IBM AntiVirus Introduction and User's Guide
Version 2.5.1

October 18, 1996

IBM AntiVirus, Version 2.5.1, October 18, 1996

This edition of the IBM AntiVirus Introduction and User's Guide applies to Version 2.5.1 of IBM AntiVirus for DOS, IBM AntiVirus for Windows, IBM AntiVirus for Windows 95, IBM AntiVirus for Windows NT, and IBM AntiVirus for OS/2.

IBM and OS/2 are trademarks of IBM Corp.

Novell and NetWare are trademarks of Novell Corp.

Stacker is a trademark of Stac Electronics.

SuperStor and SuperStor/DS are trademarks of Addstor, Inc.

PKZIP and PKUNZIP are trademarks of PKWARE, Inc.

Microsoft, Windows, Windows 95, and Windows NT are trademarks of Microsoft Corp.

© **Copyright International Business Machines Corporation 1989, 1996. All rights reserved.**
Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Contents

Chapter 1. IBM AntiVirus Introduction 1-1
1.1 IBM AntiVirus Desktop Edition 1-1
1.2 IBM AntiVirus Enterprise Edition 1-2
1.3 For More Information 1-2

Chapter 2. Protecting yourself from viruses (Important!) 2-1

Chapter 3. Installing IBM AntiVirus 3-1
3.1 Installing and updating with default settings 3-1
3.2 Installing with customized settings 3-6
3.3 Scanning the system without installing 3-8
3.4 Creating additional emergency diskettes 3-9
3.5 Online help for IBM AntiVirus Install 3-9
3.6 Installing IBM AntiVirus from the command line 3-10
3.6.1 Command line installation options 3-10
3.6.2 Command line installation examples 3-12
3.7 Format of the response file 3-12
3.7.1 Response file example 3-15
3.8 Return codes 3-15
3.9 IBM Boot Manager and Dual Boot systems 3-16
3.10 Uninstalling IBM AntiVirus 3-16
3.10.1 Uninstalling IBM AntiVirus from the command line 3-18

Chapter 4. Using IBM AntiVirus 4-1
4.1 Normal use of IBM AntiVirus 4-1
4.1.1 Starting IBM AntiVirus 4-1
4.1.2 Automated protection 4-2
4.1.3 Checking diskettes 4-4
4.1.4 Checking your system 4-5
4.1.5 Checking compressed files 4-6
4.1.6 Updating IBM AntiVirus virus data files 4-7
4.1.7 Logs 4-8
4.1.8 Online help 4-9
4.2 IBM AntiVirus time-out message 4-11
4.3 Customizing IBM AntiVirus 4-11
4.3.1 Customizing automated protection 4-11
4.3.2 Customizing diskette checking 4-13
4.3.3 Customizing system checking 4-14
4.4 When a virus is found 4-17
4.4.1 Finding viruses with the System Shield 4-18
4.4.2 Cleaning up an infected system 4-19
4.4.3 Cleaning up diskettes 4-22
4.4.4 Cleaning up nearby systems 4-22
4.4.5 Cleaning up uncommon viruses 4-22
4.4.6 Strategy for containing viruses in organizations 4-23
4.5 Using the IBM AntiVirus stand-alone program 4-24
4.5.1 Running the stand-alone program from the Emergency Diskette . . 4-25
4.5.2 Running the stand-alone program from the command line 4-25
4.5.3 Systems that use resident data compression 4-28

© Copyright IBM Corp. 1989, 1996

4.5.4 Systems that use security software 4-29

Chapter 5. Introduction to computer viruses 5-1
5.1 What is a computer virus? 5-1
5.2 How do virus infections start? 5-2
5.3 How serious is the problem? 5-2

Chapter 6. Anti-virus programs 6-1
6.1 What are anti-virus programs? 6-1
6.2 Techniques used by anti-virus programs 6-1
6.2.1 Scanning 6-1
6.2.2 Change detection 6-2
6.2.3 Heuristic analysis 6-2
6.2.4 Verification 6-2
6.2.5 Disinfection 6-2
6.2.6 Resident and non-resident operation 6-2
6.2.7 Automated operation 6-3
6.2.8 Prevention and detection 6-3
6.2.9 Missing viruses and false alarms 6-3
6.3 Techniques used by IBM AntiVirus 6-3
6.3.1 Change detection and fuzzy scanning 6-3
6.3.2 IBM AntiVirus heuristic analysis 6-4
6.3.3 Safe disinfection of known and unknown viruses 6-5
6.3.4 Thorough examination 6-6
6.3.5 Install and forget operation 6-7
6.3.6 Advanced false alarm elimination 6-7
6.3.7 System shielding 6-7
6.3.8 Intelligent incident management 6-11

Chapter 7. IBM AntiVirus products and services 7-1

Chapter 8. For further reading 8-1

Appendix A. Files installed with IBM AntiVirus for DOS and Windows . A-1

Appendix B. Files installed with IBM AntiVirus for Windows 95 . . . . . B-1

Appendix C. Files installed with IBM AntiVirus for Windows NT C-1

Appendix D. Files installed with IBM AntiVirus for OS/2 . . . . . D-1

Appendix E. Troubleshooting E-1
E.1 For the IBM AntiVirus Installation Program E-2
E.2 For IBM AntiVirus for DOS and Windows E-2
E.3 For IBM AntiVirus for OS/2 . . . . . E-3
E.4 For the System Shield Program in IBM AntiVirus for DOS and Windows E-3

Appendix F. Change history F-1

Index X-1

Figures

3-1. IBM AntiVirus Install Welcome window 3-2
3-2. Select Install or Next to continue with installation 3-2
3-3. Choose the destination directory, then select Next 3-3
3-4. An Express install will use the recommended default settings 3-3
3-5. Select Install to begin installation 3-4
3-6. A progress indicator is shown during installation 3-4
3-7. Installation has completed and your system will be checked 3-5
3-8. The settings menu 3-6
3-9. Installation settings 3-7
3-10. Initial IBM AntiVirus settings 3-7
3-11. Select Scan system to scan now instead of installing 3-8
3-12. You can just scan program files, or all files 3-9
4-1. Check menu 4-4
4-2. Check diskettes dialog 4-5
4-3. Checking the system with the Push here button 4-5
4-4. Telling IBM AntiVirus to check inside compressed files. 4-6
4-5. Updating virus data files 4-8
4-6. Enter the full path and file name of the update file 4-8
4-7. Viewing the Previous Log 4-9
4-8. Help menu 4-10
4-9. Example virus description in Help 4-10
4-10. Customizing Automated checking with the Setup menu 4-11
4-11. Automated check dialog 4-12
4-12. Customizing System Shielding 4-12
4-13. Customizing diskette checking 4-14
4-14. Customizing system checking 4-15
4-15. Specifying particular drives and directories to check 4-15
4-16. Select a drive and directory, then select Add 4-16
4-17. Specifying particular file patterns to check 4-16
4-18. Enter a file pattern, then select Add 4-17
4-19. Message when a virus is found 4-20
4-20. Virus infection report identifies viruses 4-20
4-21. Disinfection message box 4-21
4-22. Thorough examination message box 4-21
4-23. Viewing the current log after disinfection 4-21
6-1. Warn when viral activity occurs 6-5
6-2. Check diskette boot records when used 6-8
6-3. Warn when viral activity occurs 6-8
6-4. Check files when accessed 6-9
6-5. Prevent common DOS viruses 6-10
6-6. Virus descriptions 6-10

© Copyright IBM Corp. 1989, 1996

Chapter 1. IBM AntiVirus Introduction

IBM AntiVirus is a comprehensive anti-virus product for DOS, Windows, Windows 95, Windows NT, and OS/2 systems. It is designed to detect and remove viruses from your system simply and reliably. It is the software that IBM uses to protect its own internal personal computers.

This User's Guide will help you understand viruses, and how to install and use IBM AntiVirus to protect yourself from them.

Please take a moment to print or edit the **READ.ME** file. After installing IBM AntiVirus, you can access the **READ.ME** file for IBM AntiVirus for Windows, IBM AntiVirus for Windows NT, and IBM AntiVirus for OS/2 by double-clicking on the **READ.ME** icon located on your desktop. You can access the The **READ.ME** for IBM AntiVirus for Windows 95 by clicking on the **Start** icon, selecting **Programs**, **AntiVirus**, and clicking on the **READ.ME** icon. The **READ.ME** for IBM AntiVirus for DOS is located in the IBM AntiVirus directory. The **READ.ME** file contains last-minute information that might be pertinent to your configuration.

1.1 IBM AntiVirus Desktop Edition

In this document, "IBM AntiVirus" generally refers to the **IBM AntiVirus for DOS**, **IBM AntiVirus for Windows**, **IBM AntiVirus for Windows 95**, **IBM AntiVirus for Windows NT**, and **IBM AntiVirus for OS/2** products. All of these products, except IBM AntiVirus for Windows NT, are included in the IBM AntiVirus Desktop Edition.

When you receive your IBM AntiVirus Desktop Edition, there are three sets of installation diskettes, and one IBM AntiVirus Emergency Diskette. The three sets of installation diskettes consist of the following:

- IBM AntiVirus for DOS and IBM AntiVirus for Windows are provided on two 1.44MB diskettes. IBM AntiVirus for DOS requires an IBM PC, IBM PS/2, or 100% compatible system with an 8088 or higher processor, a minimum of 640KB of memory, and DOS version 3.3 or higher. IBM AntiVirus for Windows requires an IBM PC, IBM PS/2, or 100% compatible system with an 80386 or higher processor, and Windows 3.1 or Windows 3.11.
- IBM AntiVirus for Windows 95 is provided on two 1.44MB diskettes.
- IBM AntiVirus for OS/2 is provided on two 1.44MB diskettes. It requires an IBM PC, IBM PS/2, or 100% compatible system, and OS/2 version 2.0 or higher.

The IBM AntiVirus Emergency Diskette is provided on one 1.44MB diskette. It contains a minimal DOS 7.0 system, part of the System Shield, and the IBM AntiVirus stand-alone program.

© Copyright IBM Corp. 1989, 1996

1.2 IBM AntiVirus Enterprise Edition

IBM AntiVirus Enterprise Edition is intended for use within organizations. It includes everything in the Desktop Edition, plus additional features needed to fully protect shared computing environments.

For organizations with networks, IBM AntiVirus Enterprise Edition extends the protection of the Desktop Edition to include Windows NT systems and Novell NetWare servers. The IBM AntiVirus Enterprise Edition also includes a version of the IBM AntiVirus stand-alone program for DOS systems with constrained memory.

IBM AntiVirus Enterprise Edition also provides powerful administrative features to distribute, update, and control the use of IBM AntiVirus throughout an enterprise.

1.3 For More Information

For more information, contact your IBM Marketing Representative, or your local IBM AntiVirus Services representative. The section **IBM AntiVirus products and services**, later in this document, will help you contact IBM AntiVirus Services in your country.

Online information about IBM AntiVirus is also available on the Internet via the World Wide Web. Our Web site features new articles about viruses and virus protection, information on and technical support for IBM AntiVirus, and a wealth of resources for people interested in virus protection. Come visit us at **http://www.av.ibm.com**

Chapter 2. Protecting yourself from viruses (Important!)

IBM AntiVirus has been carefully designed to help you reduce your risk of virus infection as much as possible. In general, no program can entirely eliminate the risk of viruses. There are a few simple things you can do to make sure your risk is as small as possible.

1. Use IBM AntiVirus automated checking and system shielding to detect viruses as soon as possible. Use IBM AntiVirus to check diskettes for viruses before booting or running programs from them. See subsequent sections of this document for more information.
2. Keep IBM AntiVirus up to date. As new viruses are written, IBM AntiVirus will be updated to deal with them.
3. Keep good backups, and update them periodically. In some cases, the only way to clean up a system that has become infected with a virus is by restoring it from reliable backups. It is a good idea to check your system with IBM AntiVirus just before you do a backup, to help prevent backing up infected files. If you do not currently have a good backup of your system, you should make one just after you install IBM AntiVirus.
4. Whenever possible, keep your diskettes write-protected. Most infections travel from one PC to another on diskettes. Diskettes become infected when they are used in an infected system, and have not been write-protected. Write-protecting your diskettes will keep them from becoming infected.
5. Whenever possible, prevent executable files on LAN file servers from being modified by client PCs. This prevents an infected client PC from infecting the LAN file server, and causing the infection to spread widely to other client PCs. The DOS "read-only" attribute does not prevent virus infection. Your LAN administrator will know how to use the server's operating system to protect the server files.

© Copyright IBM Corp. 1989, 1996

Chapter 3. Installing IBM AntiVirus

The IBM AntiVirus installation diskettes contain everything you need to install IBM AntiVirus on your system. You can use the installation program to scan your system for viruses without installing IBM AntiVirus. They also contain an Emergency Diskette for use when your system is already infected and IBM AntiVirus cannot be installed or executed.

You can also use the IBM AntiVirus installation programs to create additional "emergency diskettes." This is useful when you cannot access the usual IBM AntiVirus program due to virus problems on your system. See the section **Creating additional emergency diskettes** for more information.

3.1 Installing and updating with default settings

Installing IBM AntiVirus for the first time and upgrading it to a new version are done in the same way. You can choose to install IBM AntiVirus with default or customized settings. You should normally accept all of the defaults without changing the settings.

To install IBM AntiVirus from an icon:

1. Insert the first diskette from the appropriate set of diskettes into the diskette drive.
2. Open the A: drive folder and double-click on the SETUP icon (or for OS/2, the SETUPOS2 icon).
3. Follow the instructions on the screen. To install with the default settings, click the Next button on each dialog.

In Windows 95, to install IBM AntiVirus from the Add/Remove Programs application:

1. Insert the first diskette from the appropriate set of diskettes into the diskette drive.
2. Launch the Add/Remove Programs application in the Control Panel folder and click the Install... button.
3. Follow the instructions on the screen. To install with the default settings, click the Next button on each dialog.

To install IBM AntiVirus from a command line:

1. Insert the first diskette from the appropriate set of diskettes into the diskette drive.
2. Type "a:\setup" (or for OS/2, "a:\setupos2").
3. Follow the instructions on the screen. To install with the default settings, click the Next button on each dialog.

After displaying an initialization dialog, the IBM AntiVirus Install Welcome window appears.

© Copyright IBM Corp. 1989, 1996

Figure 3-1. IBM AntiVirus Install Welcome window

To continue installing IBM AntiVirus with default settings:

1. Select the **Next** push button on the IBM AntiVirus Install Welcome window.
   The IBM AntiVirus Install Install/Scan system window is displayed.

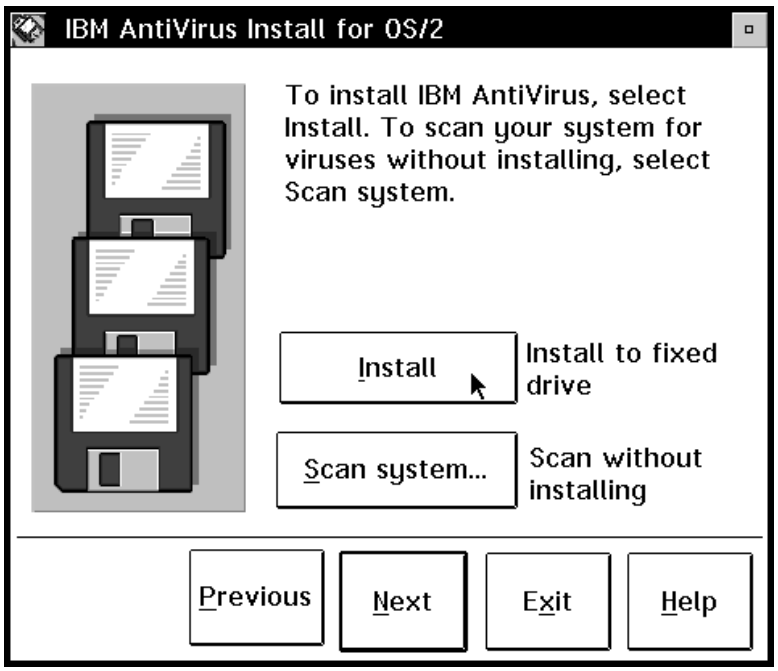

Figure 3-2. Select Install or Next to continue with installation

2. Select **Install** or **Next** to continue installing with default settings.
   The Destination Directory window is displayed.

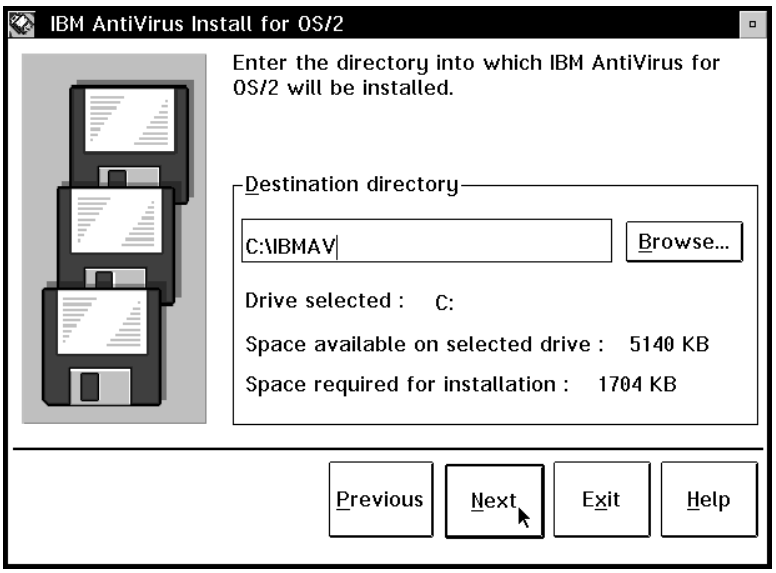

Figure 3-3. Choose the destination directory, then select Next

3. Choose the directory where you want IBM AntiVirus to be installed.

   The default directory for DOS, Windows and OS/2 is C:\IBMAV. The default directory for Windows 95 is C:\IBMAV95. The default directory for Windows NT is C:\IBMAVNT.

4. Select the **Next** push button.

   The Express/Custom Install window is displayed.

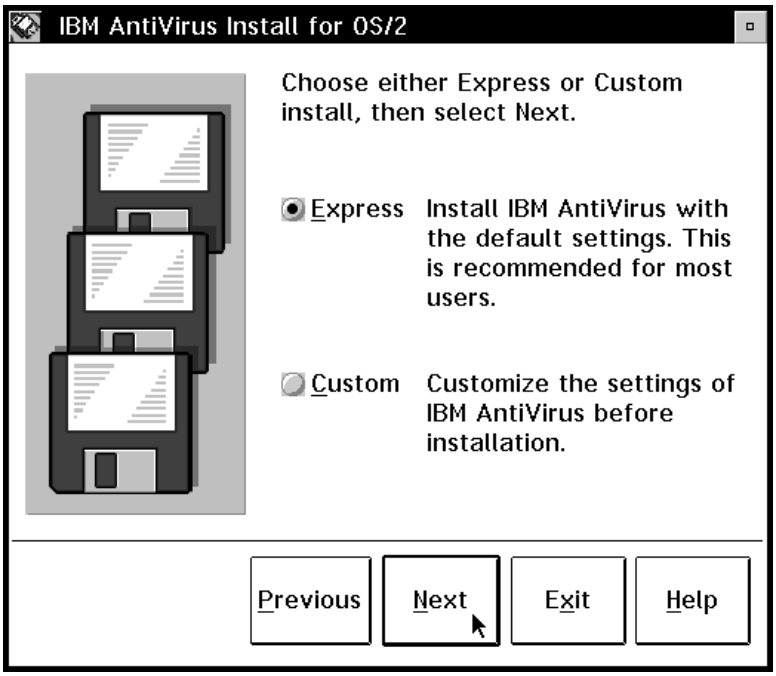

Figure 3-4. An Express install will use the recommended default settings

5. Choose **Express** to install IBM AntiVirus with the recommended default settings.
6. Select the **Next** push button to continue.

   The Begin Installation window is displayed.

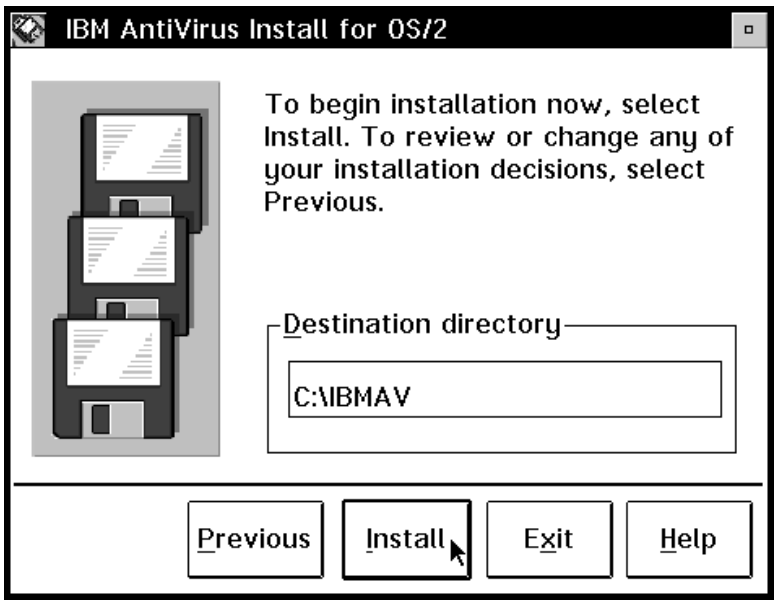

Figure 3-5. Select Install to begin installation

7. Select the **Install** push button.

   A progress indicator is shown during the installation process.

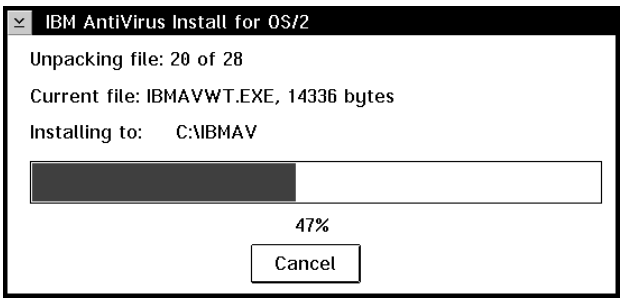

Figure 3-6. A progress indicator is shown during installation

8. When prompted, insert the second installation diskette and click on **OK**.

   When IBM AntiVirus is installed, the Installation Complete window is displayed.

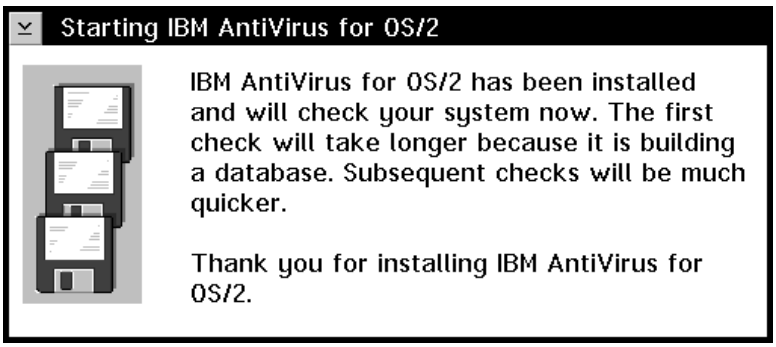

Figure 3-7. Installation has completed and your system will be checked

9. If you installed IBM AntiVirus for DOS, IBM AntiVirus for Windows, IBM AntiVirus for Windows 95, or IBM AntiVirus for Windows NT, you need to remove the installation diskette from the drive and reboot your system. If you installed IBM AntiVirus for OS/2, you do not have to reboot.

When IBM AntiVirus is installed, automated checking will be set up to run weekly. On DOS systems, it will run the first time your system is started that week. On OS/2, Windows, Windows 95, and Windows NT systems, it will run at 3:00 AM on Monday morning. If your system is not turned on at that time, it will run shortly after your system is started the next time.

If you have installed IBM AntiVirus previously, IBM AntiVirus Install will, by default, update your current version and will keep all of your current settings. This makes updating simple.

You might want to change the default settings when you install IBM AntiVirus. For information on how to do so, see the section “Customizing installation settings” later in this chapter.

Some viruses damage programs (like Windows itself) so that they cannot be run. If you are concerned about such programs, consider changing automated checking to check more frequently. You can change it to check DOS systems on every boot, for instance, and to check OS/2, Windows, Windows 95, and Windows NT systems every day at a specified time.

If you have previously installed IBM AntiVirus for OS/2 Version 1.00, please note that it was installed in C:\IBMAV2 by default. Later versions of IBM AntiVirus for OS/2 install in C:\IBMAV by default. You might want to remove the old files and directory after installing the new version.

Some viruses affect the ability of Windows systems to operate unless the proper anti-virus precautions are taken. In some cases, they can make it impossible to start Windows. For this reason, we recommend that Windows users have the "Prevent common DOS viruses" feature of the IBM AntiVirus System Shield installed at all times, and that Automated checking be set up to check the system periodically.

3.2 Installing with customized settings

The defaults for the installation program have been constructed to provide the best protection for most systems. You should normally accept all of the defaults without changing the settings.

If you need to change the installation settings:

1. Select **Custom** from the Express/Custom Install window.

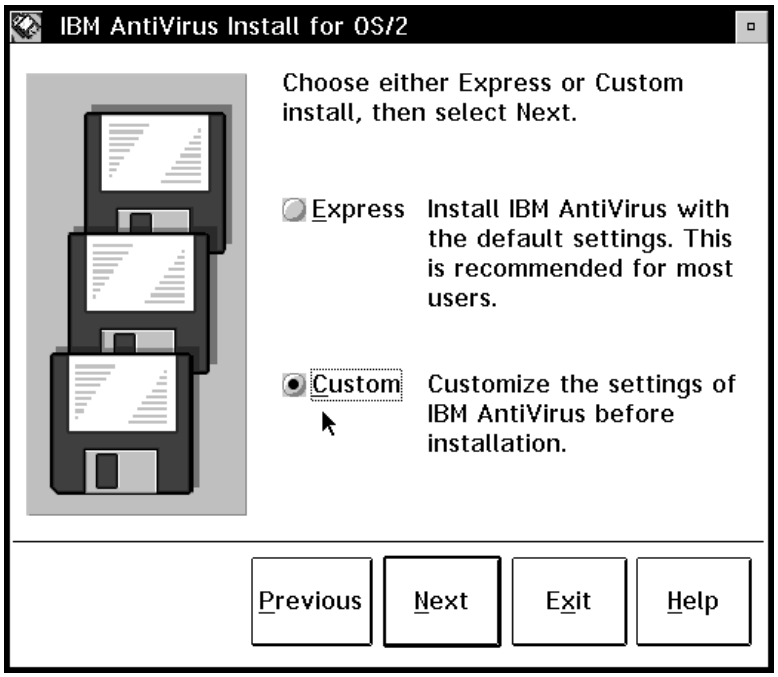

Figure 3-8. The settings menu

2. Select **Next**.

   The Installation Settings window is displayed.

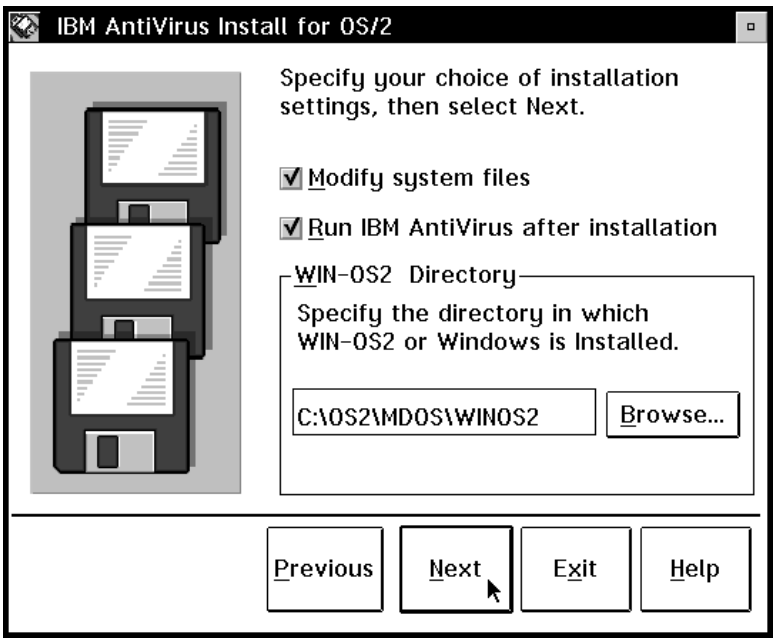

Figure 3-9. Installation settings

This window lets you specify whether or not IBM AntiVirus Install should modify your systems files (e.g. AUTOEXEC.BAT) to enable your system to be protected automatically. If you do not choose to have your system files modified, IBM AntiVirus Install will generate example files that show you how to modify the system files yourself.

You can also specify whether IBM AntiVirus should check the system as soon as installation is completed, and the location of your Windows directory if you have one.

3. Select the installation options that you want.
4. Select **Next** when you are finished selecting these settings.

   The Choose Initial Settings window is displayed.

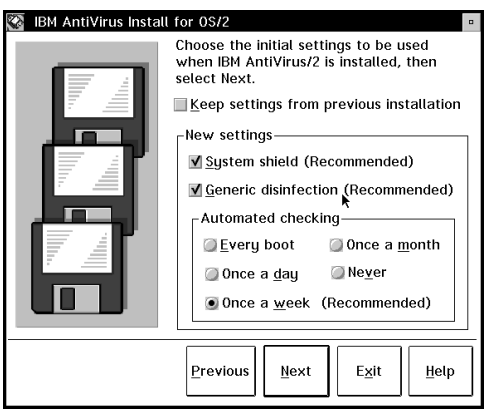

Figure 3-10. Initial IBM AntiVirus settings

This window lets you specify whether or not to keep your current settings if you have already installed IBM AntiVirus, and to specify the initial settings for automated protection and generic disinfection in IBM AntiVirus.

5. Select your settings and then press **Next**.

   The Begin Installation window is displayed.

6. Press **Install** to begin the installation process.

3.3 Scanning the system without installing

If you have found a virus on one system, you should check nearby systems to see if they are also infected. If these systems do not have IBM AntiVirus installed on them, and if you do not want to install it at this time, you can use IBM AntiVirus Install to scan the system for viruses without installing IBM AntiVirus.

In the second install window, select **Scan system** instead of **Install**. On the resulting window, select either **Scan program files** or **Scan all files**. The IBM AntiVirus stand-alone program will check your system for viruses.

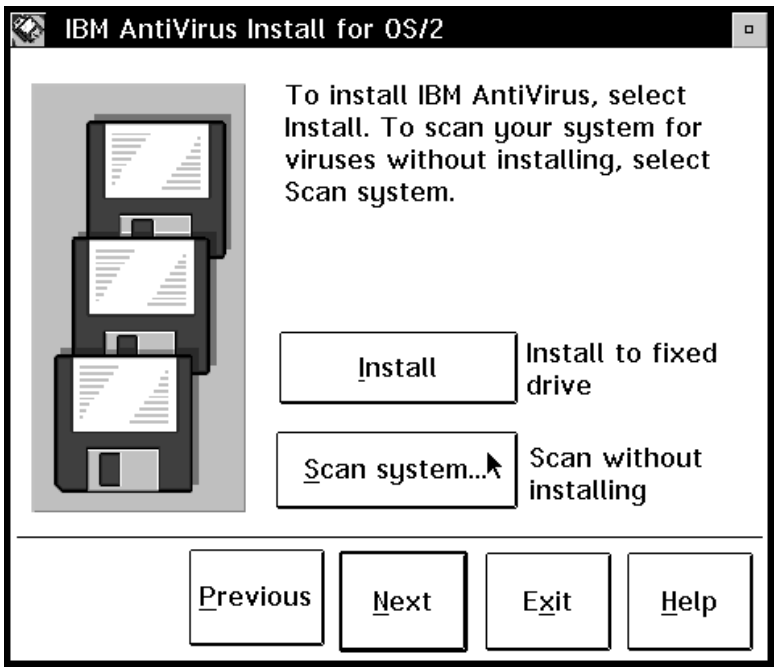

Figure 3-11. Select Scan system to scan now instead of installing

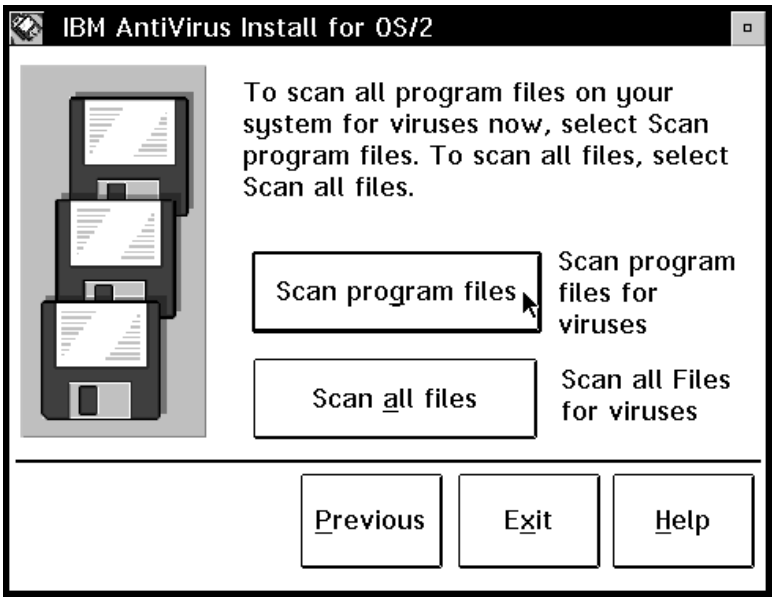

Figure 3-12. You can just scan program files, or all files

3.4 Creating additional emergency diskettes

Although an emergency diskette is distributed with IBM AntiVirus, you can use IBM AntiVirus Install to create additional “emergency diskettes.” These diskettes can be used to scan and clean up systems that cannot boot from the hard disk due to a virus problem. While the Emergency Diskette can disinfect boot record viruses and viruses that are active in memory, it is not a substitute for installing IBM AntiVirus on your system or for thoroughly scanning a system when the product is installed.

To create additional Emergency Diskettes:

1. Select the **Emergency diskettes** push button on the second install window, rather than the **Install** push button.

   You will be prompted to insert a scratch diskette into drive A: for formatting. **Be sure to use the highest density diskette that your drive will support**. Do not use a 720 KB diskette in a dual density 720 KB / 1.44 MB

2. After formatting finishes, press **Enter** when prompted for a label.
3. Reply “N” to avoid formatting another diskette. The necessary files will then be copied to your emergency diskettes. Write-protect the diskette immediately to help ensure that it does not become infected with a virus.

3.5 Online help for IBM AntiVirus Install

Context-sensitive help is always available in IBM AntiVirus Install by pressing the F1 key, or by selecting the **Help** push button on any window. The **READ.ME** file might also have installation information and last minute news that applies to you.

3.6 Installing IBM AntiVirus from the command line

You can also install IBM AntiVirus non-interactively by specifying options with the **SETUP** and **SETUPOS2** commands:

1. Insert the first diskette from the appropriate set of diskettes into the diskette drive.
2. Launch the IBM AntiVirus Install program by typing "a:\setup options" (or for OS/2, "a:\setupos2 options").

3.6.1 Command line installation options

The [options] that can be specified on the command line are specified as a keyword, optionally followed by an equal sign (=) or a colon (:), and by a value. The following list contains the installation options that you can specify.

/**AUTO[=path]** Use automatic installation to install IBM AntiVirus. If you are installing into a directory that has a previous version of IBM AntiVirus in it, your current IBM AntiVirus settings will be preserved unless the /COPY option is also specified. If "path" is specified, IBM AntiVirus will be installed in that disk and directory. If "path" is not specified, IBM AntiVirus for DOS and IBM AntiVirus for Windows will be installed in C:\IBMAV (or into whatever directory it was installed previously). IBM AntiVirus for Windows 95 will be installed in C:\IBMAV95. IBM AntiVirus for Windows NT will be installed in C:\IBMAVNT. If the /AUTO option is used, installation will be automatic unless there is a message which requires the user to respond. This option will be ignored if the /R option is specified.

/**COPY**

During installation, copy the settings contained in the profile files distributed with the installation program into the directory into which IBM AntiVirus is being installed. **These profiles will overwrite any profiles that might have been in the directory previously.** This is useful to make sure that settings in previous profiles are returned to their installed state. It can be used by administrators who have customized these settings, to ensure that their customized settings are installed. This option will be ignored if the /R option is specified.

/**DOSONLY**

This option is for IBM AntiVirus Install for DOS only. It will be ignored if it is specified by IBM AntiVirus Install for Windows. If it is specified, only IBM AntiVirus for DOS will be installed, even if Windows is installed on the system. If IBM AntiVirus for Windows had been installed previously, using the /DOSONLY option during installation will update only IBM AntiVirus for DOS. You must update IBM AntiVirus for Windows as well in order for it work properly in some cases. This option will be ignored if the /R option is specified. See the related /WINDOWS option for more information.

/**L[=path]**

"path" is a full path name of an installation log file. If the path is not specified, the log file is written to the installation directory, and is named AVINSTAL.LOG.

/LAN[=path]

The /LAN option indicates that IBM AntiVirus should be installed to execute from a file server. To use this option, you must execute the SETUP.EXE or SETUPOS2.EXE program directly from a file server, and your workstation must be permanently attached to your local area network. The install program will copy to your hard disk only the files needed to initialize IBM AntiVirus. The rest of the files used to execute IBM AntiVirus will be loaded from the file server as needed.

The install program can determine the execution directory automatically: execution directories for each platform are located in the same directory tree on the file server as the installation program. Or, the "path" to an alternate execution directory can be specified explicitly with the "/LAN[=path]" option. If the install program cannot find the execution directory, it will ignore the /LAN option.

The default for workstations that do not have an earlier release of IBM AntiVirus installed is "/NOLAN". The default for workstations that have any release of IBM AntiVirus prior to 2.5 is also "/NOLAN". The default for workstations that have release 2.5 or later installed is to keep the current setting.

/NOLAN

The /NOLAN option indicates that IBM AntiVirus should be installed to execute from the hard disk. Even if the SETUP.EXE or SETUPOS2.EXE program is executed directly from a file server, the install program will copy all files needed to initialize and execute IBM AntiVirus to your hard disk. Your workstation need not remain attached to your local area network after the install program has finished.

The default for workstations that do not have an earlier release of IBM AntiVirus installed is "/NOLAN". The default for workstations that have any release of IBM AntiVirus prior to 2.5 is also "/NOLAN". The default for workstations that have release 2.5 or later installed is to keep the current setting.

/R=path

"path" is the full path name of the response file to be used during installation. If /R is used, the path must be specified. Options that are specified on the command line override their corresponding options in a response file. If the /R option is used, installation will be entirely automatic. The user will not be asked to enter any information or respond to any messages.

/STARTUP.CMD

This option is for IBM AntiVirus Install for OS/2 only. If it is specified, the commands to start the IBM AntiVirus Automated Execution Monitor will be added to the STARTUP.CMD file rather than placed in the Startup folder. By default, IBM AntiVirus Install for OS/2 uses the Startup folder if possible.

/WINDOWS[=path]

This option is for IBM AntiVirus Install for DOS only. If it is specified, both IBM AntiVirus for DOS and IBM AntiVirus for Windows are

installed. You must also specify /AUTO for an automated installation to be done. If /AUTO is specified and /WINDOWS is not, IBM AntiVirus for Windows will be installed anyway if you have previously installed it, or if a Windows directory is currently in your PATH. If "path" is specified, it should specify the disk and directory where Windows has been installed. If "path" is not specified, Windows is assumed to be installed as determined from the current PATH or, if Windows is not in the PATH, in C:\WINDOWS. See the related /DOSONLY option for more information.

3.6.2 Command line installation examples

To install IBM AntiVirus into the directory C:\IBMAV (or into whatever directory it was installed previously), and to accept all of the default installation parameters, enter the following:

```
A:\SETUP /AUTO
```

For IBM AntiVirus for DOS, this will install both IBM AntiVirus for Windows and IBM AntiVirus for DOS, if your Windows directory is in your PATH.

To install IBM AntiVirus into the directory D:\UTIL\IBMAV and accept all of the default installation parameters, enter the following:

```
A:\SETUP /AUTO=D:\UTIL\IBMAV
```

If Windows is installed in E:\MISC\WINDOWS, and it is not in your PATH, you can install both IBM AntiVirus for DOS and IBM AntiVirus for Windows into the directory D:\UTIL\IBMAV and accept all of the default installation parameters, by entering the following:

```
A:\SETUP /AUTO=D:\UTIL\IBMAV /WINDOWS=E:\MISC\WINDOWS
```

3.7 Format of the response file

A response file can be used to specify all of the settings for IBM AntiVirus Install. The full path of the response file can be specified on the command line of IBM AntiVirus Install with the /R option. If the /R option is used, installation will be entirely automatic. The user will not be asked to enter any information or respond to any messages.

The response file consists of one tag per line, followed by an equal sign, followed by a value. If a tag is not present, the default value is used. If a tag is present, a value must be specified for it. Unrecognized tags will be ignored. The tags are as follows.

AllowUninstall

A value of 0 indicates that you cannot uninstall IBM AntiVirus unless you can supply a challenge password. A value of 1 indicates that a password is not required to uninstall IBM AntiVirus. The default is 1.

AutoCheck

A value of 0 indicates that Automated checking should occur on every boot. 1 says to check once a day. 2 says to check once a week. 3 says to check once a month. 4 says never to check. The default is 2. If you use AutoCheck, you should also use PreserveCurrentSettings=0. If IBM AntiVirus is already installed, and you use the AutoCheck tag to

change when Automated checking occurs, be sure to reboot the system after installation so that the new value will take effect. Since you are using a response file, IBM AntiVirus Install will not prompt you to do so.

BootDrive

The drive from which the system is normally booted. The default is C: for DOS, Windows, Windows NT, and Windows 95 systems. For OS/2 systems, the default is the drive from which the system was booted. Naturally, the drive you specify must be the correct boot drive for the system.

DosOnly

This option is for IBM AntiVirus Install for DOS only. It will be ignored if it is used with IBM AntiVirus Install for Windows. A value of 1 indicates that only IBM AntiVirus for DOS will be installed, even if Windows is installed on the system. 0 indicates that IBM AntiVirus for Windows will be installed if there is a valid Windows directory, or if IBM AntiVirus for Windows had been installed previously. If IBM AntiVirus for Windows had been installed previously, using the DosOnly tag during installation will update only IBM AntiVirus for DOS. You must update IBM AntiVirus for Windows as well in order for it to work properly in some cases. The default value is 0.

ExecutionDirectory=path

This option specifies the path to a directory on a file server containing the files needed to execute IBM AntiVirus when RunFromLan=1 has been specified. When this option is not specified, the default path is determined automatically by the install program.

If RunFromLan=1 has not been specified, this option is ignored.

GenericDisinfect

A value of 1 enables generic disinfection, which allows IBM AntiVirus to disinfect even previously-unknown viruses. 0 disables this feature. The default value is 1.

InstallShield

A value of 1 indicates to install the System Shield whenever DOS is started. 0 indicates that the System Shield should not be started when DOS starts. The default value is 1. If you use InstallShield, you should also use PreserveCurrentSettings=0.

ModifySystemFiles

A value of 1 indicates that IBM AntiVirus Install should modify the system files automatically (AUTOEXEC.BAT, CONFIG.SYS, WIN.INI and/or OS2.INI). 0 indicates that it should not. The default value is 1.

PreserveCurrentSettings

A value of 1 indicates that the current settings for IBM AntiVirus should be kept if this is an update. 0 indicates that the settings specified in IBM AntiVirus Install should be used instead. If you specify a value of 0 but do not specify InstallShield or AutoCheck, this is equivalent to using the /COPY command line parameter. If you specify a value of 1, the

current settings are kept, except for when InstallShield, AutoCheck, or GenericRepair are specified. The default value is 1.

RunFromLan

A value of 1 indicates that IBM AntiVirus should be installed to execute from a file server. To use this option, you must execute the SETUP.EXE or SETUPOS2.EXE program directly from a file server, and your workstation must be permanently attached to your local area network. The install program will copy to your hard disk only the files needed to initialize IBM AntiVirus. The rest of the files used to execute IBM AntiVirus will be loaded from the file server as needed.

A value of 0 indicates that IBM AntiVirus should be installed to execute from the hard disk. Even if the SETUP.EXE or SETUPOS2.EXE program is executed directly from a file server, the install program will copy all files needed to initialize and execute IBM AntiVirus to your hard disk. Your workstation need not remain attached to your local area network after the install program has finished.

The install program can determine the execution directory automatically: execution directories for each platform are located in the same directory tree on the file server as the installation program. Or, the path to an alternate execution directory can be specified explicitly with the ExecutionDirectory tag, described earlier.

The default for workstations that do not have an earlier release of IBM AntiVirus installed is 0. The default for workstations that have any release of IBM AntiVirus prior to 2.5 is also 0. The default for workstations that have release 2.5 or later installed is to keep the current setting.

If you specify RunFromLan=1 but do not specify an execution directory, IBM AntiVirus is installed to execute from a file server and the install program determines the execution directory automatically.

If you specify only ExecutionDirectory=path, and do not specify RunFromLan=1, IBM AntiVirus is installed to execute from a file server.

If you specify RunFromLan=0 and also specify an execution directory, the install program indicates an error condition.

In all cases, if you specify an invalid execution directory, the install program indicates an error condition.

RunInitialCheck

A value of 1 indicates that a thorough check of all program files should be done after completing the installation. 0 skips this check. The default value is 1.

TargetDir

The directory into which IBM AntiVirus will be installed. The default for IBM AntiVirus for DOS and IBM AntiVirus for Windows is C:\IBMAV if this is the first time IBM AntiVirus has been installed, or the current IBM AntiVirus directory if this is an update. For IBM AntiVirus for Windows 95, the default directory is C:\IBMAV95 if this is the first time IBM AntiVirus has been installed, or the current IBM AntiVirus directory if this is an update. For IBM AntiVirus for Windows NT, the default directory is

C:\IBMAVNT. if this is the first time IBM AntiVirus has been installed, or the current IBM AntiVirus directory if this is an update. If IBM AntiVirus is already installed, and you use the TargetDir tag to reinstall it into a different directory, be sure to reboot the system after installation so that the new value will take effect. Since you are using a response file, IBM AntiVirus Install will not prompt you to do so.

UpdateStartupCmd

This tag is only valid in IBM AntiVirus Install for OS/2. A value of 1 indicates that the commands to start the IBM AntiVirus Automated Execution Monitor will be added to the STARTUP.CMD file rather than placed in the Startup folder. 0 indicates that the Startup folder will be used, if possible. The default value is 0.

WindowsDir

The directory in which Windows is installed. The default is determined from your current PATH or, if Windows is not in the PATH, in C:\WINDOWS.

3.7.1 Response file example

The following response file would cause IBM AntiVirus to be installed in D:\UTIL\IBMAV and would overwrite any current IBM AntiVirus settings with the default settings used by IBM AntiVirus Install.

```
TargetDir=D:\UTIL\IBMAV
PreserveCurrentSettings=
```

3.8 Return codes

IBM AntiVirus Install can return the following return codes in DOS or OS/2. These return codes can be used by programs that invoke IBM AntiVirus Install, to determine the results of the installation process. The return codes conform to the requirements for CID (Configuration, Installation, Distribution) automated installations over networks. CID installation is supported by IBM's NetView Distribution Manager/2 program. See the section **For further reading** for information on a reference manual for NetView Distribution Manager/2.

Return codes other than 0 indicate some kind of problem, and are only returned if an automated installation is being done. If a problem is encountered during an automated installation, IBM AntiVirus Install returns immediately with the appropriate return code. If a problem is encountered during a menu-driven installation, an error pop-up occurs and the user is given a choice of how to handle the problem.

IBM AntiVirus Install for DOS can return the following return codes. The conditions under which these values are returned is consistent with the CID guidelines. The values themselves differ from the CID guidelines because DOS programs cannot return values in the range recommended by the guidelines.

0 Normal return. No errors were encountered.

1 The installation completed successfully. The system must be rebooted in order for changes in the system files to take effect.

3 An invalid tag was specified in the response file, or the response file itself is invalid.

5 A file could not be accessed.

7 A read or write error occurred on a disk.

8 There is not enough space on the disk for installation.

9 The command line arguments to IBM AntiVirus Install were incorrect.

In OS/2, IBM AntiVirus Install for OS/2 can return the following return codes. These are the values recommended by the CID guidelines.

0 Normal return. No errors were encountered.

2048 An invalid tag was specified in the response file, or the response file itself is invalid.

2052 The installation could not be completed because a WIN-OS2 session is running in OS/2 with the IBM AntiVirus System Shield active.

2056 A file could not be accessed.

4608 A read or write error occurred on a disk.

4616 There is not enough space on the disk for installation.

5632 The command line arguments to IBM AntiVirus Install were incorrect.

3.9 IBM Boot Manager and Dual Boot systems

If you are using IBM Boot Manager to boot multiple operating systems, each operating system must be protected separately. You should install IBM AntiVirus for DOS or IBM AntiVirus for Windows on each DOS partition, IBM AntiVirus for Windows 95 on each Windows 95 partition, IBM AntiVirus for Windows NT on each Windows NT partition, and IBM AntiVirus for OS/2 on each OS/2 partition.

Dual Boot systems can boot either DOS or OS/2 from the same partition. To protect both operating systems, you should boot DOS and install IBM AntiVirus for DOS, then boot OS/2 and install IBM AntiVirus for OS/2.

IBM AntiVirus for DOS and IBM AntiVirus for OS/2 use some of the same files for their operation. If you have a Dual Boot or Boot Manager system with both DOS and OS/2, and you want to install both IBM AntiVirus for DOS and IBM AntiVirus for OS/2, they can be installed into the same directory. If you do use the same directory for both, and you update one of them, you must update the other at the same time to ensure correct operation.

3.10 Uninstalling IBM AntiVirus

You should not need to remove IBM AntiVirus from your system. Doing so will reduce your protection against viruses, and could result in your system becoming infected without your knowledge. In particular, you should not remove IBM AntiVirus before updating it to a new version.

If you do invoke the IBM AntiVirus Uninstall program, it removes all installed IBM AntiVirus files and the directory in which IBM AntiVirus is installed. It also removes

any changes that IBM AntiVirus made to system files and registries when it was installed. In addition, the uninstall program removes the IBM AntiVirus program group and icon from your desktop. On OS/2 systems, it also removes the program group and removes the icon from your start-up folder. Note that if you used the IBM AntiVirus for DOS installation program and installed IBM AntiVirus for both DOS and Windows, the DOS uninstall program does not remove the Windows program group and icon. You must manually delete the Windows program group the next time you invoke Windows.

If you have multiple IBM AntiVirus platforms installed in the same directory (for example, IBM AntiVirus for DOS and IBM AntiVirus for OS/2), you must invoke the uninstall program for both DOS and OS/2 to completely remove IBM AntiVirus from your system. Otherwise, the remaining IBM AntiVirus program will not function properly.

If you are using IBM Boot Manager to boot multiple operating systems, you must uninstall IBM AntiVirus from each partition on which it was installed. The uninstall program only removes IBM AntiVirus from the currently visible partition. Similarly, on Dual Boot Systems, the uninstall program only removes IBM AntiVirus from the system that is currently booted. To completely remove IBM AntiVirus from your system, you should boot one system and invoke the uninstall program. Then, boot the remaining operating system and invoke its uninstall program.

To remove IBM AntiVirus from your system, do the following:

1. If you are uninstalling IBM AntiVirus for Windows, Windows NT, or OS/2, double-click on the Uninstall icon in the IBM AntiVirus folder on your desktop.

   If you are uninstalling IBM AntiVirus for Windows 95, click on the **Start**, icon, select **Programs**, and **AntiVirus**. Then select the IBM AntiVirus Uninstall icon.

   If you are uninstalling IBM AntiVirus for DOS, switch to the directory where IBM AntiVirus is installed and enter the command

   ```
   UNINSTD
   ```

   at a DOS prompt.

   See **Uninstalling IBM AntiVirus from the command line** for additional information.

   Before continuing, the Uninstall program prompts you for confirmation.

2. Answer "YES" if you want to continue uninstalling IBM AntiVirus.

   Note that if you have both IBM AntiVirus for DOS and IBM AntiVirus for OS/2 installed in the same directory, you must indicate if you want IBM AntiVirus to continue its uninstall program because the remaining version of IBM AntiVirus will no longer function properly.

   While IBM AntiVirus is being uninstalled, a progress indicator is displayed.

3. On Windows, Windows NT, Windows 95, and OS/2 systems, if there are any files remaining in the IBM AntiVirus installation directory, a dialog is displayed listing the names of these files. Select the files you want to delete and click on **OK**.

   On DOS systems, if there are any files remaining in the IBM AntiVirus installation directory, the IBM AntiVirus Uninstall program informs you that the directory is not empty. When asked if you want to erase the remaining files,

enter "Y" to continue with the uninstall program. If your IBM AntiVirus installation directory is C:\DOS, you are not asked to erase remaining files, and the directory is not removed.

When all files have been successfully removed, IBM AntiVirus issues a message indicating the uninstall was successful.

4. If you uninstalled IBM AntiVirus for DOS, IBM AntiVirus for Windows, IBM AntiVirus for Windows NT, or IBM AntiVirus for Windows 95, you must reboot your system. If you uninstalled IBM AntiVirus for OS/2, you do not have to reboot.

3.10.1 Uninstalling IBM AntiVirus from the command line

In addition to uninstalling IBM AntiVirus from the desktop icon, you can invoke the IBM AntiVirus Uninstall program from the command line.

IBM AntiVirus for DOS

To uninstall IBM AntiVirus for DOS from the command line, switch to the directory where IBM AntiVirus is installed and type the following at a DOS prompt:

```
UNINSTD [options]
```

IBM AntiVirus for Windows

To uninstall IBM AntiVirus for Windows from the command line, switch to the directory where IBM AntiVirus is installed and type the following at a DOS prompt:

```
UNINSTW [options]
```

IBM AntiVirus for Windows 95

To uninstall IBM AntiVirus for Windows 95 from the command line, switch to the directory where IBM AntiVirus is installed and type the following at a DOS prompt:

```
UNINST95 [options]
```

IBM AntiVirus for Windows NT

To uninstall IBM AntiVirus for Windows NT from the command line, switch to the directory where IBM AntiVirus is installed and type the following at a DOS prompt:

```
UNINSTNT [options]
```

IBM AntiVirus for OS/2

To uninstall IBM AntiVirus for OS/2 from the command line, switch to the directory where IBM AntiVirus is installed and type the following at an OS/2 prompt:

```
UNINST2 [options]
```

The [options] that can be specified on the command line are specified as a keyword, optionally followed by an equal sign (=) or a colon (:) and by a value. The following list contains the uninstall options that you can specify.

/R

When specified, the IBM AntiVirus Uninstall program automatically removes IBM AntiVirus from your system without any user interaction. It only removes IBM AntiVirus files from the installation directory; non-IBM AntiVirus files are not removed.

/P [=password]

This option is used only if AllowUninstall=0 was specified when IBM AntiVirus was installed. This indicates that you must supply a challenge password to uninstall IBM AntiVirus. If you do not specify the /P option and a password is required to uninstall IBM AntiVirus, the IBM AntiVirus Uninstall program prompts you for the challenge password.

/L [=logfile]

When specified, the IBM AntiVirus Uninstall program creates a log file containing informational messages. If this option is not specified, the log file is not created.

Chapter 4. Using IBM AntiVirus

This chapter will help you understand how to use IBM AntiVirus to protect your system from viruses. It covers normal use of the program, how to customize it, what happens when a virus is found, and how to use the stand-alone version of the program.

4.1 Normal use of IBM AntiVirus

IBM AntiVirus has been designed to protect your system automatically. You can also use it to check your system for viruses whenever you want. It is important to note that when you are using IBM AntiVirus to protect your system, you **do not** have to disable it to install other applications. It is recommended that you never disable IBM AntiVirus when installing other applications because this is when your system is most vulnerable to virus infection.

4.1.1 Starting IBM AntiVirus

After you have installed IBM AntiVirus, it can run automatically, and you might never have to start it manually. In general, you should not have two copies of IBM AntiVirus running at the same time. Having only one copy running ensures that only one program is writing to the log, and so on. IBM AntiVirus will attempt to detect when another copy is running, and not run another. In DOS and Windows systems, you must have SHARE installed for IBM AntiVirus to detect when another copy is running. (Consult your DOS manual for more information on SHARE.)

IBM AntiVirus for DOS

You can start IBM AntiVirus for DOS by switching to the directory into which you installed IBM AntiVirus (by default, this is C:\IBMAV) and typing IBMAVD as follows:

```
CD IBMAV
IBMAVD
```

You should start IBM AntiVirus for DOS from a normal DOS session, not from a DOS session within Windows.

IBM AntiVirus for OS/2

You can start IBM AntiVirus for OS/2 by double-clicking on the IBM AntiVirus for OS/2 icon which, by default, is located on your OS/2 desktop.

IBM AntiVirus for Windows and IBM AntiVirus for Windows NT

You can start IBM AntiVirus for Windows and IBM AntiVirus for Windows NT by double-clicking on the IBM AntiVirus icon, which IBM AntiVirus Install puts in the AntiVirus program group.

IBM AntiVirus for Windows 95

You can start IBM AntiVirus for Windows 95 by clicking on the **Start** icon. Select **Programs**, **AntiVirus** and then click on the IBM AntiVirus icon.

© Copyright IBM Corp. 1989, 1996

4.1.2 Automated protection

IBM AntiVirus offers three kinds of automated protection.

1. **Automated checking** checks your disks for viruses whenever you boot your system, or every so often at specified intervals (daily, weekly, etc.). With IBM AntiVirus for Windows, IBM AntiVirus for OS/2, IBM AntiVirus for Windows 95, and IBM AntiVirus for Windows NT, you can also request an automatic check to run at a specific time (hour and minute).

   When you boot your system, IBM AntiVirus checks to see if you have asked for your system to be checked on boot. In DOS, automated checks occur when your boot your system. On Windows NT systems, the automatic check occurs when you log on. If you requested an automatic check in IBM AntiVirus for Windows, the automatic check begins when you load Windows. On OS/2, Windows, Windows 95, and Windows NT, checking your system on boot will be delayed for about five minutes, so that your desktop can come up first. There is not a five minute delay on DOS systems.

   When you schedule an automatic check and save these settings in IBM AntiVirus for Windows, the scheduled check applies to Window sessions only; it does not apply to DOS sessions. Similarly, if you schedule an automatic check and save these settings in IBM AntiVirus for DOS, the scheduled check applies to DOS sessions only; it does not apply to Windows sessions. You can only schedule an automatic check for either DOS or Windows sessions, not both.

   If you have asked IBM AntiVirus for Windows 95, IBM AntiVirus for Windows NT, or IBM AntiVirus for OS/2 to check your system at a particular time, the IBM AntiVirus Automated Execution Monitor will start up when you boot. It runs as a background task, and does not appear in the Window List, so you might not notice it. It waits until the specified time, then starts a check.

   If Automated checking detects a virus, you will be given the opportunity to do a thorough examination of your system to find every instance of the virus, and to remove it.

2. **System Shield** offers a spectrum of powerful features to protect your system from viruses.

   Prevent common DOS viruses checks DOS memory for viruses when you start DOS, and monitors programs as you run them in DOS. If a virus is found when you start DOS, you will be notified and the virus will be disabled. If that happens, IBM AntiVirus for DOS, IBM AntiVirus for Windows, and IBM AntiVirus for Windows 95 will start an automated check to find the virus on your disks. If this feature finds a virus when a program is run, you will be notified. The virus will be prevented from becoming active or spreading, and you can use the infected program without spreading the infection. If a virus is found, it is very important to run IBM AntiVirus and check your entire system for viruses as soon as possible.

   Prevent common DOS viruses is a very important feature. Some common viruses damage programs in such a way that it is not possible to disinfect them reliably. Such programs, including IBM AntiVirus for DOS, IBM AntiVirus for Windows, and IBM AntiVirus for Windows 95, will not function correctly and must be reinstalled if they become damaged in this way. Keeping this feature active at all times will help prevent this from happening. This feature is active by default.

Warn when viral activity occurs can alert you when a virus, even an unknown virus, is active in your system. It warns you when a DOS, Windows, or Windows 95 program does things that are characteristic of viruses. These are likely to indicate the presence of a virus, but might also indicate programs that simply do unusual things. Some other anti-virus programs, in particular, use techniques that are similar to those used by viruses. You should use IBM AntiVirus to check your system for viruses as soon as possible. If none are found, you should try to determine if the warnings occurred because of a normal program doing unusual things, or because of an unknown virus. **Warn when viral activity occurs** is not active by default.

Check files when accessed checks every file opened and closed from DOS, Windows, Windows 95, and Windows NT for common viruses. If one is found, you will be warned. This feature provides an early warning of infected files when you copy them from a diskette, download them to your system, etc.. For example, if you downloading an infected file from the Internet, IBM AntiVirus notifies you about the infection at the end of the download. This can help you to protect your system. If a virus is found, it is a good idea to run IBM AntiVirus and check your entire system for viruses as soon as possible. **Check files when accessed** is not active by default.

Check diskette boot records when used helps catch boot record viruses on diskettes before you boot from the diskette and infect your system. Whenever you access a diskette in the A: drive, this feature quickly checks the diskette for common DOS boot record viruses. It also checks the diskette when you reboot DOS with Ctrl+Alt+Del. As a result of these checks, you might notice that the A: drive is accessed when you reboot with Ctrl+Alt+Del. **Check diskette boot records when used** is active by default. This feature does **not** operate if you reboot with Ctrl+Alt+Del from within Windows. Instead, you should exit Windows and reboot with Ctrl+Alt+Del from DOS.

When you start DOS, messages will be displayed indicating that the features of the System Shield that you have selected are active. If you start a DOS application in OS/2, you will see these same messages before the application starts. These messages are not displayed for seamless Windows sessions in OS/2, but the System Shield does protect them. **Note:** In OS/2, the System Shield shields only DOS and Windows sessions. OS/2 sessions are not shielded; there are no viruses in OS/2 that require shielding.

3. **Scan diskettes on shutdown** is an additional protective measure available in IBM AntiVirus for OS/2. When it is active, it will check the boot record of any diskette in the A: drive for known DOS boot viruses when you issue the **Shutdown** command to shut down your system. This is similar to the protection provided to DOS by the feature **Check diskette boot records when used** in the System Shield. As a result of this check, you might notice that the A: drive is accessed when you issue the **Shutdown** command. **Scan diskettes on shutdown** is active by default.

If you accepted the default options when you installed IBM AntiVirus, your system is already protected. Automated checking is enabled, as are certain features of the System Shield and (on OS/2 systems) the **Scan diskettes on shutdown** feature. This is the default and recommended way to configure IBM AntiVirus. If you disabled these features, either during installation or subsequently, refer to the section **Customizing IBM AntiVirus** for information on enabling them.

On OS/2 systems, DOS sessions and DOS programs are usually initialized from the standard AUTOEXEC.BAT file. These sessions will be protected by the System Shield if you have it installed. In OS/2 2.0 and above (including OS/2 Warp), it is possible to start DOS sessions and DOS programs from DOS diskette images, or initialize them from a file other than the standard AUTOEXEC.BAT file. In order for these DOS sessions to be shielded, you must ensure that the equivalent AUTOEXEC.BAT file starts the System Shield. Refer to the section on **Customizing IBM AntiVirus** for information on what commands the AUTOEXEC.BAT must contain.

4.1.3 Checking diskettes

It is a good idea to check diskettes for viruses before booting from them, or running programs from them. To check a diskette, select the **Check diskettes** menu item from the **Check** menu on the main IBM AntiVirus window. Boot records and files on diskettes in the selected diskette drive will be checked for viruses. If a virus is found, you will be given the opportunity of removing it from the diskette.

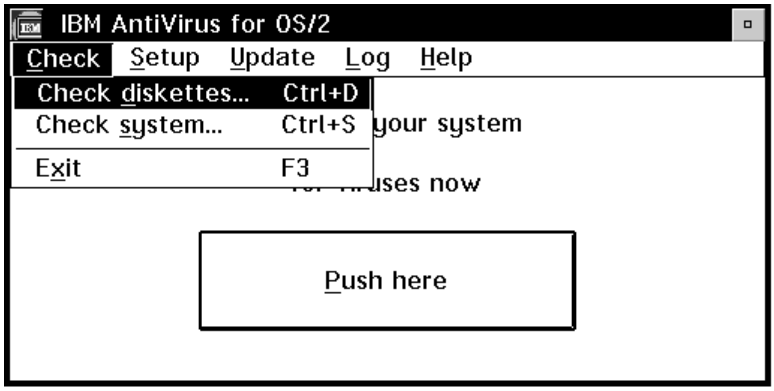

Figure 4-1. Check menu

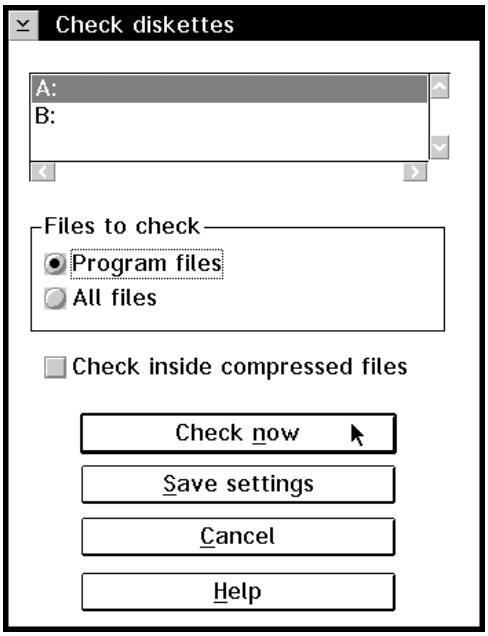

Figure 4-2. Check diskettes dialog

The **Check diskette boot records when used** feature of the System Shield will check for common DOS boot viruses on diskettes when those diskettes are accessed from DOS. Similarly, the **Scan diskettes on shutdown** features in IBM AntiVirus for OS/2 will scan them when you shut down an OS/2 system. Both of these features will help you detect infected diskettes automatically.

4.1.4 Checking your system

Normally, automated checking will check your system for viruses. You can check your system whenever you want, however, by simply selecting the **Push here** push button on the main IBM AntiVirus window.

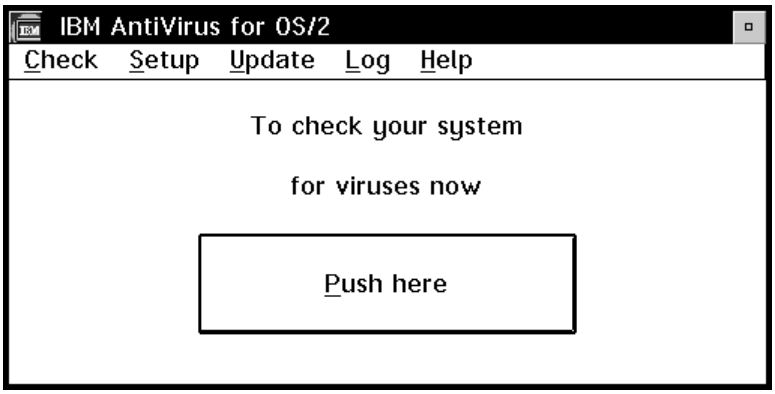

Figure 4-3. Checking the system with the Push here button

This will check boot records (including Boot Manager boot records) and files on your system for known viruses, and for changes or patterns that might indicate the presence of an unknown virus. Network drives (on LAN servers) as well as local

drives can be checked. If a virus is found, a thorough examination of your system can be done to find every instance of the virus, and you will be given the opportunity to remove it.

4.1.5 Checking compressed files

Many people use compression software to store individual program and data files. This software reduces the amount of disk space required to store a file, and reduces the amount of time required to transmit it via modem. Sometimes individual files or collections of files are compressed into a single file, which you must decompress in order to access its contents. Sometimes these compressed files are converted to program files, which decompress their contents when you run the program. Some programs are distributed in compressed form, and decompressed automatically before they are run. Because compression changes the contents of the file, it also inhibits some scanning software from examining the byte patterns within the original, decompressed file to see if they match any known viruses.

IBM AntiVirus will determine if individual compressed files have changed suspiciously. In addition, you can tell it to decompress files that have been compressed with the PKZIP or LZEXE compression algorithms, and to scan the contents of these compressed files for viruses. This is done by selecting **Compressed files** on the **Check diskettes** or the **Check system** dialogs. If you have selected these options and IBM AntiVirus checks a file that is compressed with one of these algorithms, it will be decompressed automatically and its contents will be checked for viruses. If the contents includes compressed files, they will also be decompressed, and so on.

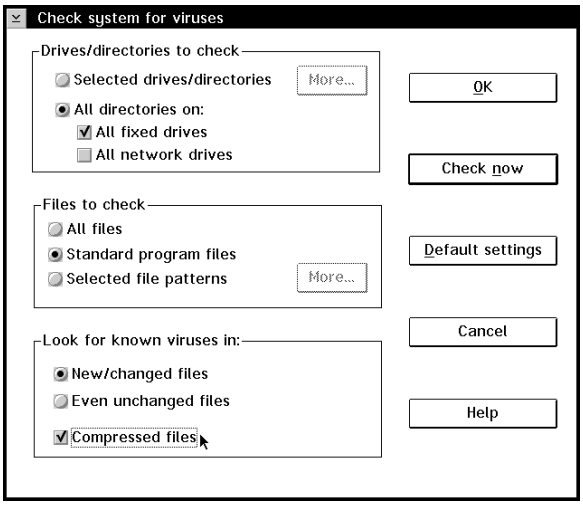

Figure 4-4. Telling IBM AntiVirus to check inside compressed files.

PKZIP is a popular compression utility that combines a number of files into a single compressed file. ZIP2EXE is a companion utility that converts the compressed file into a program file which decompresses itself when run. PKZIP uses a variety of compression formats. IBM AntiVirus can decompress and check any such files created with versions of PKZIP or ZIP2EXE up through version 2.04g.

LZEXE is a popular compression utility that takes a program file and creates a smaller, compressed program file. When run, this compressed file decompresses itself and then runs the program that it contains. IBM AntiVirus can decompress and check any such files created with versions 0.90 or 0.91 of LZEXE.

Some people compress individual files with other compression algorithms. IBM AntiVirus will not usually be able to search their contents properly for known viruses. To search them properly, decompress the files before you check your system.

IBM AntiVirus will properly check disks that have been compressed with disk-compression software, as long as the disk-compression software is currently active. It has been optimized to perform especially well with Stacker, DriveSpace, DoubleSpace, SuperStor and SuperStor/DS.

The **Prevent common DOS viruses** features of the System Shield will detect and deactivate any of the viruses it knows about if you run an infected program, no matter what compression technique is used to store the program file.

4.1.6 Updating IBM AntiVirus virus data files

IBM AntiVirus uses virus signature files to detect, verify, and disinfect known viruses. IBM publishes updates to these files on the Internet approximately once a month. These updates enhance IBM AntiVirus's ability to handle newer viruses. Each update is a single ZIP archive file with a unique name.

To update IBM AntiVirus with the latest virus signature files:

1. Launch your Internet browser, go to the IBM AntiVirus home page at http://www.av.ibm.com, and find the latest virus signature file by clicking on "Latest updates".
2. Compare the version number of the latest virus signatures available from IBM with the version number of the virus signatures installed on your workstation. Assuming that you installed IBM AntiVirus in the C:\IBMAV directory, you can display the version number of the installed virus signatures by typing "type c:\ibmav\dtsig.lst".
3. When your installed virus signatures need to be updated, download the latest virus signature file and store it temporarily on your workstation.
4. Launch the IBM AntiVirus program, select "Update..." from the menu, and enter the full path and name of the downloaded file in the dialog. For example, if you downloaded AV251B.ZIP and stored it the C:\WINDOWS directory, enter "c:\windows\av251b.zip".

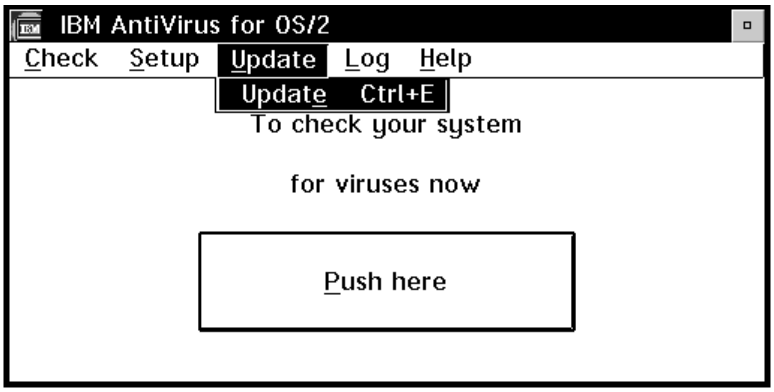

Figure 4-5. Updating virus data files

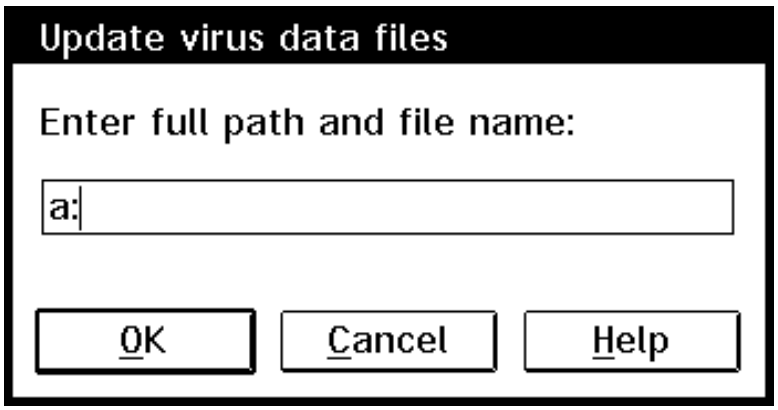

Figure 4-6. Enter the full path and file name of the update file

4.1.7 Logs

IBM AntiVirus records its activities in logs, so that you can review them later. These logs contain information about when your system was checked, what files were checked, and whether any viruses were found.

The log from your current session of IBM AntiVirus is stored in the file CURRENT.LOG. The log from your previous session is stored in PREVIOUS.LOG. A cumulative log which briefly summarizes the results of any automated checks is stored in CUMUL.LOG. All of these log files are stored in the directory into which you installed IBM AntiVirus. They are ordinary files which can be printed directly to your printer.

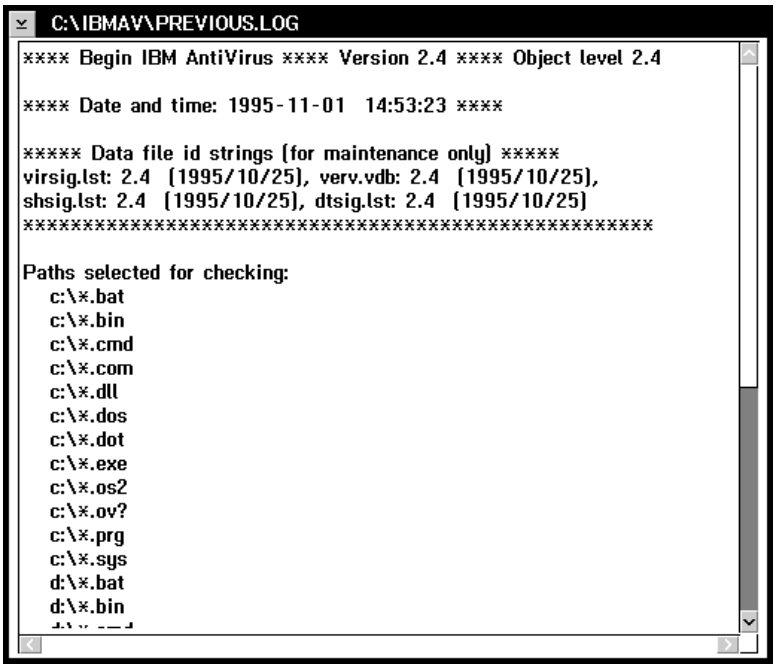

Figure 4-7. Viewing the Previous Log

An entry is added to the cumulative log each time IBM AntiVirus does an automated check. It does not record checks that you do manually. The most recent entries to the cumulative log are stored at the beginning of the file so they are easy to see. The cumulative log records entries for the most recent 50 automated checks. Entries older than this are pruned from the log when a new automated check is done.

4.1.8 Online help

Help is available from the **Help** menu for every function that is performed by IBM AntiVirus. You can also obtain online help by clicking on the **User's Guide** icon on Windows, Windows 95, Windows NT, and OS/2 systems. In addition, you can use the **Help** menu to view a list of viruses and their descriptions.

The following figures show how to select a topic and view it from the **Help** menu of IBM AntiVirus.

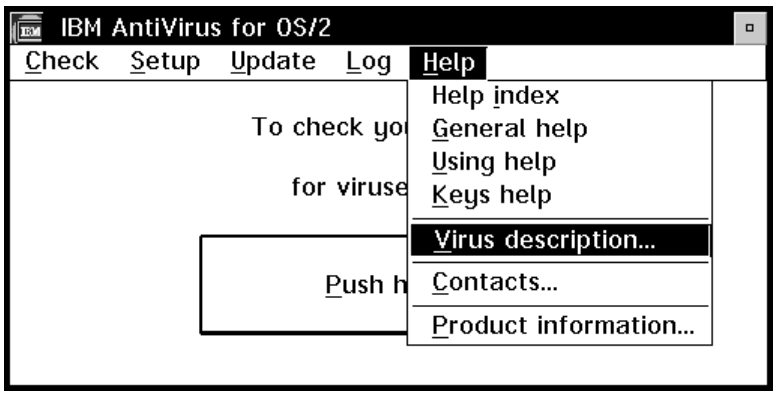

Figure 4-8. Help menu

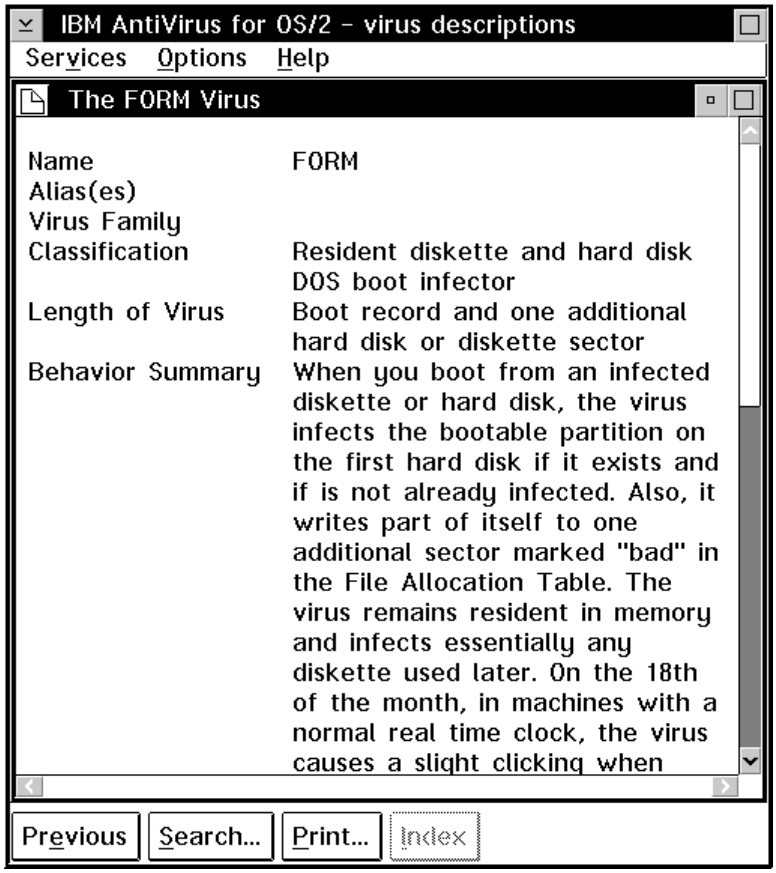

Figure 4-9. Example virus description in Help

4.2 IBM AntiVirus time-out message

IBM AntiVirus will display a time-out message if your current version should be updated. By default, this message is displayed seven months after the release of this version of IBM AntiVirus. IBM AntiVirus will not necessarily detect all viruses that have been written after your current version was released. The program will still function normally after this message is displayed. It is just a reminder that it is time to update. Please see the READ.ME file for the date on which your version of IBM AntiVirus will start displaying this message.

4.3 Customizing IBM AntiVirus

You can customize the way IBM AntiVirus protects your system. The following sections tell you how to customize automated checking, diskette checking, and system checking.

The default settings for IBM AntiVirus have been designed to do the right thing for most systems. You should use the default settings unless you have a specific reason for preferring another setting.

4.3.1 Customizing automated protection

To customize Automated check, select the **Automated check** menu item from the **Setup** menu on the main IBM AntiVirus window. You can specify an Automated check to be done either periodically, at a time that you select, or whenever you boot your system. To specify which disks to check, what kinds of files to check, and whether to check only new/changed files, select the **Check options** push button on the **Automated check** dialog. Select the **Help** push button from the **Automated check** dialog for more information on specific options.

To customize system shielding, select the **System shield** menu item from the **Setup** menu on the main IBM AntiVirus window. Select the features and DOS memory configuration that you want, then select the **OK** push button. To prevent any shielding from being installed when DOS is started, uncheck all of the System Shield features, then select the **OK** push button. Select the **Help** push button from the **System Shield** dialog for more information.

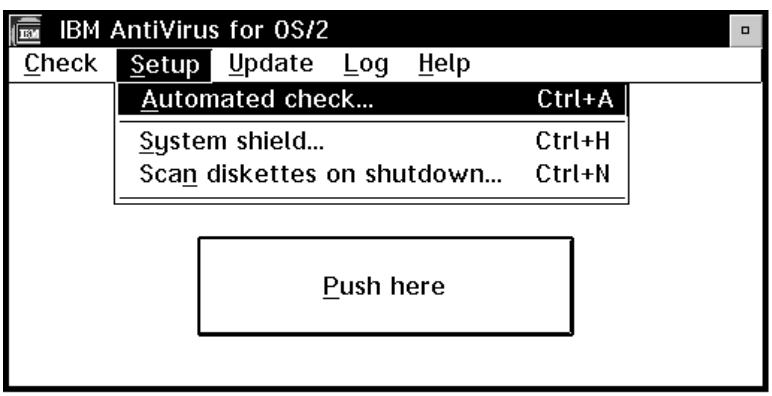

Figure 4-10. Customizing Automated checking with the Setup menu

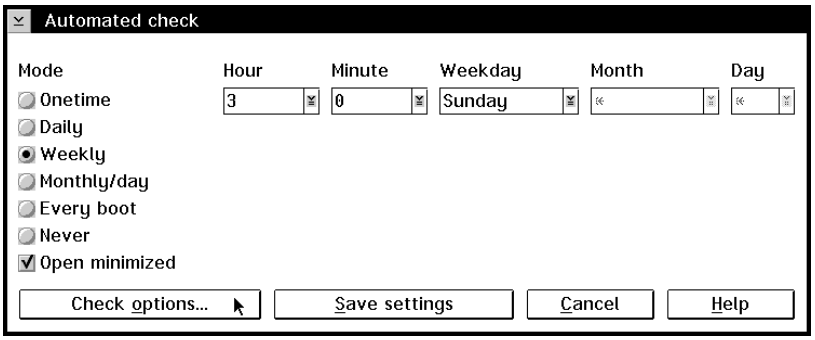

Figure 4-11. Automated check dialog

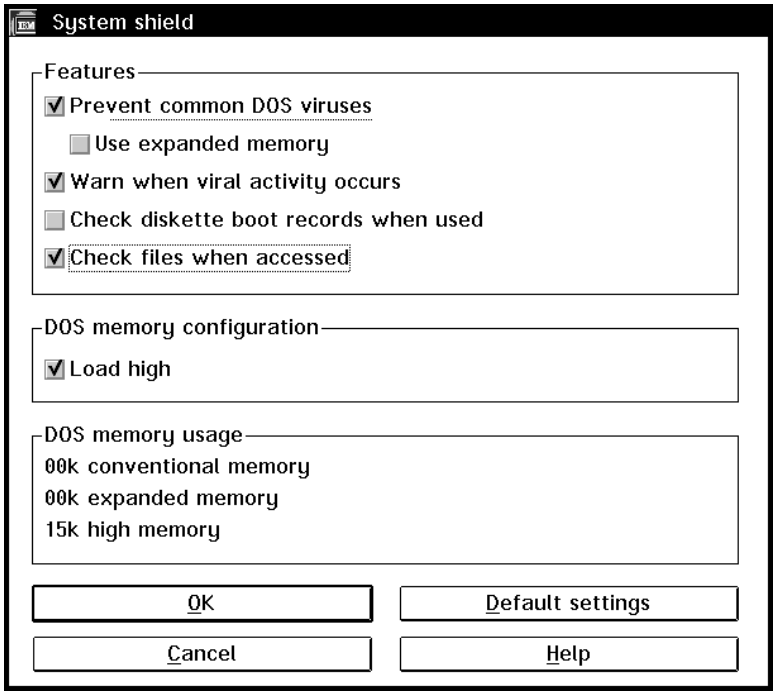

Figure 4-12. Customizing System Shielding

For Automated protection to work, you must have enabled it when you installed IBM AntiVirus. If you did, the installation program might have added statements to your AUTOEXEC.BAT. If you are using OS/2, it might have also added an object called “IBM AntiVirus for OS/2 Startup” to your Startup folder.

If you are using IBM AntiVirus for DOS or IBM AntiVirus for Windows, your AUTOEXEC.BAT will include a statement like the following, which enables automated protection:

```
@CALL C:\IBMAV\IBMAVDR C:\IBMAV\
```

It also adds a statement like the following, which specifies the directory that IBM AntiVirus uses for its log files and other program files.

```
SET IBMAV=C:\IBMAV
```

If you are using IBM AntiVirus for Windows 95, your AUTOEXEC.BAT will include a statement like the following, which enables automated protection:

```
C:\IBMAV95\IBMAVSH /F
```

If you have an existing CONFIG.SYS file, IBM AntiVirus for Windows 95 does not modify it. If the CONFIG.SYS file does not exist, IBM AntiVirus for Windows 95 does not create it.

If you are using IBM AntiVirus for OS/2, your Startup folder will contain an object that starts a program like the following:

```
C:\IBMAV\IBMAV2ST.EXE
```

The “Parameters” field in the object description will contain a line similar to the following.

```
ST C:\IBMAV C:\IBMAV
```

In addition, your AUTOEXEC.BAT will contain a line like the following, which enables the System Shield in any DOS sessions of OS/2.

```
@CALL C:\IBMAV\IBMAVDS C:\IBMAV\
```

Finally, the OS/2 installation program adds a statement like the following to your CONFIG.SYS file, which specifies the directory that IBM AntiVirus uses for its log files and other program files.

```
SET IBMAV=C:\IBMAV
```

(The above examples assume that you installed IBM AntiVirus in the directory C:\IBMAV)

If these lines are not in the relevant files and objects, Automated protection will not work properly. In that case, you should reinstall IBM AntiVirus, or edit these files to add the lines yourself.

4.3.2 Customizing diskette checking

To customize the way diskette checking is done, select the **Check diskettes** menu item from the **Check** menu on the main IBM AntiVirus window. The **Check diskettes** dialog lets you specify which drive to check, and whether to check all files or just program files. You can also select whether you want to check the contents of compressed files.

When you have completed the changes that you want, select the **Save settings** push button to save the changes.

Select the **Help** push button from the **Check diskettes** dialog for more information on specific options.

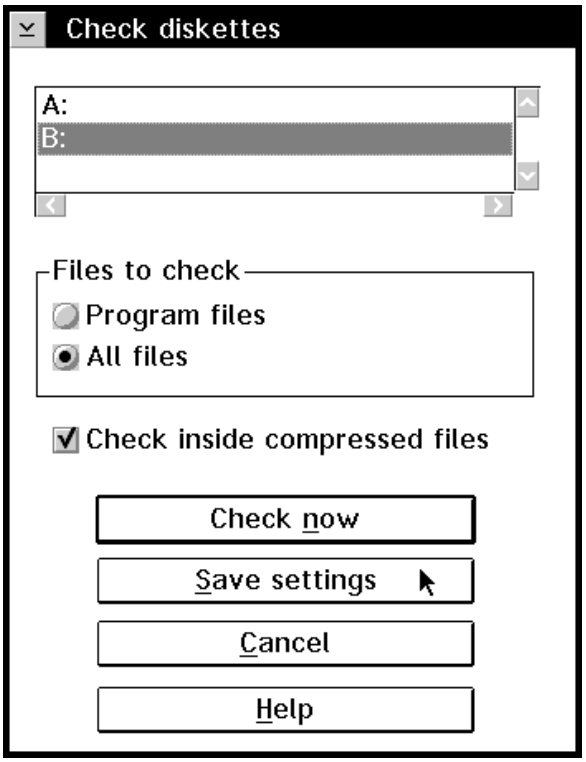

Figure 4-13. Customizing diskette checking

4.3.3 Customizing system checking

You can check the system for viruses yourself by selecting the **Push here** push button from the main IBM AntiVirus window. To customize the way in which this checking is done, select the **Check system** menu item from the **Check** menu on the main IBM AntiVirus window. The **Check system** dialog lets you specify which disks to check, what kinds of files to check, whether to check the contents of compressed files, and whether to check new and changed files, or all files. When you have completed the changes that you want, select the **OK** push button to save the changes. Select the **Help** push button from the **Check system** dialog for more information on specific options.

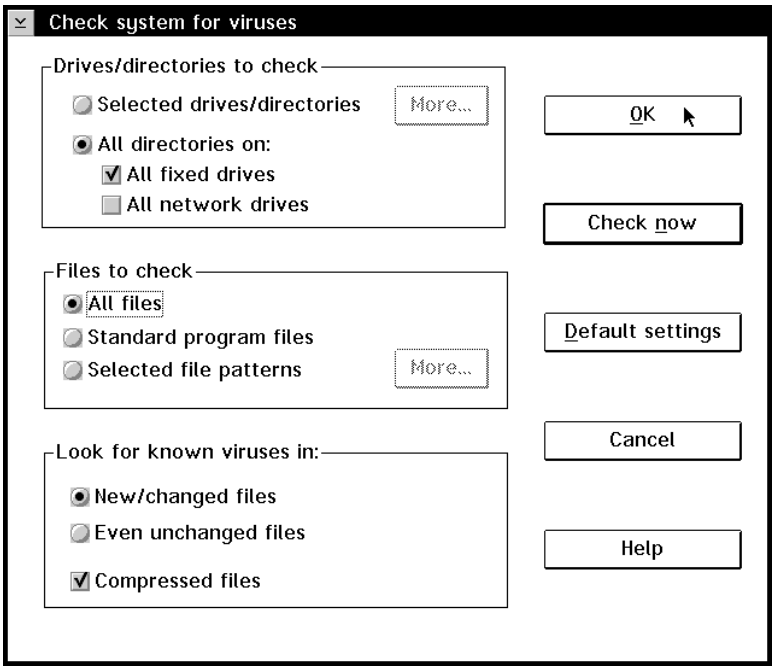

Figure 4-14. Customizing system checking

To check specific drives and directories, select the **Selected drives/directories** push button in the **Check system** dialog, then select the **More ...** push button. In the **Select drives/directories** dialog, select the drive and directory you want to check, then add it to the **Drives/directories to check** list box by selecting the **Add** push button. When you have selected all of the drives and directories that you want to check, select the **OK** push button to save the settings.

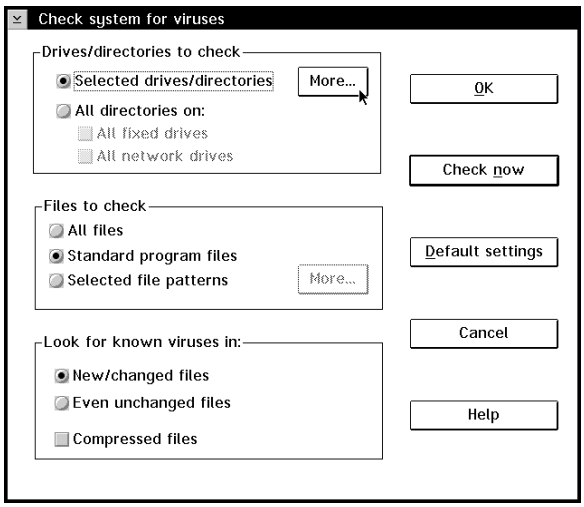

Figure 4-15. Specifying particular drives and directories to check

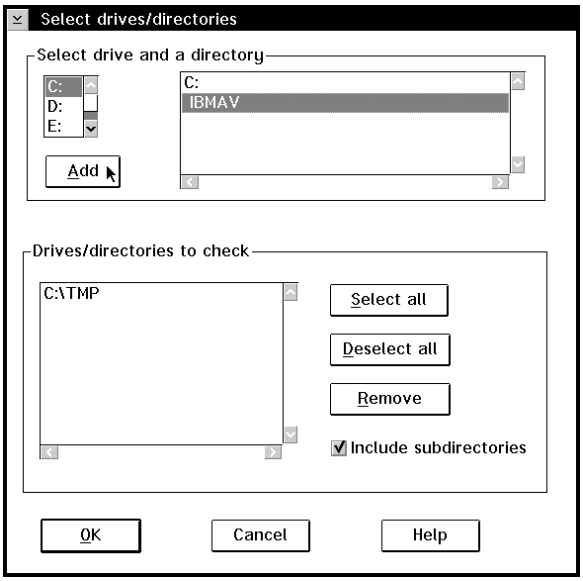

Figure 4-16. Select a drive and directory, then select Add

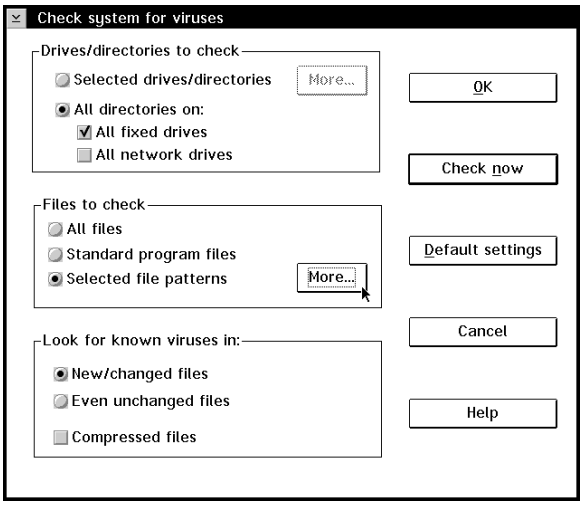

Figure 4-17. Specifying particular file patterns to check

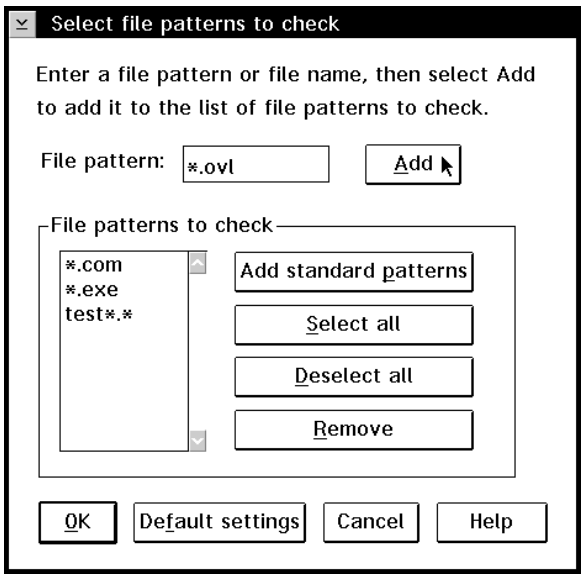

Figure 4-18. Enter a file pattern, then select Add

4.4 When a virus is found

IBM AntiVirus can find a virus on your system either during normal system operations (with the System Shield program), or during a routine check of your disks.

If the System Shield finds a virus, you will be warned. Similarly, in OS/2 systems, the feature **Scan diskettes on shutdown** can warn you of a virus. When this happens, you should use IBM AntiVirus to check your entire system for viruses as soon as possible.

When a virus is found during a check of your system, you will be given the opportunity to clean up any infected files or boot records that have been found so far. Cleaning up a virus infection does not stop there, however. It is likely that your check only examined some of the files on your system - those in which viruses are most likely to be found. It is possible that the virus has also infected other parts of your system. If you only cleaned up the infection that you had found so far, the infection that you had not found could continue to spread within your system, and perhaps to other systems as well.

Any time a routine check turns up a virus, IBM AntiVirus will provide you with the opportunity to perform a thorough check of your entire system, and let you clean up any infections found. This thorough check might take more time than your routine check, but it helps ensure that you have thoroughly cleaned your system. You should let IBM AntiVirus complete this thorough check any time you encounter a virus.

4.4.1 Finding viruses with the System Shield

If the IBM AntiVirus System Shield finds that a particular known virus is active in your system or present on a diskette boot record, it will warn you and identify the virus. In this case, it is very likely that your system (or the diskette) is infected. You should check your system (or the diskette) with IBM AntiVirus as soon as possible.

If you are using the **Prevent common DOS viruses** feature, you will be warned when a program infected with any of the common DOS viruses is executed. The name of the virus will be displayed, the virus will be disabled temporarily, and you can use the program as if it were not infected.

If you are using the **Check diskette boot records when used** feature, you will be warned when a diskette in the A: drive is accessed from DOS, and is infected with any of the common DOS boot viruses. The name of the virus will be displayed, and you can then use IBM AntiVirus to disinfect the diskette.

If you are using the **Warn when viral activity occurs** feature, you will be warned when programs do things that are characteristic of viruses. The System Shield notices these behaviors by loading itself into memory and hooking various DOS system service routines. It watches for activity that is typical of a virus loading or spreading, and unlikely to be caused by any normal program. These are likely to indicate the presence of a virus, but might also indicate programs that simply do unusual things. Some other anti-virus programs, in particular, use techniques that are similar to those used by viruses. You should use IBM AntiVirus to check your system for viruses as soon as possible. If none are found, you should try to determine if the warnings occurred because of a normal program doing unusual things, or because of an unknown virus.

In DOS, DOS sessions in OS/2, and DOS sessions in Windows enhanced mode, messages from the System Shield are written onto the screen as normal text lines. In full-screen Windows sessions, a pop-up window containing the message will appear. In other Windows environments (such as standard mode DOS sessions, or seamless Windows within OS/2), the System Shield will alert you by a series of beeps on the speaker.

In Windows 95, messages from the System Shield appear as standard system error messages. They are either on a full screen display or in a pop-up window.

The following messages may appear when the **Warn when viral activity occurs** feature is used.

IBM AntiVirus: A virus might be active in the system (file modified).

A program modified a file in an unusual way that is similar to the way in which many viruses would modify it. A file that was just accessed might be infected.

IBM AntiVirus: A virus might be active in the system (tracing DOS).

A program is tracing through DOS itself, by executing a DOS services call with the processor's “single step” facility turned on. Some viruses try to use this technique to bypass anti-virus TSRs. A virus might be active in the system.

IBM AntiVirus: A virus might be active in the system (tracing BIOS).

A program is tracing through BIOS itself, by executing a BIOS services call with the processor's “single step” facility turned on. Some viruses try to use this technique to bypass anti-virus TSRs. A virus might be active in the system.

IBM AntiVirus: A virus might be active in the system (diskette infected).

A program accessed a diskette in an unusual way that is used by many viruses. A virus might be active in the system and the diskette that was just accessed might be infected.

IBM AntiVirus: A virus might be active in the system (program infected).

DOS memory was altered in an unusual way that is used by many viruses. In particular, when a program exited, an unusual “hole” was found in the DOS memory chain, which can occur when viruses try to reserve memory for themselves. The last program that was run might be infected.

IBM AntiVirus: A virus might be active in the system (using memory).

When the System Shield was installed, it noticed that memory was allocated in an unusual way that is used by many viruses. In particular, an unusual “hole” was found in the DOS memory chain, which can occur when viruses try to reserve memory for themselves. A program that was run before the System Shield was installed might be infected by a virus.

IBM AntiVirus: A virus might have infected this file.

The indicated file was modified in an unusual way that is used by many viruses.

4.4.2 Cleaning up an infected system

When IBM AntiVirus finds a virus on your system during a check, the **Virus infection report** dialog will present you with choices on how to remove the virus. Viruses whose identity can be positively verified can usually be disinfected, restoring the infected files or boot records to their original, uninfected condition. IBM has designed IBM AntiVirus so that all common viruses can be reliably repaired this way.

IBM AntiVirus can deal with hundreds of infected objects at once. In the unlikely event that there are too many infected objects to deal with at once, you will be presented with a series of **Virus infection report** dialogs; after you have dealt with one set of infected objects, the next set will be displayed.

Some viruses damage files or boot records when they infect them. In this case, IBM AntiVirus will not disinfect them, because you would be left with damaged programs afterwards. You will be told that they could not be disinfected.

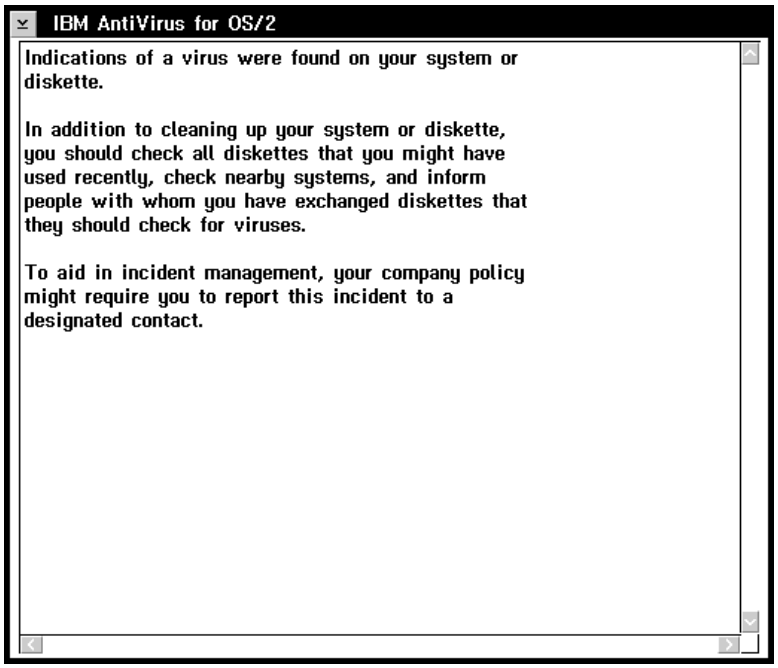

Figure 4-19. Message when a virus is found

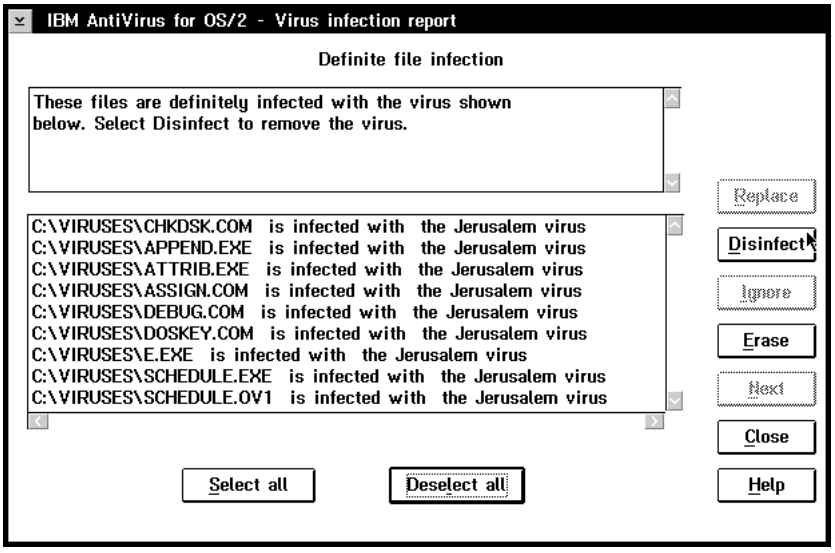

Figure 4-20. Virus infection report identifies viruses

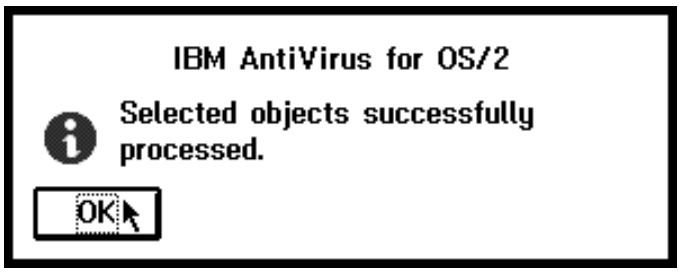

Figure 4-21. Disinfection message box

Figure 4-22. Thorough examination message box

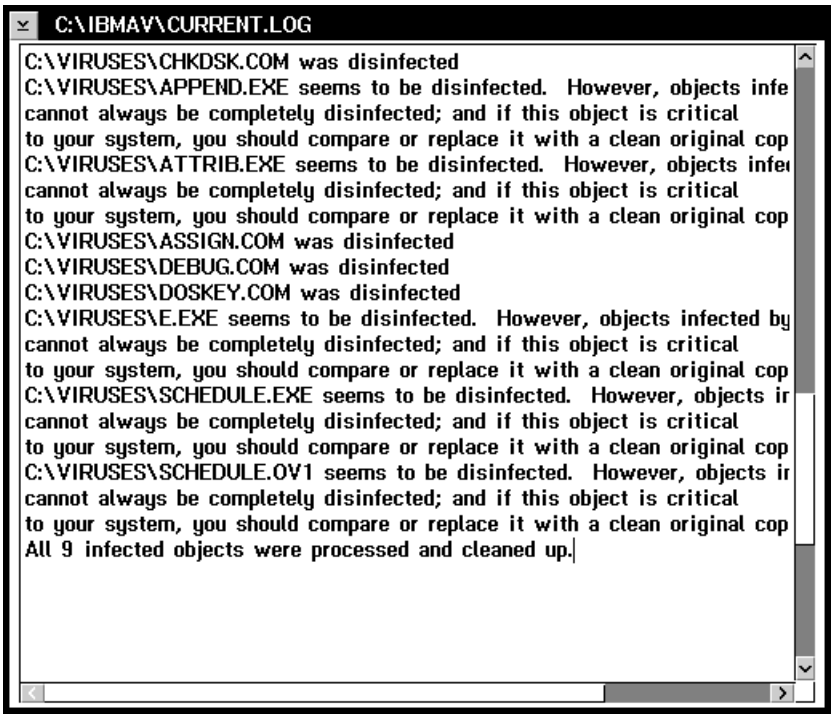

Figure 4-23. Viewing the current log after disinfection

4.4.3 Cleaning up diskettes

The virus that you found on your system came from somewhere, and might have spread beyond your system as well. If it is a boot record virus, it infected your system when the system was booted from an infected diskette. If it is a file-infecting virus, it infected your system when an infected program was started or copied from a diskette or file server. In either case, the virus might have spread to diskettes that were used in your system when they were not write-protected.

When an infection is found, it is very important to check for viruses on the diskettes that might have been used recently in the infected systems. If you do not, the virus might reinfect your system, or might spread to other systems. Select the **Check diskettes** menu item from the **Check** pull-down on the main menu to check diskettes for viruses.

4.4.4 Cleaning up nearby systems

The virus might have infected your system from another system, or vice versa. This might have happened because you share diskettes with other systems, or because you use a file server on a local area network. It is very important to notify the users of these other systems, and to make sure they check their systems for viruses too. If you do not, the virus might spread from their systems, reinfecting your system, or infecting other systems.

If you find a virus on your own system, and it uses a file server, it is very important to check that file server thoroughly for viruses. If any are found on the server, all of the client PCs that use that server should be checked as well.

Even if your system does not use a file server, nearby systems should be checked for viruses, because you might have exchanged diskettes with them recently. This includes all of the other systems in your office or lab, systems that belong to your friends, systems in your department or related departments, and systems belonging to people located near you.

Ideally, all of these other systems also have IBM AntiVirus installed on them. In this case, the users of these systems can have IBM AntiVirus check their systems for them. If IBM AntiVirus is not installed, you might want to use the IBM AntiVirus stand-alone program to check them.

4.4.5 Cleaning up uncommon viruses

Although it is unlikely to happen, your system can become infected with a new or very uncommon virus that IBM AntiVirus cannot positively verify. If you subscribe to IBM AntiVirus Services, you can get rapid updates that will allow you to detect and remove such viruses. This is the easiest and most reliable way to clean up a new or very uncommon virus. Contact IBM AntiVirus Services for more information.

If you do not subscribe to IBM AntiVirus Services, you can still use IBM AntiVirus to help you clean up infections from unverified viruses.

Infected files that cannot be disinfected reliably, either because the virus could not be positively verified or because the virus damaged them, should be erased. IBM AntiVirus will overwrite and erase infected files, so they cannot be restored accidentally. Similarly, infected boot records that cannot be disinfected should be replaced.

Names of files that you erase are written to the log, to help you in restoring them from backups if necessary. To view the log, select either **Current log** or **Previous log** from the **Log** pull-down on the main window. These logs are stored in the files CURRENT.LOG and PREVIOUS.LOG in the directory in which you installed IBM AntiVirus. These are normal files which can be printed directly on your printer.

Replacing the master boot record of a hard disk will replace it with a valid master boot record. This is almost always the right thing to do. The only exceptions are when the disk had an unusual master boot record, like those used by some DOS security products. In these cases, replacing the master boot record might leave the system in an unusable state. Contact the vendor of the security product for assistance before trying to remove an unverified virus from these systems.

System boot records infected with unverified viruses cannot be repaired automatically, because their structure depends upon the operating system and version that you are using. (This includes Boot Manager boot records.)

If you are using DOS, you can replace an infected system boot record with the SYS command. Consult your DOS documentation for more information on this command. Be sure you boot your system from a write-protected DOS diskette that is the same version as your fixed disk uses, that the diskette has been checked and is free of viruses, and that the diskette is write protected at all times. Boot your system by turning the power off, inserting the DOS diskette in the A: drive, and turning the power on. (Do not use Ctrl+Alt+Del to boot your system. Some viruses can remain active in your system if you use Ctrl+Alt+Del.) Issue the SYS command to replace the system boot record. Then reboot and use IBM AntiVirus to check your system for viruses once more, just in case.

If you are using OS/2, it is difficult to repair system boot records safely if they are infected with unverified viruses. In this case, you should reinstall OS/2 and restore any other files on that drive from backups; or contact your OS/2 support center for help in recreating the original system boot record. Then reboot and use IBM AntiVirus to check your system for viruses once more, just in case.

To repair system boot records of OS/2 Boot Manager partitions, delete and reinstall Boot Manager using FDISK. Refer to the Boot Manager documentation for details.

4.4.6 Strategy for containing viruses in organizations

In larger organizations, it can be very difficult to be sure that you have eliminated a virus infection completely. Informal notification of infections between friends might not catch all of the infected systems. Remote sites that might also have become infected might not be notified at all. A more systematic approach, pioneered by IBM, has been shown to be very effective in these cases.

Prior to any virus problems, appoint a central group whose responsibility is virus incident management. Everyone in your organization who deals with PCs should know how to get in touch with the group, and should be instructed to do so if they find a virus. The central group collects reports of virus incidents and ensures that all potentially-infected systems are cleaned up quickly and thoroughly. It can then monitor the situation to ensure that no further problems are encountered.

Because this group receives virus reports from all over, they can often see that a virus has spread within or between sites, even when that would not be obvious to

the people who are reporting. This more global viewpoint allows them to manage virus incidents centrally, which is much more effective than just cleaning up individual systems.

IBM AntiVirus Services offers virus incident management in several countries around the world. Contact your IBM marketing representative for more information.

4.5 Using the IBM AntiVirus stand-alone program

You can use the IBM AntiVirus stand-alone program in situations where your system is so damaged by a virus that it is not possible to run the usual version of IBM AntiVirus. Or, you can use it when your system is so damaged that it cannot even be booted.

The IBM AntiVirus stand-alone program is not intended to be used in place of the standard versions of IBM AntiVirus. It does not have all of the features of automated operation, heuristic virus detection, or higher performance of the standard versions.

The IBM AntiVirus stand-alone program files are contained on your original IBM AntiVirus installation diskettes and on the IBM AntiVirus Emergency Diskette. The IBM AntiVirus stand-alone program for DOS, Windows, Windows 95, Windows NT, and OS/2 consists of the following files:

ADMIN.PRF

Profile from which the IBM AntiVirus stand-alone program gets some of its settings. You should not change this file.

IBMAVSP.EXE

The IBM AntiVirus stand-alone program itself. It can be run directly from a DOS or OS/2 command line. The stand-alone program for Windows NT is IBMAVSN.EXE

LOCAL.MSG

A message that is displayed if a virus is found.

VERV.VDB

Data file used by the stand-alone program to verify the identity of viruses and disinfect them. You should not change this file.

VIRSIG.LST

Data file used by the stand-alone program to scan for indications of viruses. You should not change this file.

When you use the IBM AntiVirus stand-alone program, you will be asked if you want to check all fixed drives on the system, or selected drives. You can check diskettes by specifying their corresponding drives. If you are using the IBM AntiVirus stand-alone program from a diskette drive, you cannot use it to check a different diskette in that same drive. You can use the IBM AntiVirus stand-alone program from a fixed drive to check any diskette drive.

You will then be asked if you want to check all files on the drive, or just files that usually contain programs. If you already suspect that there are viruses on the

system, you should check all files, because viruses can infect files that are not normally thought of as program files.

If a virus is found, you will be given the opportunity to remove it. If IBM AntiVirus can determine that it is safe to disinfect the boot record or file, you will be given the opportunity to do so. Otherwise, you will be asked if you want to have the file erased or the boot record replaced. You can respond in one of three ways:

Y Yes - perform the operation on this file or boot record. This is the action you should normally take.

N No - skip this file or boot record. It will remain infected. You should not normally do this, because the infection can continue to spread.

G Go - perform the operation on this file or boot record, and perform it without asking on any others that are found to be infected. Use this option if there are many infected files and you do not wish to choose between them individually.

There are two ways to run the IBM AntiVirus stand-alone program:

- From the Emergency Diskette
- From the command line.

4.5.1 Running the stand-alone program from the Emergency Diskette

When you boot from the IBM AntiVirus Emergency Diskette, it starts DOS 7.0, installs the **Prevent common DOS viruses** component of the System Shield, and runs the IBM AntiVirus stand-alone program.

Often, when the IBM AntiVirus stand-alone program is invoked from the Emergency Diskette, it may be unable to access all of the system's hard disk partitions. This can occur with HPFS partitions in OS/2, NTFS partitions on Windows NT, and with most compressed partitions. Therefore, after you have used an Emergency Diskette, you need to execute IBM AntiVirus so that it can thoroughly scan, detect, and remove all copies of the virus.

To run the IBM AntiVirus stand-alone program from the Emergency Diskette:

1. Turn the PC power off.
2. Insert the Emergency Diskette into the diskette drive.
3. Turn the PC power on again.

   The IBM AntiVirus stand-alone program automatically starts.
4. Follow the instructions on the screen from the stand-alone program.
5. When you are finished running the stand-alone program from the Emergency Diskette, be sure to execute IBM AntiVirus so that it can perform a thorough scan to detect and remove all copies of the virus.

4.5.2 Running the stand-alone program from the command line

You can run the IBM AntiVirus stand-alone program by typing the following at a DOS, OS/2, or Windows 95 command prompt:

```
IBMAVSP
```

In OS/2, the IBM AntiVirus stand-alone program should be run in an OS/2 session, not a DOS session, because of limitations of DOS sessions in OS/2. Programs running in DOS sessions of OS/2 cannot, for instance, check files with long file names on HPFS drives, and cannot repair master boot records.

On a Windows NT system, you can run the IBM AntiVirus stand-alone program by typing the following at a command prompt:

```
IBMAVSN
```

You will probably prefer to run the IBM AntiVirus stand-alone program interactively; however, if you need to use it in BAT or CMD files, you can specify command line arguments to the IBM AntiVirus stand-alone program as follows:

```
IBMAVSP [options]
```

where **[options]** can be any of the following. (Note that long options can be abbreviated to the first three letters of the option.)

? To get help information for the IBM AntiVirus stand-alone program.

***** Scan all local fixed drives for viruses. If this option is used, the IBM AntiVirus stand-alone program will not ask the user what drives to scan.

***N** Scan all network drives. If this option is used, the IBM AntiVirus stand-alone program will not ask the user what drives to scan.

C: Scan the C: drive. Other drive letters can also be specified. If one or more drive letters are specified on the command line, the IBM AntiVirus stand-alone program will not ask the user what drives to scan.

C:\T\F.EXE Scan the file C:\T\F.EXE. The full pathname to the file must be given.

C:\T Scan the subdirectory C:\T and all of its subdirectories. File types checked can be selected interactively or with the -PROGRAMS or -ALLFILES switches. The full pathname to the directory must be given.

C:\T\F.*,*.V?? Check files with names that match F.* or *.V?? in the subdirectory C:\T and its subdirectories. The full pathname to the directory must be given.

-MEM Scan memory. This can be used when only memory (not drives) needs to be checked. If this option is used, the IBM AntiVirus stand-alone program will not ask the user what drives to scan. This option is only available when running in DOS, or in DOS sessions of OS/2. It is not available in OS/2 protect-mode sessions or in Windows NT sessions.

-ALLFILES Scan all files on the specified drives for viruses. If this option is used, the IBM AntiVirus stand-alone program will not ask the user whether all files or just programs should be scanned.

-PROGRAMS Scan only programs on the specified drives for viruses. If this option is used, the IBM AntiVirus stand-alone program will not ask the user whether all files or just programs should be scanned.

-SCOMP Scan inside compressed files. Files compressed with PKZIP, ZIP2EXE and LZEXE will be decompressed and their contents will be scanned. If only program files are to be scanned, files of type *.ZIP are also scanned, and any program files inside of them are decompressed and scanned. If any other combination of files are to be scanned, any

compressed files that are encountered are decompressed, and all files inside of them are scanned.

-ONEFLOP Do not offer to scan another diskette in a diskette drive. If this option is used, the IBM AntiVirus stand-alone program will not ask the user if a second diskette should be scanned.

-LOGlogfilename To tell the IBM AntiVirus stand-alone program where to place the log file. If "logfilename" is not specified, the log will be written to the file IBMAVSP.LOG in the current directory. If "logfilename" is a simple file name, the log will be written to the current directory. If it is a fully-qualified file name, the log will be written to the specified drive and directory. The specified directory must be writable. It cannot be on a write-protected diskette, for instance. If this option is used, the IBM AntiVirus stand-alone program will not ask the user where the log file should be placed.

-VLOG Verbose log. Put the name of everything that is scanned into the log file, regardless of whether an object was infected or not.

-VVLOG Very verbose log. Will record, in the log, the contents of every boot record that is scanned.

-NLOG Do not create a log file.

-NB To tell the IBM AntiVirus stand-alone program not to beep when it finds a virus.

-NLMSG No local message. Do not pause and do not display the information in the file LOCAL.MSG if a virus is found.

-IDLETIME This option is only available when the IBM AntiVirus stand-alone program is run in an OS/2 session. It tells the IBM AntiVirus stand-alone program to run in idle-time at a priority level of 1. When run this way, it will have a minimal effect on system performance. This switch should not be used if a higher-priority task is consuming all available processor time.

-NBREAK Prevents Ctrl+Break and Ctrl+C from stopping a scan.

-COPENERR Continue checking for viruses, without asking the user, even if a file cannot be opened for scanning.

-CERR Continue checking for viruses, without asking the user, if a non-fatal error is encountered.

-NREP Do not repair infected files or boot records. If this option is used, the IBM AntiVirus stand-alone program will not ask the user if infected files or boot records should be repaired.

-NWIPE Do not erase infected files or replace infected boot records that cannot be repaired. If this option is used, the IBM AntiVirus stand-alone program will not ask the user if these objects should be erased or replaced.

-NFSCAN Do not offer to perform a final, thorough scan if viruses are found.

-YREP Repair infected files or boot records. If this option is used, the IBM AntiVirus stand-alone program will not ask the user if infected files or boot records should be repaired.

-YWIPE Erase infected files and replace infected boot records that cannot be repaired. If this option is used, the IBM AntiVirus stand-alone program will not ask the user if these objects should be erased or replaced.

-YFSCAN Perform a final, thorough scan if viruses are found, without asking the user.

@filename Load command line options from the response file **filename**. Nested response files are not supported.

For example, to scan all programs on all local hard drives and place the log into the file "c:\ibmavsp.log", type the following command.

```
IBMAVSP * -PROGRAMS -LOGc:\ibmavsp.log
```

This method of operation is useful in BAT and CMD files, and whenever user interaction is not desired.

The IBM AntiVirus stand-alone program returns DOS and OS/2 return codes based on the results of it execution. These can be used when you are executing the stand-alone program from BAT or CMD files. These return codes are as follows.

0 Normal return. No errors or viruses were encountered.

5 Not enough memory to run the program.

10 One or more of the command line parameters was invalid.

20 An error occurred during initialization, perhaps because a necessary file could not be found.

30 The program was interrupted by the user.

40 A severe error occurred during scanning.

60 An internal error occurred in the program.

70 The program has been modified, possibly by a virus.

100 Viruses were found on a fixed disk, but not in memory, and all infected objects were cleaned up. Check the log file for the stand-alone program for details.

105 Viruses were found on a diskette, but not in memory or on fixed disks. At least one infection remains on at least one diskette. Check the log file for the stand-alone program for details.

110 Viruses were found on a fixed disk, but not in memory. At least one infection remains. Note that the infection can also be on a diskette in this case. Check the log file for the stand-alone program for details.

120 A virus was found in memory, and is probably still active in the system.

4.5.3 Systems that use resident data compression

Some systems use resident data compression software to allow them to store more data on the fixed disks. This software operates by intercepting reads and writes to the disk, compressing data as it is written and decompressing it as it is read back. Although the data is stored in compressed form on the disk, most programs will only see it in decompressed form.

If you boot from a diskette, you might not have the necessary software resident to access the compressed data correctly. In particular, the IBM AntiVirus stand-alone program might not be able to correctly check or repair your disk if you have booted such a system from a diskette.

In these cases, consult the product documentation for your data compression software to determine proper operation after booting from a diskette, or contact the data compression software vendor for assistance.

The IBM AntiVirus stand-alone program can scan the contents of files that have been compressed with certain compression utilities. See the description of the **-SCOMP** command line option of the IBM AntiVirus stand-alone program for more information.

4.5.4 Systems that use security software

Some systems use security software that is designed to prevent unauthorized users from accessing individual files, disks, or the entire system. In some cases, this software modifies the fixed disk so that it cannot be accessed without going through the security software. In particular, such disks might not be accessed correctly when your system is booted from a diskette. This might cause the IBM AntiVirus stand-alone program to be unable to check or repair your disk, if you have booted from a diskette.

In these cases, consult the product documentation for your security software to determine proper operation after booting from a diskette, or contact the security software vendor for assistance.

Chapter 5. Introduction to computer viruses

This section gives a brief introduction to computer viruses: what they are, how they can spread, and what they can do.

5.1 What is a computer virus?

A computer virus is a program that can "infect" other programs by modifying them to include a (possibly "evolved") copy of itself.

Viruses can spread themselves, without the knowledge or permission of the workstation users, to potentially large numbers of programs on many machines. Viruses can also contain instructions that cause damage or annoyance; the combination of possibly-damaging code with the ability to spread is what makes viruses a considerable concern.

Viruses are not mysterious. They are just computer programs and only do things that programs can do. However, unlike most other programs, they are specifically designed to spread themselves.

Viruses can often spread without any readily visible symptoms. When a virus is started on a workstation, it can run any instructions that its author chooses to include. These instructions can be event-driven effects (for example, triggered after a specific number of executions), time-driven effects (triggered on a specific date, such as Friday the 13th or April 1st), or can occur at random.

Depending on the motives of the virus author, a virus can contain no intentionally harmful or disruptive instructions. Or, it can cause damage simply by replicating itself and taking up scarce resources, such as hard disk space, CPU time, or network connections. Some typical things that some current Personal Computer (PC) viruses do are:

- Display a message.
- Erase files.
- Scramble data on a hard disk.
- Cause erratic screen behavior.
- Halt the PC.

Many viruses do nothing obvious at all except spread! You cannot rely on strange behavior to find viruses. The most reliable way to find viruses is to use competent anti-virus software as discussed later.

The idea of computer viruses was first developed in its current form in 1983. Since then, people have written many viruses. Viruses are a relatively new problem and require some new approaches to deal with them effectively.

Although it is possible to write a virus for virtually any computer, the viruses that are commonly spreading in the world today are limited to microcomputers. There are no known viruses in circulation that run in native sessions of IBM's OS/2, AIX, VM, MVS or OS/400 operating systems. Any of these operating systems that run PC-DOS programs are capable, though, of spreading PC-DOS viruses, including DOS sessions of OS/2 and the DOS Emulation Mode of AIX.

© Copyright IBM Corp. 1989, 1996

Infected files can be stored almost anywhere. They can be stored as files on servers (such as OS/2 LAN servers, AIX LAN servers, or OS/400 network "folders"). Even when they cannot run on the server machine, an infected file on the server can be run by DOS machines on the network and can spread the infection to them.

5.2 How do virus infections start?

The viruses under discussion enter organizations (such as companies and businesses) because an infected diskette or program is brought into that organization. Unlike other security problems, viruses often spread from system to system without anyone's knowledge. Viruses are usually spread within an organization by innocent people going about their normal business activities.

Here is an example. Suppose the organization hires an outside person to come in and perform some work. Part of that person's work involves working on one of the organization's personal computers or microcomputers. The person brings in a few programs to aid in this work, such as a favorite text editor.

Without the person having realized it, the text editor was infected by a virus. By using that editor on one of the organization's machines, the virus spread from the editor to one of the programs stored on the organization's machine, perhaps to a spreadsheet program. The virus has now entered the organization.

Even after the outside person took their personal programs when they left, the virus remained on the machine that it infected in the spreadsheet program. When another employee used that spreadsheet subsequently, the virus spread to another program, such as a directory listing program that the employee kept on the same diskette as the spreadsheet data files. The listing program now is also infected. The infection might spread to other computers to which this diskette is taken or, if the employee's personal computer is connected to the organization's network, the employee might send the listing program to another user over the network. In either case, the virus can spread to more users and more machines using diskettes or networks. Each copy of the virus can make multiple copies of itself and can infect any program to which it has access. As a result, the virus can spread widely in the organization.

Each of the infected programs in each of the infected machines can start whatever other instructions the virus author intended. If these instructions are harmful or disruptive, the pervasiveness of the virus causes the harm to be widespread.

5.3 How serious is the problem?

Traditional security measures have attempted to limit the number of security incidents to an acceptable level. A single incident of lost files in a year might be an acceptable loss, for instance. Although this is important, it only addresses part of the problem of viruses. Because a single virus could potentially spread throughout an organization, the damage it could cause might be much greater than what could be caused by any individual computer user. The problem is that viruses modify software in an uncontrolled way, which can damage the software. In addition, some viruses actually tamper with data files and can damage the data.

Limiting the number of initial virus infections in an organization is important, but it is often not feasible to prevent them entirely. As a result, it is important to be able to deal with them when they occur.

The **potential** damage is indeed large. By using IBM AntiVirus, and following the advice given here, our experience is that most virus incidents can be managed with little difficulty.

Chapter 6. Anti-virus programs

In this section, we discuss the principles and functions of anti-virus programs. It is impossible to completely prevent systems from becoming infected as long as new programs can be introduced on them or their existing programs can be modified. It is also impossible to detect all possible viruses without error. Therefore, it is always possible for systems to become infected. It is important to plan for prevention to the extent possible but equally important to plan for containment and recovery of infections when they do occur.

6.1 What are anti-virus programs?

To understand anti-virus programs, it is useful to understand the basic behavior of known viruses. Generally, all viruses insert copies of themselves in one or more of the following:

- Boot records (initialization areas on diskettes or hard disks).
- Files (typically stored on diskettes or hard disks). There are two major types of file-infecting viruses: those that infect binary executable files, and those that infect macros in files containing data.

Anti-virus programs take advantage of either the general characteristics of all viruses (that they change file or boot records), or characteristics of specific viruses or classes of viruses. The latter kind of program examines the system for something characteristic of either the behavior, or the appearance of specific viruses or classes of viruses. When it finds something with one of these characteristics, it can warn the user, try to prevent the virus from spreading, and so forth.

6.2 Techniques used by anti-virus programs

This section discusses some of the common techniques used by anti-virus programs—their advantages and their limitations. It is intended as a technical introduction for people who want to understand how anti-virus programs work.

6.2.1 Scanning

When a virus is known and has been analyzed, it is possible to write a program that detects any file or boot record that is infected with that virus. In most cases, the detector can simply look for a pattern of bytes found in the virus but not found in normal programs. Detectors that look for these patterns of bytes are called scanners.

For many viruses, this pattern is a simple, sequential string of fixed bytes. For other viruses, more complicated byte patterns are needed. Care must be taken to ensure that the pattern of bytes is not also found in normal programs, or the detector will report a virus when there is none.

© Copyright IBM Corp. 1989, 1996

6.2.2 Change detection

Viruses must change files or boot records in order to infect them. A program that notices when files and boot records change can be used to detect viruses even if these viruses were not previously known. But files and boot records change for many normal reasons unrelated to viruses. By itself, change detection is of limited usefulness because it requires users to understand which changes are normal and which changes indicate a virus.

6.2.3 Heuristic analysis

Heuristic analysis attempts to detect viruses by watching for appearance or behavior that is characteristic of some class of known viruses. It can look in files for operations that viruses use but that are seldom used in normal programs. Or it can watch for attempts to write to hard disks or diskettes in unusual ways.

Like change detection, it can potentially detect whole classes of viruses, but care must be taken to ensure that normal programs are not identified as infected.

6.2.4 Verification

The above techniques can indicate that a file or boot record is infected with a virus, but by themselves they cannot be sure nor can they identify with certainty which virus it is. Programs that perform this identification task are called verifiers. Verifiers can be written for known viruses after careful analysis of them.

6.2.5 Disinfection

When a virus is found in a file or boot record, it might be possible to remove it and restore the file or boot record to its original, uninfected state. This process is called disinfection.

There are two basic strategies for disinfection. The first, and most common, uses specific knowledge about how a particular virus works in order to reverse its actions. This requires knowledge of how each individual virus infects. The second, referred to as “generic disinfection,” records information about what each uninfected file or boot record looks like. This information must be recorded before an infection occurs. When a virus infection occurs, this information is used to reconstruct the original file or boot record.

Virus disinfection must be done carefully. Some viruses damage the files or boot records that they infect so that it is not possible to disinfect them successfully. It is also possible for two different viruses to be identified as the same virus by a scanner and for a disinfector to work correctly on one virus but not the other. Thus the disinfector must be absolutely certain as to the exact identity of the virus.

Because disinfectors change your programs, they must be very reliable.

6.2.6 Resident and non-resident operation

The techniques discussed above can be used in a variety of ways. One common way for them to be used is in programs that examine everything on your disks, trying to find and eliminate viruses. Another common use is in resident programs in DOS that are always actively monitoring your system for viruses.

Resident programs have the advantage of checking programs for infection every time you run them. Unless they are carefully constructed, they can cause delays in program loading and execution.

Non-resident programs have the advantage of looking for and dealing with viruses on your entire system at one time. They serve as a complementary function to resident programs.

6.2.7 Automated operation

If users have to remember to run an anti-virus program periodically, experience has shown that they will forget, increasing their risk of infecting their systems with a virus and of spreading the virus to other systems.

A better approach is to make sure that the anti-virus program operates automatically. Such programs protect the system without requiring you to take any explicit action. This protection can be accomplished by installing resident anti-virus programs when the system is started and by running non-resident programs, either at startup or periodically at a specified time.

6.2.8 Prevention and detection

Detecting that a virus exists and determining what is infected are important first steps in taking corrective action in a virus incident. Preventing a virus from spreading is important in limiting the size of the infection.

6.2.9 Missing viruses and false alarms

In general, it is impossible to detect all viruses that might ever exist and never make mistakes. Virus detectors will always fail to detect some viruses, incorrectly claim that a normal program is infected, or both.

This failure is not a limitation of current technology. Rather, it can be proven mathematically. Any claim that a program can detect all possible viruses and not make mistakes is untrue.

It is possible, on the other hand, to correctly identify infections from all viruses that we currently know. It is also possible to detect large classes of viruses without making mistakes. By carefully balancing accurate detection with techniques for avoiding false alarms, the risk due to viruses can be drastically reduced.

6.3 Techniques used by IBM AntiVirus

This section discusses the techniques used by IBM AntiVirus to provide you with extremely reliable virus protection.

6.3.1 Change detection and fuzzy scanning

IBM AntiVirus uses change detection for two purposes. The first purpose is as a starting point for some of the heuristic analysis algorithms to detect new viruses, which is discussed in the next section. The second purpose is to make known virus detection faster.

Viruses must change files or boot records in order to infect them. If a file did not have a virus yesterday when we checked it and if we know that the file has not

changed, then we know that it does not have a virus today. As it is normally used, IBM AntiVirus only looks in changed and new files for the viruses that it knows about. It is faster to see if a file has changed or is new than it is to examine it for known viruses. This process speeds up the check. (All specified boot records and files are checked for changes and other features, even if they are not examined for known viruses.)

When IBM AntiVirus looks in files and boot records for known viruses, it uses a technique called "fuzzy scanning." This scanning technology used by IBM AntiVirus looks for sequences of bytes that indicate the presence of a virus, as do most scanners. In addition, it recognizes when the sequence of bytes is almost (but not exactly) matched. An inexact match is likely to indicate the presence of a variant of a known virus, and IBM AntiVirus reports the file or boot record as probably infected when it shows you the virus infection report. You will be given the opportunity to remove any such virus.

This technique allows IBM AntiVirus to detect, and correctly identify, a wide range of new virus variants. Without additional measures, this “fuzzy matching” could lead to more false alarms. IBM AntiVirus keeps its identifications highly reliable by advanced false alarm elimination, which is discussed in a subsequent section.

6.3.2 IBM AntiVirus heuristic analysis

IBM AntiVirus is not limited to detecting viruses that we already know about. It uses heuristic analysis to detect previously unknown viruses as well. It looks for patterns of changes in files, and for features of programs, that are typical of large classes of known DOS viruses. It also uses a patent-pending neural network technology from IBM which distinguishes infected disk boot records from normal boot records. If it finds anything that matches these criteria, IBM AntiVirus will report the files or boot records as “suspicious” when it shows you the virus infection report. You will be given the opportunity to erase suspicious files and replace suspicious boot records.

The System Shield can also detect large classes of unknown viruses if you enable **Warn when viral activity occurs**.

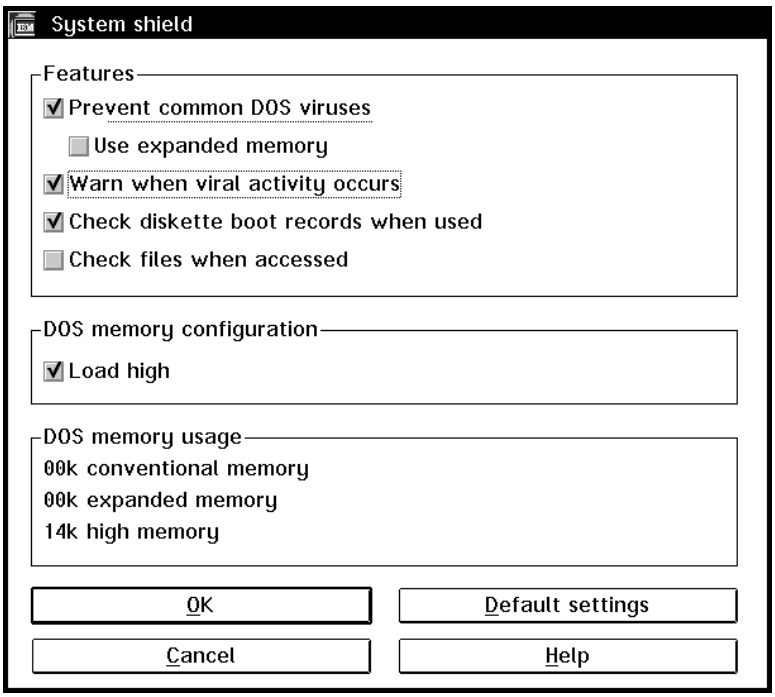

Figure 6-1. Warn when viral activity occurs

IBM AntiVirus heuristic analysis has been carefully designed to avoid false alarms. It does not report boot records or files as suspicious just because they have changed. Boot records and files change on computers all the time for reasons unrelated to viruses. It only reports files as suspicious if their pattern of change is typical of virus infections.

Similarly, **Warn when viral activity occurs** will not warn you when common system actions occur, such as a DOS program going resident or a legitimate modification of a program. It only warns you when the activity appears to be due to a virus.

6.3.3 Safe disinfection of known and unknown viruses

If your system becomes infected with a virus, one of the most important things you will do is to clean it up. IBM AntiVirus can help you remove both known and previously unknown viruses and do so safely, without leaving damaged files or boot records that can cause more problems later.

When IBM AntiVirus finds what appears to be a common, known virus, it checks every relevant byte of the virus to determine that it is exactly as expected. This check is very important. If the virus can be verified to be the one expected, then the file or boot record can often be disinfected safely. If the virus turns out to be different, it might have changed the file or boot record in unexpected ways. Attempting to disinfect it as if it were infected with a different virus could result in a damaged file or boot record.

Once it has verified that the virus is exactly as expected, IBM AntiVirus uses built-in information about that virus to remove it. IBM's expertise and careful analysis of common viruses has been incorporated into the design of IBM AntiVirus so that

almost every virus you will encounter in an actual infection can be disinfected safely in this way.

Even if your system is infected with a rare virus, or a previously unknown virus, IBM AntiVirus can often help you disinfect your system. IBM AntiVirus Install has an option to enable “generic disinfection,” a patent-pending IBM technology that records information about your files for later use in disinfection. This option is enabled by default. If your files are infected with a rare or unknown virus, generic disinfection will use the recorded information to try to reconstruct the original uninfected file. If generic disinfection can verify that its reconstruction exactly matches the original, the file will be disinfected safely. Otherwise, the file is left alone, and IBM AntiVirus will inform you that it could not be disinfected. In neither case will you be left with damaged or incorrectly repaired files.

No matter what type of virus you have, IBM AntiVirus will never damage files or boot records in an attempt to remove it. Instead, it gives you the option of erasing infected files or replacing infected boot records. In cases where disinfection could result in damaged files, but it might not, IBM AntiVirus records this fact in the log file of your IBM AntiVirus session. You can then examine these programs in more detail and determine whether you should restore them from backups.

Some viruses damage programs that they infect and make it impossible to disinfect them safely. IBM AntiVirus recognizes these cases and deals with them properly. When it disinfects files and boot records, IBM AntiVirus does everything it can to make sure you are not left with malfunctioning programs.

6.3.4 Thorough examination

When you do an initial check for viruses, you might be checking only some of the files or drives on your system. For instance, you might check only program files, because viruses do not typically infect any other files. Checking only program files is how IBM AntiVirus is normally used and is a good way to minimize the time it takes to do an initial check.

If the initial check finds a virus, it is possible there are files you have not yet checked that are also infected. When you do not find all of the infected files and boot records, it is very likely the virus will continue to spread on your system and perhaps spread to other systems as well.

When IBM AntiVirus finds a virus during the initial check, it can then check your entire system thoroughly. It checks all files on all local fixed disks, even if they have not changed, and lets you eliminate any viruses found.

If your system is infected, it is likely that the virus came from a diskette recently or that you have accidentally spread the virus to a diskette. IBM AntiVirus reminds you to check all diskettes that you might have used recently, and lets you eliminate any viruses you find on them. This check is an important step to take to stop the local spread of the virus.

6.3.5 Install and forget operation

IBM AntiVirus is designed to do the correct thing automatically. You do not need to develop a detailed understanding of viruses or anti-virus technology for IBM AntiVirus to protect your system. In most cases, all you have to do is install it.

When you installed IBM AntiVirus, the installation program recommended that you enable automated check and system shielding. If you accepted this default configuration, you might never have to run IBM AntiVirus manually. Unless you change the default settings for IBM AntiVirus your system will be checked periodically for viruses, and known viruses that attempt to spread in DOS will be detected and stopped. You are notified of any viruses that are found, and are given recommendations about what to do.

6.3.6 Advanced false alarm elimination

Anti-virus programs should both reduce the risk of your system being affected by a virus and avoid bothering you if you do not have a virus. IBM AntiVirus uses a variety of techniques to ensure that known viruses are found and removed reliably and that variants and unknown viruses are likely to be found as well.

IBM has gone to great lengths to eliminate false alarms from IBM AntiVirus. IBM AntiVirus is tested on a collection of several hundred megabytes of normal (uninfected) programs to help ensure that common programs are not identified as infected. However, this is not enough. It is impossible to have every program in the world in this collection so there might be a program somewhere that causes problems.

To help solve this problem, IBM has developed an advanced statistical model to characterize what normal programs look like. All virus search patterns used by IBM AntiVirus are tested against this model and any that have too high a chance of being found in normal programs are rejected, even if they are not found in any of the normal programs in the test collection.

Finally, IBM's internal Personal Computers (PCs) are used as a test population. IBM has over 250,000 PCs. We test IBM AntiVirus on a large number of these PCs before releasing it to help ensure that any problems are found and corrected before you ever see them.

6.3.7 System shielding

The IBM AntiVirus System Shield offers a variety of powerful features that can always be active in DOS to prevent and detect viruses. **Warn when viral activity occurs** will warn you when a virus appears to be active in your system, even if it is a rare or unknown virus. **Check diskette boot records when used** will warn you if any diskette that is accessed by DOS is infected with a common boot virus. **Check files when accessed** will check files for common DOS viruses whenever DOS opens and closes them for reading or writing. So, it can warn you about a virus when you are copying an infected file onto your system, or when you are downloading an infected file.

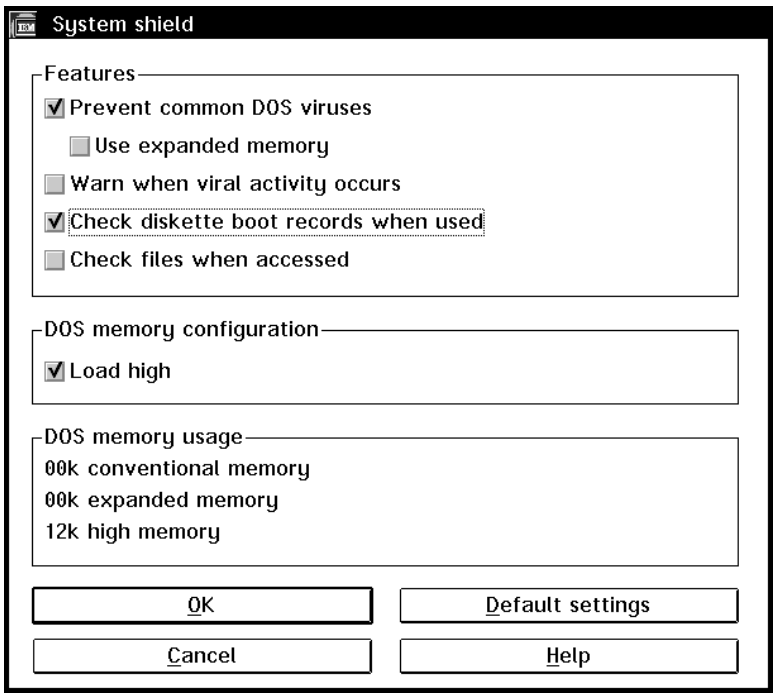

Figure 6-2. Check diskette boot records when used

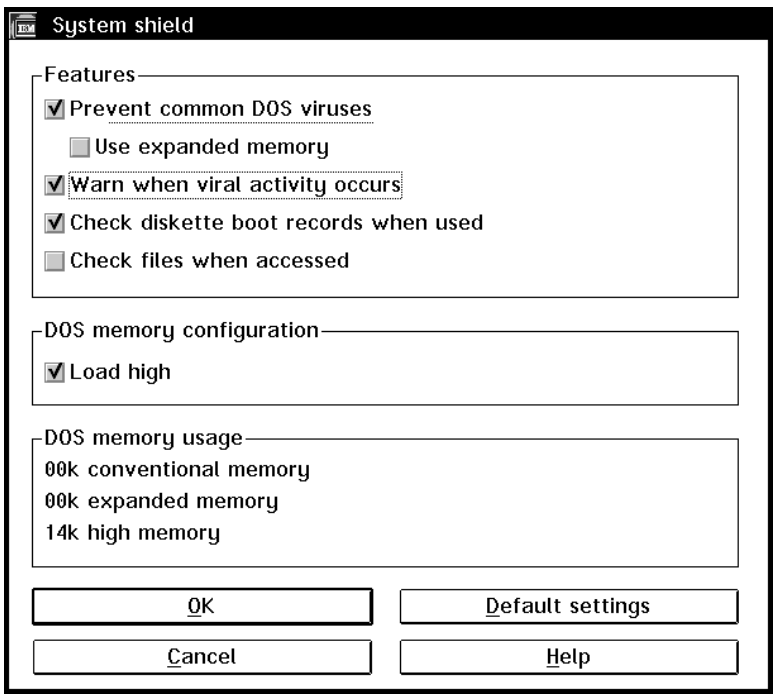

Figure 6-3. Warn when viral activity occurs

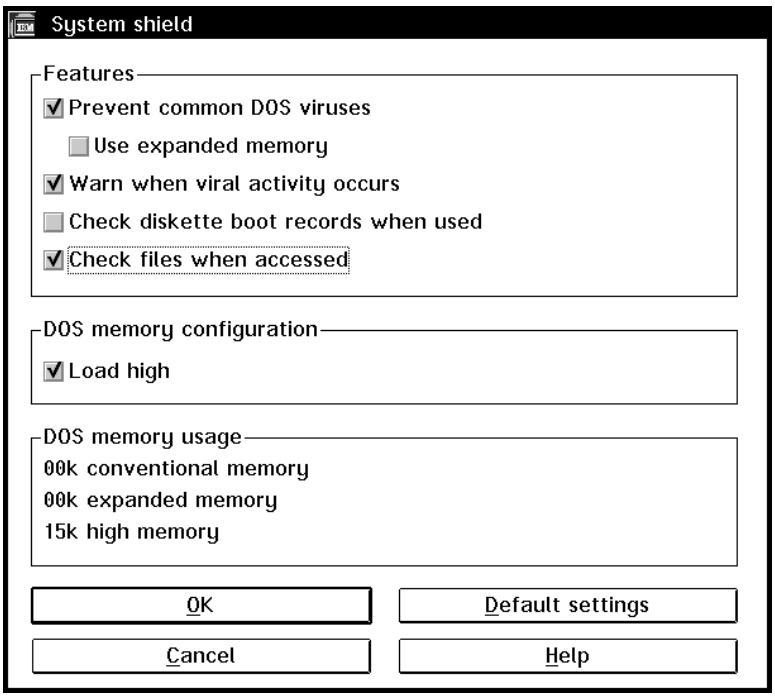

Figure 6-4. Check files when accessed

The **Prevent common DOS viruses** feature will warn you when a program that you are running is infected with common, known viruses. In addition, it prevents these viruses from spreading and lets you run the program as if it was not infected at all.

This has two important benefits. First, you can usually run your critical applications even if you have just discovered that they are infected. It is not necessary to shut down your system and deal with the virus immediately (though it is a good idea). Second, you can usually run IBM AntiVirus from your fixed disk, even if the system is infected. It is seldom necessary to shut your system down and restart from a diskette to handle a virus infection. Instead, you can tell IBM AntiVirus to remove the virus and quickly go on with what you were doing. This ability makes it more likely that the infection is taken care of quickly and safely.

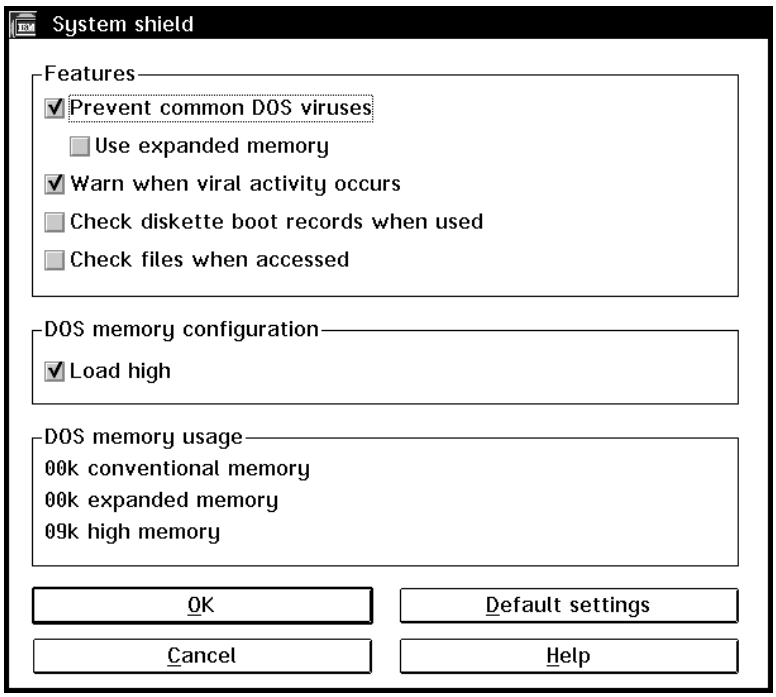

Figure 6-5. Prevent common DOS viruses

To view the list of viruses that IBM AntiVirus knows about, select **Virus descriptions** from the **Help** pull-down on the main window. Then select **List of viruses detected by IBM AntiVirus** from the help screen. Viruses that are prevented by the shield are marked on this list.

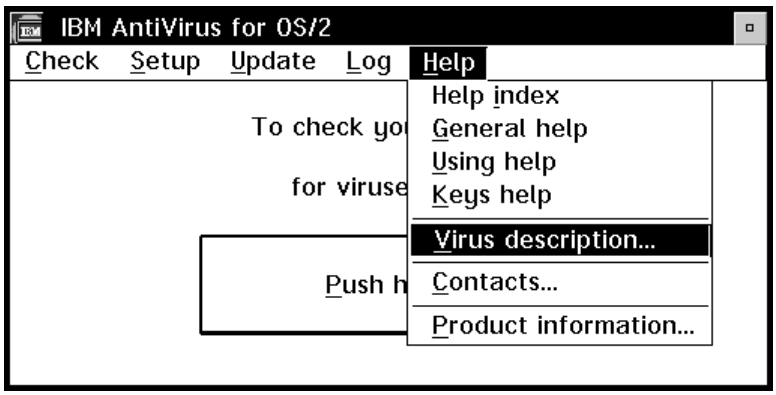

Figure 6-6. Virus descriptions

6.3.8 Intelligent incident management

IBM AntiVirus is based on IBM's years of experience in handling virus incidents around the world. Dealing with viruses correctly and safely without the proper training can be difficult. We have built our anti-virus expertise right into IBM AntiVirus so that you can protect your systems from viruses without becoming a virus expert.

IBM AntiVirus provides default settings that offer the right protection for most systems. If a virus is found, IBM AntiVirus will lead you through the proper steps to remove the virus from your system.

Chapter 7. IBM AntiVirus products and services

IBM AntiVirus products and services are available in countries around the world.

IBM AntiVirus Desktop Edition provides premier protection for individuals and small businesses. It includes protection for DOS, Windows, Windows 95, and OS/2 systems.

IBM AntiVirus Enterprise Edition extends this protection to larger businesses. It includes protection for DOS, Windows, Windows 95, and OS/2 systems, and also for Novell NetWare servers, Windows NT systems, and DOS systems that have very little free memory or disk space. In addition, it provides powerful features that let administrators easily distribute and update IBM AntiVirus from LAN servers, monitor virus activity within their organizations, and enforce their own anti-virus policies.

IBM AntiVirus support includes technical support for the product, as well as assistance in managing virus incidents. Regular updates are available to help you keep your protection up to date as new viruses emerge.

For IBM AntiVirus technical support, consult the list below:

United States and Puerto Rico

For technical support, call 800-237-5511.

Canada

For technical support, call 800-699-6605.

In all other countries, refer to the appropriate Customer Service and Support Guide for your country. Or, refer to other contact information contained in the program package.

© Copyright IBM Corp. 1989, 1996

Chapter 8. For further reading

The following recommended reading is for those who want more information about viruses and related topics:

1. **IBM AntiVirus Administrator's Guide.** This document describes how administrators can distribute and control the use of IBM AntiVirus in enterprises. It describes installation from LAN servers, execution on client system from LAN servers, and the creation of profiles which control the features of IBM AntiVirus which users can access.
2. **IBM AntiVirus for NetWare User's Guide.** This document describes the operation of IBM AntiVirus for NetWare, a component of IBM AntiVirus that provides real-time and scheduled scanning for Novell NetWare servers. It is only available to customers of IBM AntiVirus Services.
3. Jeffrey O. Kephart, Steve R. White, David M. Chess, "Computer Viruses", cover article in **IEEE Spectrum,** May, 1993. This article describes IBM's research on worldwide virus prevalence and spread.
4. David Ferbrache, **A Pathology of Computer Viruses,** Springer-Verlag, London (1992), ISBN 0-387-19610-2. This book provides a good technical introduction to the problem of computer viruses.
5. Lance J. Hoffman (ed.), **Rogue Programs: Viruses, Worms, and Trojan Horses,** Van Nostrand Reinhold, New York (1990), ISBN 0-442-00454-0. This book is a very good collection of articles spanning many aspects of the virus problem.
6. **Virus Bulletin,** published by Virus Bulletin, Ltd.; 21 The Quadrant; Abingdon Science Park; Abingdon, Oxfordshire OX143YS; England, UK. This monthly newsletter can help technical personnel keep up with the PC virus field.
7. Fred Cohen, “Computer Viruses: Theory and Experiment,” **Computers and Security,** Vol. 6 (1987) pp. 22-35. This is the first paper that defined viruses in the form that they appear today.
8. **Communications of the ACM,** Vol. 32 No. 6 (June 1989) has several good articles on the Internet Worm incident.
9. **NetView DM/2 Change Distribution Manager User's Guide**, IBM document number SH19-5048. This provides an introduction to CID (Configuration, Installation and Distribution) services in NetView Distribution Manager/2, to help you set up automated installation and updates for IBM AntiVirus for OS/2.

© Copyright IBM Corp. 1989, 1996

Appendix A. Files installed with IBM AntiVirus for DOS and Windows

The following files can be installed on your system when you install IBM AntiVirus for DOS and IBM AntiVirus for Windows:

ADMIN.PRF

Profile used to record settings in IBM AntiVirus. You should not change this file directly.

AUTORUN.PRF

Profile used to record your choice of settings in IBM AntiVirus. You should not change this file directly.

AVINSTAL.LOG

A file containing information about the installation process, if an automated installation was done. It is not intended to be used by the user.

CONTACT.LST

A list of contacts for IBM AntiVirus or for anti-virus assistance. It is displayed by selecting the **Contacts** menu item from the **Help** pull-down on the main window of IBM AntiVirus. This file can be modified by your local site to contain local contact information. The modified file can be replaced on a copy of the installation diskettes so that it can be installed with IBM AntiVirus.

CURRENT.LOG

Log file generated by the most recent use of IBM AntiVirus. It can be viewed by using the **Log** pull-down from the main window of IBM AntiVirus. It can also be printed directly on your printer.

DB_CHCKP._00

Database used to record information about your files for IBM AntiVirus. You should not change this file directly.

DB_DCF._00

Database used to record information about your files for IBM AntiVirus. You should not change this file directly.

DTSIG.LST

Data file used by IBM AntiVirus as part of the System Shield. You should not change this file.

IAVVXD1.386

Virtual device driver used for virus detection.

IBMAV.ICO

Icon file used for IBM AntiVirus.

© Copyright IBM Corp. 1989, 1996

IBMAVBH.COM

Part of the IBM AntiVirus System Shield. It is not intended to be run separately by the user.

IBMAVD.EXE

The IBM AntiVirus for DOS program. It can be started directly from the DOS command line.

IBMAVD.RES

Data file used by IBM AntiVirus. You should not change this file.

IBMAVDQ.EXE

Used by IBMAVDR.BAT to check profiles and determine what actions IBM AntiVirus should take on boot. It is not intended to be run separately by the user.

IBMAVDR.BAT

The install program causes this file to be called from your AUTOEXEC.BAT. It is used to install the System Shield and check your system on boot if you have requested IBM AntiVirus to do so. It is not intended to be run separately by the user.

IBMAVDL.BAT

This file is used in the "execute from LAN" option. It is used to install the System Shield and check your system on boot if you have requested IBM AntiVirus to do so. It is not intended to be run separately by the user.

IBMAVDT.COM

Part of the IBM AntiVirus System Shield. It is not intended to be run separately by the user.

IBMAVFC.COM

Part of the IBM AntiVirus System Shield. It is not intended to be run separately by the user.

IBMAVLM.COM

Part of the IBM AntiVirus System Shield. It is not intended to be run separately by the user.

IBMAVSH.COM

Part of the IBM AntiVirus System Shield. It is used during installation and by IBM AntiVirus for DOS. It is not intended to be run separately by the user.

IBMAVSP.EXE

The IBM AntiVirus stand-alone program. This can be used after booting from a diskette in the event your system cannot boot from the hard drive due to virus problems.

IBMAVTIW.EXE

The scheduler program. It is not intended to be run separately by the user.

IBMAVW.EXE

The IBM AntiVirus for Windows program. It can be started by double-clicking on the IBM AntiVirus icon while running Windows.

IBMAVWH.HLP

Online help file for IBM AntiVirus for Windows.

IBMAVWMG.EXE

This program is used by the DOS install program. When using the DOS install program to install IBM AntiVirus for Windows, it creates the group icon.

IBMAVWU.HLP

Help file for IBM AntiVirus for Windows online User's Guide.

IBMAVWV.HLP

Online help file IBM AntiVirus for Windows.

KILLTIM.EXE

A program that terminates IBMAVTIM.EXE

LOCAL.MSG

A message that is displayed if a virus is found. This file can be modified by your local site to contain local procedures, such as contacting a local help desk or anti-virus group. The modified file can be replaced on a copy of the installation diskettes so that it can be installed with IBM AntiVirus.

PRODINFO.LST

Data file used by IBM AntiVirus for DOS. You should not change this file.

PRODUCT.MSG

Data file used by IBM AntiVirus for Windows. You should not change this file.

READ.ME

Contains information on this release of IBM AntiVirus. It is displayed by the install program, and can be edited or printed by the user after installation.

SHSIG.LST

Data file used by IBM AntiVirus for Windows by scheduling scans.

STARTTIM.EXE

A program used by IBM AntiVirus for Windows for scheduling scans.

UNINSTD.EXE

Uninstall program for IBM AntiVirus for DOS.

UNINSTD.LST

File used by Uninstall program. You should not change this file.

UNINSTW.EXE

Uninstall program for IBM AntiVirus for Windows.

UPUPD.EXE

The Update/Upgrade program for IBM AntiVirus for DOS.

UPUPW.EXE

The Update/Upgrade program for IBM AntiVirus for Windows.

USER.PRF

Profile used to record your choice of settings in IBM AntiVirus. You should not change this file directly.

USERCMD.PIF

Data file used by IBM AntiVirus for Windows. You should not change this file directly.

USING.LST

"Using Help" file for IBM AntiVirus for DOS.

VERV.VDB

Data file used by IBM AntiVirus (and the stand-alone program) to scan for indication of viruses. You should not change this file.

VIRSIG.LST

Data file used by IBM AntiVirus (and the stand-alone program) to scan for indications of viruses. You should not change this file.

The following files can be generated as you use IBM AntiVirus for DOS and IBM AntiVirus for Windows:

CUMUL.LOG

Log file containing a cumulative history of automated checks done by IBM AntiVirus when you boot. It can be viewed by using the **Log** pull-down from the main window of IBM AntiVirus. It can also be printed directly on your printer.

IBMAVTIM.LOC

File used by the scheduler program.

IBMAVTIM.LOG

Log file generated by the scheduler program.

PREVIOUS.LOG

Log file generated by the previous use of IBM AntiVirus. It can be viewed by using the **Log** pull-down from the main window of IBM AntiVirus. It can also be printed directly on your printer.

PROFILE.PRF

Profile used to record your choice of settings in IBM AntiVirus. You should not change this file directly.

USERCMD.BAT

File used to run commands specified by administrators. This file is only created if you use Windows and if your administrator has used IBM AntiVirus Administrator to specify a command that should be executed when a virus is found. It is located in the directory in which you have Windows installed.

Appendix B. Files installed with IBM AntiVirus for Windows 95

The following files can be installed on your system when you install IBM AntiVirus for Windows 95:

ADMIN.PRF

Profile used to record settings in IBM AntiVirus. You should not change this file directly.

AUTORUN.PRF

Profile used to record your choice of settings in IBM AntiVirus. You should not change this file directly.

AVINSTAL.LOG

A file containing information about the installation process, if an automated installation was done. It is not intended to be used by the user.

DB_CHCKP._00

Database used to record information about your files for IBM AntiVirus. You should not change this file directly.

DB_DCF._00

Database used to record information about your files for IBM AntiVirus. You should not change this file directly.

CONTACT.LST

A list of contacts for IBM AntiVirus or for anti-virus assistance. It is displayed by selecting the **Contacts** menu item from the **Help** pull-down on the main window of IBM AntiVirus. This file can be modified by your local site to contain local contact information. The modified file can be replaced on a copy of the installation diskettes so that it can be installed with IBM AntiVirus.

CURRENT.LOG

Log file generated by the most recent use of IBM AntiVirus. It can be viewed by using the **Log** pull-down from the main window of IBM AntiVirus. It can also be printed directly on your printer.

DTSIG.LST

Data file used by IBM AntiVirus as part of the System Shield. You should not change this file.

IBMAVDR.BAT

The install program causes this file to be called from your AUTOEXEC.BAT. It is used to install the System Shield and check your system on boot if you have requested IBM AntiVirus to do so. It is not intended to be run separately by the user.

© Copyright IBM Corp. 1989, 1996

IBMAVSH.COM

Part of the IBM AntiVirus System Shield. It is used during installation and by IBM AntiVirus for Windows 95. It is not intended to be run separately by the user.

IAVVXD1.VxD

Virtual device driver used for virus detection.

IBMAVSP.EXE

The IBM AntiVirus stand-alone program. This can be used after booting from a diskette in the event that your system cannot boot from the hard drive due to virus problems.

IBMAVTIM.EXE

Scheduler program for IBM AntiVirus for Windows 95.

IBMAVWH5.CNT

Contents tab file used for IBM AntiVirus for Windows 95 online help.

IBMAVWH5.HLP

Online help file used by IBM AntiVirus for Windows 95.

IBMAVWU5.CNT

Contents tab file used for IBM AntiVirus for Windows 95 online help.

IBMAVWU5.HLP

Online help file used by IBM AntiVirus for Windows 95.

IBMAVWV5.CNT

Contents tab file used for IBM AntiVirus for Windows 95 online help.

IBMAVWV5.HLP

Online help file used by IBM AntiVirus for Windows 95.

IBMAVW95.EXE

The IBM AntiVirus for Windows 95 program.

LOCAL.MSG

A message that is displayed if a virus is found. This file can be modified by your local site to contain local procedures, such as contacting a local help desk or anti-virus group. The modified file can be replaced on a copy of the installation diskettes so that it can be installed with IBM AntiVirus.

PROD95.MSG

Data file used by IBM AntiVirus for Windows 95. You should not change this file.

READ.ME

Contains information on this release of IBM AntiVirus. It is displayed by the install program, and can be edited or printed by the user after installation.

STARTTIM.EXE

A time program used by IBM AntiVirus for Windows 95 for scheduling scans.

SHSIG.LST

Data file used by IBM AntiVirus as part of the System Shield. You should not change this file.

UNINST95.EXE

Uninstall program for IBM AntiVirus for Windows 95.

UNINST95.LST

File used by the Uninstall program for IBM AntiVirus for Windows 95. You should not change this file.

UPUP.EXE

The Update/Upgrade program for IBM AntiVirus for Windows 95.

USER.PRF

Profile used to record your choice of settings in IBM AntiVirus. You should not change this file directly.

USERCMD.PIF

Data file used by IBM AntiVirus for Windows 95. You should not change this file directly.

VERV.VDB

Data file used by IBM AntiVirus (and the stand-alone program) to verify the identity of viruses and disinfect them. You should not change this file.

VIRSIG.LST

Data file used by IBM AntiVirus (and the stand-alone program) to scan for indications of viruses. You should not change this file.

The following files can be generated as you use IBM AntiVirus for Windows 95:

CUMUL.LOG

Log file containing a cumulative history of automated checks done by IBM AntiVirus when you boot. It can be viewed by using the **Log** pull-down from the main window of IBM AntiVirus. It can also be printed directly on your printer.

IBMAVTIM.LOC

File used by the scheduler program.

IBMAVTIM.LOG

Log file generated by the scheduler program.

PREVIOUS.LOG

Log file generated by the previous use of IBM AntiVirus. It can be viewed by using the **Log** pull-down from the main window of IBM AntiVirus. It can also be printed directly on your printer.

PROFILE.PRF

Profile used to record your choice of settings in IBM AntiVirus. You should not change this file directly.

USERCMD.BAT

File used to run commands specified by administrators. This file is only created if you use Windows and if your administrator has used IBM AntiVirus Administrator to specify a command that should be executed when a virus is found. It is located in the directory in which you have Windows installed.

Appendix C. Files installed with IBM AntiVirus for Windows NT

The following files can be installed on your system when you install IBM AntiVirus for Windows NT:

ADMIN.PRF

Profile used to record settings in IBM AntiVirus. You should not change this file directly.

AUTORUN.PRF

Profile used to record your choice of settings in IBM AntiVirus. You should not change this file directly.

AVINSTAL.LOG

A file containing information about the installation process, if an automated installation was done. It is not intended to be used by the user.

CONTACT.LST

A list of contacts for IBM AntiVirus or for anti-virus assistance. It is displayed by selecting the Contacts menu item from the Help pull-down on the main window of IBM AntiVirus. This file can be modified by your local site to contain local contact information. The modified file can be replaced on a copy of the installation diskettes so that it can be installed with IBM AntiVirus for OS/2.

CURRENT.LOG

Log file generated by the most recent use of IBM AntiVirus. It can be viewed by using the **Log** pull-down from the main window of IBM AntiVirus. It can also be printed directly on your printer.

DB_CHCKP._00

Database used to record information about your files for IBM AntiVirus. You should not change this file directly.

DB_DCF._00

Database used to record information about your files for IBM AntiVirus. You should not change this file directly.

IBMAV.ICO

Icon file for IBM AntiVirus for Windows NT.

IBMAVDR.BAT

The install program causes this file to be called from your AUTOEXEC.BAT. It is used to install the System Shield and check your system on boot if you have requested IBM AntiVirus to do so. It is not intended to be run separately by the user.

IBMAVSN.EXE

The IBM AntiVirus stand-alone program for Windows NT.

© Copyright IBM Corp. 1989, 1996

IBMAVTIM.EXE

The scheduler program for IBM AntiVirus for Windows NT.

IBMAVWH.HLP

Online help file used by IBM AntiVirus for Windows NT.

IBMAVWU.HLP

Help file used for the IBM AntiVirus for Windows NT online User's Guide.

IBMAVWV.HLP

Online help file used by IBM AntiVirus for Windows NT.

IBMAVWNT.EXE

The IBM AntiVirus for Windows NT program.

LOCAL.MSG

A message that is displayed if a virus is found. This file can be modified by your local site to contain local procedures, such as contacting a local help desk or anti-virus group. The modified file can be replaced on a copy of the installation diskettes so that it can be installed with IBM AntiVirus.

PRODNT.MSG

Data file used by IBM AntiVirus for Windows NT. You should not change this file.

READ.ME

Contains information on this release of IBM AntiVirus. It is displayed by the install program, and can be edited or printed by the user after installation.

STARTTIM.EXE

A time program used by IBM AntiVirus for Windows NT for scheduling scans.

UNINSTNT.EXE

The IBM AntiVirus Uninstall Program.

UNINSTNT.LST

A date file used by the Uninstall program. It should not be modified directly by the user.

UPUP.EXE

The Update/Upgrade program for IBM AntiVirus for Windows NT.

USER.PRF

Profile used to record your choice of settings in IBM AntiVirus. You should not change this file directly.

USERCMD.PIF

Data file used by IBM AntiVirus for Windows NT. You should not change this file.

VERV.VDB

Data file used by IBM AntiVirus (and the stand-alone program) to verify the identity of viruses and disinfect them. You should not change this file.

VIRSIG.LST

Data file used by IBM AntiVirus (and the stand-alone program) to scan for indications of viruses. You should not change this file.

The following files can be generated as you use IBM AntiVirus for Windows NT:

CUMUL.LOG

Log file containing a cumulative history of automated checks done by IBM AntiVirus when you boot. It can be viewed by using the **Log** pull-down from the main window of IBM AntiVirus. It can also be printed directly on your printer.

IBMAVTIM.LOC

File used by the scheduler program.

IBMAVTIM.LOG

Log file generated by the scheduler program.

PREVIOUS.LOG

Log file generated by the previous use of IBM AntiVirus. It can be viewed by using the **Log** pull-down from the main window of IBM AntiVirus. It can also be printed directly on your printer.

PROFILE.PRF

Profile used to record your choice of settings in IBM AntiVirus. You should not change this file directly.

USERCMD.BAT

File used to run commands specified by administrators. This file is only created if you use Windows and if your administrator has used IBM AntiVirus Administrator to specify a command that should be executed when a virus is found. It is located in the directory in which you have Windows installed.

Appendix D. Files installed with IBM AntiVirus for OS/2

The following files can be installed on your system when you install IBM AntiVirus for OS/2:

ADMIN.PRF

Profile used to record settings in IBM AntiVirus. You should not change this file directly.

AUTORUN.PRF

Profile used to record your choice of settings in IBM AntiVirus. You should not change this file directly.

AVINSTAL.LOG

A file containing information about the installation process, if an automated installation was done. It is not intended to be used by the user.

DB_CHCKP._00

Database used to record information about your files for IBM AntiVirus. You should not change this file directly.

DB_DCF._00

Database used to record information about your files for IBM AntiVirus. You should not change this file directly.

CONTACT.LST

A list of contacts for IBM AntiVirus or for anti-virus assistance. It is displayed by selecting the **Contacts** menu item from the **Help** pull-down on the main window of IBM AntiVirus. This file can be modified by your local site to contain local contact information. The modified file can be replaced on a copy of the installation diskettes so that it can be installed with IBM AntiVirus.

CURRENT.LOG

Log file generated by the most recent use of IBM AntiVirus. It can be viewed by using the **Log** pull-down from the main window of IBM AntiVirus. It can also be printed directly on your printer.

DTSIG.LST

Data file used by IBM AntiVirus as part of the System Shield. You should not change this file.

IBMAV2.EXE

The main program for IBM AntiVirus for OS/2. It should be started by double-clicking on the IBM AntiVirus for OS/2 icon in the IBM AntiVirus/2 folder or program group.

IBMAV2.ICO

Icon file for IBM AntiVirus for OS/2 folder.

© Copyright IBM Corp. 1989, 1996

IBMAV2ST.EXE

Called from your Startup folder and used to check your system when you boot, or to set up an automated check at a specified time, if you have requested IBM AntiVirus for OS/2 to do so. It is also used by the installation program. It is not intended to be run separately by the user.

IBMAVBH.COM

Part of the IBM AntiVirus System Shield. It is not intended to be run separately by the user.

IBMAVDQ.EXE

Used by IBMAVDS.BAT to check profiles and determine what actions IBM AntiVirus for OS/2 should take when you start DOS sessions.

IBMAVDS.BAT

Called from your AUTOEXEC.BAT and used to install the System Shield when you start DOS sessions if you have requested IBM AntiVirus to do so. It is not intended to be run separately by the user.

IBMAVDT.COM

Part of the IBM AntiVirus System Shield. It is not intended to be run separately by the user.

IBMAVFC.COM

Part of the IBM AntiVirus System Shield. It is not intended to be run separately by the user.

IBMAVHLP.HLP

Online help file used by IBM AntiVirus for OS/2.

IBMAVLM.COM

Part of the IBM AntiVirus System Shield. It is not intended to be run separately by the user.

IBMAVSD.EXE

IBM AntiVirus for OS/2 shutdown scanner. This is used by IBM AntiVirus for OS/2 to check diskettes for boot record viruses when you shut down your system. It is also used by the installation program. It is not intended to be run separately by the user.

IBMAVSH.COM

The IBM AntiVirus System Shield. It is not intended to be run separately by the user.

IBMAVSP.EXE

The IBM AntiVirus stand-alone program. This can be done after booting from a diskette in the event that your system cannot boot from the hard drive due to virus problems.

IBMAVTIM.EXE

The IBM AntiVirus for OS/2 Automated Execution Monitor. It is used by IBM AntiVirus for OS/2 to schedule automated checks. It is also used

by the installation program. It is not intended to be run separately by the user.

IBMAVTUT.INF

Help file for User's Guide icon.

IBMAVVDS.HLP

Online virus list and descriptions used by IBM AntiVirus for OS/2.

IBMAVWT.EXE

Windows utility used by the System Shield. It is not intended to be run separately by the user.

LOCAL.MSG

A message that is displayed if a virus is found. This file can be modified by your local site to contain local procedures, such as contacting a local help desk or anti-virus group. The modified file can be replaced on a copy of the installation diskettes so that it can be installed with IBM AntiVirus.

PRODUCT2.MSG

Date file used by IBM AntiVirus for OS/2. You should not change this file.

READ.ME

Contains information on this release of IBM AntiVirus. It is displayed by the install program, and can be edited or printed by the user after installation.

SHSIG.LST

Data file used by IBM AntiVirus as part of the System Shield. You should not change this file.

UNINST2.EXE

Uninstall program for IBM AntiVirus for OS/2.

UNINST2.LST

File used by the Uninstall program. You should not change this file.

USER.PRF

Profile used to record your choice of settings in IBM AntiVirus. You should not change this file directly.

VERV.VDB

Data file used by IBM AntiVirus for OS/2 (and the stand-alone program) to verify the identity of viruses and disinfect them. You should not change this file.

VIRSIG.LST

Data file used by IBM AntiVirus for OS/2 (and the stand-alone program) to scan for indications of viruses. You should not change this file.

UPUP.EXE

Update/Upgrade program used by IBM AntiVirus for OS/2.

The following files can be generated as you use IBM AntiVirus for OS/2:

CUMUL.LOG

Log file containing a cumulative history of automated checks done by IBM AntiVirus when you boot. It can be viewed by using the Log pull-down from the main window of IBM AntiVirus. It can also be printed directly on your printer.

IBMAVTIM.LOC

File used by the scheduler program.

IBMAVTIM.LOG

Log file generated by the scheduler program.

PREVIOUS.LOG

Log file generated by the previous use of IBM AntiVirus. It can be viewed by using the **Log** pull-down from the main window of IBM AntiVirus. It can also be printed directly on your printer.

PROFILE.PRF

Profile used to record your choice of settings in IBM AntiVirus. You should not change this file directly.

Appendix E. Troubleshooting

Every effort has been made to ensure that IBM AntiVirus is compatible with your system. This section describes some problems that can be encountered, and how you can deal with them.

New viruses continue to be written and released. A small fraction of them become widespread problems. To deal with these new viruses most effectively, any anti-virus software should be kept up to date. If IBM AntiVirus determines (from your system clock) that it is over seven months since this version was released, it will tell you that it should be updated. You will see this message whenever IBM AntiVirus completes a check of your system. If you see this message, you should obtain and install the most recent version of IBM AntiVirus.

When IBM AntiVirus loads, it performs a self-integrity test, and warns you if something has changed one of the IBM AntiVirus programs. If you get this warning, it might indicate that a virus is active, or that some accident has damaged the program. To check for viruses, power off your system, reboot from the Emergency Diskette and use the IBM AntiVirus stand-alone program (IBMAVSP) to check and repair your system. If no virus is found, restore the IBM AntiVirus programs from a working backup, or re-install the package.

Viruses that infect boot records are found by IBM AntiVirus only in boot records, not in files. If you have a diskette-image file that you want to check for viruses, create a diskette from the image, and check the diskette. The only exceptions to this rule are the files BOOT.DOS and BOOT.OS2 that hold boot-record images when you use the Dual Boot utility. If IBM AntiVirus finds a virus that infects boot records in one of these files, it will warn you, and offer to erase the file. You should obtain a clean copy of the file from a similarly-configured machine or from a service center before using the Dual Boot feature again.

In many cases, automated checking in IBM AntiVirus will only work correctly if the date and time on your computer are set correctly. Some PCs (usually older ones), don't remember the date and time when you turn them on, or need a special program to be executed before the date and time are set correctly. On these computers, make sure that the lines in the AUTOEXEC.BAT file (and the Startup folder object) that invoke IBM AntiVirus are placed after the lines that set the date and time correctly. Otherwise, automated checks might not run as scheduled.

When **Check inside compressed files** is used, either for checking diskettes or hard disks, IBM AntiVirus decompresses compressed files into temporary files before scanning them. These files are written into the directory specified by the TMP environment variable in your CONFIG.SYS, if this variable is defined. This decompression is faster if the directory specified by your TMP variable is a large, very fast drive. Examples of such drives include a virtual disk drive or a disk with a lazy-write or write-back cache.

© Copyright IBM Corp. 1989, 1996

E.1 For the IBM AntiVirus Installation Program

When IBM AntiVirus for DOS and IBM AntiVirus for Windows are being run immediately after installation you might encounter a message like "Cannot initialize for virus checking". The log will contain the message "Could not open input file - VERV.VDB." This indicates that insufficient file handles were available on your system when installation began. The installation program will set the number of file handles so that enough are available, but any increase will only occur when you reboot your system. You should reboot your system and reinstall IBM AntiVirus for DOS and IBM AntiVirus for Windows

Problems during install might also indicate the presence of a virus. To check for viruses, power off your system, reboot from a write-protected, virus-free system diskette, and use the IBM AntiVirus stand-alone program (IBMAVSP) to check and repair your system.

A previous version of IBM anti-virus software included a program named VSTOP.COM. As a convenience to users of this earlier version, the IBM AntiVirus installation program examines the AUTOEXEC.BAT file for statements that seem to refer to this program, and either adds the word REM at the beginning of the line (converting the statement into a comment), or displays a message advising you that VSTOP should be removed from the AUTOEXEC. If you use some other program named VSTOP, not related to IBM AntiVirus, you should examine your AUTOEXEC.BAT file after installation to ensure that it is still correct.

Some systems allow you to boot from the internal ROM, rather than from a diskette or hard drive. Some IBM PS/1 and PS/2 models have this feature. If these systems are set up to boot from ROM, it might not be possible for the IBM AntiVirus installation program to modify the AUTOEXEC.BAT file to enable Automated checking. If this occurs, change the system configuration to boot from the hard drive, and try installing IBM AntiVirus again.

E.2 For IBM AntiVirus for DOS and Windows

On DOS systems, you might encounter the message "Abnormal program termination" when first loading IBM AntiVirus for DOS and IBM AntiVirus for Windows. This indicates that insufficient memory is available to run the program. Remove some of your resident programs and try again, add more memory to your system, or use the IBM AntiVirus stand-alone program instead. This message might also occur if a virus has damaged the IBM AntiVirus program files.

If you encounter the message "Out of environment space" when your DOS system is booting, just after you have installed IBM AntiVirus for DOS or IBM AntiVirus for Windows, you might need to increase your DOS environment space. You can do this by increasing the numeric value after the /E parameter of the SHELL= command in your AUTOEXEC.BAT. See your DOS documentation for more information on the SHELL= command.

Although IBM AntiVirus for Windows correctly detects infected boot records, it is not always able to disinfect them. If your system has infected boot records, you should start IBM AntiVirus for DOS by going to a DOS prompt, changing to the directory you installed IBM AntiVirus for DOS in, and issuing the command IBMAVD.

On Windows systems, you can only have one copy of IBM AntiVirus open at a time. If you try to open a second session of IBM AntiVirus, the session that is already open will be given focus, but the second session will not start.

OS/2 users should use IBM AntiVirus for OS/2 to protect their systems. Although IBM AntiVirus for DOS will in general work correctly in DOS session under OS/2, it will be somewhat limited in what it can do. For instance, it will not be able to check the boot records of drives that use the HPFS file system, and it will not be able to repair infected master boot records.

E.3 For IBM AntiVirus for OS/2

On OS/2 systems, automated checking will not be done if you already have an IBM AntiVirus for OS/2 session open. So, you should make sure you have closed any IBM AntiVirus for OS/2 session before the automated check is scheduled to be done.

In OS/2 Warp 3.0, if you have the IBM AntiVirus System Shield active and you notice that it does not appear to start when you start a DOS session, check to see if the DualBoot window is open. If it is, close the DualBoot window and restart your DOS programs or sessions. The System Shield will then start as usual. In general, you should keep the DualBoot window closed unless you are rebooting to DOS right away.

If a DOS full-screen session has the focus when IBM AntiVirus for OS/2 starts an automated check, the DOS full-screen session can lose focus, which might make the DOS session appear to not respond to keystrokes. This only occurs if you have unchecked **Open minimized** in the **Automated check** dialog, and if the DOS full-screen session has **DOS_BACKGROUND_EXECUTION** set to **OFF** in its **DOS Session** settings. Neither of these are the default settings. To avoid this, make sure that **Open minimized** is checked. If it does occur, press Alt+Esc to get back to the OS/2 desktop. Then select the DOS session again by double-clicking on its icon.

OS/2 locks some system files (for example, EA DATA . SF) for its own use. Some applications lock others. Locked files cannot be opened for checking. This is normal behavior, and will be noted in the log.

The IBM AntiVirus stand-alone program might report errors when run from diskettes in DOS sessions of some versions of OS/2. This is due to limitations in DOS sessions of OS/2. You should run the IBM AntiVirus stand-alone program in OS/2 sessions of OS/2.

E.4 For the System Shield Program in IBM AntiVirus for DOS and Windows

The IBM AntiVirus System Shield programs install themselves as resident extensions in your DOS system if you request it. Although it is rare, some other resident extensions might conflict with the System Shield. If you encounter a problem with other resident programs, and the problem goes away if you tell IBM AntiVirus not to install the System Shield features, this might indicate a conflict. In this case, move the call to IBMAVDR (or IBMAVDS, if you are using IBM AntiVirus

for OS/2) further down in your AUTOEXEC.BAT file, after the calls to resident extensions with which it might conflict.

Some resident extensions that intercept keystrokes fail to pass those keystrokes to resident extensions that were installed previously. This can prevent the **Check diskette boot records when used** feature from checking a diskette in the A: drive when you reboot your system with Ctrl+Alt+Del. If you have selected **Check diskette boot records when used** and the diskette light for the A: drive does not come on immediately after you press Ctrl+Alt+Del, move the call to IBMAVDR further down in your AUTOEXEC.BAT file, after the calls to resident extensions that might intercept Ctrl+Alt+Del.

Normally, the **Prevent common DOS viruses** feature of the System Shield in IBM AntiVirus for DOS checks high memory (memory above the 640k DOS limit) for resident viruses. This might cause problems on some systems, especially where hardware adapters are sensitive to having their memory space read. A common symptom of this problem is that the hardware adapter (often a communications adapter) will not function properly when this feature is installed. If this is a problem, uncheck the **Check high memory** check box on the **System Shield** dialog, select the **OK** button to save the settings, and then reboot your system to let the new settings take effect. This problem does not occur under OS/2 with IBM AntiVirus for OS/2, since the System Shield does not check high memory under OS/2.

Appendix F. Change history

You can review the changes that have been made to the current version of IBM AntiVirus, and/or previous versions.

Further information is available for the following releases:

Version 2.5.1

All Platforms

IBM AntiVirus can now fully verify, disinfect and shield macro viruses, like the Laroux virus, that infect Microsoft Excel spreadsheets. Protection is included from over 30 newer macro viruses, including the MDMA virus and the Wazzu family of macro viruses, which infect Microsoft Word documents. Files which match the pattern "*.XL?", the usual types for Excel files, are now examined when you check program files. Protection from new macro viruses is available as part of our regular virus signature updates, published on the Internet at http://www.av.ibm.com.

Protection was added for hundreds more viruses, including the Hare virus and the Moloch virus. The technology used by IBM AntiVirus to detect unknown and polymorphic boot viruses has been greatly extended, enabling it to detect many more viruses.

Support is now included for OS/2 Warp version 4 "Merlin", and for VFAT32 file systems that are used by Microsoft Windows 95 release 2.

IBM AntiVirus now identifies the EICAR standard test file, a widely-adopted file which can be used by customers to see what would happen if IBM AntiVirus found a virus. The EICAR test file is not itself a virus.

The IBM AntiVirus install programs now look for temporary space on all available drives rather than just the C: drive.

Problems were resolved in scanning Microsoft Word documents that were larger than 8 megabytes and in scanning files with the same name as device drivers.

The AE_DELAY profile tag has been moved from the USER.PRF profile to the AUTORUN.PRF profile.

Windows 95

An infrequent conflict was resolved between the IBM AntiVirus System Shield and the Scandisk program on Windows 95.

A similar conflict was resolved between the IBM AntiVirus System Shield and certain Novell Netware clients on Windows 95.

DOS and Windows

The DOS and Windows install programs now return CID completion codes via Interrupt 2F. They continue to return completion codes via the system ERRORLEVEL variable as well.

© Copyright IBM Corp. 1989, 1996

Version 2.5

It is important to note that if you have an IBM AntiVirus 2.5 beta-version installed on your system, you need to use the Uninstall feature and remove it before you install this production version of IBM AntiVirus.

All Platforms

Protection from macro viruses has been greatly extended. The Concept virus, currently one of the most prevalent in the world, can now be verified and disinfected extremely reliably, and is shielded on all platforms. The macro viruses Boom, LBYNJ, and Wazzu are detected and shielded. Protection from new macro viruses will be available as part of our regular virus data file updates.

Protection was added for hundreds more viruses, including the Tentacle virus (which infects Windows executables). Verification and disinfection was also added for the Majo-1644 and Werewolf-1500B viruses, which have been seen in recent large incidents.

Incorporation of new technology for integrity checking, database management and virus scanning has resulted in a substantial performance increase in virus checking and scanning on all platforms.

The installation procedure has been revised. All platforms other than OS/2 now use the SETUP command to install. For OS/2, use SETUPOS2. IBM AntiVirus Desktop Edition now includes a bootable Emergency Diskette, which you can use to clean your system if a virus prevents your system from starting properly.

The System Shield has been enhanced to find viruses before they enter your system, whether from the Web, via FTP, downloaded from bulletin board systems, or copied from diskettes or file servers. This was done by extending the "Scan files when opened" function to "Scan files when accessed." Files are now scanned for common viruses when they are created, modified or read on your system. This provides broad, system-level protection against viruses in incoming files. "Scan files when accessed" is not enabled by default, but will be enabled if you previously had "Scan files when opened" enabled. You can also enable it from the System Shield dialog.

An Uninstall program is now included on all platforms, and its function is fully integrated with the Registry in Windows 95 and Windows NT. Note, however, that IBM AntiVirus is fully compatible with your software, and does not need to be removed. Removing it makes your system vulnerable to viruses. Several options are available to enterprise administrators to control the use of Uninstall in their enterprise. These are discussed in the section of the User's Guide that explains command-line parameters and response files for the installation programs.

An IBM AntiVirus folder is now created on the desktop on all platforms other than DOS. IBM AntiVirus itself, the User's Guide, the READ.ME file and Uninstall are all accessible directly from this folder.

A memory scanning conflict with S3 video adapters has been fixed on all platforms. Long file names, and file names that include spaces, are

now fully supported on platforms which allow them. The installation procedure now coexists with Netbind.

Windows NT

A new, native version of IBM AntiVirus for Windows NT was introduced into IBM AntiVirus Enterprise Edition. It features a full GUI, and the same detection, disinfection and automated checking abilities as on other platforms. Full installation and uninstall programs are also included. Shield functions are not enabled in this release.

DOS

A Windows-style help system was added, with full hypertext support. The files IBMAVD*.HLP, formerly used by IBM AntiVirus for DOS, are no longer needed and are erased by the install program.

Windows 3.x

Automated checking is now available in IBM AntiVirus for Windows. The System Shield is now implemented with VxD technology in Windows 3.x. This extends its protection and provides better integration with Windows 3.x. CD-ROM drives now appear as removable media, and can be scanned for viruses from the Scan Diskette dialog.

Windows 95

The Help system now uses the standard Windows 95 help style, for better integration with Windows 95. A problem was corrected that sometimes caused a shift in focus when an automated check began.

OS/2

An IBM AntiVirus folder is now created on the desktop. It contains the icons for IBM AntiVirus for OS/2, the User's Guide, the Read Me file, and Uninstall.

Version 2.4.1

By default, IBM AntiVirus now scans *.DOC files and *.SMM files as standard program files.

A problem was corrected so that users with S3 video chips can now use IBM AntiVirus to scan memory on Windows 3.1 systems.

A scheduling problem on Windows 95 systems has been corrected to eliminate unnecessary scans.

IBM AntiVirus has been modified to scan laptops after they have returned from suspend mode. This has been implemented on OS/2 and Windows 95 systems and ensures that laptops are scanned on a regular basis, although they may not have been rebooted.

IBM AntiVirus is now compatible with the Advanced Power Management (APM) function on 755CX ThinkPads running OS/2.

A new convention for version numbers has been implemented. Version numbers have been modified slightly to accommodate IBM AntiVirus maintenance releases.

Many more known viruses are detected, including the Boza virus, a non-resident file infector for Windows 95 systems. IBM AntiVirus also detects the viruses Hot and Green Stripe.

Version 2.4

The IBM AntiVirus product line now includes a native version for Windows 95 systems. IBM AntiVirus for Windows 95 requires 2.0MB of disk space when installed. Information for installing and using IBM AntiVirus for Windows 95 has been added to the documentation.

There is now a standardized distribution for IBM AntiVirus. IBM AntiVirus for DOS and IBM AntiVirus for Windows are provided on two 1.44MB diskettes. IBM AntiVirus for Windows 95 is provided on two 1.44MB diskettes. IBM AntiVirus for OS/2 is provided on two 1.44MB diskettes.

The product names have been changed from IBM AntiVirus/DOS to IBM AntiVirus for DOS and IBM AntiVirus for Windows. IBM AntiVirus/2 is now called IBM AntiVirus for OS/2. In addition, the DOS Shield has been changed to the System Shield. This change is reflected on several dialogs.

The Contact List has been revised so that it only contains technical support telephone numbers for the United States, Puerto Rico, and Canada. In all other countries, you must refer to the appropriate Customer Service and Support Guide for your country. Or, you can refer to other contact information contained in the program package.

The performance of IBM AntiVirus for Windows has been improved.

The response file tag UpdateStartCmd was incorrectly identified as the UseStartCmd in an earlier edition of this document.

Many more viruses are detected, including a new class of viruses which infect Word for Windows version 6 document templates. By default, IBM AntiVirus now scans *.DOT files, and the Word macro viruses named Concept, Colors, Nuclear, and DMV are all detected.

Version 2.3

The user interface for IBM AntiVirus Install was redesigned for easier use. IBM AntiVirus Install for DOS supports new command line parameters /**DOSONLY** and /**STARTUP.CMD**, with corresponding response file tags **DosOnly** and **UpdateStartupCmd**. A new return code from IBM AntiVirus Install indicates an invalid tag in a response file, or an invalid response file.

The performance of IBM AntiVirus for DOS and IBM AntiVirus for OS/2 was enhanced for typical system checks, in which only a few files have changed.

A problem was corrected in which IBM AntiVirus for OS/2 could fail when trying to check files in directories that have a path name longer than the allowed length of OS/2 path names. IBM AntiVirus for OS/2 will now skip those directories and record in the log that they were not accessible for checking.

New icons were incorporated into the entire IBM AntiVirus product line.

Many more viruses are detected, including ByWay (a polymorphic file system infector) and Manzon (a polymorphic file infector).

Version 2.2

A new tag, **GenericDisinfect**, can be included in the response file. This tag determines whether IBM AntiVirus will be able to disinfect previously unknown viruses when it discovers them.

A problem was corrected in the Windows install program which prevented response files from being used properly.

Many more viruses are detected, including BUPT, NWAIT and Bua-2263.

Several more viruses, including Turbo, NWAIT and Jimi, were added to the System Shield because they were seen in verified incidents.

Version 2.1

If the System Shield feature called **Check files when accessed** is in use, it will now prevent infected files from being copied, rather than simply warn you.

The performance of the Update feature has been enhanced, as has the performance of checking the system with the DOS portion of IBM AntiVirus for DOS.

If IBM AntiVirus for OS/2 has found a virus, subsequent automated checks will not try to run until you have closed IBM AntiVirus for OS/2. Previously, they would try to run, and would display a pop-up saying they couldn't. Multiple pop-ups, one for each attempt, would get displayed until IBM AntiVirus for OS/2 was closed. Now, only a single pop-up will be displayed.

If you are installing over a previous version of IBM AntiVirus, IBM AntiVirus Install now removes a number of older IBM AntiVirus files that are no longer needed. IBM AntiVirus Install for Windows no longer asks you if you want to create an AntiVirus program group if one already exists. The memory scan in IBM AntiVirus Install for Windows no longer hangs on systems with adapters that use memory-mapped I/O. If IBM AntiVirus Install for OS/2 is unable to update the Startup folder (which can happen if your OS2.INI file has been corrupted), the STARTUP.CMD file is updated instead.

IBM AntiVirus for OS/2 and IBM AntiVirus Install for OS/2 no longer steal focus when dialogs and pop-up messages are displayed. IBM AntiVirus no longer reports an out-of-memory error when scanning locked files. Files shorter than 24 bytes can now be repaired correctly with generic disinfection. A problem was fixed that sometimes caused IBM AntiVirus for Windows to stop after counting files during a check.

Many more known viruses are detected, including the Cocanium virus. Verification and disinfection were added for a number of viruses, including Wix (also known as Die Hard) and Turbo (also known as Sampo).

Version 2.0

Starting with this release, IBM AntiVirus for DOS runs on DOS 3.3 and above, and on Windows 3.1 and above; Windows versions below 3.1 are no longer supported. Similarly, IBM AntiVirus for OS/2 is now a full

32-bit application, and runs on OS/2 2.0 and above. OS/2 version 1.3 is no longer supported.

IBM AntiVirus now has the ability to disinfect files even if they are infected with uncommon or new viruses. IBM AntiVirus needs to be installed on the system prior to the infection, so that it knows what the files looked like before they were infected. This ability, called “generic disinfection” can be selected in IBM AntiVirus Install by selecting **IBM AntiVirus settings** from the **Settings** main menu item, then checking the **Generic disinfection** check-box and installing as usual.

The neural network responsible for generic virus detection has been further refined to detect larger classes of new viruses, while reducing the chances of false alarms even further.

There is a new main menu item in IBM AntiVirus that helps update virus data files, which helps you keep your protection up-to-date.

A new, simpler way of selecting drives, directories and files to check was added to the **Check system** dialog. This replaces the **Advanced options** dialog. Similarly, the **Virus infection report** dialog was redesigned to be clearer and provide more information.

Virus data file formats were enhanced. The formats used in 2.0 are not compatible with version 1.x. The scanning technology used in IBM AntiVirus was enhanced to better detect polymorphic and encrypted viruses. And of course, detection was added for hundreds of new viruses, including the One_half virus and the Goldbug virus.

IBM AntiVirus for OS/2 now puts an icon into the Startup Folder for IBM AntiVirus for OS/2 Startup for automated checking, rather than adding lines to the STARTUP.CMD file. If you are reinstalling over a previous version, the lines that were present in STARTUP.CMD are removed.

New return codes were documented for IBM AntiVirus Install for DOS. IBM AntiVirus for OS/2 is now fully CID enabled for NetView Distribution Manager/2. CID (Configuration, Installation and Distribution) is a way of installing and configuring programs in a LAN environment with little or no user interaction. (See the **References** section of this User's Guide for more information on CID.)

The DOS portion of IBM AntiVirus for DOS now requires 450k of free RAM in order to run, rather than 400k in previous releases. The cumulative log now keeps the most recent entries at the top rather than the bottom, to make viewing the current entry easier. The cumulative log now prunes older entries automatically; only the latest 50 entries are kept. IBM AntiVirus is now optimized to perform better on disks compressed with Microsoft DiskSpace. A problem was corrected that caused the first check after installation to be slow. The contact phone numbers were updated for Canada, Greece and the Netherlands.

Automatic priority adjustment in IBM AntiVirus for OS/2 works differently in this release. Please see the **READ.ME**. file for more information.

Several common viruses were renamed to be consistent with the CARO naming convention, a widely-used convention for naming viruses. The intent is to make it easier to determine when IBM AntiVirus and other

anti-virus products detect the same virus rather than different viruses. The viruses whose names changed are:

Old Name	New Name
1575	Green Caterpillar
17 1	Cascade.17 1
17 4	Cascade.17 4
1813	Jerusalem
4 96	Frodo
Bouncing Ball	Ping Pong
Brunswick	Stoned.16
Campana	Kampana Boot
Cansu	V-Sign
CHV 2.1	iichv 2.1
D3	AntiEXE
Flip-2153	Flip.2153
Grain of Sand	Maltese Amoeba
Hell-1182	Helloween.1182
Monkey-1	Monkey.A
Monkey-2	Monkey.B
Parity Boot	Parity Boot.B
Scream-696	Screaming Fist.II.696
Stelboo	Stealth Boot.B
stonheng	Stoned.Manitoba
TP16VIR	Vacsina.TP.16

Version 1.07

Many more known viruses are detected, including the Natas, Kaos4 and Junkie viruses. Several viruses, including D3, were added to the System Shield because they were seen in verified incidents.

A problem was corrected in the install program for IBM AntiVirus in Windows 3.1 systems with SHARE loaded, which caused one of the install diskettes to be misidentified.

Version 1.06

A substantial number of new features were added to extend the ability of IBM AntiVirus to detect both known and unknown viruses. A new part of the System Shield detects common viruses when DOS opens infected files during copying, downloading, etc.. IBM AntiVirus now has an option for scanning inside of files compressed with PKZIP, ZIP2EXE or LZEXE. Finally, many unknown boot record viruses can now be detected with an extension to IBM AntiVirus heuristic scanning. This extension uses patent-pending neural network technology from IBM which distinguishes viruses from normal boot records.

IBM AntiVirus for NetWare now supports real-time scanning in NetWare 3.11 and 3.12, based on a new, architected Novell API. IBM AntiVirus for NetWare is available to customers of IBM AntiVirus Services.

There are new, smaller, native install programs for DOS, Windows and OS/2. Windows users can now install IBM AntiVirus directly from Windows. IBM AntiVirus for DOS can now be installed after booting DOS from a diskette. Return codes, a “response file” option and other command line options were added to the install programs to support CID installation. IBM AntiVirus now knows to check files thoroughly

whenever the virus data files are updated. It is no longer necessary to run IBMAVD /INSTALL or IBMAV2 /INSTALL after updating virus data files.

The IBM AntiVirus stand-alone program now obeys administrative profiles set up with IBM AntiVirus Administrator, so it is now installed as part of the normal IBM AntiVirus installation process. The IBM AntiVirus for OS/2 Automated Execution Monitor is now a PM application. It does not appear in a window, and does not appear in the Window List. It sits in the background until a check is scheduled to occur, then starts the check. The **Ignore** button on the **Virus Infection Report** dialog has been extended so you can tell IBM AntiVirus to ignore boot records that are reported as suspicious. A problem with the **Ignore** button for suspicious files in IBM AntiVirus for OS/2 has been corrected. The heuristic for suspicious files has been improved to give even fewer false alarms. The clarity and completeness of the documentation has been improved.

Starting with this release, IBM AntiVirus for OS/2 requires OS/2 version 2.0 or later. “Compatibility” versions of IBM AntiVirus for OS/2 which run on OS/2 1.3 are available to customers of IBM AntiVirus Services in some countries for a limited time.

Many new viruses are detected, including Queeg, Pathogen, some viruses in the SMEG family, and TrJP (a new virus that captures NetWare logon passwords). More viruses are dealt with by the **Prevent Common DOS Viruses** feature of the System Shield, and more viruses can now be disinfected.

Version 1.05

Many more known viruses are detected, including the Power Pump virus. Several viruses, including Ripper and EXEBUG, were added to the System Shield because they were seen in verified incidents.

A problem was corrected in the install program for IBM AntiVirus/DOS for 3.5" diskettes. This problem made it difficult for administrators to distribute updated virus data files on these diskettes.

The appearance of the DOS portion of IBM AntiVirus/DOS on monochrome displays has been improved.

IBM AntiVirus no longer queries all drives when a DOS session is started. This had caused problems when a non-data CD was present in a CD-ROM drive when DOS sessions were started.

Version 1.04

Many more known viruses are detected, including SatanBug, Stelboo and D3, bringing the total to well over 2,000. All DOS components of IBM AntiVirus now run in less than 400k of free RAM.

IBM AntiVirus for NetWare, a new component for Novell NetWare servers, is now available to customers of IBM AntiVirus Services.

IBM AntiVirus can now have its virus prevention, detection, verification and disinfection features updated with data files. The data file updates are available in various countries to customers of IBM AntiVirus

Services. The log files now record the version number of the data files as well as the version number of the programs.

The install program now offers users the option of just scanning their system instead of installing the program. The DOS install program now invokes IBM AntiVirus/DOS at the end of an installation as an option. The DOS install program also offers to create an "emergency" diskette. When you boot DOS from this "emergency" diskette, it will check your system for known viruses and, in most cases, clean them up. This is useful when your system cannot boot from the hard disk due to a virus problem.

An **Ignore** button is now included in the **Virus infection report** dialog. This allows users to tell IBM AntiVirus to not report apparent infections in selected files. Messages from the System Shield now appear in message boxes within Windows. IBM AntiVirus for OS/2 now adjusts the priority of itself automatically during automated checking, to further reduce its impact on normal activities. The System Shield is no longer limited to displaying the first 512 characters of LOCAL.MSG.

The OS/2 installation program now correctly handles STARTUP.CMD files written in REXX. A problem with specifying INSTALL /WINDOWS without the /AUTO parameter was corrected.

Version 1.03

Many more known viruses are detected, including the Butterfly virus and viruses created by the PS-MPC virus creation program, bringing the total to well over 1700. A number of new viruses can now be verified and disinfected.

Significant enhancements were made to the System Shield. These include the ability to detect rare and unknown viruses by their behavior and the ability to check diskettes for boot record viruses when they are accessed by DOS, and when Ctrl+Alt+Del or the OS/2 shutdown command is used to restart the system. The user can now control System Shield's use of high and expanded memory. The System Shield no longer conflicts with some other programs that use Expanded Memory when it is loaded into Expanded Memory.

IBM AntiVirus now contains support for a wide variety of administrative features, used in conjunction with the IBM AntiVirus Administrator program available as part of IBM AntiVirus Services. This includes LAN messaging, automatic disinfection to support unattended operation, and the ability for administrators to restrict the user from changing some of the behaviors of IBM AntiVirus.

The installation program now runs in less than 400k of memory. Automatic installation now preserves all existing settings in IBM AntiVirus unless the new /COPY option is specified. INSTALL /AUTO now installs the Windows portion of IBM AntiVirus if it had been installed previously or if a WINDOWS directory is in the current PATH. Automatic installation now defaults to installing in the directory to which the IBMAV environment variable points, so updates will be installed in the directory into which you had previously installed IBM AntiVirus. The OS/2 install program now supports STARTUP.CMD files in REXX. The install program recommends a reboot if the IBMAV environment variable

or CONFIG.SYS settings change. In OS/2 2.0 and above, the IBM AntiVirus/2 program object is created directly on the desktop, rather than in a program group.

Several more command line options were added to the IBM AntiVirus stand-alone program, including the ability to scan a particular directory or a particular file. Its return codes were documented in more detail.

Version 1.02

IBM AntiVirus now beeps when any indication of a virus is found. Checking can be cancelled during initial file counting. The button on the main window has been relabelled for clarity. Save settings for diskettes now saves the drive to be checked.

Many new viruses are detected, including the Tremor virus and a number of boot record viruses. Occasional false positive reports on CPAVSCAN.DLL and MSAVSCAN.DLL were eliminated. These reports were caused by these files leaving virus signatures in the clear, contrary to the standard practice in the anti-virus industry. Virus signatures found in these files will not be reported. Since these are Windows DLL files which are not infected by currently known viruses, this does not decrease the protection you get from IBM AntiVirus. These files will be flagged as “suspicious” if they change suspiciously.

IBM AntiVirus for DOS now allows activation of the main menu bar with the Alt key. Memory requirements have been further reduced.

IBM AntiVirus for OS/2 can now be invoked from an OS/2 session from any directory; it is not necessary to switch to the directory in which IBM AntiVirus for OS/2 was installed.\ The problem has been fixed in IBM AntiVirus for OS/2 that sometimes caused automated checking to occur at other than the scheduled times.

The System Shield does not re-load itself if it is already loaded.

The IBM AntiVirus stand-alone program now uses the file ADMIN.PRF in addition to the files it previously used.

An environment variable is added by the install program which points to the directory used for logs, personal profiles and the database file. The problem has been fixed that sometimes caused an empty Windows group to be added on install. The problem has been fixed that caused IBM AntiVirus for DOS to complain that it could not continue its check on installation when the system was infected with certain viruses. The installation program does not currently create example files.

Version 1.01

Memory requirements have been reduced for IBM AntiVirus for DOS. In IBM AntiVirus for OS/2, the automated execution monitor now runs hidden, so it does not appear on the desktop; automated checking can be run minimized so that nothing appears on the desktop in OS/2 2.0 systems unless a virus is found. The virus list now includes a cross-reference of virus names, so you can see the name IBM AntiVirus uses for viruses named by other products. False alarm elimination for heuristic analysis has been improved further. Customers of IBM AntiVirus Services can now install IBM AntiVirus from a LAN server, run it directly from a server, and disable users from cleaning up their own

systems with IBM AntiVirus; these features are only available to IBM AntiVirus Services customers and are documented separately for them.

Version 1.00

Initial release.

Index

A

Anti-virus programs 6-1
  techniques used by 6-1
  what are anti-virus programs? 6-1
Anti-virus techniques 6-1
  automated operation 6-3
  change detection 6-2
  disinfection 6-2
  heuristic analysis 6-2
  missing viruses and false alarms 6-3
  prevention and detection 6-3
  resident and non-resident operation 6-2
  scanning 6-1
  techniques used by IBM AntiVirus 6-3
  verification 6-2
Automated check 4-2
Automated protection 4-2, 4-11
  customizing 4-11

B

Boot Manager systems 3-16

C

Change history F-1
Check diskette boot records when used 4-2
Check files when accessed 4-2
Checking for viruses 4-4, 4-5
  compressed disks 4-6
  compressed files 4-6
  diskettes 4-4
  local drives 4-5
  network drives 4-5
  your system 4-5
CID 3-15
Cleaning up a virus 4-17, 4-19, 4-22, 4-23
  diskettes 4-22
  infected system 4-19
  nearby systems 4-22
  strategy for organizations 4-23
  uncommon viruses 4-22
Compressed files 4-6
  checking for viruses 4-6
Cumulative log 4-8
Current log 4-8
Customizing 4-11, 4-13, 4-14
  automated check 4-11
  automated protection 4-11
  checking specific directories 4-14
  checking specific files 4-14
Customizing *(continued)*
  diskette checking 4-13
  drive checking 4-14
  IBM AntiVirus 4-11
  installation settings 3-6
  system checking 4-14
  system shield 4-11

D

Descriptions of viruses 4-9
Disk compression 4-6, 4-28
  checking compressed disks for viruses 4-6
  using the IBM AntiVirus stand-alone program on compressed disks 4-28
Diskette
  emergency, creating 3-9
Diskettes 1-1, 4-4, 4-13
  checking for viruses 4-4
  customizing checking 4-13
  quantities of 1-1
Diskettes, Rescue - See Emergency diskettes 3-9
Drives 4-5, 4-14
  checking for viruses 4-5
  customizing checking 4-14
Dual Boot systems 3-16

E

Emergency diskette 3-1, 3-9

F

Files A-1, B-1
  checking compressed files 4-6
  installed with IBM AntiVirus for DOS and IBM AntiVirus for Windows A-1
  installed with IBM AntiVirus for OS/2 D-1
  installed with IBM AntiVirus for Windows 95 B-1

H

Help 4-9
  online 4-9

I

IBM AntiVirus 4-1, 7-1
  anti-virus techniques used by 6-3
  automated protection 4-2
  creating additional emergency diskettes 3-9
  customizing 4-11

© Copyright IBM Corp. 1989, 1996

IBM AntiVirus *(continued)*
emergency diskette 3-1
files installed with IBM AntiVirus for DOS and IBM AntiVirus for Windows A-1
files installed with IBM AntiVirus for OS/2 D-1
files installed with IBM AntiVirus for Windows 95 B-1
installing 3-1
normal use of 4-1
phone numbers 7-1
problems with E-1
products 7-1
services 7-1
site licensing 7-1
stand-alone program 3-1
starting 4-1
technical support 7-1
time-out message 4-11
uninstalling 3-16
updates 7-1
updating 3-1
using 4-1
using with IBM Boot Manager and Dual Boot systems 3-16
IBM AntiVirus stand-alone program 4-24
on systems that use resident data compression 4-28
on systems that use security software 4-29
IBM AntiVirus, anti-virus techniques used by 6-3
change detection and fuzzy scanning 6-3
false alarm elimination 6-7
heuristic analysis 6-4
install and forget operation 6-7
intelligent incident management 6-11
neural networks 6-4
safe disinfection 6-5
system shielding 6-7
thorough examination 6-6
verification before disinfection 6-5
Installing 3-1
customizing installation settings 3-6
scanning the system without installing 3-8
Installing IBM AntiVirus 3-1
CID 3-15
command line examples 3-12
command line installation options 3-10
command line options 3-10
creating additional emergency diskettes 3-9
emergency diskettes 3-1
format of the response file 3-12
installation options 3-10
NetView Distribution Manager/2 3-15
online help 3-9
READ.ME file 3-9
response file 3-12
Installing IBM AntiVirus *(continued)*
response file example 3-15
return codes 3-15
Introduction 1-1
to IBM AntiVirus 1-1

L

Local drives 4-5
checking for viruses 4-5
Logs 4-8
LZEXE 4-6

N

NetView Distribution Manager/2 3-15
Network drives 4-5
checking for viruses 4-5

O

Online help 4-9

P

PKZIP 4-6
Prevent common DOS viruses 4-2
Previous log 4-8
Protecting yourself from viruses 2-1

Q

Quantities of diskettes 1-1

R

Reading list 8-1
READ.ME file 1-1, 3-9
References 8-1
Rescue diskettes - See Emergency diskettes 3-9
Running IBM AntiVirus 4-1

S

Scan diskettes on shutdown 4-2
Scanning the system without installing 3-8
Stand-alone program 4-24
on systems that use resident data compression 4-28
on systems that use security software 4-29
Starting IBM AntiVirus 4-1
System 4-5, 4-14
checking for viruses 4-5
customizing checking 4-14
System requirements 1-1
operating system levels 1-1

System requirements *(continued)*
RAM 1-1
System Shield 4-2, 4-18
finding viruses with 4-18
messages issued by 4-18

T

Technical support 7-1
Time-out message 4-11
Troubleshooting E-1
IBM AntiVirus for DOS E-2
IBM AntiVirus for OS/2 E-3
IBM AntiVirus for Windows E-2
installation program E-2
System Shield program E-3

U

Uninstalling IBM AntiVirus
command line options 3-18
Update 4-7
Updating 3-1
Using IBM AntiVirus 4-1

V

Virus data files, updating 4-7
Virus descriptions 4-9
Viruses 2-1, 5-1
cleaning up a virus 4-17
how do virus infections start? 5-2
how serious is the problem? 5-2
introduction to 5-1
protecting yourself from 2-1
what is a computer virus? 5-1
when a virus is found 4-17

W

Warn when viral activity occurs 4-2