskettes) and all file types for known viruses, type the following command:

     ```
     scan /adl /all
     ```

     where:

     - /ADL specifies all local drives as the target of the scan.
     - /ALL instructs VirusScan to scan all infectable file types.

3. VirusScan might take several minutes to check for viruses in memory and on drives, but will keep you informed of its progress. Read the information on the screen carefully. The following information is a sample of what VirusScan reports when checking a drive for viruses.

```
Scan v.3.1.2 Copyright (c) McAfee, Inc. 1994 - 1997.
All rights reserved.
(408) 988-3832 LICENSED COPY - Sep 25 1997

Virus data file V3009 created 10/01/97 13:33:29
10/10/97 16:26:59


Options:
/REPORT SCAN.TXT
Scanning C: [MS-DOS_6]
Summary report on C:
File(s)
   Analyzed:..............11577
   Scanned:................1644
   Possibly infected:....... 0
Master Boot Record(s):...... 1
   Possibly infected:....... 0
Boot Sector(s):............. 1
   Possibly infected:....... 0
Time: 00:02.28
```

- **Analyzed** indicates the number of infectable files found in the specified location.

- **Scanned** indicates the number of files scanned for viruses. If you are using the default settings, VirusScan only checks executable files and Microsoft Word documents with standard executable or document file extensions (i.e., .COM, .EXE, .SYS, .BIN, .OVL, .DLL, .DOC, .DOT). To check all infectable files, use the /ALL command line option.

- **Possibly infected** indicates the number of infected files found.

4. Do one of the following:

- If VirusScan reports No Viruses Found, your system is most likely virus-free. Copy important files to fresh diskettes or tape backup so your current and clean files are maintained should a virus later infect your system.

  ✍ *VirusScan's ability to detect viruses must be maintained through regular updates of the VirusScan data files. For more information about updating VirusScan, see "Updating your VirusScan data files" on page 54.*

- If VirusScan finds one or more viruses, a message similar to the following is displayed:

  ```
  Scanning C:
  Scanning file C:\DOS\ATTRIB.EXE
  Found the Jerusalem Virus
  ```

  ✍ *An unknown macro virus detected by heuristic scanning technology, is reported as a PROBABLE MACRO VIRUS.*

  Do not panic, even if the virus has infected many files. Do not run any other programs. Immediately see "If VirusScan Detects a Virus" on page 48.

Advanced Scanning

By default, VirusScan runs with the most common scanning options enabled. Because a large number of custom scanning options are available, VirusScan can use a scanning profile, a text file that contains scanning options, to govern how it performs a scan.

- For information on selecting scanning options, see "Selecting scanning options," below.
- For information on creating a scanning profile, see "Creating a scanning profile" on page 38.
- To run the scanning profile, see "Running the scanning profile" on page 39.

Selecting scanning options

Before creating a scanning profile, determine which parameters are necessary for your environment.

✍ *For a list of scanning options and their usage, use the* `cd` *command to change to the VirusScan directory and type* `scan /?` *or see* Appendix D, *on* page 70.

Target options

The following table lists some target-related scanning options.

✍ *You must select a target location to scan (e.g. C:\, A:\, /ADL, /ADN).*

Command-line Option	Description
`/?` or `/HELP`	Does not scan. Instead, displays a list of VirusScan command-line options with a brief description of each. Use either of these options alone on the command line (with no other options).
`/ADL` For OS/2, includes CD-ROM when used with `/NODDA.` OS/2 recognizes CD-ROM drives as local drives	Scans all local drives (including compressed drives and PCMCIA drives, but not diskettes), 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.
`/ADN` For OS/2, does not include CD-ROM drives—see `/ADL,` above	Scans all mapped network drives (including CD-ROM drives) for viruses, in addition to other drives specified on the command line. To scan both the local drives and network drives, use /ADL and /ADN together in the same command line.
`/ALL`	By default, VirusScan only scans file types that are most susceptible to viruses. This option overrides the default settings by scanning all infectable file types. This option substantially increases the scanning time required. Use it if you found a virus or suspect you have one.
`/BOOT` Not valid for OS/2	Scans only the boot sector and Master Boot Record on the specified drive.

Command-line Option	Description
`/EXCLUDE filename(s)` or `directory`	Excludes any files listed in [filename] from the scan. This option allows you to exclude files from /AF and /AV validation and /CF and /CV checking. Also can be used to exclude directories and multiple files; e.g., `c:\dos` excludes all c:\dos directory files, and `c:\dos\fo` excudes all c:\dos\fo*.* files. ✍ *Self-modifying or self-checking files can cause a false alarm during a scan.*

`/MEMEXCL`
`hhhh[-hhhh]`
Not valid for OS/2
	Excludes memory area from scanning. (The default is A000-FFFF, 0000=Scan all.)
	This command-line option has been added to prevent VirusScan from checking areas in upper memory that might contain memory-mapped hardware and might cause false alarms.

`/NOCOMP`	By default, VirusScan checks executable or self-decompressing files created using the LZEXE or PkLite file-compression programs. VirusScan decompresses each file in memory and checks for virus signatures, which takes time but results in a more thorough scan. Selecting this option skips checking of compressed executables created with the LZEXE or PkLite file-compression programs. This reduces scanning time when a full scan is not needed.
`/NODDA`	No direct disk access. Prevents VirusScan from scanning the boot record. You may need to use this option on some device-driven drives. ✍ *Using /NODDA with the /ADN or /ADL switches may generate errors when scanning empty CD-ROM drives or empty Zip drives. If this occurs, type F (for Fail) in response to the error message to allow the scan to continue.*

Command-line Option	Description
`/NOMEM` Not valid for OS/2	By default, VirusScan checks system memory for all known computer viruses inhabiting memory. In addition to main memory from 0KB to 640KB, VirusScan 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 not presently susceptible to viruses. Selecting this option reduces scan time by omitting all memory checks. Only use /NOMEM when you are absolutely certain the system is virus-free.
`/PLAD` *Not valid for ScanPM*	Preserves last access dates (on proprietary drives only). Prevents changing the last access date attribute for files stored on a network drive in a proprietary network. Normally, proprietary network drives update the last access date when VirusScan 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 the last access date does not change as the result of scanning.
`/SUB`	Scans subdirectories inside a directory. By default, when you specify a directory to scan rather than a drive, VirusScan will examine only the files it contains, not its subdirectories. Use /SUB to scan all subdirectories inside any specified directories. Do not use /SUB if you are scanning an entire drive.

Response and notification options

The following table lists some response and notification options upon detection of a virus.

Command-line Option	Description
`/CLEAN`	Cleans viruses from infected files and system areas.
`/CONTACTFILE filename`	Displays the contents of the specified text file when a virus is found. This option is especially useful in network environments, allowing you to maintain the message text in a central file rather than on each workstation. Any character is valid except a backslash (\). Messages beginning with a slash (/)or a hyphen (-) should be placed in quotation marks.
`/LOCK` Not valid for OS/2	Halts the system to stop further infection if VirusScan finds a virus. /LOCK is appropriate in highly vulnerable network environments, such as open-use computer labs. If you use /LOCK, also use /CONTACTFILE to tell users what to do or whom to contact.
`/MOVE directory`	Moves all infected files found during a scan to the specified (quarantine) directory, preserving drive letter and directory structure. To preserve drive and directory structure, this option has no effect if the Master Boot Record or boot sector is infected, since these are not actually files.
`/MOVE *.???`	Replaces the /MOVE object on the command line. Causes the scanner to change the extensions on the infected files; e.g., `scan c:\test /MOVE*.BAD` would give all the infected files a .BAD extension, but would NOT actually move any of them.

Report options

The following table lists the options necessary to configure VirusScan to maintain a log of all virus scanning activity.

✍ *The option /REPORT must precede all other report options.*

To view the log file, type the following command in the VirusScan directory:

```
scan /showlog /pause
```

Command-line Option	**Description**
`/REPORT filename`	Creates a report of infected files and system errors. Saves the output of VirusScan to [filename] in ASCII text file format. If [filename] exists, /REPORT erases and replaces it. To append or add the information to the end of the file, use the /APPEND option. Make sure to include the destination drive and directory (such as `D:\VSREPRT\ALL.TXT`). If the destination is a network drive, you must have create and delete file rights.
`/ALERTPATH`	Designates the directory as a network path monitored by NetShield for centralized alerting.
`/APPEND`	By default, /REPORT creates a new report file and overwrites the old one for each VirusScan session. This option instructs /REPORT to append the report message text to the specified report file, allowing you to maintain a log file that contains all virus scanning activity.
`/RPTALL`	When used in conjunction with /REPORT, adds list of files scanned to the report file.

Command-line Option	Description
`/RPTCOR`	When used in conjunction with /REPORT, adds the names of corrupted files to the report file. A corrupted file may have been damaged by a virus. The options /RPTCOR, /RPTMOD, and /RPTERR may be used on the same command line. ✍ *Some files that require an overlay or another executable to run properly may be falsely reported as corrupted.*
`/RPTERR`	Adds a list of system errors to the report file. This option is used in conjunction with /REPORT. System errors include errors reading or writing to a diskette or hard disk, file system or network errors, problems creating reports, and other system-related problems. The options /RPTCOR, /RPTMOD, and /RPTERR may be used on the same command line.
`/RPTMOD`	Adds a list of modified files to the report file. This option is used in conjunction with /REPORT. VirusScan identifies modified files when the validation codes do not match (using the /CF or /CV options). The options /RPTCOR, /RPTMOD, and /RPTERR may be used on the same command line.
`/LOG`	Stores the time, date, and target VirusScan is being run by updating or creating a file called SCAN.LOG in the root directory of the target drive. For best results, use this option in conjunction with the /NOBREAK and /PAUSE commands

Command-line Option	Description
`/SHOWLOG`	Displays the contents of SCAN.LOG. SCAN.LOG stores the time and date VirusScan is being run by updating or creating a file called SCAN.LOG in the target directory, and 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.

Creating a scanning profile

Before creating a scanning profile, select scanning options appropriate for your environment. See “Selecting scanning options” on page 30.

To create a scanning profile, complete the following procedure:

Step	Action
1.	Using the `cd` command, change to the VirusScan directory.
2.	Type the following: `edit profile.txt` ✍ *You may choose any filename for the scanning profile and you may use any text editor to create the profile.* **Response**: The program Edit opens.
3.	Enter a scanning option (e.g. /ADL, /ADN, etc.).
4.	Press ENTER. **Response**: The cursor is moved to the next line.
5.	Repeat steps 3 and 4 until all options are entered.
6.	To save the file, press ALT+F to access the File menu then press S to save.
7.	To exit and return to the command prompt, press ALT+F to access the File menu then press X to exit. **Response**: The file is created. To run the file, see “Running the scanning profile,” below.

Running the scanning profile

To run the scanning profile, complete the following procedure.

Step	Action
1.	Using the `cd` command, change to the VirusScan directory.
2.	Type the following: `scan /load filename` where *filename* is the name of the scanning profile. **Response**: VirusScan runs according to the options specified in the scanning profile. ✍ *To automate a scan during start-up, add this command to your AUTOEXEC.BAT file.*

Configuring Validation Options

The Validation features in VirusScan help discover and isolate new or unknown viruses. Validation works by storing codes in executable files. During a scan, the authenticity of the codes is verified. If the codes change, VirusScan will inform you.

✍ *Do not use Validation on data files or files that change frequently. This will generate false alarms.*

Storing validation codes

Use the following options to create validation information.

Command-line Option	Description
`/AF filename`	Stores validation codes in [filename]. /AF logs validation and recovery data for executable files, the boot sector, and Master Boot Record in a file you specify. The log file is about 89 bytes per file validated. You must specify a filename, including the full path. If the target path is a network drive, you must have create and delete file rights on that drive. If the specified filename exists, VirusScan updates it. /AF increases scanning time by about 300%. Using any of the /AF, /CF, or /RF options together in a command line returns an error. ✍ */AF performs the same function as /AV, but stores its data in a separate file rather than changing the executable files themselves.*

Command-line Option	**Description**
`/AV`	/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 network drive, you must have write access rights. To exclude self-modifying or self-checking files, and damaged files that might cause false alarms, use the /EXCLUDE option. Using any of the /AV, /CV, or /RV options together in the same command line returns an error. ✍ *The /AV option does not store any information about the Master Boot Record or boot sector of the drive being scanned.*
`/EXCLUDE filename(s)` or `directory`	Excludes any files listed in [filename] from the scan. This option allows you to exclude files from /AF and /AV validation and /CF and /CV checking. Also can be used to exclude directories and multiple files; e.g., `c:\dos` excludes all c:\dos directory files, and `c:\dos\fo` excudes all c:\dos\fo*.* files. ✍ *Self-modifying or self-checking files can cause a false alarm during a scan.*

Scanning using Validation

Use the following options to scan for new or unknown viruses using the Validation codes generated in "Storing validation codes" on page 40.

✍ *These lines may be added to your scanning profile. For more information, see “Creating a scanning profile” on page 38.*

Command-line Option	**Description**
`/CF filename`	Checks validation data stored by the /AF option in [filename]. If a file or system area changes, VirusScan reports that a virus infection may have occurred. The /CF option increases scanning time by about 250%. Using any of the /AF, /CF, or /RF options together in the same command line returns an error. ✍ *Some older Hewlett-Packard and Zenith PCs modify the boot sector each time the system is started. If you use /CF, VirusScan will continuously report that the boot sector was modified. Check your computer’s reference manual to determine whether the system has self-modifying boot code.*
`/CV`	Checks validation data added by the /AV option. If a file is modified, VirusScan reports that a virus infection may have occurred. The /CV option increses scanning time by about 50%. Using any of the /AV, /CV, or /RV options together in the same command line returns an error. ✍ *The /CV option does not check the boot sector for changes.*

Removing Validation codes

Use the following options to remove Validation codes.

Command-line Option	Description
`/RF filename`	Removes recovery and validation data from [filename] created by the /AF option. If [filename] resides on a shared network drive, you must have delete file rights on that drive. Using any of the /AF, /CF, or /RF options together in the same command line returns an error.
`/RV`	Removes validation and recovery data from files validated with the /AV option. To update files on a shared network drive, you must have access and update rights. Using any of the /AV, /CV, or /RV options together in the same command line returns an error.

Viewing the Virus List

The Virus List is a comprehensive list of viruses detected by VirusScan. The list provides a description of the viruses, including the infector type, virus characteristics, virus size, and cleaning status. To view the list of viruses detected by VirusScan, complete the following procedure:

Step **Action**

1. Using the `cd` command, change to the VirusScan directory.
2. Type the following command:

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

   Response: The virus list is saved as `filename.txt`

   ✍ *To view the Virus List without saving it to a file, type* `scan /virlist`*. Since VirusScan can detect many viruses and this file is more than 250 pages long, McAfee recommends using the command line* `scan /virlist /pause`*.*

Scanning Your Diskettes

Although the on-access scanning component of VirusScan (VShield) monitors for viruses, you should scan all diskettes used on your system. Most viruses invade your system when you boot from an infected diskette, attempt to boot from an infected diskette, or when you copy, run, or install programs or files that are infected.

✍ *Always make sure your diskette drives are empty before turning on your computer. A diskette does not have to be bootable for the system to catch a boot sector virus from it.*

Whenever you insert unknown diskettes in your drive—including diskettes received from friends, co-workers, and others—run VirusScan before executing, installing, or copying their files. To scan diskettes, complete the following procedure.

Step	Action
1.	Using the `cd` command, change to the VirusScan directory.
2.	Type the following command: `scan a: /many`
3.	Insert the first diskette to scan and press ENTER. **Response:** The diskette is scanned and the names of any infected files are displayed. ✍ *If VirusScan detects a virus on this diskette, it will carry out the command-line option you chose for dealing with the virus. See “Removing a virus found in a file” on page 49 for details on virus removal.*
4.	Insert the next diskette and press ENTER. Repeat this step for all diskettes you wish to scan.

5

Removing a Virus

If You Suspect You Have a Virus

If you have or suspect you have a virus before installing VirusScan, follow this procedure to create a virus-free environment.

Step	Action
1.	Turn off your computer. ✍ *Do not reboot using the reset button or* CTRL+ALT+DELETE*; if you do, some viruses might remain intact or drop destructive payloads.*
2.	Place a clean start-up diskette into the floppy disk drive. If you do not have a clean start-up diskette, see “Making a Clean Start-up Diskette” on page 57.
3.	Turn on your computer.
4.	At the command prompt, type `scan /ADL /ALL /CLEAN`.

If viruses were removed

If VirusScan successfully removes all the viruses, shut down your computer and remove the diskette. Begin the installation procedure described in Chapter 2, “Installing VirusScan.”

To find and eliminate the source of infection, scan your diskettes immediately after installation. For information on scanning your diskettes, see “Scanning Your Diskettes” on page 45.

If viruses were not removed

If VirusScan cannot remove a virus, you will receive one of the following messages:

```
Virus could not be removed.
```

```
There is no remover currently available for the virus.
```

If the virus was found in a file and cannot be removed by VirusScan, delete the file and restore from backups. If the virus was found in the Master Boot Record, refer to documents on the McAfee website related to manually removing viruses. For more information, see “How to Contact McAfee” on page 13.

If VirusScan Detects a Virus

Viruses attack computer systems by infecting files—usually executable program files or Microsoft Word documents and templates. VirusScan can safely remove most common viruses from infected files and repair any damage.

Some viruses, however, are designed to damage your files beyond repair. These irreparably damaged files, called “corrupted” files, can be moved by VirusScan to a quarantine directory or deleted permanently to prevent another virus infection of your system.

Removing a virus found in memory

If VirusScan discovers a memory-resident virus, complete the following steps:

Step	**Action**
1.	Turn off your computer.
	✍ *Do not reboot using the reset button or* CTRL+ALT+DELETE*; if you do, some viruses might remain intact or drop their destructive payloads.*
2.	Place a clean start-up diskette into the floppy disk drive. If you do not have a clean start-up diskette see “Making a Clean Start-up Diskette” on page 57.
3.	Turn on your computer.
4.	At the command prompt, type `scan /ADL /ALL /CLEAN` .

If viruses were removed

If VirusScan successfully removes all the viruses, shut down your computer and remove the diskette. Begin the installation procedure again, as described in Chapter 2, “Installing VirusScan.”

To find and eliminate the source of infection, scan your diskettes immediately after installation. For information on scanning your diskettes, see “Scanning Your Diskettes” on page 45.

If viruses were not removed

If VirusScan cannot remove a virus, you will receive the message:

```
Virus could not be removed.

There is no remover currently available for the virus.
```

If the virus was found in a file and cannot be removed by VirusScan, you should delete the file and repeat the steps described in “If You Suspect You Have a Virus” on page 46. If the virus was found in the Master Boot Record, refer to documents on the McAfee website related to manually removing viruses. For more information, see “How to Contact McAfee” on page 13.

Removing a virus found in a file

If VirusScan detects a virus in a file, it will display the `path/names` of infected files and take the action specified in the scanning profile or command-line options. (See “Advanced Scanning” on page 30.) For example:

- If you selected /MOVE, VirusScan will automatically move the infected files to the specified quarantine directory.
- If you selected /CLEAN, VirusScan will attempt to repair the file.
- If you selected /DEL, VirusScan will delete and permanently overwrite the infected file.

Cleaning macro viruses from password-protected files

✍ *VirusScan detects macro virus infections in password-protected Microsoft Word 95 (Word 7.0) files in at least six languages.*

VirusScan is designed to respect users' passwords and leave them intact as often as possible. For example, in password-protected Microsoft Excel 95 files, VirusScan removes macro viruses without disturbing users’ passwords.

Macro viruses that infect Microsoft Word files, however, sometimes plant their own passwords. Depending on the capabilities of the particular virus, VirusScan will take one of the following actions when it is instructed to clean a password-protected file:

- If the macro virus cannot plant its own password: VirusScan notes the infection but does not clean it.
- If the macro virus can plant its own password: VirusScan cleans the file, removing the password along with the virus.

Understanding false alarms

A false alarm is a report of a virus in a file or in memory when a virus does not actually exist. False alarms are more likely if you are using more than one brand of virus protection software, because some anti-virus programs store their virus signature strings unprotected in memory. As a result, VirusScan may “detect” them falsely as a virus.

Always assume that any virus reported by VirusScan is real and dangerous and take steps to remove it from your system. If, however, you have reason to believe that VirusScan is generating false alarms (e.g., it detected a virus in a file that you have been using safely for years), refer to the list of potential sources below:

- If more than one anti-virus program is running, VirusScan may report a false alarm. Set up your computer so only one anti-virus program is running at a time. Remark out lines in the AUTOEXEC.BAT file that refer to other anti-virus programs. Turn off your computer, wait a few seconds, and turn it on again so all code from other anti-virus programs is cleared from memory.

- Some BIOS chips include an anti-virus feature that could be the source of false alarms. Refer to your computer’s reference manual for details.

- If you set up validation codes, subsequent scans can detect changes in validated files. If the executable files are self-modifying or self-checking, this can trigger false alarms. When using validation codes, specify an exceptions list to exclude such files from checking.

- Some older Hewlett-Packard and Zenith PCs modify the boot sector each time the system is booted. VirusScan may detect these modifications as a possible infection. Check your computer’s reference manual to determine if your PC has self-modifying boot code. To solve this problem, save validation information to the executable files themselves; this method does not save information about the boot sector or Master Boot Record. See “Storing validation codes” on page 40.

- VirusScan may report viruses in the boot sector or Master Boot Record of certain write-protected diskettes.

A

Preventing Virus Infection

Keys to a Secure System Environment

VirusScan is an effective tool for preventing, detecting, and recovering from virus infection. It is most effective, however, when used in conjunction with a comprehensive computing security program that includes a variety of safety measures, such as regular backups, meaningful password protection, user training, and awareness.

To create a secure system environment and minimize your chance of infection, McAfee recommends that you take the following steps:

Step	**Action**
1.	Follow the installation procedures as outlined in Chapter 2, “Installing VirusScan.” ✍ *If you suspect you have a virus, take steps to clean your system before installing VirusScan. See “If You Suspect You Have a Virus” on page 46.*
2.	Create a DOS start-up diskette containing the VirusScan command-line program by following the procedure outlined in “Making a Clean Start-up Diskette” on page 57. Make sure the diskette is write protected so that it cannot become infected.
3.	Make frequent backups of important files. Even with VirusScan, some viruses (as well as fire, theft, vandalism, or ordinary disk failure) can render a disk unrecoverable without a recent backup.
4.	Scan all diskettes. See “Scanning Your Diskettes” on page 45.

5. Never start your computer from an unchecked diskette. Always make sure your disk drives are empty before starting your computer.

6. Re-scan whenever you introduce new programs onto your computer. If you download or install software from a network server, bulletin board, World Wide Web or online service, run VirusScan on the directory you placed the new files in before running the software.

Outlining a full security program is beyond the scope of this manual. However, by following the steps provided in this appendix and reading the information provided in Appendix B, “Understanding Viruses,” you can gain a clearer understanding of what viruses are, how they affect your system, and what you can do to prevent an infection.

Detecting New Viruses

There are two ways for you to deal with new viruses that may infect your system:

- Update your VirusScan data files
- Validate the VirusScan program files

Updating your VirusScan data files

To offer the best virus protection possible, McAfee continually updates the files VirusScan uses to detect viruses. After a certain time period, you are notified that you need to update the virus definition database. McAfee recommends that you update these files on a regular basis for maximum protection.

What is a data file?

The files CLEAN.DAT, NAMES.DAT, and SCAN.DAT all provide virus information to the VirusScan software. These are the data files we're referring to in this section.

Why would I need a new data file?

New viruses are discovered at a rate of more than 200 per month. Often, these new viruses are not detected using older data files. The data files that came with your copy of VirusScan might not be able to help VirusScan detect a virus that was discovered months after you bought the product.

McAfee's virus researchers are working constantly to update the data files with more and newer virus definitions. The new data files are released approximately every four to six weeks.

✍ *McAfee cannot guarantee backward compatibility of the virus signature files with a previous version's software. By subscribing to a maintenance plan and upgrading your VirusScan software, you ensure complete virus protection for at least one year after your VirusScan purchase.*

Updating the data file

To update your McAfee data files, take the following steps.

Step **Action**

1. Download the data file (for example, DAT-3009.ZIP) from one of McAfee’s electronic services. On most services, it is located in the anti-virus area.

✍ *Please note that your ability to access these updates is legally restricted by the maintenance terms outlined in the README.1ST file accompanying the software and detailed in the software license agreement. See “McAfee Support Services” on page 63 for more information.*

2. Copy the file to a new directory.

3. The file is in a compressed format. Decompress the file using any PKUNZIP-compatible decompression software. If you don’t have the decompression software, you can download PKUNZIP (shareware) from McAfee electronic sites.

4. Locate the directories on your hard drive where your VirusScan software is currently loaded. Typically, the files are stored in C:\MCAFEE\VIRUSCAN.

5. Copy the new files into the directory or directories, overwriting the old data files.

✍ *There might be part of the software in more than one directory. If so, place the updated files in each directory.*

6. Reboot your computer so that changes take place immediately.

Validating the VirusScan program files

When you download a file from any source other than the McAfee bulletin board on other McAfee service, it is important to verify that it is authentic, unaltered, and uninfected. McAfee anti-virus software includes a utility program called Validate that you can use to ensure that your version of VirusScan is authentic. When you receive a new version of VirusScan, run Validate on all of its program files and .DAT files. For details on the Validate program, see the README.1ST text file that accompanied your software.

Making a Clean Start-up Diskette

In case your system becomes infected, you should have a clean start-up (boot) diskette. This section describes how to create that boot diskette.

✍ *Your system must be virus-free to make a boot diskette. Any virus residing in your system could be transferred to your boot diskette and reinfect your system. If your computer is infected, go to another computer, scan it, and if it is virus-free, follow the steps below.*

Start this procedure from a command-line prompt (`C:\>`) and complete the following procedure:

✍ *Exit from Windows or any applications to get the command-line prompt.*

Step **Action**

1. Insert a blank diskette in drive A:.

2. Format the diskette by typing the following command at the `C:\>` prompt:

   ```
   format a: /s /u
   ```

   This overwrites any information already on the diskette.

   ✍ *If you are using DOS 5.0 or earlier, do not type the* `/u`. *If you are unsure of which version you are using, type* `ver` *at the* `C:\>` *prompt.*

3. When the system prompts you for a volume label, enter an appropriate name using no more than eleven characters.

4. Change to the VirusScan directory by typing the following command at the `C:\>` prompt:

   ```
   cd mcafee\viruscan
   ```

5. Copy the command-line version of VirusScan to the diskette by typing the following commands at the prompt:

```
copy scan.exe a:

copy scan.dat a:

copy clean.dat a:

copy names.dat a:
```

6. Change to the DOS directory by typing:

```
cd c:\dos
```

7. Copy useful command-line programs to the diskette:

   - debug.*
   - diskcopy.*
   - fdisk.*
   - format.*
   - label.*
   - mem.*
   - sys.*
   - xcopy.*

✍ *If you use a disk compression utility or a password encryption utility, be sure to copy the drivers required to access your drives onto the clean boot diskette. See the documentation for those utilities for more information about those drivers.*

8. For optimal performance of your boot diskette, create a file called CONFIG.SYS and add the following lines:

   ```
   [CONFIG.SYS]

   DEVICE=HIMEM.SYS
   DOS=HIGH
   ```

9. Label and write protect this diskette, then store it in a secure place. See "Write Protecting a Diskette" on page 60 for more information.

Write Protecting a Diskette

Floppy diskettes are convenient, portable devices for storage and retrieval of computer data. Diskettes are used to save files (write) and recover files (read). They are also the most common vehicle viruses use to invade your computer's system.

One way to help avoid infection via floppy diskette is to *write protect* the diskettes you are using for read-only data. If your system becomes infected with a virus, the write-protection feature keeps your diskettes from also becoming infected, preventing reinfection after your system is cleaned.

✍ *Any diskettes that are not write protected should be scanned and cleaned before you write protect them.*

Write protecting 3.5” floppy diskettes

Step	**Action**
1.	Position the diskette face down with the metal slide facing you.
2.	Examine the small rectangular hole on the upper left side. There should be a square, plastic tab that you can slide up and down across the hole. To write protect the diskette, slide the plastic tab upward toward the edge of the diskette so that the hole is open This stops you from accidentally changing data on the disk. It also prevents viruses from infecting the diskette.

✍ *If there is no tab and the hole is open, the diskette is permanently write protected.*

Write protecting 5.25” floppy diskettes

Step	Action
1.	Position the diskette face up with the label facing away from you. The notch on the upper right hand side is called the *write-protect* notch. When you can see this notch, you can read and write data to and from the diskette. When the notch is covered with an adhesive tab, you can no longer write to the diskette. This stops you from accidentally changing data on the disk. It also prevents viruses from infecting the diskette.
2.	Cover the notch with an adhesive tab or tape to write protect the diskette.

B

Testing Your Installation

The Eicar Standard AntiVirus Test File is a combined effort by anti-virus vendors throughout the world to come up with one standard by which customers can verify their anti-virus installations. To test your installation, copy the following line into its own file and name it EICAR.COM.

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

✍ *The characters in the test file must all appear on one line*

When finished, you will have a 69- or 70-byte file.

When VirusScan is applied to this file, it will report finding the EICAR-STANDARD-AV-TEST-FILE virus.

It is important to know that THIS IS NOT A VIRUS. However, users often have the need to test that their installations function correctly. The anti-virus industry, through the European Institute for Computer Antivirus Research, has adopted this standard to facilitate this need.

Delete the file when installation testing is completed so unsuspecting users are not unnecessarily alarmed.

✍ *Because the Eicar Standard AntiVirus Test File is not a true virus infection, you will not be able to clean or repair the infected file.*

C

McAfee Support Services

McAfee is pleased to offer many different types of technical assistance to customers. These flexible support programs are designed to meet the needs of individuals and businesses at any level. By offering support solutions that range from a complimentary 90-day introductory technical support program to an optional one-year personal online maintenance and support program, McAfee helps to ensure that you receive the level of technical assistance you require.

McAfee also offers a variety of technical assistance plans designed to meet the needs of business customers, including training, consulting, enterprise support, and a Jump Start program. Please review each of the different support service plans and benefits listed in this appendix and pick the one best suited for you.

✍ *The term update refers only to the virus definition files; the term upgrade refers to product version revisions, executables, and definition files. McAfee offers free online virus signature file updates (.DATs) for the life of your product. However, we cannot guarantee backward compatibility of the signature files with previous versions' executable files (.EXEs). By upgrading your software to the latest product version and latest .DAT files, you ensure complete virus protection for the term of your software subscription or maintenance plan.*

Customer Service Programs

Free 90-day introductory support program

All registered owners of single-node (one computer) products, such as those purchased at local retail stores or downloaded from the McAfee Mall on our website, are entitled to:

- Free online virus updates (new .DAT files)
- One free online product upgrade (product version revision) with the newest features within 90 days of purchase
- Free support services listed below

Support services

- Electronic and online support, available 24 hours a day, seven days a week on each of the forums listed below:
  - Automated voice and fax system: (408) 988-3034
  - McAfee BBS (electronic bulletin board system): (408) 988-4004
  - World Wide Web site: http://www.mcafee.com
  - CompuServe: GO MCAFEE
  - America Online: keyword MCAFEE
- Technical support phone assistance, available during regular business hours, 6:00 A.M.– 6:00 P.M. Pacific time, Monday through Friday, from our professionally trained support representatives at (408) 988-3832.

To receive your free one-time online upgrade, please contact our Customer Care department at (408) 988-3832. Please supply your proof of purchase when you request the upgrade. You will be given a password to the upgrade area on either the McAfee BBS, FTP site, or World Wide Web site so that you can download a registered version of the latest product. This password is valid for one access only.

Free subscription maintenance and support program

McAfee offers all registered owners of licensed multiple-node (ten computers or more) subscription products the following free support services and maintenance during the two-year term of the software subscription.

✍ *You must be registered to receive these services.*

Support services

- Electronic and online support, available 24 hours a day, seven days a week on each of the forums listed below:
    - Automated voice and fax system: (408) 988-3034
    - McAfee BBS (electronic bulletin board system): (408) 988-4004
    - World Wide Web site: http://www.mcafee.com
    - CompuServe: GO MCAFEE
    - America Online: keyword MCAFEE
- Technical support phone assistance during regular business hours, 6:00 A.M.–6:00 P.M. Pacific time, Monday through Friday, from our professionally trained support representatives at (408) 988-3832.
- Two years of free online product upgrades with the newest features and virus definition data. If you upgrade your operating system, you can also extend the upgrade of your McAfee product to the new platform.

Optional support plans

✍ *Contact McAfee for current pricing structures.*

Option 1: One-year personal support plan

For registered owners of single-node products who want to extend their support coverage, this plan allows you to call in for unlimited technical support, download the latest virus protection updates each month, and periodically download upgrades from any of McAfee’s registered online services—all for a full year. If you upgrade your operating system, you can also upgrade your product program to the new platform.

Option 2: One-year quarterly disk/CD-ROM maintenance and support programs

This plan is for registered owners of either single- or multiple-node subscription products. It offers all the features of Option 1, while adding a quarterly mailing of software upgrade diskettes or CD-ROMs (depending on the product) and a quarterly update newsletter. With this option, you can update your product to include the latest features and virus data files without having to download from an online service.

Each optional support plan begins as soon as you purchase the product and is good for one year, at which time you can renew your support program through McAfee’s Customer Care department at (408) 988-3832.

✍ *McAfee reserves the right to change part or all of its Customer Service Programs at any time without notice.*

Professional Services Programs

McAfee Professional Services provide a wide range of on-site services. Whether for short-term assistance or long-term strategic planning, a highly qualified consultant can help you achieve positive results. McAfee consultants are trained on NetWare, Microsoft NT Advanced Server, Windows 95, and a multitude of desktop applications.

Before work begins, a project manager discusses the project scope and objective with you and comes to a mutual agreement on the job objective. When the consultant leaves the site, you can be sure that the objective has been achieved.

Training

McAfee's expertise and experience is available to your personnel, allowing an organization to take full advantage of its computing resources. McAfee offers on-site training on all McAfee products, network management seminars, anti-virus seminars, customized curriculums for site-specific applications as well as product and personnel certification. McAfee's consultants provide extensive training with curriculum tailored to your organization's needs.

Consulting

McAfee Professional Services offer a number of hourly and daily consulting services including:

- Troubleshooting an existing installation
- Writing PowerScript or SaberBASIC scripts
- Planning and designing networks
- Installing and configuring McAfee products
- Configuring Windows 95
- One-on-one consulting

McAfee Professional Services are available on a quotable time and materials basis to perform project management, product research, and a number of other consulting services.

Jump Start program

This fixed-fee consulting program is designed to get clients up and running on McAfee products as soon as possible. It includes training, installation, and configuration services as needed on a single server. It is designed to demonstrate how to connect various PCs to the LAN, train administrators how to use the program, and master the roll-out process.

Enterprise support

McAfee’s Enterprise Support Program provides customers with the highest level of support possible. This fee-based program is designed for those customers who need a higher level of personal service.

The Enterprise Support Program offers the following features:

- Direct pager number to your assigned senior Enterprise Support Program analyst
- Extended support hours: 7:00 A.M. to 7:00 P.M. Central time, Monday through Friday
- Five designated McAfee contacts
- Proactive support, providing updated company and product information as it becomes available
- On-site services at a 25% discount
- VIP issues review list
- Beta site (if desired)

Every Enterprise Support Representative calls clients each week. This phone call is used to forward any information such as technical notes and application anomalies of which you should be aware. This call also ensures that you have no unresolved problems or complications with the product. Enterprise Support representatives will return your page on the day it is received.

Optional 7 x 24 enterprise support

Frequently, customers are responsible for their own LANs, which run 24 hours a day, seven days a week. This feature offers round-the-clock support for clients requiring support outside normal business hours.

✍ *McAfee reserves the right to change part or all of its Professional Services Programs at any time without notice.*

D

Reference

VirusScan Command-line Options

The following table lists all of the VirusScan options. For information on basic scanning, see “Basic Scanning” on page 26.

✍ *When specifying a filename as part of a command-line option, you must include the full path to the file if it is not located in the directory where VirusScan is installed.*

Command-line Option	Description
`/?` or `/HELP`	Does not scan. Instead, displays a list of valid VirusScan command-line options with a brief description of each. Use either of these options alone on the command line (with no other options).
`/ADL` For OS/2, includes CD-ROM when used with `/NODDA`	Scans all local drives (including compressed and PCMCIA drives, but not diskettes), 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.
`/ADN` For OS/2, use `/ADL,` above, plus `/NODDA` for CD-ROM	Scans all network drives (including CD-ROM) for viruses, in addition to those specified on the command line. To scan both the local drives and network drives, use /ADL and /ADN together in the same command line.

Command-line Option	**Description**
`/AF filename`	Stores validation codes in [filename]. Helps you detect new or unknown viruses. /AF logs validation and recovery data for executable files, the boot sector, and Master Boot Record on a hard disk or diskette in a file you specify. The log file is about 89 bytes per file validated. You must specify a [filename], including the full path. If the target path is a network drive, you must have rights to create and delete files on that drive. If [filename] exists, VirusScan updates it. /AF increases scanning time by about 300%. ✍ */AF performs the same function as /AV, but stores its data in a separate file rather than changing the executable files themselves.* *The /AF option does not store any information about the Master Boot Record or boot sector of the drive being scanned.*
`/ALERTPATH`	Designates a directory as a network path monitored by centralized alerting.
`/ALL`	Overrides the default settings by scanning all infectable files. This option substantially increases the scanning time required. Use it if you have found a virus or suspect one. ✍ *The list of extensions for standard executables has changed from previous releases of VirusScan.*
`/APPEND`	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.

Command-line Option	Description
`/AV`	To help 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. To exclude self-modifying or self-checking files, and damaged files that might cause false alarms, use the /EXCLUDE option. Using any of the /AV, /CV, or /RV options together in the same command line returns an error. ✍ *The /AV option does not store any information about the Master Boot Record or boot sector of the drive being scanned.*
`/BOOT`	Scans only the boot sector and Master Boot Record on the specified drive.
`/CF 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, VirusScan reports that a viral infection may have occurred. The /CF option increases scanning time by about 250%. Using any of the /AF, /CF, or /RF options together in a command line returns an error. ✍ *Some older Hewlett-Packard and Zenith PCs modify the boot sector each time the system is booted. If you use /CF, VirusScan continuously reports that the boot sector has been modified even though no virus may be present. Check your computer's reference manual to determine whether your PC has self-modifying boot code.*
`/CLEAN`	Cleans viruses from infected files and system areas.

Command-line Option	Description
`/CLEANDOC`	Cleans viruses from infected Microsoft Word and Office document files only.
`/CLEANDOCALL`	Cleans all macros from Microsoft Word and Office documents. ✍ *This option deletes all macros, including macros not infected by a virus.*
`/CONTACTFILE filename`	Identifies a file containing a 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 on each workstation. Any character is valid except a backslash (\\). Messages that begin with a slash (/)or a hyphen (-) should be placed in quotation marks.
`/CV`	Helps you detect new or unknown viruses. Checks validation data added by the /AV option. If a file is modified, VirusScan reports that a viral infection may have occurred. The /CV option increases scanning time by about 50%. Using any of the /AV, /CV, or /RV options together in the same command line returns an error. ✍ *The /CV option does not check the boot sector for changes.*
`/DEL`	Deletes infected files permanently.
`/EXCLUDE filename(s) or directory name`	Excludes any files listed in [filename] from the scan. This option allows you to exclude files from /AF and /AV validation and /CF and /CV checking. Also can be used to exclude directories and multiple files; e.g., `c:\dos` excludes all c:\dos directory files, and `c:\dos\fo` excudes all c:\dos\fo*.* files. ✍ *Self-modifying or self-checking files can cause a false alarm during a scan.*

Command-line Option	**Description**
`/FAST`	Speeds up the scan. Reduces scanning time by about 15%. Using the /FAST option, VirusScan examines a smaller portion of each file for viruses. 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.
`/FORCE`	Uses generic Master Boot Record when cleaning partition table viruses. Cleans infected boot sectors of diskettes. Works even if a remover is not yet available for the boot sector virus.
`/FREQUENCY hours`	The number of hours that must occur between subsequent successful scans (Example: `/FREQUENCY 1`). 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.
`/?` or `/HELP`	Displays a list of VirusScan command-line options with a brief description of each. Use either of these options alone on the command line (with no other options).
`/LOAD filename`	Performs a scan using the information saved in [filename]. You can store all custom settings in a separate configuration file (an ASCII text file), then use /LOAD to load those settings from that file.

Command-line Option	Description
`/LOCK` Not valid for OS/2	Halts the system to stop further infection if VirusScan finds a virus. /LOCK is appropriate in highly vulnerable network environments, such as open-use computer labs. If you use /LOCK, we recommend you use it with /CONTACTFILE to tell users what to do or whom to contact if a virus is found and the system locks up.
`/LOG`	Stores the time and date VirusScan is being run by updating or creating a file called SCAN.LOG in the root of the target drive.
`/LONGYEAR`	Reports dates on-screen and in generated reports in four-digit format, i.e., 1998. (The default is two-digit, i.e., 98.)
`/MANY`	Scans multiple diskettes consecutively in a single drive. VirusScan prompts you for each diskette. Once you have established a virus-free system, use this option to check multiple diskettes quickly. The VirusScan program should reside on a disk that will not be removed during the scan. For example, if you are scanning disks in the computer's A: drive, and you are running the program from a disk in the A: drive, the program will become unavailable as soon as you remove the diskette to put another in. The following command causes an error during execution: `a:\scan a: /many`
`/MAXFILESIZE xxx.x`	Scans only files under the specified size (xxx.x) in megabytes
`/MEMEXCL` Not valid for OS/2	Exclude memory area from scanning. (The default is A000-FFFF, 0000=Scan all.) This command-line option has been added to prevent VirusScan from checking areas in upper memory which might contain memory-mapped hardware and might cause false alarms.

Command-line Option	Description
`/MOVE directory`	Moves all infected files found during a scan to the specified directory, preserving drive letter and directory structure. To preserve drive and directory structure, this option has no effect if the Master Boot Record or boot sector is infected, since these are not actually files.
`/MOVE *.???`	Replaces the /MOVE object on the command line. Causes the scanner to change the extensions on the infected files; e.g., `scan c:\test /MOVE*.BAD` would give all the infected files a `.BAD` extension, but would NOT actually move any of them.
`/NOBEEP`	Disables the tone that sounds whenever VirusScan finds a virus.
`/NOBREAK`	Disables CTRL-C and CTRL-BREAK during scans. Users will not be able to halt scans in progress using CTRL-C or CTRL-BREAK. Use this option in conjunction with /LOG to create a meaningful audit trail of regularly scheduled scans.
`/NOCOMP`	Skips checking of compressed executables created with the LZEXE or PkLite file-compression programs. Reduces scanning time when a full scan is not needed. Otherwise, by default, VirusScan checks inside executable, or self-decompressing, files that have been created using the LZEXE or PkLite file-compression programs. VirusScan decompresses each file in memory and checks for virus signatures, which takes time but results in a more thorough scan. If you use /NOCOMP, VirusScan does not check inside compressed files for viruses, although it can check for modifications to those files if they have been validated using validation codes.

Command-line Option	Description
`/NODDA`	No direct disk access. Prevents VirusScan from accessing the boot record. This feature has been added to allow VirusScan to run under Windows NT. You might need to use this option on some device-driven drives. ✍ *Using /NODDA with the /ADN or /ADL switches may generate errors when accessing empty CD-ROM drives or empty Zip drives. If this occurs, typing F (for Fail) in response to the error messages will allow the scan to continue.*
`/NODOC`	Does not scan Microsoft Office files.
`/NOEMS` Not valid for OS/2 Not valid for ScanPM	Prevents VirusScan from using expanded memory (LIM EMS 3.2), ensuring that EMS is available to other programs.
`/NOEXPIRE`	Disables the “expiration date” message if the VirusScan data files are out of date.
`/NOMEM` Not valid for OS/2	Reduces scan time by omitting all memory checks for viruses. Use /NOMEM only when you are absolutely certain that your computer is virus-free. VirusScan can check system memory for all critical known computer viruses that can inhabit memory. In addition to main memory from 0KB to 640KB, VirusScan 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 not presently susceptible to viruses.

Command-line Option	Description
`/PAUSE`	Enables screen pause. If you specify /PAUSE, the "Press any key to continue" prompt appears when VirusScan fills up a screen with messages (for example, when you're using the /SHOWLOG or /VIRLIST options). Otherwise, by default, VirusScan fills and scrolls a screen continuously without stopping, which allows VirusScan 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 VirusScan's messages using the report options (/REPORT, /RPTCOR, /RPTMOD, and /RPTERR).
`/PLAD` Not valid for ScanPM	Preserve last access dates (on proprietary drives only). Prevents changing the last access date attribute for files stored on a network drive in a proprietary network. Normally, proprietary network drives update the last access date when VirusScan 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.

Command-line Option	**Description**
`/REPORT filename`	Creates a report of infected files and system errors. Saves the output of VirusScan to [filename] in ASCII text file format. If [filename] exists, /REPORT erases and replaces it (or, if you use /APPEND, adds the report information to the end of the existing file). 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 /RPTALL, /RPTCOR, /RPTMOD, and /RPTERR to add scanned files, corrupted files, modified files, and system errors to the report.
`/RF 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.
`/RPTALL`	Adds list of files scanned to the report file (used with /REPORT).
`/RPTCOR`	When used in conjunction with /REPORT, adds the names of corrupted files to the report file. A corrupted file may be a file that has been damaged by a virus. You can use /RPTCOR with /RPTMOD and /RPTERR on the same command line. ✍ *There may be false readings in some files that require an overlay or another executable to run properly (that is, a file that is not executable on its own).*

Command-line Option	Description
`/RPTERR`	Adds a list of system errors to the report file. This option is used in conjunction with /REPORT. 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`	Adds list of modified files to the report file. This option is used in conjunction with /REPORT. VirusScan identifies modified files when the validation codes do not match (using the /CF or /CV options). You can use /RPTMOD with /RPTCOR and /RPTERR on the same command line.
`/RV`	Removes validation and recovery data from files validated with the /AV option. 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`	Displays the contents of SCAN.LOG. SCAN.LOG stores the time and date VirusScan is being run by updating or creating a file called SCAN.LOG in the target directory and 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.

Command-line Option	Description
`/SUB`	Scans subdirectories inside a directory. By default, when you specify a directory to scan rather than a drive, VirusScan will examine only the files it contains, not its subdirectories. Use /SUB to scan all subdirectories inside any directories you have specified. Do not use /SUB if you are scanning an entire drive.
`/VIRLIST`	Displays the name and a brief description of each virus 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, enter: `scan /virlist > filename.txt` ✍ *Because VirusScan can detect many viruses, this file is more than 250 pages long.*

VirusScan Error Levels

When you run VirusScan in the DOS environment, a DOS error level is set. 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.*

VirusScan can return the following error levels:

ERRORLEVEL	Description
0	No errors occurred; no viruses were found.
1	Error occurred while accessing a file (reading or writing).
2	A VirusScan data (*.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 has occurred (out of memory error).
7	An error occurred 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) specified in the command line.
10	A virus was found in memory.
11	An internal program error occurred.

ERRORLEVEL	Description
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 were found in the Master Boot Record, boot sector, or files.
14	The SCAN.DAT file is out of date; update VirusScan data files.
15	VirusScan self-check failed; it may be infected or damaged.
16	An error occurred while accessing a specified drive or file.
18	A validated file has been modified (/CF or /CV options).
19	Multiple viruses were detected and removed.
20	The /FREQUENCY option prevented scanning.
21-99	Reserved.
100+	Operating system error; VirusScan adds 100 to the original number.
102	CTRL+C or CTRL+BREAK was used to interrupt the Scan. (You can disable CTRL+C or CTRL+BREAK with the /NOBREAK command-line option.)

Glossary

The following list defines some terms you might encounter while using VirusScan to guard your computer against viruses.

BIOS

A read-only memory chip that contains the coded instructions for using hardware such as a keyboard or monitor. Always present in portable computers, a BIOS (boot ROM) is not susceptible to infection (unlike the boot sector on a disk). Some BIOS chips contain anti-virus features that can generate a false alarm, installation failure, and other problems.

boot

To start a computer. The computer will load start-up instructions from a disk's boot ROM (BIOS) or boot sector. See also "cold boot" and "warm boot."

boot disk

A write-protected diskette that contains the computer's system and start-up files. You can use this diskette to start up your computer. It is important to use a virus-free boot disk to guarantee that a virus is not introduced into the computer.

boot sector

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

boot sector infection

Contamination of the boot sector by a virus. A boot sector infection is particularly dangerous because information in the boot sector is loaded into memory first, *before* virus protection code can be executed. The only certain way to eliminate a boot sector infection is to start your computer from a clean start-up diskette, then remove the infection using VirusScan.

cold boot

To turn on a computer, or to restart a computer by turning it off, waiting a few seconds, and turning it on again. Other methods of restarting (such as pressing a reset button or pressing CTRL+ALT+DEL) may not remove all traces of a virus infection from memory. See also "boot" and "warm boot."

compressed executable

A file that has been compressed using a file compression utility such as LZEXE or PkLite. See also "compressed file."

compressed file

A file that has been compressed using a file compression utility such as PKZIP or LZEXE. See also "compressed executable."

conventional memory

Up to 640KB of main memory in which DOS executes programs.

corrupted file

A file that has been irreparably damaged, by a virus for example.

detection

Scanning memory and disks for clues that a virus may be present. Some detection methods include searching for common viral patterns or strings, comparing suspicious file activity with known virus activity, and monitoring files for unauthorized changes.

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 have built-in virus detection, contain self-modifying code, or are unlikely to be infected by a virus. Such files are usually skipped in validation checking because they may trigger a false alarm.

executable (file)

A file containing coded instructions to be executed by the computer. Executable files include programs and overlays (auxiliary program code which cannot be executed directly by the user).

expanded memory

Computer memory above the DOS 1MB 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 1MB limit of conventional memory. Often used for RAM disks and print spoolers.

false alarm

Reporting a viral infection when none is present.

infected file

A file contaminated by a virus.

macro virus

The most common widespread virus today. Uses an application's macro language to spread to other documents within that application and perform unsolicited actions. A Word macro virus is obtained by opening a macro-infected Microsoft Word document (.DOC) or Word template (.DOT) file. Some macro viruses can plant their own passwords.

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. The MBR accesses the boot sector.

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 (EMS), extended memory (XMS), or an upper memory block (UMB).

memory infection

Contamination of memory by a virus. The only certain way to eliminate memory infection is to shut down your computer*,* restart from a clean start-up diskette, and clean up the source of the infection using VirusScan.

modified file

A file that has changed after validation codes have been added, possibly by a virus.

overlay infection

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

polymorphic virus

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

read operation

Any operation in which information is read from a disk, including a hard drive, floppy diskette, CD-ROM, or network drive. 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 VirusScan records about an executable file in order to recover (repair) it if it is damaged by a virus. See also "validation codes."

self-modifying program

Software that changes its own program files, often to protect against viruses or illegal copying. These programs should be included in an exception list to prevent these modifications from being reported as a false alarm by VirusScan.

system errors

Errors that can prevent VirusScan from completing its job successfully. System error conditions include disk format errors, media errors, file system errors, network errors, device access errors, and report failures.

unknown virus

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

upper memory block (UMB)

Memory in the range 640KB to 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 VirusScan 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 on a disk or lurks in a computer’s memory, and spreads from one program to another. Viruses may damage data, cause computers to crash, display messages, and so on.

warm boot

To restart (reset) a computer by pressing CTRL+ALT+DEL. See also “boot” and “cold boot.”

write operation

Any operation in which information is recorded to a disk. Commands that perform write operations include those that save, move, or copy files. See also “read operation.”

write protection

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

Index