Index to Help with VIRUSCAN for Windows

This index lists all of the help topics available for Scan for Windows, Version 97. Indexed items are arranged alphabetically within each category.

Introduction

Overview of VIRUSCAN

Overview of Operation

Scan Switches

Registration

Tech Support

Advanced User's Options

Creating a Virus String File

What VIRUSCAN Is

VIRUSCAN (SCAN) is a virus detection and identification progam for the IBM PC and compatible computers. VIRUSCAN will search a PC for known computer viruses in memory, the boot sector, the partition table, and the files of a PC and its disks. VIRUSCAN will also detect the presence of unknown viruses.

SCAN works by searching the system for instruction sequences or patterns that are unique to each computer virus, and then reporting their presence if found. This method works for viruses that VIRUSCAN recognizes. SCAN can detect unknown viruses in files and boot sector by appending validation (CRC) codes to .COM and .EXE files and then checking the files against their codes for changes, warning that an infection may have occurred if the file has been modified in any way, and by checking boot sectors for generic routines that a boot sector virus must have. SCAN can check for new viruses from a user-supplied list of virus search strings.

System Requirements

VIRUSCAN, the MS-DOS version will run on any PC with 320Kb of memory and DOS version 2.00 or greater. VIRUSCAN for Windows will run on any PC that has the Windows environment installed on it.

VIRUSCAN for Windows runs best in the 386 Enhanced mode.

Verifying the Integrity of VIRUSCAN

VIRUSCAN runs a self-test when executed. If SCAN has been modified in any way, a warning will be displayed. The program will still continue to check for viruses, though. If SCAN reports that it has been damaged, it is recommended that a clean copy be obtained.

VIRUSCAN versions 46 and above are packaged with the VALIDATE program to ensure the integrity of the SCAN.EXE file. The VALIDATE.DOC instructions tell how to use the VALIDATE program. The VALIDATE program distributed with VIRUSCAN may be used to check for all further versions of SCAN.

The validation results for SCAN.EXE, Version 97 should be:

```
        FILE NAME : SCAN.EXE
             SIZE : 81,681
             DATE : 10-15-1992
FILE AUTHENTICATION
        CHECK METHOD 1 : 86AD
        CHECK METHOD 2 : 16B6
```

The validation results for WSCAN97.EXE should be:

```
        FILE NAME : WSCAN97.EXE
             SIZE : 90,128
             DATE : 10-15-1992
FILE AUTHENTICATION
        CHECK METHOD 1 : 3786
        CHECK METHOD 2 : 17C9
```

If your copy of SCAN.EXE or WSCAN97.EXE differs, they may have been modified. Always obtain your copy of VIRUSCAN from a known source. The latest version of VIRUSCAN, VIRUSCAN for Windows, and validation data for both can be obtained off of McAfee Associates' bulletin board system at (408)988-4004 or from the Computer Virus Help Forum on CompuServe.

Beginning with Version 72, all McAfee Associates programs for download are archived with PKWare's PKZIP Authentic File Verification. If you do not see the "-AV" message after every file is unzipped and receive the message "Authentic Files Verified! #NWN405 Zip Source: McAFEE ASSOCIATES" when you unzip the files then do not run them. If your version of PKUNZIP does not have verification ability, then this message may not be displayed. Please contact McAfee Associates if you .ZIP file has been tampered with.

Additions to VIRUSCAN

Version 97 adds detection of 68 new viruses, bringing the total number of known viruses to 753, or counting variants, 1,469. For a complete description of known viruses, please refer to Patricia Hoffman's VSUM.

Beginning with 97 of Scan for Windows, there is a new flexibility added to the installation process. Different directories can be specified when running WINSTALL, that allows users to place SCAN.EXE, WSCAN.EXE and supporting files, and the .DAT files in different areas. This gives network supervisors more control over the scanning procedures.

Viruses reported at multiple sites include the 644, an encrypted memory-resident infector of COM and EXE files, ane the Tabulero, a .COM and .EXE infector from Vanezuela.

THE COMPUSERVE COMPUTER VIRUS HELP FORUM

We are now sponsoring the Computer Virus Help Forum on CompuServe. Updates to VIRUSCAN, VIRUSCAN for Windows, information about computer viruses, and technical support may be obtained by typing GO VIRUSFORUM at any CompuServe prompt. A free introductory membership to CompuServe is also available. Please read the COMPUSER.NOT file for details.

INTERNET ACCESS TO McAFEE ASSOCIATES SOFTWARE

The latest version of McAfee Associates' anti-viral software is now available by anonymous ftp (file transfer protocol over the Internet from the site mcafee.COM. If your domain resolver does not support names, use the IP# 192.187.128.1).

McAfee associates' anti-viral software may alsoe be found at the Simtel20 archive site WSMR-SIMTEL20.Army.MIL in the PD1:<MSDOS.TROJAN-PRO> directory and its associated mirror sites.

Detailed Description of VIRUSCAN

VIRUSCAN scan diskettes or entire systems for pre-existing computer virus infections. It will identify the virus infecting the system, and tell what area of the system (memory, boot sector, file) the virus occupies. An infected file can be removed with the "Overwrite and Delete Infected File" switch, which will erase the file. The CLEAN-UP program is also available to automatically disinfect the system and repair damaged areas whenever possible.

VIRUSCAN Version 97 identifies all 753 known computer viruses along with their variants. Some viruses have been modified so that more than one "strain" exists. Counting such modifications, there are 1,401 virus variants. This includes the twenty most common viruses which account for over 95% of all reported PC infections. The Virus Characteristics List menu item under the Help Menu lists and describes all new, public domain, and extinct computer viruses identified by SCAN.

All known computer viruses infect one or more of the following areas: the hard or fixed disk partition table (also known as the master boot record); the DOS boot sector of hard disks and floppy disks; or one or more executable files within the system. Executable files include operating system files, .COM files, .EXE files, overlay files, or any other files loaded into memory and executed. A virus that infects more than one area, such as a boot sector and an executable file is called a multipartite virus.

VIRUSCAN identifies every area or file that is infected, and indicates both the name of the virus and CLEAN-UP I.D. code used to remove it. SCAN will check the entire system, an individual diskette, subdirectory, or individual files for pre-existing virus infection.

VIRUSCAN will also check files for unknown viruses with the "Add Validation Codes" and "Check Validation Codes" switches. This is done by computing a code for a file, appending it to the file, and then validating the file against that code. If the file has been modified, the check will no longer match, indicating that viral infection may have occurred. With the "Add Recovery/Validation Codes to Files" switch, the validation codes will save information that can be used to restore files or areas of the system that have been damaged by an unknown virus.

VIRUSCAN calculates checksums using two independently generated CRC (Cyclic Redundancy Check). Files which are self-checking should not be validated since this will set off their own internal checks. VIRUSCAN adds validation codes to .COM and .EXE files only. The validation codes for the partition table, boot sector, and system files, are kept in a hidden file called SCANVAL.VAL in the root directory. To detect boot sector and partition table (MBR) viruses, SCAN checks the boot sector and MBR for signs of viral code. If suspicious code is found, SCAN will report that it has found a Generic Boot Sector or MBR virus.

VIRUSCAN can also be updated to search for new viruses via an "External Virus Data File" switch, which allows the user to provide the VIRUSCAN program with new search strings for viruses.

VIRUSCAN can display messages in either English, French, or Spanish.

VIRUSCAN works on stand-alone and networked PC's, but not on a file server. For networks, use the NETSCAN file server scanner instead.

An aging notice is built into the SCAN program. When the program is more than seven months old, a notice will be displayed to the user that SCAN may be out of date. SCAN will

continue to function normally, however. The aging notice can be bypassed by using the "Do Not Display Expiration Notice" switch.

Differences Between the DOS and Windows Versions of VIRUSCAN

The DOS and Windows version of VIRUSCAN perform the exact same function: to scan selected disk drives, files, and memory for known viruses. The difference in these two versions lies in the way VIRUSCAN is called.

In the DOS version, the filename SCAN is entered at the DOS prompt, followed by the drive and directory that SCAN is to search, followed by any options the user wishes to use. For example, at the DOS prompt, the user enters

C:>SCAN C: /NOMEM

to scan the C drive and skip the memory search.

With the Windows version of VIRUSCAN, the user is allowed to select the options by pointing and clicking with the mouse. There are two basic areas the user can make decisions: where to scan, and with what switches. Where to scan is handled with the "Scan Paths" item under the "Scan Options" menu. The various switches are located under "Scan Switches" under the "Scan Options" menu.

In many instances, all the user needs to do is click on the item desired. In situations where typing is required, such as stating which path(s) to scan, the item ends with "...", indicating that that item will need input from the user to carry out that option.

Two data files, WSCAN.DAT and WSCAN2.DAT will be created in the directory specified during the installation process. In the event that one or both are missing, VIRUSCAN for Windows will create new data files.

While running WINSTALL.EXE, the user will be asked for a location to install WSCAN. Different directories can be used to place SCAN.EXE, WSCANXX.EXE and support files, and the .DAT files. During this time, a file called WSCAN.CFG will be created and kept with the WSCANXX.EXE file. This file must be present when WSCAN.EXE is running. If this file gets erased or relocated, the WINSTALL program must be executed again.

Virus Characteristics Listing

The "Virus Characteristics Listing" menu item displays an overview of the viruses that the current version of VIRUSCAN can detect. This chart can be viewed from the Help menu by selecting the "Virus Characteristics List" option. The menu item requires the VIRLIST.TXT file that comes with VIRUSCAN. The window is automatically maximized to view the entire chart and cannot be resized.

To exit the listing at any time, the user can select another option from the menu or open up the Help menu again and select Exit Virus Listing. This will clear the window and restore it to its original size.

How to Use VIRUSCAN for Windows

VIRUSCAN will check each area or file on the designated drive(s) that could be host to a virus. If a virus is found, a message is displayed telling the name of the infected file or system area and the name of the identified virus. SCAN will examine files for viruses based on their extensions. The default file extensions supported by SCAN are .APP, .BIN, .COM, .EXE, .OV?, .PGM, .PIF, .PRG, .SWP, .SYS, and .XTP. Additional extensions can be added to SCAN or all files on disk can be selected for scanning.

The Windows version of VIRUSCAN is built to take advantage of the Graphical User Interface. Three menu titles are displayed: "Scan", "Scan Options", and "Help". The Help menu offers "Help", which is what you are viewing now. This flexible help function allows the user to look up topics in our help index, as well as to "Browse" sequentially through the help subjects.

"Virus Characteristics List", the second option under the "Help" menu, displays the VIRLIST.TXT file, which contains a listing of all the viruses detected by SCAN. For more information see

Virus Characteristics Listing

"About Scan for Windows" is the next option under the "Help" menu. This displays our company name, McAfee Associates, along with our logo and copyright statements, and the Version number of our software.

The middle menu, "Scan Options", gives the user a range of choices in how to use SCAN. The first item on the list, "Scan Switches", are functions that allow specific implementations of VIRUSCAN, such as bypassing memory checking. These options can be "switched" on or off. Any options chosen will be kept in a data file called WSCAN.DAT, created by VIRUSCAN for Windows. A complete description of these switches are given in the following section called

Selecting Viruscan Switches

The second option under "Scan Options" is entitled "Scan Paths(s)...", and prompts the user to enter in the drive(s) and path(s) to be scanned. If this option is not changed, VIRUSCAN will default to the drive and path where Windows resides. The last drive and path chosen will always be kept in a data file called WSCAN.DAT, created by SCAN for Windows. A detailed explanation of how the drive and path are chosen can be found in the section called

Selecting VIRUSCAN Paths

The left-most menu entitled "Scan", deals with the actual execution and termination of VIRUSCAN. The first option, entitiled "Begin Scan", starts the DOS VIRUSCAN program. This process is described in

Executing VIRUSCAN for Windows

The last option in the "Scan" menu is "Exit Scan". This is described in

Exiting VIRUSCAN for Windows

Selecting VIRUSCAN Switches

The middle menu item, "Scan Options", allows the user to make decisions about how SCAN is to execute. The first option, "Scan Switches", shows a window of options listed, with a checkbox beside each one. If the box beside the switch is empty, then that selection is not turned on. If there is an "X" in the box, then that switch will be implemented when VIRUSCAN is executed. To turn a selection "on", merely click on that switch. To turn it off, click on that selection again. Some items are not compatible with each other, such as "Scan Memory for All Viruses", and "Skip Memory Check". If, for instance, "Scan Memory for All Viruses" was checked, and the user attempted to select "Skip Memory Check", an error box would pop up stating that "Scan Memory for All Viruses" must be turned off first.

The switches are divided up into two pages. The first page contains more common switches. Hitting the MORE button will reveal page two, which contains all switches dealing with validation (checksum) codes, as well as some of the more advanced options, such as "SCAN Using External Virus Info File...". The user can move back and forth between the two pages, but the CANCEL button on either page will cancel all changes made to either page. Likewise, the OK button will save all changes made to both pages, regardless of which page the user was on when OK was clicked on.

The following is a list of Scan Switches:

Add Recovery/Validation Codes to Files...
Add Validation Codes to Files...
Append SCAN Report to File...
Beep Whenever a Virus is Found
Check Memory From 0Kb to 1088Kb
Check Recovery/Validation Codes in Files
Check Recovery/Validation Codes Stored in File...
Check Validation Codes in Files
Create Report of Infected Files...
Disable Ctrl-C/Ctrl-Brk During Scan
Disable Screen Pause
Display Messages in French
Display Messages in Spanish
Do Not Display Expiration Notice
List Files Not Having a Validation Code
Overwrite and Delete Infected Files
Remove Recovery/Validation Codes from Files
Remove Recovery/Validation Codes Stored in File...
Remove Validation Codes from Files
Save Date and Time VIRUSCAN Was Last Run
Scan All Files, Including Data Files
Scan Memory for All Viruses
Scan Multiple Floppies
Scan Overlay Extensions...
Scan Root Directory and Boot Area Only
Scan Subdirectories
Scan Using External Virus Info File...
Show Date and Time VIRUSCAN Was Last Run
Skip Internal Scan of LZEXE Compressed Files
Skip Internal Scan of PKLITE Compressed Files
Skip Memory Checking
Speed Up VIRUSCAN's Output
Store Recovery/Validation Codes in File...

Unattend Mode

Unattend Mode

The Unattend switch allows the SCAN program to continue checking a disk if it comes across open files (files in use) on the disk while scanning.

NOTE: This option requires DOS 3.1 or higher.

NOTE: This is one of the default options with VIRUSCAN for Windows. It is highly recommended to leave this switch on to avoid Memory Violation errors.

Add Recovery/Validation Codes to Files...

This option allows the user to store recovery data and validation codes for .COM and .EXE files, the boot sector, and partition table of a disk. Recovery information adds fifty-two (52) bytes to files. The recovery information for the partition table and boot sector is stored separately in a hidden file in the root directory. It is otherwise similar to the Add Validation Codes to Files switch, including an option to include an "exception list", a text file containing a list of files that are not to have this information added to it. A dialog box will ask for this filename; you may click on "CANCEL" to bypass this option.

Recovery requires the CLEAN-UP (CLEAN.EXE) program.

NOTE: This switch cannot be used with the following switches:

"Add Validation Codes to Files..."
"Check Validation Codes in Files"
"Remove Validation Codes from Files"
"Remove Recovery/Validation Codes from Files"
"Store Recovery/Validation Codes in File..."
"Check Recovery/Validation Codes Stored in File..."
"Remove Recovery/Validation Codes Stored in File..."

Add Validation Codes to Files...

This switch allows the user to add validation codes to the files being scanned. If a full drive is specified, SCAN will create validation data for the partition table, boot sector, and system files of the disk as well. Validation adds ten (10) bytes to files; the validation data for the partition table, boot sector, and system files is stored separately in a hidden file in the root directory of the scanned drive. Files which are already immunized against computer viruses or contain self-modifying code should not have validation codes added to them. To prevent VIRUSCAN from adding validation codes to these files, a validation exception list can be created with the complete path and filename of the each file NOT to be validated listed on each line. Only one file should be on a line, and each line should terminate with a carriage return. To put a comment in, start a line with the asterisk "*" character. A sample file might look like this:

```
* This is Clipper Corp's database program, Clipper
C:\CLIPPER\BIN\CLIPPER.EXE
* This is Lotus' spreadsheet program, 1-2-3
C:\123\123.COM
* This is MS-DOS 5.00's self-modifying program, SETVER
C:\DOS\SETVER.EXE
* PKWare's PKZIP programs already perform a self-check for   * viruses
C:\PKWARE\PKLITE.EXE
C:\PKWARE\PKZIP.EXE
C:\PKWARE\PKUNZIP.EXE
* Stac Technologies hard disk swapping program
C:\SWAPVOL.COM
* Symantec's Norton Utilities V6.01 disk caching program
C:\NORTON\NCACHE.EXE
* WordStar
C:\WORDSTAR\WS.EXE
```

The validation exception list should be an ASCII text file. If a word processor is used to create the list, be sure to save the file as ASCII.

After choosing the "Add Validation Codes" option from the VIRUSCAN switch menu, a dialog box will appear, prompting for the name of your text file. At this point, enter the path and name of the text file to be used. If an exception list is not to be used, simply click on the CANCEL button. The "Add Validation Codes" switch will still be in effect, but without an exception list.

NOTE: This switch cannot be used with the following switches:

"Remove Validation Codes from File"
"Add Recovery/Validation Codes to Files..."
"Check Recovery/Validation Codes in Files"
"Remove Recovery/Validation Codes from Files"
"Store Recovery/Validation Codes in File..."
"Check Recovery/Validation Codes Stored in File..."
"Remove Recovery/Validation Codes Stored in File..."

Append SCAN Report to File...

This switch saves a list of infected files to the disk. The list is saved to disk as an ASCII text file. If a list exists, then the results of the current scan will be added to its end. If the file does not exist, it will be created. If the user clicks on the OK button, the option will be saved. If the user clicks on CANCEL, the switch will be turned off.

NOTE: This options cannot be used with the following switch:

"Create Report of Infected Files..."

Beep Whenever a Virus is Found

This switch will cause VIRUSCAN to beep each time a computer virus is found.

Check Validation Codes in Files

This switch checks the validation codes inserted with the "Add Validtion Codes to Files..." switch. If the file has been changed, SCAN will report that the file has been modified and that a viral infection may have occured. Using this option adds about 25% more time to scanning.

NOTE: Some older Hewlett Packard and Zenith PC's modify the boot sector or partition table each time the system is booted. This will cause SCAN to continually notify the user of boot sector or partition table modifications if this switch is selected. Check your system's manual to determine if your system contains self-modifying code.

NOTE: This option cannot be used with the following switches:

"Remove Validation Codes from Files"
"Add Recovery/Validation Codes to Files..."
"Check Recovery/Validation Codes to Files"
"Remove Recovery/Validation Codes to Files"
"Store Recovery/Validation Codes in File..."
"Check Recovery/Validation Codes Stored in File..."
"Remove Recovery/Validation Codes Stored in File..."

Remove Validation Codes from Files

This switch is used to remove validation codes from a file or files. It can be used to remove the validation code from a diskette, subdirectory, or files(s). Using this option on a disk will remove the partition table, boot sector and system file validation.

NOTE: This switch cannot be used with the following switches:

"Add Validation Codes to File..."
"Check Validation Codes in Files"
"Add Recovery/Validation Codes to Files..."
"Check Recovery/Validation Codes in Files"
"Remove Recovery/Validation Codes from Files"
"Store Recovery/Validation Codes in File..."
"Check Recovery/Validation Codes in File..."
"Remove Recovery/Validation Codes in File..."

Save Date and Time of VIRUSCAN's Last Run

This switch will save the date and time that VIRUSCAN was last run by updating the date of the SCANVAL.VAL file. If no SCANVAL.VAL file exists, VIRUSCAN will create one.

Scan All Files, Including Data Files

This switch will cause SCAN to check all files on the referenced drive. This should only be used if a file-infecting virus has already been detected. Otherwise this option should only be used when checking a new program. This switch will add a substantial time to scanning.

NOTE: This switch cannot be used with the "Scan Overlay Extensions..." switch.

Scan Overlay Extensions...

This switch allows the user to specify an extension or set of extensions to scan. After "checking" this option, an editing box will appear and prompt you for the extension(s) to be used. Extensions should include the period character "." and be separated by a space. Up to three extensions can be added. If more extensions are desired, the user is advised to check the "Scan All Files, Including Data Files" switch.

NOTE: This switch cannot be used with the "Scan All Files" switch.

Skip Internal Scan of LZEXE Compressed Files

This switch tells VIRUSCAN not to look inside files compressed with LZEXE file compression program. SCAN will still check the programs for external infection.

Skip Internal Scan of PKLITE Compressed Files

This option tells VIRUSCAN not to look inside of files compressed with the PKLITE file compression program. SCAN will still check the programs for external infections.

Scan Multiple Floppies

This switch is used to scan multiple diskettes placed in a given drive. If the user has more than one floppy disk to check for viruses, this option allows the user to check them without having to run SCAN multiple times. If a system has been disinfected, this switch and the "Skip Memory Checking" switch can be used to speed up the scanning of disks.

Scan Memory for All Viruses

This switch tells VIRUSCAN to check system memory for all known computer viruses that can inhabit memory. SCAN by default only checks memory for critical and "stealth" viruses, which are viruses which can cause catastrophic damage or spread the infection during the scanning process. SCAN will check memory for the following viruses in any case:

1024, 1253, 1554, 1963, 1971, 2560, 337, 3445-Stealth, 4096, 512, Anthrax, Antitelefonica, Brain, Caz, CD, Dark Avenger, DIR-2, Doom II, Empire, Fish, Flu-2, Form, Greemlin, Irish, Joshi, Leech, Lozinsky, Microbes, Mirror, Nomenclature, NOP, No-Int (Stoned III), P1R (Phoenix), Phantom, Plastique, Pogue, SBC, Sentinel, Stoned, Sunday-2, SVC, Taiwan3, Tequilla, Turbo (Polish-2), Twin-351, V2100, V2P6, Whale

If one of these virus is found in memory, SCAN will stop and advise the user to power down, and reboot the system from a virus-free system disk. Using this switch with another anti-viral software package may result in false alarms if the other package does not remove it virus search strings from memory. The "Scan Memory for All Viruses" switch will add 6 to 20 seconds to the scanning time.

VIRUSCAN for Windows can perform a quick check for viruses in memory only. In this mode, the SCAN program will not check disk for computer viruses. Simply switch on the "Scan Memory for All Viruses" option, and under the "Scan Options" menu, choose "Scan Paths...". When prompted for the path, type "NUL" without quotes.

NOTE: This switch cannot be used with the "Skip Memory Checking" option.

Scan Root Directory and Boot Area Only

This switch offers the convenience of checking your boot sector, partition table (for hard drives), and root directory files only.

NOTE: This switch cannot be used with the "Scan Subdirectories" option.

Skip Memory Checking

This switch is used to turn off all memory checking for viruses. It should only be used when a system is known to be free of viruses.

NOTE: This switch cannot be used with the following switches:

"Scan Memory For All Viruses"
"Check Memory From 0Kb to 1088Kb" option.

Speed Up VIRUSCAN's Output

This switch will speed VIRUSCAN up by displaying less information on the screen during scanning, skipping scanning inside of LZEXE- and PKLITE-compressed files, and examining a smaller portion of files during scanning. This may cause some viruses to be missed.

Store Recovery/Validation Codes in File...

This option logs recovery data and validation codes for .COM and .EXE files, boot sector, and partition table of a disk to a user-specified file that can be located on any drive. The size of the file is about 20K per 1,000 files validated. When choosing this switch, a dialog box will appear, prompting the user for a filename. If no path is specified before the filename, the directory where WSCAN.EXE resides will contain the file. Clicking on OK saves the option; clicking on CANCEL will cancel this switch.

NOTE: This option cannot be used with the following switches:

"Check Recovery/Validation Codes Stored in File..." (if the file has not been created yet)
"Remove Recovery/Validation Codes Stored in File..."
"Add Validation Codes to File..."
"Check Validation Codes in File"
"Remove Validataion Codes in File"
"Add Recovery/Validation Codes to File..."
"Check Recovery/Validation Codes to File"
"Remove Recovery/Validation Codes to File"

Overwrite and Delete Infected Files

This switch tells VIRUSCAN to prompt the user to overwrite and delete an infected file when one is found. If the user selects "Y" the infected file will be overwritten with hex code C3 [the Return-to-Dos instruction] and then deleted. A file erased by this switch cannot be recovered. If the McAfee Associates' CLEAN-UP program is available, it is recommended that CLEAN be used to remove the virus instead of SCAN, since in most cases it will recover the infected file. Boot sector and partition table infectors can not be removed by this switch and require the CLEAN-UP virus disinfection program.

Remove Recovery/Validation Codes From Files

This option will remove validatation codes and recovery information from files added with the "Add Recover/Validation Codes to Files" switch.

NOTE: The following switches cannot be used with this option:

"Add Recovery/Validation Codes to Files..."
"Check Recovery/Validation Codes to Files"
"Add Validation Codes to Files..."
"Check Validation Codes to Files"
"Remove Validation Codes from Files"
"Store Recovery/Validation Codes in File..."
"Check Recovery/Validation Codes Stored in File..."
"Remove Recovery/Validation Codes Stored in File..."

Remove Recovery/Validation Codes Stored in File...

This switch will remove recovery data and validation codes for files from the recovery data and validation code file. When this box is clicked on, a dialog box will pop up, prompting the user for a filename. If no path is given, the file will be searched for in the same directory that WCAN.EXE resides in . Clicking on OK will save the option; clicking on CANCEL will turn the switch off.

An error box will pop up if the file cannot be found.

NOTE: This option cannot be used with the following switches:

"Store Recovery/Validation Codes in File..."
"Check Recovery/Validiton Codes Stored in File..."
"Add Validation Codes to File..."
"Check Validation Codes in File"
"Remove Validation Codes From Files"
"Add Recovery/Validation Codes to Files..."
"Check Recovery/Validation Codes in Files"
"Remove Recovery/Validation Codes From Files"

Create Report of Infected Files...

This switch is used to generate a listing of infected files. The resulting list is saved to disk as an ASCII text file. When this option is checked, an editing box will appear, prompting the user for the name of the file. This can include the device and path. For example:

B:VIRUS.RPT

will create a file called VIRUS.RPT and save to a disk on the B drive.

When the user is done entering the path and filename, clicking the "OK" button will add it to your list of options. If the user wishes to abort this option, clicking on "CANCEL" will remove the editing box and leave the "Create Report of Infected Files..." checkbox empty.

Disable Ctrl-C/Ctrl-Brk During Scan

This switch prevents Control-C and Control-Break from stopping the VIRUSCAN program.

NOTE: This is one of the default options with VIRUSCAN for Windows.

Disable Screen Pause

This switch disables the "More..." prompt that appears when SCAN fills up a window with data. This allows VIRUSCAN to run on a machine with multiple infections without requiring operator intervention when the screen fills up with messages from the SCAN program.

NOTE: This option is one of the default options with VIRUSCAN for Windows.

Display Messages in French

This VIRUSCAN switch outputs all messages in French instead of English.

NOTE: This option cannot be run with the "Display Messages in Spanish" switch.

Display Messages in Spanish

This option will display VIRUSCAN's messages in Spanish, rather than English.

NOTE: This option cannot be run with the "Display Messages in French" switch.

Do Not Display Expiration Notice

This switch disables the aging message this is displayed when SCAN is more than seven months old.

List Files Not Having a Validation Code

This option will audit a system for files that have validation codes added to them with the "Add Validation Codes" option. Files that have no validation code will be reported as being uncertified by VIRUSCAN.

Scan Using External Virus Info File...

This switch allows VIRUSCAN to search for viruses from a text file containing user-defined search strings in addition to the viruses that SCAN already checks for. When the check box for this switch is clicked on, an editing box will appear, prompting the user for the path and filename of the external virus data file. For instructions on how to create an external virus data file, see:

Creating a Virus String File

Show Date and Time VIRUSCAN Was Last Run

This switch will display the time and date VIRUSCAN was last run.

NOTE: When this switch is activated, VIRUSCAN will only show the information; no files or memory will be scanned, regardless of any options chosen.

Scan Subdirectories

This switch allows SCAN to scan subdirectories under a subdirectory when scanned. Previously, SCAN would only recursively check subdirectories if a logical device (e.g., C:) was scanned.

Check Memory From 0Kb to 1088Kb

This option checks the memory above 640Kb that can be used on AT(286) and 386 systems for computer viruses. This includes the 384Kb Upper Memory Area from 640Kb to 1024Kb, and the 64Kb High Memory Area from 1024Kb to 1088Kb. On XT systems with extended memory cards installed, this will cause the first 64K of RAM to be scanned again.

NOTE: This option cannot be switched on with the "Skip Memory Checking" switch.

Check Recovery/Validation Codes in Files

This switch tells SCAN to check restoration information and validation codes inserted by the "Add Recovery/Validation Codes to Files..." option. If the file or system has been changed, SCAN will report that the file has been modified.

NOTE: This switch cannot be used with the following switches:

"Remove Recovery/Validation Codes from Files"
"Add Validation Codes to Files..."
"Check Validation Codes in Files"
"Remove Validation Codes from Files"
"Store Recovery/Validation Codes in File..."
"Check Recovery/Validation Codes Stored in File..."
"Remove Recovery/Validation Codes Stored in File..."

Check Recovery/Validation Codes Stored in File...

This option checks recovery data and validation codes that have been accumulated with the "Store Recovery/Validation Codes in File..." switch. A dialog box will pop up when this switch is turned on, prompting the user for a filename. If no path is specified, the file will be searched for in the same directory WSCAN.EXE resides in. Clicking on OK will save the option; clicking on CANCEL will turn off the switch.

In the even the file is not found, an error box will appear.

NOTE: This switch will not work with the following switches:

"Remove Recovery/Validation Codes Stored in File..."
"Add Validation Codes to Files..."
"Check Validation Codes in Files"
"Remove Validation Codes from Files"
"Add Recovery/Validation Codes to Files..."
"Check Recovery/Validition Codes in Files"
"Remove Recovery/Validition Codes in Files"

Selecting VIRUSCAN Paths

The last item on the "Scan Options" menu is "Scan Paths...". Here the user is invited to enter in the drive(s) and path(s) for VIRUSCAN to examine for possible infection.

To enter the drive(s) and path(s) to be scanned, click the mouse on the "Scan Options" menu heading. From there, click the mouse button on the "Scan Paths..." option. Or the user may simply keep the left mouse button held down and release it when the mouse pointer is on the "Scan Paths..." option. A dialog box will then open up. If you have never used this option before, it will default to the C: drive. Otherwise, your last choice will be displayed.

At this point, the user can click the mouse pointer on "OK" and that path will be kept.

If a different path is desired, the user may type in the new drive(s) and path(s), such as:

C:\GAMES D:\WORK

When done, the user click the mouse pointer on the "OK" box, or simply hit the Enter key and new data will be kept.

At any time, the user may click on the "CANCEL" BOX. This will discard any changes the user has made, and when SCAN is activated it will examine the previous drive and path.

Executing VIRUSCAN for Windows

To begin scanning your drive, click the mouse on the "Scan" menu title. There you will see two options: "Begin Scan" and "Exit Scan". Either click on "Begin Scan" or simply keep the left mouse button depressed after selecting the "Scan" menu title, and bring the pointer down to the "Begin Scan" menu item and release the button.

At this point, Windows will call the MS-DOS version of VIRUSCAN with the options you have chosen, or the default options if none have been specified. A DOS window will open up and the scanning operation can be observed. The title bar of this window will say

"Scanning for Viruses..."

At the conclusion of the scan, the title bar will say

"[Inactive - Scanning for Viruses...]"

meaning that the program has terminated normally. To close this window, either double click on the control-menu box, located at the upper left corner of the Window, or do a single click to open up the menu and choose the Close option.

It is recommended that VIRUSCAN be allowed to run without simultaneously opening other windows, as this will slow the scanning process.

Exiting VIRUSCAN for Windows

To exit VIRUSCAN for Windows, the user can do this several ways:

1. Double click on the control-menu box.

2. Open the control-menu box by clicking once on it, and choose the "Close" option.

3. Open the "Scan" Menu by clicking once on it, and either hold the left mouse button down and release on the "Exit Scan" bar or simply click once on the "Scan" Menu and once on the "Close" bar.

How to Register VIRUSCAN for Windows

A registration fee of $35.00 is required for the use of VIRUSCAN by individual home users. Registration is for one year and entitles the holder to unlimited free upgrades off of the McAfee Associates BBS. When registering, a diskette containing the latest version may be requested. Add $9.00US for diskette mailings. Only one diskette mailing will be made.

Registration is for home users only and does not apply to businesses, corporations, organizations, government agencies, or schools, who must obtain a license for use. Contact McAfee Associates for more information.

Outside of the United States, registration and support may be obtained from the Agents listed in the accompanying AGENTS.TXT file.

Tech Support for VIRUSCAN for Windows

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

- Program name and version number.
- Type and brand of computer, hard disk, plus any peripherals.
- Version of DOS you are running, plus any TSRs or device drivers in use.
- Printouts of your AUTOEXEC.BAT and CONFIG.SYS files.
- The exact problem you are having. Please be as specific as possible. Having a printout of the screen and/or being at your computer will help also.

McAfee Associates can be contacted by BBS, fax, or Internet 24 hours a day, or call our business office at (408)988-3832, Monday through Friday, 8:30AM to 6:00PM Pacific Standard Time.

McAfee Associates
3350 Scott Blvd. Bldg. 14
Santa Clara, CA. 95054-3107
U.S.A.

(408)988-3832 office
(408)970-9727 fax
(408)988-4004 BBS (32 lines)
USR HST /v.32/v.42bis/MNP 1-5
CompuServe GO VIRUSFORUM
Internet: mcafee@netcom.com

If you are overseas, please refer to the AGENTS.TXT file for a listing of McAfee Associates Agents for support or sales.

How to Manually Remove a Virus

What do you do if a virus is found? You can contact McAfee Associates for help with removing viruses by BBS, FAX, telephone, or Internet. There is no charge for support calls to McAfee Associates.

The CLEAN-UP universal virus disinfection program is available and will disinfect the majority of reported computer viruses. It is updated with each release of the SCAN program to remove new viruses. The CLEAN-UP program can be downloaded from McAfee Associates BBS, the SIMTEL20 archives on the Internet, or from the agents listed in the enclosed text file.

It is strongly recommended that you get experienced help in dealing with viruses, especially critical viruses that can damage or destroy data. For a listing of critical viruses, see the description of the switch

Scan Memory for All Viruses

Partition table or boot sector infecting viruses are especially dangerous, since improper removal of these virus could result in the loss of all data and the use of the disk(s).

For qualified assistance in removing a virus, please contact McAfee Associates directly or check the enclosed AGENTS.TXT file for an authorized McAfee Associates Agent in your area. Agents may charge McAfee Associates normal support rates for their services.

NOTE ON DOS 5 AND REFORMATTING INFECTED FLOPPIES

If you are reformatting infected floppy disks under DOS 5.0, be sure to add the /U switch to the FORMAT command. This tells DOS to do an unconditional format of the disk, and not to save the original (infected) boot sector of the disk. This should be done to prevent the virus from reappearing by unformatting the disk.

Creating a Virus String File

The External Virus Data file should be created with an editor or a word processor and saved as an ASCII text file. Be sure each line end with a CR/LF pair.

NOTE: This option is intended for emergency and research use only. It is a temporary method for identifying new viruses prior to the subsequent release of SCAN. A sound understanding of viruses and string-search techniques is advised as a prerequisite for using this option.

The virus string file uses the following format:

```
#Comment about Virus_1
"aabbccddeeff..." Virus_1_Name
#comment about Virus_2
"gghhiijjkkll..." Virus_2_Name
        .
        .
        .
"uuvvwwxxyyzz..." Virus_n_Name
```

where aa, bb, cc, etc. are the hexadecimal bytes that you wish to scan for. Each line in the file represents one virus. The Virus Name for each virus is mandatory, and may be up to 25 characters in length. The double quotes (") are required at the beginning and end of each hexadecimal string.

SCAN will use the string file to search memory, the Partition Table, Boot Sector, System files, all .COM and .EXE file, and Overlay files with the
extension .BIN, .OV?, .PGM, .PIF, .PRG, .SYS and .XTP

Virus strings may contain wild cards. The two wildcard options are:

FIXED POSITION WILDCARD

The question mark "?" may be used to represent a wildcard in a fixed position within the string. For example, the string:

"E9 7C 00 10 ? 37 CB"

would match "E9 7C 00 10 27 37 CB", "E9 7C 00 10 9C 37 CB", or any other similar string, no matter what byte was in the fifth place.

RANGE WILDCARD

The asterisk "*", followed by range number in parentheses "(" and ")" is used to represent a variable number of adjoining random bytes. For example, the string:

"E9 7C *(4) 37 CB"

would match "E9 7C 00 37 CB", "E9 7C 00 11 37 CB", and "E9 7C 00 11 22 37 CB". The string "E9 7C 00 11 22 33 44 37 CB" would not match since the distance between 7C and 37 is greater than four bytes. You may specify a range of up to 99 bytes. Up to 10 different wildcards of either kind may be used in one virus string.

COMMENTS

A pound sign "$" at the beginning of a line will denote that it is a comment. Use this for adding notes to the external virus data file. For example:

```
#New .COM virus found in file FRITZ.EXE from
#Schneiderland on 01-22-91
"53 48 45 50" Fritz-1 [F-1]
```

could be used to store a description of the virus, name of the original infected file, where and when it was received, and so forth.