User's Guide

BootShield

McAfee, Inc.
2710 Walsh Avenue
Santa Clara, CA 95051-0963

Phone: (408) 988-3832
Monday - Friday
6:00 am - 5:00 pm

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

(For international contact information, see the following page.)

TRADEMARK NOTICES

McAfee is a registered trademark of McAfee, Inc. SiteMeter, SiteExpress, ServerStor, and NetRemote are trademarks of McAfee, Inc. All other products or services mentioned in this document are identified by the trademarks or service marks of their respective companies or organizations.

"SABRE" is a trademark of American Airlines, Inc. and is licensed for use to Saber Software Corporation, a wholly owned subsidiary of McAfee. Saber Software is not affiliated with American Airlines, Inc. or SABRE Travel Information Network. All trademarks are the property of their respective owners.

FEEDBACK

A Reader's Comment Form is provided in the back of this publication. 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. If the form has been removed, please address your comments to: McAfee, Inc., Documentation, P.O. Box 9088, Dallas, Texas 75209.

SUPPORT

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

- Program name and version number
- Type and brand of your computer, hard drive, and any peripherals
- DOS type and version
- Network name, operating system, and version
- Contents of your AUTOEXEC.BAT, CONFIG.SYS, and system LOGIN script
- Specific steps to reproduce the problem.

INTERNATIONAL CONTACT INFORMATION

McAfee Canada
178 Main Street
Unionville, Ontario
Canada L3R 2G9
Voice: (905) 479-4189
Fax: (905) 479-4540

McAfee Europe B.V.
Orlyplein 81 - Busitel 1
1043 DS Amsterdam
The Netherlands
Voice: (0) 31 20 6815500
Fax: (0) 31 20 6810229

McAfee (UK) Ltd.
Hayley House, London Road
Bracknell, Berkshire
RG12 2TH United Kingdom
Voice: 44 1344 304730
Fax: 44 1344 306902

McAfee France S.A.
50 rue de Londres
75008 Paris
France
Voice: 33 1 44 908733
Fax: 33 1 45 227554

McAfee Deutschland GmbH
Weltenburger Strasse 70
81677 Munich
Germany
Voice: 49 89 92404214
Fax: 49 89 92404211

Issued February 1996

Table of Contents

About This Document

Who Should Read This Manual

Anyone responsible for protecting computer data against possible viruses should read this manual. Whether you're responsible for maintaining a large network with multiple servers and workstations, or you're using your computer at home, this manual is written for you.

Read the next section to get a quick view of what you'll find in this book.

Installation and usage instructions and guidelines for protecting computers against viruses are all here. It's not necessary to read this entire document at once; therefore, you'll want to look at the introductory material first to decide which tasks are most important to you. The next section outlines the chapters and indicates what major tasks are covered.

What You'll Find in This Manual

This user's guide contains information you need for installing and using the product components. BootShield documentation provides a clear and easy path to information you need to use the product effectively.

✍ *The manual gives you full product details and procedures. Release Notes contain last minute updates made to the product.*

The following topics are covered:

Getting the basics

Chapter 1, "About This Document." Tells you how this book is organized and describes the notation and symbols used in this book.

Chapter 2, "Product Overview." Describes the key features and benefits of using BootShield and provides recommendations for using each component.

Using BootShield

Chapter 3, "Protecting the Boot Sector." Provides procedures for installing and activating BootShield for protection against boot sector viruses. Instructions for uninstalling the product are also provided.

Chapter 4, "Detecting Boot Viruses." Provides instructions for ensuring that the computer's boot sector is virus-free.

Chapter 5, "Backing Up and Restoring Data." Identifies system requirements for ImageStor and gives you step-by-step instructions for installing and using the software for storage management.

Chapter A, "Checking Files and Memory for Viruses." Describes how to use Scan to check user files and RAM memory for viruses, in addition to checking the boot sector.

"Glossary." Defines the types of viruses mentioned in this manual as well as special BootShield terms.

Notation and Symbols

In this section, we've illustrated and described the conventions we've used throughout the manual. Our style is designed to eliminate clutter so that you can focus on the important task of protecting your data. Take a look now, before you begin using the guidelines, so that you'll know how to interpret the information in this manual.

Procedures

Procedures begin with a feature description followed by step-by-step procedures. Specific text you are to type is shown in uppercase letters. Placeholders for items such as file names that you must supply yourself are shown in lowercase letters.

We assume you have a working knowledge of the DOS environment. For example, we do not tell you to press ENTER after every command.

The following paragraphs show how procedures appear:

Step	Action

1. Numbered steps tell you what action to take.

Response: Tells how the system responds to the actions you take.

Action: Tells what further action, if necessary, you need to perform to complete the step.

Once you become familiar with how to use BootShield, you can skip the feature description and go straight to the procedure for a quick reference.

Information references

Key notation. This notation represents a key on the keyboard. In a step-by-step instruction, we instruct you to press one key or a combination of keys to perform a function.

For example, press the ENTER key. Or, press SHIFT+F10

This note contains important information for all users.

Author note. The author note emphasizes information about any of the following:

- Options
- Functions
- Procedures
- References to information in the current chapter, a different chapter, or another manual.

Text note. The text note emphasizes supplemental information that provides tips about options, functions, or procedures.

Introducing BootShield

Because viruses in the computer's boot sector (the area that contains the starting instructions) can be introduced from so many different sources, it is important to find a reliable, effective, and easy-to-use method for this kind of virus protection. Once a computer is started from a diskette or a drive is infected with a boot sector virus, the system is immediately contaminated. Although the machine can continue processing without noticeable side-effects, extended use of virus-infected computers may spread these viruses to other machines through shared diskettes and files. And, eventually, the boot virus can render the computers inoperable.

Unfortunately, traditional anti-virus software is insufficient for defending against all boot sector virus types. Traditional virus protection methods are activated after the computer is started. Therefore, these methods are *not* adequate for protecting against viruses in the boot sector. Boot viruses are executed as the computer looks for startup instructions (for example from an infected diskette or drive during system startup or restart).

Why use BootShield?

Now McAfee delivers an "immune system" to eliminate this common and expensive boot virus threat. BootShield protects the computer from boot sector viruses. Since an estimated 70% of all reported virus incidents are boot virus related, McAfee's BootShield is an essential part of your anti-virus protection solution.

BootShield combines a secure installation process with leading-edge boot sector virus protection technology. Using BootShield, users are alerted to boot virus activity and can instantly restore the computer back to its virus-free state. In addition, BootShield offers an optional, easy-to-use disaster recovery utility that allows you to quickly recover from data loss situations.

BootShield is the ideal companion to McAfee's VirusScan. It guards against virus attacks in the computer's boot sector, while VirusScan allows you to scan for and remove viruses from areas other than the computer's boot sector. Together, BootShield and VirusScan are the perfect anti-virus solution.

BootShield components

BootShield contains these three components:

- Scan—to identify boot sector viruses identification prior to installation
- BootLock—for boot virus protection
- ImageStor—as an option for image backup to enable disaster recovery.

The following paragraphs provide a brief description of each component.

McAfee Scan

A critical prerequisite to using BootLock is to start with a virus-free boot sector. To ensure that the boot sector is virus free before you install BootLock, we've provided the Scan component of this product. Scan identifies whether boot sector viruses are present so that you can be sure this portion of the system is clean before installing BootShield.

Please note that the VirusScan product (not included with BootShield) allows you to scan for and automatically remove viruses found in the boot sector and other areas of the computer. If a virus is detected before you install BootShield, you need to run VirusScan to clean your system.

BootLock

Since boot viruses are executed as the computer looks for startup instructions (for example, from an infected diskette or drive during system startup or restart), BootLock creates and uses a copy of the boot image and locks out changes to this area of the computer. Changes characteristic to boot virus actions are immediately recognized and you are alerted. By activating Boot-Lock, you “lock out” viruses from the boot sector of your computer. To install, see “Protecting the Boot Sector” on page 13.

ImageStor

To guard against data loss, BootShield provides ImageStor, the easy-to-use image backup utility. Using ImageStor is optional; however, if you don’t use ImageStor, we recommend you use another reliable backup utility for disaster recovery.

ImageStor allows you to create a disk image that can be used for disaster recovery, and you won’t have to install the operating system and applications again after data is restored. Chapter 5, “Backing Up and Restoring Data,” provides instructions for creating a backup image using ImageStor.

Key Features and Benefits

BootShield offers an unobtrusive, automated protection mechanism that secures the computer against known and unknown boot sector viruses. The table below outlines the key features and benefits of using BootShield.

Key Features	Benefits
BootLock	
Proprietary BootLock technology	Effectively stops boot viruses, including those known, new, multi-partite, stealth, polymorphic, or encrypted
NCSA approved	Guarantees protection based on independent testing and approval by the National Computer Security Association.
Ease of use	BootLock's menu-driven interface is intuitive and easy to use.
Option customization	You can use the default BootLock setup, or you can customize the options.
Alerting capabilities	BootLock alerts users to virus activity in the boot sector and prevents infections.
McAfee Scan	
Secure installation	Running Scan before installing BootLock ensures that BootLock begins protecting the system with a clean boot sector.
Consistent virus detection	Scan consistently detects over 99% of the more than 200 known boot viruses, thereby ensuring adequate virus protection.
ImageStor	
Instant disk image backup and restoration	Reduces the time involved in backing up and restoring your system since there's no need to install the operating system or applications again.

Key Features	Benefits
Command-line driven user interface	Reduces learning curve and the time it takes to become productive.
Creates an image of the entire system.	Provides for disaster recovery, should it become necessary.

How to Contact Us

To order or for more information about our products, we invite you to contact our Customer Service department at (408) 988-3832. Or you can contact us at the following address:

McAfee, Inc.
2710 Walsh Avenue
Santa Clara, CA 95051-0963
U.S.A.

McAfee's customer and technical support

McAfee is famous for its dedication to customer satisfaction. McAfee's customer support, technical support, and product development departments provide real-time technical support and problem resolutions. Use the following information to contact McAfee Support.

Phone	(408) 988-3832
FAX	(408) 970-9727
Hours	6 a.m. to 5 p.m. PST Monday through Friday
McAfee BBS	(408) 988-4004 1200 bps to 28,800 bps 8 bits, no parity, 1 stop bit 24 hours, 365 days a year
McAfee FAX-back and voice response system	(408) 988-3034
CompuServe	GO MCAFEE
Internet	support@mcafee.com
America On-line	keyword MCAFEE
Microsoft Network (MSN)	GO MCAFEE
World Wide Web	http://www.mcafee.com

To speed the process of helping you use our products, please make note of the following before you call:

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

McAfee training

For more information about scheduling onsite training for any McAfee product, call Customer Service at 800/338-8754.

Where to Go from Here

This manual gives you the instructions you need to install and use BootShield effectively. The table below shows where you can find instructions for the task you want to perform.

If you want to. . .	See. . .
Scan your system's boot sector for virus detection before installation	"Checking for Boot Viruses" on page 36
Create a backup system image using ImageStor	"Backing Up and Restoring Data" on page 39
Install BootLock for virus protection	"Protecting the Boot Sector" on page 13

Protecting the Boot Sector

The BootLock component of BootShield is a powerful solution to locking virus activity out of the computer's boot sector. Therefore, you must consider the best way to implement this technology. For example, some programs write to the boot sector to perform legal operations. Therefore, it's possible to receive a BootLock warning of a potential virus when these types of programs are at work. To accommodate these types of programs, you can specify how BootLock responds if changes need to be made to the boot sector.

Before implementing the BootLock technology, you need to understand how BootLock performs virus protection functions. Understanding how BootLock works will allow you to use its functions in the most productive way for your working environment. Review the following section for details on making BootLock work for you.

In this chapter, you will find the following instructions:

- Planning to use the BootLock technology
- Installing BootShield
- Recovering from a boot virus incident
- Customizing BootLock settings
- Uninstalling BootLock, including the emergency procedure.

What Is BootLock?

BootLock is a powerful solution to locking virus activity out of the computer's boot sector. It offers unobtrusive virus protection (users are unaware of its presence during normal processing) that immediately identifies any computer activity characteristic of boot viruses and prevents virus infection. BootLock effectively stops boot viruses, including known viruses, new viruses, multi-partite, stealth, polymorphic, and encrypted viruses.

✍ *The "Glossary" on page 65 provides a full definition of the types of viruses mentioned in this section.*

How BootLock works

Since boot viruses are executed as the computer looks for instructions during startup or restart, BootLock masks the computer's boot image and then locks out changes to this area of the computer. Specifically, BootLock displays a warning if an attempt is made to modify the boot sector, master boot record, memory size, and system interrupt vectors. Changes characteristic to boot virus actions are immediately recognized and prevented.

While BootLock is the ideal solution for protecting the computer's boot sector, BootLock is *not* designed to protect the file allocation table (FAT) and the system setup (CMOS) areas of the computer. To secure these areas of the computer, you need to use an effective image backup and disaster recovery tool. You can use BootShield's ImageStor as a disaster recovery solution (see "Backing Up and Restoring Data" on page 39).

Planning to use BootLock

To implement the BootLock technology in the most productive manner for your work environment, you'll need to do some planning. Review the checklist below to help you decide how best to use BootLock.

- ✓ The key to using BootLock is to begin with a virus-free boot sector. Therefore, the installation program automatically scans the boot sector to detect viruses.
- ✓ As part of the installation process, you **must** be sure to label the BootLock backup diskette that is created for each workstation. It is critical to keep the diskette specific to each workstation on hand. Should you need to remove BootLock from the computer, you must have the BootLock diskette available before you can perform this task.
- ✓ We recommend scanning areas of the computer other than the boot sector to determine if any viruses exist. McAfee offers VirusScan, our award-winning, NCSA-certified virus scanner, to ensure automatic detection and removal of computer viruses.
- ✓ Before you install, we recommend creating a backup image of the computer disk. BootShield offers ImageStor as an option for completing this task. However, if you don't use ImageStor for disaster recovery, you'll need to use another reliable image backup utility.
- ✓ You should keep in mind that once it's activated, BootLock does not allow changes to the boot sector. Note that some programs write to the boot sector to perform legal operations. Therefore, it's possible for users to receive a BootLock warning of a potential virus when these types of programs are at work. To accommodate these types of programs, you can specify how BootLock responds if changes need to be made to the boot sector. For example, BootLock responses to virus activity can be customized so that users can enter a password to continue processing if legal operations are being performed by a program.

  Be aware that there is some risk associated with entering a password to continue processing. You'll only want to implement this option for computers that have programs installed that must write to the computer's boot sector. In the event that a boot sector virus is encountered, you can use BootLock's on-demand repair feature as discussed later in this chapter.

- ✓ There may be some software compatibility issues to consider for certain workstations. Therefore, before you decide on which machines to install BootLock, review the section “Special software compatibility considerations” on page 18.
- ✓ To make legal changes to the boot sector, such as installing software packages that modify the master boot record, we recommend that you uninstall BootLock first. This prevents the display of BootLock alert messages while the software is being installed. After the installation is complete, you’ll need to install BootLock again.

Installing BootShield

This section provides instructions for installing BootShield and setting up BootLock. Be sure to review the following paragraphs for the prerequisite tasks you need to perform before you install.

Before you begin

Be sure to review the prerequisites in the previous section before you install.

You need to have a blank, virus-free, formatted diskette available. During installation, BootLock copies the boot sector image to the diskette you supply. Also, if you choose the option to create a backup image of the computer during installation, BootLock creates a bootable diskette. This is the diskette you'll use to restore the system using ImageStor for disaster recovery.

To install successfully, this diskette must *not* be write protected; otherwise, you'll receive an error message. Also, be sure to label the diskette so that you'll know the workstation for which it should be used.

As part of the installation process, you **must** be sure to label the BootLock backup diskette that is created for each workstation. It is critical to keep the diskette specific to each workstation on hand. Should you need to remove BootLock from the computer, you must have the BootLock diskette available before you can perform this task.

System requirements

To install and run BootShield, you will need the following workstation configuration:

BootShield is not compatible with the Windows 95 and NT environments.

- PC with a 386SX processor or better
- DOS version as follows:
  - For BootLock and Scan you need DOS version 3.3 or later
  - For ImageStor you need DOS version 6.0 or later
- 512 kilobytes of Random Access Memory (RAM)
- 2 megabytes of disk space
- For tape backup, a SCSI tape device that uses ASPI.

Review the next section for special software compatibility considerations you should make before installing BootShield.

Special software compatibility considerations

The following paragraphs tell you the software compatibility issues of which we are aware for running BootLock. Please review them before you install.

- If the computer is running Quarterdeck, do the following:
  - Move the BootLock device statement after all QEMM drivers in the CONFIG.SYS file. Here's an example.

    ```
    ...
    DEVICE=C:\QEMM\DOSDATA.SYS
    SET LOADHIDATA=C:\QEMM\LOADHI.RF
    DEVICE=C:\QEMM\QEMM386.SYS rf ram
    DEVICE=C:\QEMM\DOS-UP.SYS @c:\qemm\dos-up.dat
    DEVICE=C:\MCAFEE\BTSHIELD\BTLOCK.SYS
    ...
    ```

  - If a computer is running QEMM, you need to make the QuickBoot function inactive before installing BootLock. When QuickBoot is inactive, the following command is displayed in the CONFIG.SYS file:

    ```
    DEVICE=C:\QEMM\QEMM386.SYS RAM BE:N R X=C000-C7FF R:3
    ```

- If the computer is running the DOS 5.x or 6.x multiboot option, you need to move the BootLock device statement to the [Common] section in the CONFIG.SYS file. By default, the following line is added to the beginning of the CONFIG.SYS file when BootLock is installed:

  ```
  DEVICE=C:\MCAFEE\BTSHIELD\BTLOCK.SYS
  ```

Installation procedure

Follow the procedure below to install BootShield.

BootShield is not compatible with the Windows 95 and NT environments.

✍ *To implement BootShield on multiple computers, you need to perform this procedure for each machine separately.*

Step	Action

BootLock is *not* designed to be installed from a temporary DOS shell (DOS box).

1. Insert **Disk 1** into the floppy drive. Or, if you downloaded the product from a McAfee online service, change to the location where the files were stored after they were decompressed.

Enter the following command:

```
a:install a:
```

where ‘a’ is the drive that contains the BootShield diskette.

Response: The workstation’s boot sector is scanned for viruses. Afterwards, the BootShield program files are copied to the destination drive.

2. When you are prompted to do so, remove the program disk and insert a blank, virus-free diskette into the floppy drive. Then type C to continue.

Response: A message prompts you to back up your hard drive.

3. Do one of the following:

- If you do *not* want to perform the backup at this time, type N and go to Step 7 below.

or

- To perform the backup now, continue with the next step.

4. Type Y to perform the backup now.

   Response: The system files and drivers required to boot up the computer are copied to the diskette located in the floppy drive. Also, the ImageStor program files are copied to this diskette. (For more information about ImageStor, refer to "Backing Up and Restoring Data" on page 39.)

   Action: To send the backup disk image to a network file, go to Step 5. To send the backup to an external hard drive or to tape, go to Step 6.

5. To send the backup disk image **to a network file**, do the following:

   - Enter the path name (you don't have to enter a file name since DRVIMG.ISF is automatically created in the path you specify).

     ✍ *Be sure the target drive has an adequate amount of disk space to accommodate this backup.*

     Response: The amount of available disk space for the path you specified and the amount of space required to create the backup file are displayed. A description of the source drive (the hard drive) and the backup file are displayed, and an ID number is automatically assigned and shown to left of each description.

   - Type the ID number assigned to the hard drive (most likely, this number is 0).

   - Type the ID number assigned to the file DRVIMG.ISF (most likely, this number is 1).

     Response: The following message is displayed:

     ```
     Proceeding will DESTROY ALL DATA now on
     DEVIMG.ISF. Are you CERTAIN you want to proceed
     (y/n)?
     ```

     This message means that the backup image will be sent to DRVIMG.ISF in the path you specified. And if a backup already exists in this path, the file will be overwritten.

   - Type Y to confirm the backup operation.

Response: A backup image is created in the path you specified.

✍ *The amount of time required to complete the backup depends on the storage capacity and how much data resides on this hard drive. If this workstation has a large-capacity hard drive that's full, you might want to take a break while the backup is in progress.*

Action: Once the backup is complete, go to Step 7 to finish the installation process.

6. To send the backup **to an external hard drive** or **to tape**, press the ENTER key to bypass the file name field. Then do the following:

- Type the ID number assigned to the hard drive that you want to be backed up.

  Response: A message prompts you to specify the drive that is the destination for the backup. A list of possible drives is shown.

- Type the ID number assigned the target drive (the location to send the backup of the disk image).

  ✍ *Be sure the target drive has an adequate amount of disk space to accommodate this backup.*

  Response: A backup image is created on the target drive you specified.

7. Select **File/Install BootLock**.

Response: The installation screen is displayed. The installation options are listed on the left, and the installation details are listed on the right of the screen.

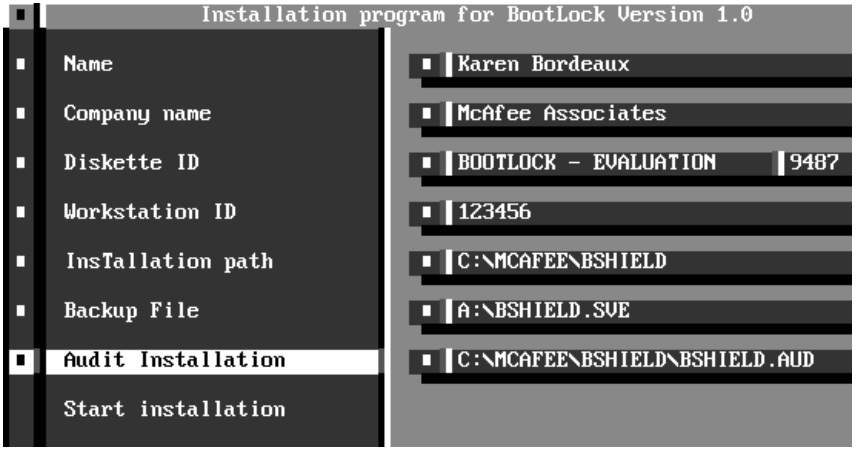

Figure 3-1. BootLock installation screen

8. Enter the following information on the installation screen:

   - Your name and company name
   - Diskette ID—identifies the BootLock version installed on this workstation.
   - Workstation ID (you can use the specific station ID or a name you create)
   - Installation path—the default path is C:\MCAFEE\BSHIELD, or the path that you entered when you typed the command to start the installation program

Be sure to keep the diskette on hand that contains the backup file. Without this diskette, you won't be able to remove BootLock should you need to.

- Backup File—the default file is A:\BSHIELD.SVE. This is the backup of the computer's original boot image.

  ✍ *Be sure you have inserted the blank, formatted diskette so that this boot sector backup file can be copied to it and, therefore, will be available in case you need to restore the machine after a boot virus incident.*

- Audit Installation—the default audit file is C:\MCAFEE\BSHEILD\BSHIELD.AUD. This is the file that contains a description of the BootLock installation status. For example, it indicates whether BootShield is installed and which control settings are active.

9. Select the 'Start installation' option.

Response: BootLock is set up on your system. A message lets you know that the installation process is complete, and then your computer is restarted to activate BootLock.

To complete the installation successfully, BootLock must restart the computer.

Action: When you are prompted to do so, remove the diskette from the drive. We recommend that you write-protect it and then store it in a safe place. Be sure to label it with this workstation's ID so that you'll know which workstation this startup disk belongs to.

If you have problems

If problems occur during installation and the process cannot be completed successfully, follow the steps below.

Step	Action
1.	Insert the BootLock diskette that was created in Step 2 of the installation procedure. Then enter the following command: **BSSETUP**
2.	Select **File/Emergency uninstallation** from the menu bar.

How to Recover from a Boot Virus

BootLock allows you customize its functions so that users can override boot sector virus warning messages (for example, to allow changes to the boot sector during legal operations performed by some software packages). However, there is some risk associated with overriding these alert messages. Therefore, BootLock offers an on-demand recovery feature so users can quickly remove the boot virus and continue with their work.

If you need to use the recover function, keep in mind that the computer is restored using the boot image created when BootLock was installed. Therefore, any boot sector changes made after you installed BootLock are lost (for example, the user accepted changes made to the master boot record by a software package).

✍ *Another option for recovering the boot sector is to use the restoration feature in your image backup utility (see "Backing Up and Restoring Data" on page 39 for instructions).*

If a boot sector virus is encountered, BootLock displays an alert message. To recover from a boot virus incident, type Y to overwrite the current boot image with the virus-free image saved during installation.

✍ *Before you use the on-demand recovery function, we recommend that you use VirusScan to determine if a boot sector virus is found.*

Customizing BootLock Settings

After installation, BootLock is already set up and running on your machine. If you wish, you can change the default program settings. This section describes the BootLock settings, and tells you what you can change and how.

Displaying the current settings

After installation, you have the option to display the current BootLock program settings. To do so, choose **File/BootLock Status** from the menu bar. The information that is displayed is only for review. Refer to the following procedures if you need to make changes.

What you can change

BootLock has two groups of program settings:

- Control—determines how BootLock operates. You can make these controls active or inactive (see the following for a description of each setting).
- Messages—determines the text displayed on the screen as a result of BootLock operations. You can customize the message text.

How to make changes

Changing control settings

The table below describes the BootLock control settings and lets you know the default. Following the table is the procedure for making changes.

Setting	Description	Default
Master boot record	Controls whether information can be written to the master boot record.	Active
DOS Boot Sector Control	Controls whether information can be written to the boot sector.	Active
Memory integrity	Determines whether an alert message is displayed when a change occurs in total memory size.	Active
Vector integrity	Controls whether changes can be made to the first 128 interrupt vectors.	Active
Vector implantation	Determines whether an alert message is displayed if activity characteristic of a boot sector virus occurs in the interrupt vectors.	Inactive
Control boot from a floppy	Determines whether the computer can be started from a floppy diskette. This option is available only for systems that allow you to configure the boot sequence.	Active
Control startup in protected mode	Determines whether the computer can be started in protected mode.	Active
Activate audits in case of error	Determines whether virus alerts are recorded. You must specify an audit file before activating this control (see “Name of audit file” below).	Inactive
Display startup screen	Turns the splash screen on and off.	Active

Setting	Description	Default
Name of audit file	Allows you to specify a file for recording BootLock program settings and activity. This information is only recorded after you activate the setting 'Activate audits in case of error'. We recommend that you specify a file name that is different from the Audit Installation file specified during installation (by default, BSHIELD.AUD).	Inactive
Name of program to launch	Allows you to specify the specific program to run if BootLock detects a change in the boot sector based on the active control settings. For example, you can run VirusScan to detect and remove boot sector viruses, if present, before allowing the user to continue processing. To use this option, the following setting must appear at the end of each workstation's CONFIG.SYS file: **DEVICE=path\BOOTLOCK.SYS** Also, you must specify the particular BootLock alerts for which the program is run (see Step 4 under "Changing alert and system messages" on page 29).	Inactive
Change password	Allows you to specify the password that users must enter to continue processing after BootLock displays a particular alert message. This option must be set to 'Active' if you want users to enter a password after an alert message is displayed. See "Changing alert and system messages" on page 29 to select the actions for which this password is required.	Inactive
List interrupt vectors	Allows you to select the interrupt vectors for which BootLock checks for changes.	Active

To customize control settings, change to the BootShield directory and follow the procedure below:

Step	Action

1. Enter the following command to run BootLock:

   BSSETUP

2. Select **Setup** from the menu bar.

3. Select **Control Settings**.

   Response: The Installation settings dialog (Figure 3-2) is displayed.

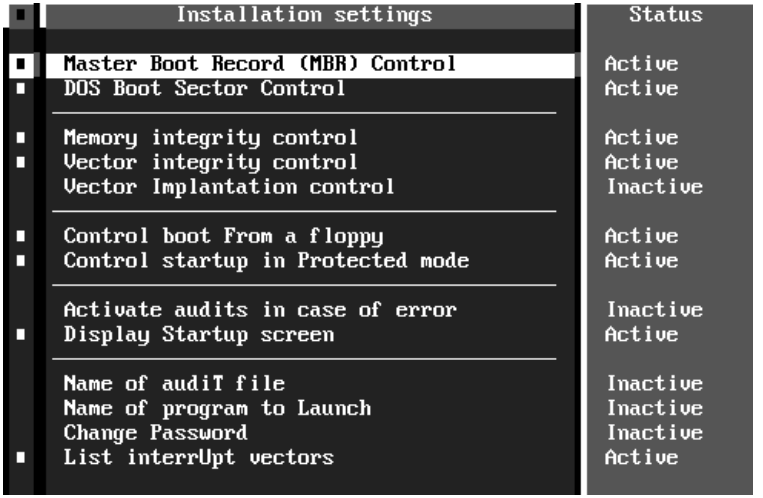

Figure 3-2. Installation settings dialog

4. Change the desired settings. Use the arrow keys to move between settings and press the SPACEBAR or ENTER key to toggle between 'Active' and 'Inactive' status.

   ✍ *If you activated the 'Name of program to launch' option, be sure to update the workstation's CONFIG.SYS file. See the preceding table for details.*

5. Press the ESCAPE key to close the dialog.

6. Select **Settings/Controls Updating** to complete the process.

Changing alert and system messages

Messages are grouped into two categories: alert and system. Alert messages are displayed if a potential boot sector virus is detected, and system messages are displayed if BootLock encounters a system problem during processing (for example, the user enters the wrong password in response to an alert message).

To customize alert and system messages, change to the BootShield directory and follow the procedure below:

Step	Action

1. Enter the following command to run BootLock:

   BSSETUP

2. Select **Setup** from the menu bar.

3. Do one of the following:

   - To change alert messages, select **Alert message settings**.

     Response: The Message settings procedure dialog (Figure 3-3) is displayed.

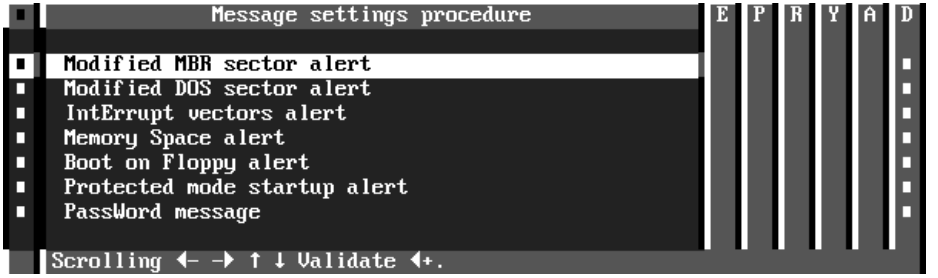

Figure 3-3. Message settings procedure dialog

or

- To change system messages, go to Step 5.

4. For alert messages, do the following:

- Press the ENTER key on the Message settings procedure screen (Figure 3-3) to display the alert text. Then enter your changes. Press the F10 key to save the changes. (Refer to "What are the alert messages?" on page 32 for a description.)

- Use the arrow keys to move between the columns of actions that can be performed when a message is displayed to the user. Press the SPACEBAR to toggle between the active and inactive status. (When the action is active a marker appears in the column.)

  You can choose one or more of the following actions for each alert message:

  - E—executes a particular program if this error is encountered. For example, you can run VirusScan to determine whether a boot sector virus is present before allowing the user to continue processing. You must specify the program to launch under Control Settings (see "Changing control settings" on page 26 to specify the program to run).
  - P—requires the user to enter a password to continue processing after this message is displayed (see "Changing control settings" on page 26 to specify the password to enter).
  - R—reboots the machine if this error occurs.
  - Y—automatically responds to the alert message by restoring the setting to its status as of the time BootLock was installed (see "Changing control settings" on page 26 for a description of the BootLock control settings). To use this option, you must also select 'A' to activate automatic mode.
  - A—enables the automatic response to the alert message.
  - D—displays the specified alert message if this error is encountered.

  Action: Press the ESCAPE key to close the dialog.

5. Select **System message settings** from the **Settings** menu.

Response: The Setup system messages dialog (Figure 3-4) is displayed.

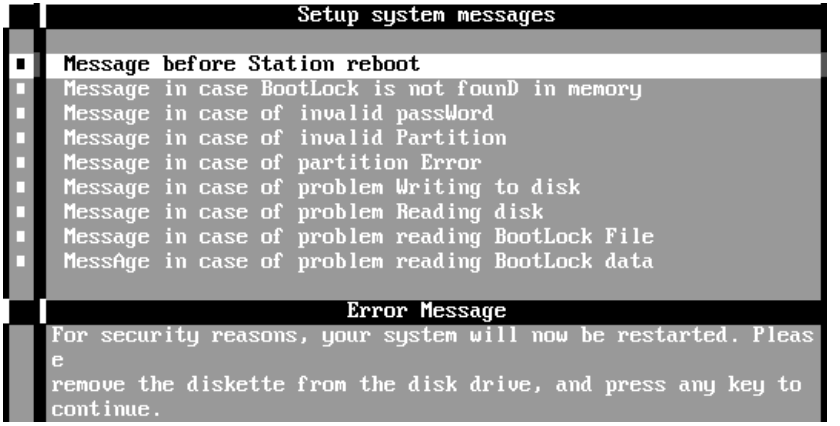

Figure 3-4. Setup system messages dialog

6. Use the arrow keys to move through the list of message types.

Response: The current message text is displayed in the lower portion of the dialog.

7. To make changes, do the following:

   - Highlight the desired message type and then press the ENTER key to display the message text. (Refer to "What are the system messages?" on page 33 for a description.)

   - Enter the changes and press the ENTER key until the dialog is closed.

Action: Repeat this step for the desired message types.

8. Select **Settings/Messages updating** to complete the process.

What are the alert messages?

Here's a list and description of each type of BootLock alert message. When an alert message is displayed, the user must decide whether to continue processing or reboot using the BootLock backup disk created during installation.

- Modified MBR sector alert—BootLock detected a change in the MBR (Master Boot Record). This sector does not match the image created by BootLock during the last system startup.
- Modified DOS sector alert—BootLock detected a change in the DOS Boot Sector. This sector does not match the image created by BootLock during the last system startup.
- Interrupt vectors alert—BootLock detected a change in the Interrupt Vector Table (IVT). The table does not match the image created by BootLock during the last system startup.
- Memory space alert—BootLock detected a change in the size of available memory. The size does not match the one saved by BootLock during the last system startup.
- Boot on floppy alert—BootLock detected that your computer was started from a non-system diskette in the A: drive. This disk has instructed your PC to load the Boot Sector from the C: drive. Some viruses are known to infect this way.
- Protected mode startup alert—BootLock detected the system starting in protected mode. This behavior is highly suspicious and may indicate viral activity.
- Password message—The user must enter the correct password when a BootLock alert message is displayed. To set the password, see "Changing control settings" on page 26.

What are the system messages?

Here's a list of each type of BootLock system message.

- For security reasons the station must be rebooted
- BootLock is not found in memory
- The user enters an invalid password
- An active partition could not be found or the master boot record is corrupted
- There is a problem writing the master boot record
- There is a problem reading the master boot record
- There is a problem reading the BootLock backup file
- There is a problem reading boot sector data.

Uninstalling BootLock

This section gives you instructions for uninstalling BootLock. If you only want to make particular BootLock operations inactive, see "Customizing BootLock Settings" on page 25. However, if changes must be made to the master boot record (for example, you're installing some software), use the procedures in this section. After you use the uninstall procedure, BootLock is not active on the computer; however, the BootShield program files are still available in the installation directory to allow you to quickly install BootLock again.

Under normal conditions

If you decide to make BootLock inactive on a computer, change to the BootShield directory and run **BSSETUP**. Then select **File/Uninstall BootLock** from the menu. When you choose this option, the BootLock function is removed from the system and the computer is restarted.

In case of emergency

BootLock provides an emergency method of removing the program from the computer. You should only perform this procedure in an emergency, such as when the normal uninstallation procedure was not completed successfully or a boot virus has destroyed the computer's hard drive.

Unlike the normal uninstall function, when you choose the emergency uninstall BootLock restores the original, virus-free boot image created during installation rather than simply removing BootLock from the current boot image.

When the C: drive can be recognized

To uninstall BootLock in an emergency, change to the BootShield directory, insert the BootLock backup diskette created during installation for this workstation, and run **BSSETUP**. Then select **File/Emergency uninstallation**.

When the C: drive is not recognized

Some boot viruses may destroy the boot sector or the master boot record so that the C: drive is not recognized. In this case, you need to use the emergency uninstallation procedure. To do so, start the computer using a clean system diskette. If the workstation's system setup allows you to choose the boot sequence, select the option to boot the computer using the A: sequence. Then run **BSSETUP** from the BootLock backup diskette created during installation for this workstation and choose **File/Emergency uninstallation**.

Detecting Boot Viruses

Checking for Boot Viruses

Many viruses are introduced into the computer through the boot sector of your computer's hard disk. Therefore, you need to be sure the boot sector is virus-free. BootShield offers the Scan component which allows you to identify viruses in a computer's boot sector.

✍ *McAfee offers VirusScan for removal of computer viruses in the boot sector and other areas of the computer. If you don't already have a licensed copy of McAfee VirusScan, see* *"How to Contact Us" on page 10* *for the phone number to place an order.*

What is McAfee Scan?

McAfee Scan is the BootShield component that scans for viruses in the computer's boot sector and alerts you if any are found. If Scan finds any viruses, you must remove them before you do anything else.

✍ *The Scan component of BootShield is intended to check only the boot sector. However, you can also use Scan to find viruses in files on the hard disk, on a floppy disk, or in RAM memory. See* *"Checking Files and Memory for Viruses" on page 45* *for more information.*

How Scan detects known viruses

Scan detects known viruses by searching the system for characteristics (sequences of code) unique to each computer virus and reporting their presence. For viruses that are encrypted (secured), Scan uses detection algorithms that work by statistical analysis, heuristics, and code disassembly.

To obtain a list of all the viruses that Scan detects, run Scan with the /VIRLIST option. See "Scanning the boot sector" on page 37 for instructions on running the Scan command.

Scanning the boot sector

To check the computer's boot sector for viruses, enter the following command at the DOS prompt:

Syntax	**SCAN drives /BOOT [options]**	
Variables	SCAN	launches the Scan program.
	drives	indicates one or more drives to be scanned. You must specify at least one drive to be scanned.
	/BOOT	tells Scan to check only the boot sector and master boot record.
	options	is one or more of the Scan options listed under "Scan Command-line Options" on page 52.
		✍ *If you are only scanning the computer's boot sector for viruses, you don't have to use any of these options. However, you can scan other areas of the computer. For more information about scanning memory and files for viruses, refer to "Performing Expanded Virus Checking" on page 47.*

If no boot sector viruses are reported, you're ready to continue normal operations with this computer. However, if a virus is found you'll need to clean the boot sector before you continue.

Cleaning the boot sector

If a virus is detected during the scan, a message alerts you. You'll need to perform a one-time manual process of repairing the boot sector. Once you've activated BootShield, the on-demand restoration features completely eliminate this traditional, manual process.

McAfee offers VirusScan, our award-winning, NCSA-certified virus scanner, to ensure automatic detection and removal of computer viruses. If you don't already have a licensed copy of VirusScan, see "How to Contact Us" on page 10 for the phone number to place an order.

Backing Up and Restoring Data

Introducing ImageStor

ImageStor is an easy-to-use storage management program. It provides a quick method for backing up and restoring your computer's entire hard disk. This chapter describes how to use ImageStor to back up and restore a disk or partition on your computer.

Why use ImageStor?

To guard against data loss, BootShield provides the ImageStor image backup utility. Using ImageStor is optional; however, if you don't use ImageStor, we recommend you use another reliable backup utility for disaster recovery.

ImageStor allows you to create a disk image that can be used for disaster recovery. With ImageStor, you won't have to install the operating system and applications again after the disk is restored.

What does ImageStor do?

Using ImageStor, you take a "snapshot" of the computer's system disk and create a bootable diskette which you can use to restart your computer and restore files in the event of data loss. The main function of ImageStor is to provide you with a rapid restoration of workstation data.

ImageStor is different from other backup products in that it creates an image of the entire system, rather than performing a file-by-file backup. ImageStor allows you to create an image of any system running a DOS partition. This process greatly decreases the time it takes you to back up and restore a system, and you don't have to learn a lot about the storage management program before getting started.

ImageStor allows you to copy the disk image to the following media:

- Tape (SCSI)
- External hard disk (SCSI, IDE)
- A file on a mapped network drive.

You can quickly recover from a disaster caused by losing system data. Just back up your system using ImageStor on a regular basis.

✍ *We recommend that you back up your files at least once each week.*

Backing Up and Restoring a Hard Disk

It is important to back up your files regularly, so that you can easily recover in the event of a disk failure. ImageStor's messages prompt you for the necessary information for a quick and easy method of backing up and restoring data.

ImageStor writes backups to and restores from external storage devices. However, it can only talk to SCSI devices that use ASPI.

Before you begin

Before you can use ImageStor, you need to have a bootable diskette for the workstation. The bootable diskette contains the programs and files necessary for the computer to load the operating system and then restore data to the primary hard drive. In the event of a system crash, you can use the bootable diskette created with ImageStor to restore the system.

If you chose the option to back up the computer's hard disk during BootShield installation (see "Installing BootShield" on page 17), you'll want to continue to use this same diskette. It contains the system files and drivers for the workstation, plus all of the BootShield programs you need including ImageStor.

Alternately, you can create a separate bootable diskette as follows:

To create a bootable diskette for use with ImageStor, insert a virus-free, blank diskette and enter the following command at the DOS prompt:

```
ISBOOT [drive]
```

ImageStor is *not* designed to run in a temporary DOS shell (DOS box) running in Windows.

where **[drive]** is the drive that contains your virus-free diskette. (If you don't enter a drive letter, the default drive A: is used.)

The DOS system files, the appropriate drivers, and the ImageStor program files are copied to the diskette. For example, a copy of your AUTOEXEC.BAT and CONFIG.SYS are placed on the disk. These files contain only the required lines of information to start up the computer. You can use the bootable diskette to start the computer in the event of a system failure.

Creating a copy (backup) of your data

To create a backup of your data, follow the steps below. If you want to store the backup image in a file on a network drive, be sure there is sufficient space on this drive to accommodate the backup (at least as much as the amount of space on the hard drive to be backed up).

You should back up your data at least once a week.

Step **Action**

1. If a tape drive is the destination for this backup, insert the tape in the backup device.

2. Do one of the following to run ImageStor from the DOS command line:

- If you are creating the image on an external SCSI hard disk or on tape, enter the following command:

  ISENG

or

- If you are sending the image to a file on a network drive, enter the following command:

  ISENG *path*

  where *path* is the location to which you want to copy the file containing the backup image. The file DRVIMG.ISF is automatically created in the path you specify. This path must already exist; otherwise, you'll receive an error message.

Response: A message prompts you to specify the source from which you are backing up files. A list of possible source devices is displayed.

3. Enter the ID number that corresponds to the device from which you want to copy data.

✍ *Each device is automatically assigned an ID number (0, 1, 2, etc.). The ID number is shown to the left of the device description. The boot drive is usually 0.*

Response: A message prompts you to specify the drive that is the destination for the backup. A list of possible drives is displayed.

4. Enter the ID number that corresponds to the drive to which you want to save the backup image.

   Response: The disk image is copied to the destination.

   Action: If you copied to tape, when the backup is complete, remove the backup media, label it, and store it in a safe place.

Restoring files

In the event of system failure, follow the steps below to restore your system to its state as of the last backup.

Step	Action

1. Reboot the computer using a DOS bootable floppy diskette. (See "Before you begin" on page 41.) You can use the bootable diskette created when you installed BootShield, or the one you created on page 41.

2. If a tape drive is the destination for this backup, insert the tape in the backup device.

3. Run ImageStor from the DOS command line using the following command:

   `ISENG`

   Response: A message prompts you to specify the source from which you are restoring data. A list of possible source devices is displayed.

4. Enter the ID number that corresponds to the device from which you want to restore data.

   ✍ *Each device is automatically assigned an ID number (0, 1, 2, etc.). The ID number is shown to the left of the device description. The boot drive is usually 0.*

Response: A message prompts you to specify the drive to which you want to copy the data. A list of possible drives is displayed.

5. Enter the ID number that corresponds to the destination drive.

Response: The data from the source drive is restored to the destination drive.

6. After the restoration process is complete, reboot your computer from the hard drive or the usual boot drive.

Checking Files and Memory for Viruses

About Virus Checking

In addition to scanning the computer's boot sector for viruses (see "Checking for Boot Viruses" on page 36), you can use Scan to check the RAM memory and the computer's hard drive. This appendix describes the Scan syntax and command-line options available for additional virus checking.

How Scan detects viruses

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

To obtain a list of all the viruses that Scan detects, run the Scan command with the /VIRLIST option. See "Scan Command-line Options" on page 52 for more information about the /VIRLIST option.

How Scan detects unknown viruses

Scan can also check for new or unknown viruses by comparing files against previously recorded validation data. If a file has been modified, it will no longer match the validation data and Scan reports that the file may have become infected.

Note to network users

If you are using Scan to check files on a network drive (or directory), you must be connected to that drive and have Read access to it. Some of the options described in “Scan Command-line Options” on page 52 create, change, and delete files during processing. To use these options, you must have sufficient access rights.

Performing Expanded Virus Checking

To use Scan to check for viruses, run the SCAN command from the DOS command line. (See “Entering the SCAN command” on page 49.)

The BootShield version of Scan is meant to scan the boot sector for viruses. However, you can use Scan’s full capabilities by entering command-line options. These options define where and how Scan looks for viruses.

You can specify the options you want in either of two ways:

- On the command line
- In the configuration file. If you enter options in the configuration file, these options are used each time you run Scan.

For more information about the options you can specify, see “Scan Command-line Options” on page 52. For more information about using the configuration file, see the following section, “Creating and editing the configuration file.”

Creating and editing the configuration file

To create a configuration file, use a DOS-based word processing application or text editor to create a text file. Then simply type in any options and parameters that you want to use as defaults for the Scan command.

You can enter options into the configuration file in either of two ways:

- Enter all options and parameters on a single line as shown:

```
c:\user /sub /report d:\virus.rpt /rpterr /append
```

- Enter each option or parameter on a separate line followed by a hard carriage return and line feed, as shown:

```
c:\user
/sub
/report
d:\virus.rpt
/rpterr
/append
```

In both examples, the directory “C:\USER” and all its associated subdirectories are scanned. A report file, called “VIRUS.RPT,” will be saved to the D drive. This report file will also include any errors encountered during the Scan. If “VIRUS.RPT” already exists, Scan will add the new information to the end of the existing file.

✍ *The above example does not scan the boot sector.*

When you have entered the desired options, save the file as “DEFAULT.CFG” in the same directory with Scan.

✍ *The configuration file must be saved as an ASCII or DOS text file. If you use a word processor to create it, be sure to save the file as ASCII or DOS text.*

Entering the SCAN command

The SCAN command is run from the DOS command line. If you are in Windows, exit before attempting to run Scan.

To scan for viruses, enter the following command at the DOS prompt:

`SCAN drives [options]`

where:

SCAN	launches the Scan program.
drives	indicates one or more drives to be scanned. You must specify at least one drive to be scanned. If you specify a drive with just the drive letter and a colon (for example. **`SCAN C`**:), all its subdirectories are scanned. If you specify only a back-slash (for example, **`SCAN \`**), only the root directory of the active drive is scanned. You can also scan a specific directory (for example, **`SCAN C:\MCAFEE`**). ✍ *If you do not specify a drive to be scanned, Scan will search for a virus in memory, then return the message "No target for Scan was specified!"*
options	is one or more of the Scan options listed under "Scan Command-line Options" on page 52.

It might take several minutes for Scan to check for viruses in memory, in the system, and in user portions of the computer's drives. Scan keeps you informed of its progress. Read the information on the screen carefully.

The following is an example of the information that is displayed as Scan is checking a drive for viruses:

```
Virus data file V9511 created 11/15/95 12:47:11
No viruses found in memory.
Scanning C:
Summary report on C:
File(s)
        Analyzed:.......          1500
        Scanned:........           750
        Possibly Infected:.......    0
Master Boot Record(s):............   1
        Possibly Infected:.......    0
Boot Sector(s):..................    1
        Possibly Infected:.......    0
Time: 60.00 sec.
```

✍ *See the "Glossary" on page 65 for definitions of master boot record and boot sector.*

In the above example,

- **Analyzed** indicates how many files Scan has found on the computer.
- **Scanned** indicates how many files Scan has scanned for viruses. If you are using the default scanning settings, Scan will only check files with .COM, .EXE, .BIN, .OVL, .SYS, .DLL, .DOC, and .DOT extensions. To override those default extensions, use the /ALL command-line option.
- **Possibly Infected** indicates how many infected files Scan has found.
- **Master Boot Record** indicates how many master boot records have been scanned.
- **Boot Sector** indicates how many boot sectors have been scanned.

If no viruses are found

If Scan does not find any viruses, congratulations! Most likely, your computer is virus free. Copy any important files to diskettes or tape backup so you have current, clean files should a virus infect the system and damage your work.

If Scan finds a virus

If Scan 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
```

Do not panic, even if the virus has infected many files. But **do not run any other programs**, especially if the virus is found in memory. You need to follow the procedures in "Cleaning the boot sector" on page 38 to clean files.

Scanning diskettes

After scanning the computer's hard drives, you should scan **all** the diskettes you use. To do so, insert a diskette into drive A: and enter the following command:

```
scan a: /many /report c:\virus.log /all
```

Scan checks the diskette in drive A: then displays a message that prompts you to insert the next diskette. Insert the next diskette and then press any key to continue scanning. Continue until all diskettes have been scanned. When you are finished, press the ESC key.

✍ *The Scan program files should be on a drive that is not removed. For example, an error may result if you use the following command line:*

```
a:Scan a: /many
```

The command above assumes that you want to scan more than one diskette. If you are running Scan from one diskette, you no longer have the Scan program available once you remove the first diskette.

Scan Command-line Options

The following table lists all of the Scan command-line options.

Command-line Option	Description
/? or /HELP	Does not scan. Instead, displays a list of Scan command-line options with a brief description of each. Use either of these options alone on the command line (with no other options).
/ADL	Scans all local drives (including compressed, CD-ROM, 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	Scans all network drives 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/recovery 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*, which can include 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, Scan updates it. /AF adds about 300% more time to scanning. ✍ */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.*
/ALL	Overrides the default settings by scanning more files. By default, Scan checks files with .COM, .EXE, .SYS, .BIN, .OVL, .DLL, .DOC, and .DOT extensions, which are the files most likely to be infected by a virus. 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 Scan.*
/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, Scan reports that a viral infection may have occurred. The /CF option adds about 250% more time to scanning. 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, Scan 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.*

Command-line Option	Description
/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, Scan reports that a viral infection may have occurred. The /CV option adds about 50% more time to scanning. 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.*
/EXCLUDE *filename*	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. Self-modifying or self-checking files can cause a false alarm during a scan.
/FAST	Speeds up the scan. Reduces scanning time by about 15%. Using the /FAST option, Scan 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.

Command-line Option	Description
/FREQUENCY *hours*	The number of hours that must occur between subsequent successful scans. 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.
/LOAD *filename*	Uses the Scan settings stored in *filename*. Scan gets its settings from the default configuration file, DEFAULT.CFG, which is delivered with BootShield. You can specify any additional options on the command line. Alternatively, 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. Use the /LOAD *filename* command-line option to perform a scan using the information saved in this file. For example, if you have created a configuration file called FLOPPY.CFG, enter: **`scan /load floppy.cfg`** The above command line initiates a scan using its internal default settings plus any options specified in FLOPPY.CFG. See “Creating and editing the configuration file” on page 47 for more information about configuration files.
/LOCK	Halts the system to stop further infection if Scan 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.

Command-line Option	Description
/LOG	Stores the time and date Scan is being run by updating or creating a file called SCAN.LOG in the root of the current drive.
/MANY	Scans multiple diskettes consecutively in a single drive. Scan prompts you for each diskette. Once you have established a virus-free system, use this option to check multiple diskettes quickly. The Scan 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`**
/MEMEXCL	Exclude memory area from scanning. (The default is A000-FFFF, 0000=Scan all.) This command-line option has been added to prevent Scan from checking areas in upper memory which might contain memory-mapped hardware and might cause false alarms.
/MOVE *directory*	Moves all infected files found during a scan to the specified directory. 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.
NOBEEP	Disables the tone that sounds whenever Scan 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.

Command-line Option	Description
/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, Scan checks inside executable, or self-decompressing, files that have been created using the LZEXE or PKLITE file compression programs. Scan decompresses each file in memory and checks for virus signatures, which takes time but results in a more thorough scan. If you use /NOCOMP, Scan does not check inside compressed files for viruses, although it can check for modifications to those files if they have been validated using validation/recovery codes. ✍ *Scan does not check compressed files, such as .ZIP and .ARC files.*
/NODDA	No direct disk access. Prevents Scan from accessing the boot record. This feature has been added to allow Scan to run under Windows NT. You might need to use this option on some device-driven drives.
/NOEMS	Prevents Scan from using expanded memory (LIM EMS 3.2), ensuring that EMS is available to other programs.
/NOEXPIRE	Disables the “expiration date” message if the Scan data files are out of date.

Command-line Option	Description
/NOMEM	Reduces scan time by omitting all memory checks for viruses. Use /NOMEM only when you are absolutely certain that your computer is virus-free. Scan can check system memory for all critical known computer viruses that can inhabit memory. In addition to main memory from 0Kb to 640Kb, Scan checks system memory from 640Kb to 1088Kb that can be used by computer viruses on 286 and later systems. Memory above 1088Kb is not addressed directly by the processor and is not presently susceptible to viruses.
/PAUSE	Enables screen pause. If you specify /PAUSE, the “Press any key to continue” prompt appears when Scan fills up a screen with messages (for example, when you’re using the /SHOWLOG or /VIRLIST options). Otherwise, by default, Scan fills and scrolls a screen continuously without stopping, which allows Scan to run on PCs with many drives or that have severe infections without requiring you to attend. We recommend that you omit /PAUSE when keeping a record of Scan’s messages using the report options (/ REPORT, /RPTCOR, /RPTMOD, and /RPTERR).
/PLAD	Preserve last access dates (on NetWare drives only). Prevents changing the last access date attribute for files stored on a network drive in a Novell network. Normally, NetWare updates the last access date when Scan opens and examines a file. However, some tape backup systems use this last access date to decide whether to back up the file. Use /PLAD to ensure that the last access date does not change as the result of scanning.

Command-line Option	Description
/REPORT *filename*	Creates a report of infected files and system errors. Saves the output of Scan to *filename* in ASCII text file format. If *filename* exists, /REPORT erases and replaces it (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. Scan identifies modified files when the validation/recovery codes do not match (using the /CF or /CV options). You can use /RPTMOD with /RPTCOR and /RPTERR on the same command line.
/RV	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 Scan is being run by updating or creating a file called SCAN.LOG in the current 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, Scan 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 Scan detects. To pause when the screen fills with messages, specify the /PAUSE option. Use /VIRLIST alone or with /PAUSE on the command line. You can save the list of virus names and descriptions to a file by redirecting the output of the command. For example, in DOS, enter: **`scan /virlist > filename.txt`** ✍ *Because Scan can detect many viruses, this file is more than 50 pages long.*

Scan command-line examples

The following examples show the Scan command using various option settings. Remember that you can use the DEFAULT.CFG file to specify the commands used each time Scan is run (see "Creating and editing the configuration file" on page 47).

These examples show how to scan all files, not just the boot sector.

- To scan your computer's C: drive:

  `SCAN C:`

  Scan checks executable files on C:, plus the boot sector and boot master record and RAM memory file viruses.

- To scan the computer's boot sector and master boot record:

  SCAN C: /BOOT

  This command also scans memory.

- To scan executable files on drive F:, a network drive:

  SCAN F:

- To scan executable files on multiple diskettes on drive A:

  SCAN A: /MANY

  Scan checks the diskette in drive A:, then prompts the user to insert more disks to continue checking. This command also scans the diskette's boot sectors.

- To scan all local and network drives (including compressed, CD-ROM, and PCMCIA drives, but not diskettes):

  SCAN C: /ADL /ADN

- To scan for viruses in files and add validation codes to executable files on drives C:, D:, and E:

  SCAN C: D: E: /AV /ALL

- To scan for viruses on network drive M: and create a log file of infections, corruptions, and errors in the file INFECTN.RPT on drive D:

  SCAN M: /REPORT D:\INFECTN.RPT /RPTCOR /RPTERR /APPEND

  If D:\INFECTN.RPT already exists, Scan appends the new information to the existing report file.

- To scan files in the directories USER\MAC, USER\BILL, and USER\DAVE:, including their associated subdirectories, on drive E:

  SCAN E:\USER\MAC E:\USER\BILL E:\USER\DAVE /SUB /ALL

- To quickly scan drives C:, D:, and E: and report any executable files that have associated validation codes and have been modified:

  SCAN C: D: E: /FAST /CV

- To scan a single file, in this case COMMAND.COM:

  SCAN C:\COMMAND.COM

Glossary

The following list defines some terms you might encounter while using BootShield to guard your computer against boot sector viruses and other types of viruses.

boot

To start the computer; to reload DOS into memory using start-up instructions from a disk's boot sector.

bootable diskette

A floppy diskette that contains the DOS system to be loaded into memory upon rebooting.

boot record

Part of the boot sector, defining the logical characteristics of the disk.

boot sector

The portion of the computer's hard drive that contains the instructions for the operating system to start the computer. Boot sector viruses are particularly serious because information in the boot sector is loaded into memory first, before virus protection code can be executed.

boot virus

A computer virus that infects the boot sector or master boot record.

clean

To remove viruses from the computer's hard drive, floppy drive, and boot sector.

CMOS

A part of the computer's memory that contains the time, date, and other information about the computer's configuration.

configuration file

A file that Scan uses to load default options so that you do not need to enter the options on the command line. The configuration file for BootShield's Scan program is DEFAULT.CFG.

corrupted file

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

encrypted virus

A virus that is encoded to prevent detection.

FAT table

In DOS, the file allocation table, which sets up the file structure for the hard drive.

infected file

A file contaminated by a computer virus.

interrupt vector

Four bytes that point to an interrupt service routine address.

interrupt vector table

The bottom 1024 bytes of system memory that represent 256 interrupt vectors.

master boot record (MBR)

A portion of a hard disk containing a partition table that divides the drive into chunks, some of which may be assigned to operating systems other than DOS. The MBR also contains executable code that loads the boot sector.

memory

A storage medium where data and program code are kept temporarily while being used by the computer. DOS supports up to 640KB of conventional memory. Memory beyond that limit may be accessed as EMS, XMS, or an upper memory block.

memory infection

Contamination of a computer's memory by a virus. The only certain way to eliminate memory infections is to turn off the computer, restart from a disk known to be uninfected, and clean up the source of the infection.

modified file

A file that has changed after validation/recovery codes were added.

multi-partite virus

A virus that has two parts. The first part infects the master boot record and/or the boot sector. The second infects files.

partition table

A table that the computer uses to represent any partitioning (logical divisions) of a hard drive.

polymorphic virus

A virus that attempts to evade detection by changing its internal structure or encryption technique in each infection.

recovery codes

Along with validation codes, Scan uses these to detect and recover from unknown viruses. These codes help Scan know if an executable file has been altered. See also validation codes.

stealth virus

A virus that can hide from detection when active in memory. Any type of virus might employ stealth technology.

validation codes

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

vector

See interrupt vector.

virus

A software program that attaches itself to another program or system area (MBR or boot sector) on a disk, and spreads throughout the system. Viruses can damage data, cause the computer to crash, display messages, or do nothing.

Index

C

D

E

N

O

P

Q

R

S

T

U

V

W