Index to Help with VIRUSCAN for Windows

This index lists all of the help topics available for the Windows version of VIRUSCAN. 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 program 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 on 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 256Kb 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 is 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 all further versions of SCAN.

The validation results for SCAN.EXE, Version 84 should be:

```
        FILE NAME : SCAN.EXE
             SIZE : 51,870
             DATE : 10-7-91
    FILE AUTHENTICATION
        CHECK METHOD 1 : 9008
        CHECK METHOD 2 : 03A7
```

The validation results for WSCAN.EXE, Version 84B should be:

```
        FILE NAME : WSCAN.EXE
             SIZE : 49,577
             DATE : 10-11-1991
    FILE AUTHENTICATION
        CHECK METHOD 1 : 31F3
        CHECK METHOD 2 : 14A1
```

If your copy of SCAN.EXE or WSCAN.EXE differs, they may have been modified, Always obtain you 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.

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 your .ZIP file has been tampered with.

Additions to VIRUSCAN

Version 83 of VIRUSCAN was skipped due to a trojan version that appeared last January.

Version 84 of SCAN is being released early due to the appearance of an entirely new type of virus, called the DIR2 or FAT virus that was recently discovered. This virus does not attach directly to programs, but instead modifies directory entries for executable files so that the cluster pointers point to the virus instead of the executable files. The virus in turn loads and executes the programs. This means that if the virus is resident on an infected system, then any executable file copies or backups will transfer the virus. If the virus is not memory resident, then the executable files cannot be copied or backed up. Only the virus will be copied. There is no current technique, short of a re-format, that can remove this virus. CLEAN-UP is therefore also being modified to deal with this virus and will be released simultaneously with this version of SCAN.

One new option, Check Memory from 0Kb to 1088Kb, has been added. This will check memory beyond the standard 640Kb limit.

49 new viruses were added. Viruses that were reported at multiple sites include: 748 reported in California and Texas, the Dec 28 from Zargoza University in Spain, Miky from Bolivia and Florida, Mosquito, the Sunday-2 from Canada, R-11, and Tokyo. Other viruses added in this release include the #1, 789, 1014, 1661, 1840, 2480, BackTime, Boys, Burghofer, CADKill, CD, Cinderella, Damage, Demon, Dropper, Europe-'92, ETC, Gotcha, Hero, Hitchcock, Jerk, Klaeren, M128, mini-45, Manta, Mule, NewCom, Nobock, Possessed, QP3, R10, R11, Scud, Spanish, Spanz, Topo, Tuesday, Twin-351, V125, V-483, V812, and Zabaras viruses.

For a listing of the viruses that were added, please refer to the "Virus Characteristics Listing" option under the Help Menu. For a more complete description, please refer to Patricia Hoffman's VSUM listing.

Detailed Description of VIRUSCAN

VIRUSCAN scans 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 Files" 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 84 identifies all 297 known computer viruses along with their variants. Some viruses have been modified so that more than one "strain" exists. Counting such modifications, there are 893 virus variants. The twenty most common viruses which account for over 98% of all reported PC infections are also identified by SCAN. The Virus Characteristics List menu item under the Help Menu lists and describes all new, public domain, and extinct computer viruses identified by SCAN. The number of variants of each virus is listed in parentheses after the virus name.

All known 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 existing viruses.

VIRUSCAN will also check files for unknown viruses with the "Add Validation Codes" and "Check Validation Code" 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. SCAN uses two independently generated CRC (Cyclic Redundancy Check) checks that are added to the end of program files to do this. Files which are self-checking should not be validated since this will "set off" the program's self-check. Files which are self-modifying may have different values for the same program depending upon the modifications. 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 viruses, SCAN checks the boot sector for signs of viral code. If suspicious code if sound, SCAN will report that it has found a Suspicious Boot Sector 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 or French.

VIRUSCAN works on stand-alone and networked PC's, but not on a file server. For networks, the NETSCAN server drive scanning program must be used.

Differences Between the DOS and Windows Versions of VIRUSCAN

The DOS and Windows versions 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 instance, 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 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".

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.

NOTE: In order for VIRUSCAN Windows to work properly, all of the files, SCAN.EXE, WSCAN.EXE, SCAN.ICO, SCANHLP.HLP, VIRLIST.TXT, should reside in the same directory, with SCAN.PIF residing in the Windows directory. That is the purpose of the install program.

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.   This 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

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, and to look up important keywords to help the user pinpoint the item in question.

"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.

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 implantations 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 Path(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 alway be kept in the data file 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, entitled "Begin Scan", starts the original 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 following is a list of Scan Switches:

Add Validation Codes
Check Memory From 0Kb to 1088Kb
Check Validation Codes
Create Report of Infected Files...
Disable Ctrl-C/Ctrl-Brk During Scan
Disable Screen Pause
Display Messages in French
Overwrite and Delete Infected Files
Remove Validation Codes
Scan All Files, Including Data Files
Scan Memory for All Viruses
Scan Multiple Floppies
Scan Overlay Extensions...
Scan Subdirectories
Scan Using External Virus Info File...
Skip Internal Scan of LZEXE Files
Skip Memory Checking
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.

Add Validation Codes

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.

NOTE: This switch cannot be turned on if the "Remove Validation Codes" switch is on.

Check Validation Codes

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

If you have installed new software on your system, and are running the "Check Validation Codes" option, you will need to install validation codes to the new files with the "Add Validation Codes" switch of VIRUSCAN for Windows. Additionally, the SCANVAL.VAL hidden file containing validation codes for the partition table, boot sector, COMMAND.COM, and system files will have to be replaced. The MS-DOS 5.00 contains self-modifying code and can not have a validation code added to it. The quickest way to update the validation codes is to remove all validation codes from the hard disk and then add them back on by running VIRUSCAN for Windows with the "Remove Validation codes" switch on, and then with the "Add Validation Codes" switch. Then remove the validation code from SETVER.EXE by running VIRUSCAN again with the "Remove Validation Codes" switch, and choose the "Scan Paths..." menu item from the "Scan Options" menu. When you are prompted for the path, type "C:\DOS\SETVER.EXE" without the quotes.

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 "Remove Validation Codes" switch.

Remove Validation Codes

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 turned on if the "Add Validation Codes" or "Check Validation Codes" switches are on.

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 "Scan All Files" switch.

Skip Internal Scan of LZEXE 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.

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:

1554, 1971, 1253, 2100, 3445-Stealth, 4096,
512, Anthrax, Brain, Dark Avenger, Disk Killer,
Doom-2, EDV, Fish6, Form, Invader, Joshi,
Microbes, Mirror, Murphy, Nomenclature,
Phantom, Plastique, Polish-2, P1R(Phoenix),
Taiwan-3, Whale, Zero-Hunt

If one of these viruses 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 its virus search string 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 the 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.

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

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.

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.

Display Messages in French

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

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

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.

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 open then up. If you have never used this option before, it will default to the drive and directory that Windows resides in. 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 clicks the mouse pointer on the "OK" and the 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 windows 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. To close this windows, either double click on 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 in 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 $25.00 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 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 in 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.

Note: the 900 number previously used for registration has been discontinued.

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
4423 Cheeney Street
Santa Clara, CA 95054-0253
U.S.A.

(408)988-3832 office
(408)970-9727 fax
(408)988-4004 BBS 2400 bps
(408)988-5190 BBS v32 9600
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] and partition table or boot sector infecting viruses, as improper removal of these viruses could result in the loss of all data and 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.

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 ends 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 files, 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 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.