Table of Contents

Table of Contents

If You Suspect a Virus Infection

If your computer is infected with a virus — DON'T PANIC! Sometimes a badly thought out attempt to remove a virus will do much more damage than the virus could have done. Follow the instructions found in the next section “Curing a Virus Infection”. If you are not sure what to do, leave your computer turned off until you find someone to remove the virus for you.

Finally, remember that some viruses may interfere with the disinfection operation if they are active in memory at that time. Therefore, before attempting to disinfect you MUST boot the computer from a CLEAN, write-protected DOS diskette.

Curing a Virus Infection

1 If you are currently working in a program, save your work, and exit the program.

2 Turn off the computer for at least 10 seconds.

3 Find your original bootable DOS disk and make sure it is write protected.

Write-Protecting Disks
5¼" disks : Put a write protect label over the notch on the right side of the disk.
3½" disks : The notch on the right side of the disk must be open for the disk to be write protected.

4 Insert the write-protected DOS disk into the A: drive and turn the computer on.

5 After the computer has booted, insert a write-protected copy of VirusNet into drive A: (If using drive b: substitute B: for A: in the examples below.)

6 To find and remove viruses, run CLEANHD from the floppy drive DOS prompt.

7 If a virus is found when the memory check is done, your bootable DOS disk is also infected. Find another write-protected bootable DOS disk, insert it into drive A:, and reboot the computer. Follow from Step 4 above until no virus is found by the memory virus check.

8 Any viruses found will be automatically removed. Infected program files which cannot be recovered will be deleted. When scanning is complete, the virus scanner findings will be displayed on screen.

9 After the computer has booted from the hard disk, insert the write-protected VirusNet disk into the floppy drive and run CLEANHD from the floppy disk.

10 If you receive a message that memory is infected, repeat the virus removal procedure from Step 2. When the scanner does not report a virus in Step 9, your virus problem has been corrected and you may safely use your computer.

If VirusNet has been installed on the hard disk, you may run CLEANHD from the hard disk to start the scanner. However, if a virus is already in memory, the scanner may become infected when it is run, possibly preventing it from running properly. For this reason, it is recommended that the scanner be run from a write-protected floppy disk.

CLEANHD is a batch program that contains the following switch \VN /HARD /DISINF. For a list of all the command-line switches run VN from the \VN directory.

Virus Overview

What is a Computer Virus?

The best definition we have been able to come up with is the following:

1 A virus is a program that is able to replicate, that is create (possibly modified) copies of itself.

2 The replication is intentional, not just a side-effect.

3 At least some of replicants in turn are also viruses by the same definition.

4 A virus has to attach itself to a "host", in the sense that execution of the host implies execution of the virus.

#1 distinguishes viruses from non-replicating malware, such as Trojans, ANSI bombs and logic bombs.

#2 distinguishes between viruses and programs such as DISKCOPY.COM that can replicate.

#3 is needed to exclude certain "intended viruses", that attempt to replicate, but fail - they simply do not qualify as "real" viruses.

#4 is necessary to distinguish between viruses and worms, which do not require a host.

A Trojan is a program that pretends to do something useful (or at least interesting), but when it is run, it may have some harmful effect, like scrambling your FAT (File Allocation Table) or formatting the hard disk.

Viruses and Trojans may contain a "time-bomb", intended to destroy programs or data on a specific date or when some condition has been fulfilled.

A time bomb is often designed to be harmful, maybe doing something like formatting the hard disk. Sometimes it is relatively harmless, perhaps slowing the computer down every Friday or making a ball bounce around the screen. However, there is really no such thing as a harmless virus. Even if a virus has been intended to cause no damage, it may do so in certain cases, often due to the incompetence of the virus writer or unexpected hardware
or software revisions.

A virus may be modified, either by the original author or someone else, so that a more harmful version of it appears. It is also possible that the modification produces a less harmful virus, but that has only rarely happened.

The damage caused by a virus may consist of the deletion of data or programs, maybe even reformatting of the hard disk, but more subtle damage is also possible. Some viruses may modify data or introduce typing errors into text. Other viruses may have no intentional effects other than just replicating.

The major groups of viruses on PCs are boot sector viruses (BSV), program viruses and application viruses.

Boot Sector Viruses

A BSV infects boot sectors on diskettes and/or hard disks. On diskettes, the boot sector normally contains code to load the operating system files. The BSV replaces the original boot sector with itself and stores the original boot sector somewhere else on the diskette or simply replaces it totally. When a computer is then later booted from this diskette, the

virus takes control and hides in RAM. It will then load and execute the original boot sector, and from then on everything will be as usual. Except, of course, that every diskette inserted in the computer will be infected with the virus, unless it is write-protected.

A BSV will usually hide at the top of memory, reducing the amount of memory that the DOS sees. For example, a computer with 640K might appear to have only 639K.

Most BSVs are also able to infect hard disks, where the process is similar to that described above, although they usually infect the master boot record instead of the DOS boot record.

Program Viruses

Program viruses, the second type of computer viruses, infect executable programs, usually .COM and .EXE files, but sometimes also overlay files, device drivers or even object files.

An infected program will contain a copy of the virus, usually at the end, in some cases at the beginning of the original program, and in a few cases the virus is inserted in the middle of the original program.

When an infected program is run, the virus may stay resident in memory and infect every program run. Viruses using this method to spread the infection are called "Resident Viruses".

Other viruses may search for a new file to infect, when an infected program is executed. The virus then transfers control to the original program. Viruses using this method to spread the infection are called "Direct Action Viruses". It is possible for a virus to use both methods of infection.

Most viruses try to recognize existing infections, so they do not infect what has already been infected. This makes it possible to inoculate against specific viruses, by making the "victim" appear to be infected. However, this method is useless as a general defense, as it is not possible to inoculate the same program against multiple viruses.

Application Viruses

The third type of viruses are application viruses, which do not infect normal programs, but instead spread as "macros" in various types of files, typically word-processor documents or spreadsheets.

In general, viruses are just program - rather unusual programs perhaps, but written just like any other program. It does not take a genius to write one - any average assembly language programmer can easily do it. Fortunately, few of them do.

Virus Myths
Virus Tips

Virus Myths

Now — to correct some common misconceptions, here are a few bits of information about what viruses cannot do:

1. A virus cannot appear all by itself. It has to be written, just like any other program.
2. Not all viruses are intentionally harmful - some may only cause minor damage as a side effect - however, there is no such thing as a "harmless" virus.
3. Reading data from an infected diskette cannot cause an infection.
4. A write-protected diskette cannot become infected, if the hardware is working properly.

It used to be the case that a virus could not infect a computer unless it was booted from an infected diskette or an infected program was run on it, but alas, this is no longer true. It is possible for a virus infection to spread, just by the act of reading an infected Microsoft Word document, for example, or through use of Lotus Notes, to name two well-known applications.

It also used to be the case that a virus could not infect data files or spread from one type of computer to another - a virus designed to infect Macintosh computers could not infect PCs or vice versa, but with the appearance of application viruses this has changed as well - there are now a few viruses that can infect WinWord as well as MacWord.

Virus Overview
Virus Tips

Virus Tips

VirusNet provides protection against viruses, but there are other methods that also should be used. Before listing them, please be advised of three methods that are of very limited use.

Don't Bother With These

1 One anti-virus measure consists of making every executable file read-only, by issuing commands like:

ATTRIB +R *.EXE

This is actually not a bad idea, but it will not provide much protection against viruses. Most program viruses will remove this protection before they infect files, and restore it afterwards. Making files read-only will of course have no effect on BSVs. The main purpose of this method is actually to protect the user from his own mistakes, because this makes it harder to delete programs by mistake. However, some viruses are stopped by this method, “Lehigh” and “South African” in particular.

2 Another method is to hide the COMMAND.COM file, by giving the following sequence of instructions:

```
MKDIR C:\HIDDEN
COPY COMMAND.COM C:\HIDDEN
DEL COMMAND.COM

CONFIG.SYS:
SHELL=C:\HIDDEN\COMMAND.COM /P

AUTOEXEC.BAT:
SET COMSPEC=C:\HIDDEN\COMMAND.COM
```

This method is quite useless, to say the least. Few viruses infect COMMAND.COM, and some of them are able to do it even if it has been hidden using this method.

3 A third useless method is to change the name of COMMAND.COM and patch other programs so they use the new name. Somebody who had only heard of the “Lehigh” virus got this “bright” idea. Apparently he thought that all other viruses operated like it, so he wrote and distributed a program to do this automatically. He thought it was a general cure for the virus problem, but he was wrong.

Better Ways To Protect Yourself

On the other hand, there are a number of ways to provide useful protection.

1 Rule #1 is: MAKE BACKUPS!!! Keep good backups (more than one) of everything you do not want to lose. This will not only protect you from serious damage caused by viruses, but is also necessary in the case of a serious hardware failure.

2 Unless removing a virus, never boot a computer with a hard disk from a diskette because that is the only way the hard disk could become infected with a BSV. (well, strictly speaking, it can happen if you run a "dropper" program too, but that happens extremely rarely).

If your BIOS allows you to change the boot sequence to "C: A:", do it. This will give you very good protection against boot sector virus infections.

Should you, by accident, have left a non-bootable diskette in drive A: when you turn the computer on, the message "Not a system disk" may appear. If the diskette was infected with a virus, it will now be active, but may not have infected the hard disk yet. if this happens, turn the

computer off, or press the reset button. It is important to note that pressing Ctrl-Alt-Del will not be sufficient, as a few viruses can survive that.

3 If the computer has no hard disk, but is booted from a diskette, you should always use the same diskette, and keep it write-protected.

4 Keep all diskettes write-protected unless you need to write to them. When you obtain new software on a diskette, write-protect the diskette before you make a backup copy of it.

5 Be very careful regarding your sources of software. In general, shrink-wrapped commercial software should be “clean”, but there have been a few documented cases of infected commercial software. Public-Domain, Freeware and Shareware packages do not have to be any more dangerous — it all depends on the source. If you obtain software from a BBS, check what precautions the SysOp takes against viruses. If he does not screen the software made available for downloading, you should find another source.

6 Check all new software for infection before you run them for the first time.

7 Obtain Shareware, Freeware and Public-Domain software from the original author, if at all possible.

8 Look out for any “unusual” behavior on your computer, like:

Does it take longer than usually to load programs?
Do unusual error messages appear?
Does the memory size seem to have decreased?
Do the disk lights stay on longer than they used to?
Do files just disappear?

Anything like this might indicate a virus infection.

Virus Overview
Virus Myths

Table of Contents

Express Scan

Express Scan is a great way to scan for viruses manually. You can specify what hard drive(s), directories or files to scan simply by highlighting it and clicking on the corresponding scan button.

There are two views associated with the Express Scan. The Scan By Drive view and the Scan By Directory view. The Scan By Drive view is sutable for most cases, however if you only want to scan a specific directory or file, you must switch to the Scan By Directroy view by clicking on the Switch View button.

Scan by Drive

To scan a specific drive, simply highlight the appropriate drive letter and click on the Scan Drive button. You may select multiple drives by holding down the Ctrl key and clicking on the drives that you want scanned. You may easily select a group of drives, by checking the appropriate box under Scan Multiple Drives. When all the drives that you want scanned are highlighted click on the Scan Drive button to begin the scan.

Scan by Directory

This view enables you to scan only a directory or file. To scan by drive letter click on the Switch View button again to return to the Scan By Drive View.

Highlight the directory that you want scanned if you want all the sub-directories under the highlighted directory scanned check the Scan all sub-directroies check box. Click on the Scan Directory button to begin the scan.

To scan only a file, double click on the directory that the file is in to bring up a file list on the right. Highlight the specific file and click on the Scan File button to begin the scan on that file only.

If an Infection is Found

If VirusNet found a virus infection a window will come up prompting you to eiter Disinfect, Delete, Rename, or Ignore the infected fie.

Disinfect

If the Disinfect option is chosen VirusNet will automatically remove the virus if it can't remove the virus it will be deleted.

Delete

If you choose to delete the file VirusNet will not attempt to remove the virus instead it will just delete the file and you will loose the information contained in the infected file.

Rename

If the Rename option is selected the infected file will be renamed with a V as teh first letter of the file extension.
Example,
If COMMAND.COM is infected it will be renamed to COMMAND.VOM

Ignore

This will simply ignore the infected file completely.

Scanner Results

Scanner Results

The VirusNet scanner results are displayed by clicking on the details button when the scan finishes.

From the result screen you can print out the information or save it to a file for future reference.

Spectrum Scan

Using the Spectrum Scanner

The Spectrum Scan feature of VirusNet enables you to run VirusNet automatically without any user interaction until a virus is found. It gives you the freedom to decide what VirusNet scans for, what drives to scan and when to start the scanner. If a virus is found the Spectrum Scanner will prompt you with the option to disinfect, delete, rename or ignore the infected file.

To get started with the Spectrum Scanner immediately, just follow these simple steps:

1 Select the Spectrum Scanner option from the VirusNet desktop.

2 Decide what to scan (Program Files, All Files, Memory Only) and whether or not you wish to have the boot sector scanned

3 Select the drive(s) you what VirusNet to scan from the list shown.

4 Tell VirusNet when to run. You may have it run on Windows startup or in a specified amount of time from the last scan, or after a period of system inactivity.

5 When you have defined all the options according to your specific need you can click on the Scan Now button to scan the system immediately.

6 The final step is to clicl on the OK button. This will activate all of your settings and will scan the system according to your selections.

What to Scan

The Spectrum Scanner gives you the option to scan program files, all files or to scan only memory. Memory will be scanned once before any files are scanned.

What Drives to Scan

You should normally configure the Spectrum Scanner to scan all workstation hard drives. Only the system administrator should scan all network hard drives because the user will only be able to scan the directories and files that they have rights to.

When to Run

You can configure the Spectrum Scanner to run on Windows startup, After a specified period of inactivity, or during a specified time interval.

If a Virus is Found

A message box will appear if a virus is found on your system. You will then be prompted to decide what VirusNet should do. You have the following options...

- Disinfect - this is the option that should be used in most cases. If the file can not be disinfected VirusNet will delete it.
- Delete - deletes the infected file by overwriting them and then deleting them their entry from the directory.
- Rename - will rename the infected file by replacing the first letter of the extension with a “V.” COMMAND.COM changes COMMAND.VOM if infected with a virus.
- Ignore - ignores the infected file and leaves it active on the machine.

If multiple viruses were found on your machine the scanner will prompt you for every infected file with the same options listed above.

Scan Settings

The Scan Settings option allows you to specify the type of scan that takes place when the scanner is run. It also allows you to define what the scanner scans by giving you the options to scan Standard Files or All Files, you can also have it scan the boot sector of the disk in the process.

Scan Type

VirusNet offers three different types of scanning protection. Select the type of scan you wish to perform by selecting the check-box next to the appropriate scan type.

Secure

The Secure scan detects known viruses and many variants through a combination of signatures and algorithms. It is capable of detecting stealth and polymorphic viruses. If you have a virus infection, Secure scan is the only option which allows you to remove infected files. This is the option you should use most of the time. If you suspect that you have a virus that Secure scan does not detect, try the Heuristic or Checksum options described below.

Heuristic

Through powerful rules-based-algorithms, Heuristic scanning can detect known and unknown viruses based on characteristics. Heuristic scanning first checks for viruses with the Secure scan algorithm described above. If a file or boot track does not appear to be infected, a heuristic analysis is performed to see if there is anything virus-like or dangerous about the file/boot track.

Checksum

Checksum scanning looks for changes in programs. The first time a program is scanned, a CRC (cyclical redundancy check) signature is created of that file. On subsequent scans, if the file has changed, the checksum scanner will notify of the change. Checksum scanning is a powerful tool in detecting unknown viruses. However, a file that changes does not always indicate that there is a virus. Some files modify themselves with configuration information. If a checksum scan detects a changed file, it is recommended that you run the Heuristic or Secure scan to determine if the file is infected.

Scan Location

The Scan Location window allows you to select the type of files that the Secure or Heuristic scanner looks for. You can choose between Standard and All files.

Standard files are any files that contain code that the computer runs. Examples include files that have extensions of EXE, COM, OVL, SYS, CMD and BIN.

All files should only be selected if a virus infection has already been detected. With this option selected, all program and data files will be scanned. This option can lengthen the time of the scan considerably and is not recommended for normal use.

Boot Sectors allows you to determine if the scanner looks at the DOS and Master Boot Sectors as part of its scan. This option should normally be selected, since many of the most common viruses are boot sector viruses. If the scanner does not read your boot sectors properly, you can disable this option. Boot sectors may not be read properly if you are running security software or DOS emulation under another operating system.

Other Options

There are several other options that are available to you from this screen that are explained in the following few paragraphs.

Allow Scanning of network drives

This option allows you to define whether or not the network drives are displayed in the Express Scan drive window.

Audiable alert if virus found

This will cause a warning tone to be emitted from the PC's speaker if a virus is found

Rescue Data Full Pathname

Allows you to save information used to recover a PC on a floppy disk, network drive, or hard drive. Type in the location and file name you wish to use to store the Rescue Disk information. For example, type A:\RESCUE.VN to store rescue information to the root directory of a floppy drive.

Important! Do not store the rescue file permanently on a hard disk, since the file will not be accessible if the hard drive becomes corrupted.

CRC Scanner Data File

CRC Scanner Data File is the name of the file where Checksum Scanner information is stored. Each drive has a file of this name stored in its root directory. Since viruses have been known to delete checksum files that use a fixed name, you may wish to use a different name than the one that is supplied with VirusNet.

Display

This button opens up a VirusNet Display Settings Window that lets you change the appearence of the desktop to make it look the best on your monitor. You can change the Highlight Color, Highlight Style, Hightlight Pattern and Highlight Draw Mode. Each of these options will have a different effect dependent on the type of video card and monitor that your system uses.

If you experience difficulty with the highlighting on the desktop uncheck the check-box next to Display object highlighting. This will make the title of each object appear in bold.

Rescue Disk

The Rescue Disk stores vital parts of a PCs hard disk and CMOS. This information can be used to regain access to a PC that fails to boot properly. Reasons that a PC may fail to boot include a virus, dead CMOS battery and corrupted boot areas.

The Rescue Disk file can store information for many PCs in a central database, making it ideal for storing critical information for all PCs in a department. Once the file has been created, it should be kept in a safe place, preferably on a write-protected diskette. The rescue file can also be stored to a network drive. If it is stored on a LAN and a workstation fails to boot, the rescue file will have to be copied to a floppy disk and accessed from that PCs floppy drive, or the PC must be logged into the network by loading the necessary files from diskette. The location and name of the Rescue Disk file can be set in the Scan Settings section.

Create Button

Select the Create button to create and save rescue information for a PC. You will then be asked to provide a description of up to 30 characters to uniquely identify the PC. After you provide a unique identifier for the PC, the Master Boot Track, DOS Boot Track and CMOS will be saved. To help in identification of the computer for future recovery, the PC CPU type and BIOS date, along with current date and time, will also be saved.

If you change a computer's hard disk, delete its entry from the Rescue Database and create a new entry. This will prevent any loss of data should the previous hard disk values be restored to the new hard disk.

Recover Button

Select this feature to restore the highlighted PCs rescue information to the PC you are working on. This option should only be used if the PC cannot be booted or accessed because of a disk or CMOS battery failure.

Before selecting Recover, make sure that the correct PC is highlighted from the list. When Recover is selected, the saved information for the currently highlighted PC will be used. To add a margin of safety to the recovery process, the CPU type and BIOS date of the original PC is compared to that of the current PC. If they do not match, you will receive strong warning messages indicating that the recovery information selected may not be for this computer.

NOTE! The only time you should ignore this warning message is if you have upgraded the CPU or BIOS since the recovery information was first saved. Do not proceed if you are not certain that the saved information is from this computer. Disastrous results can occur if the recovery information is from a different computer.

Please refer to the "Restore Rescue Information Window" in this section.

Delete Button

Select this choice to remove the rescue information for a particular PC. If this PC fails to boot in the future, you will not be able to use the rescue feature until a new rescue record is created.

View Button

It is quite interesting and informative to view a PC's CMOS and boot track information. Highlight a PC and select this button, or simply press Enter when the cursor is on a highlighted PC. Information presented in the Rescue Viewer is beyond the scope of this documentation. You may wish to refer

to a PC technical manual for more information on hard disks and CMOS.

Restore Rescue Information Window

Restore Rescue Information Window

After the recovery button is selected, you have the option of restoring any combination of rescue information.

The first panel shows the name of the workstation. The second panel displays the results of the safety check. The first line indicates if the CPU type of the original rescue PC matches the current PC, and the second line indicates if the two BIOS dates match.

If either the CPU or BIOS dates does not match, you should be certain that the reason was a replacement BIOS or CPU upgrade. Otherwise, do not continue with the restore procedure. Also, if you change your hard disk, do not restore the previous disks Partition Table and DOS Boot Sector. This can result in loss of data.

Select which information you wish to restore by placing a check mark in the box in front of that item. When you are satisfied with your selection, select the Restore button. In less than a second, the recovery information will be restored. To have the new information take effect, you must reboot the computer. Shut down Windows, if it is currently running, before rebooting.

Virus Information

This feature provides a comprehensive and complete list of all the viruses that VirusNet detects. It also tells whether or not the virus can be removed and if it is a boot sector virus or not.

Virus Name

Lists the name of the virus based on the CARO naming standard.

Removable?

If the virus can be removed "Yes" will be written in the colum under Removable? if it can not be removed due to complete destruction of the file or Boot Sector then "Impossible" will be displayed, if it can not be removed by the VirusNet scanner then "No" will be displayed.

Boot Sector Virus?

If the virus is a boot sector virus "Boot" will be written in the colum under Boot Sector Virus? if is not a boot sector virus then nothing will be written in the colum.

Display Section

This combo box allows you to simply look up the virus alphanumerically and also enables you to quickly view the statistics of the VirusNet scanner.

Options

Scan Settings

This will bring you to the Scan Settings window, for more help on this feature go to the Scan Settings section.

Virus Information

This will open the Virus Informaiton window, for more help on this feature go to the Virus Information section

Update Scanner

This will bring up a VirusNet Scanner Update window that informs you of when your last update was done, when the next update should be done and when your license for updates expires.

You can optain a VirusNet scanner update from the Internet, CompuServe or our BBS by accessing the sites listed under Updates and Technical Support link below.

After you have obtained a VirusNet scanner update click on the DO Update button and the scanner will automatically be updated.

When your license for updates expires you must contact Safetynet, or Just SoftWorks for a new subscription.

Scan Settings
Virus Infomation
Updates and Technical Support

Updates and Technical Support

Since new viruses are being developed every day, it is important to keep your copy of VirusNet up to date. New updates to VirusNet are created every four to six weeks. More frequent updates are sometimes created if there is a special threat. Updates can be applied for free during your license period and are available electronically from one of the sites listed below.

To Update VirusNet, follow these steps:

1 Connect to one of the electronic sites listed below.
2 Download the update file VNUPDATE.EXE.
3 Copy VNUPDATE.EXE to the VirusNet directory (usually C:\VNWIN).
4 From the VirusNet Windows scanner, select the Options menu and then the Update Scanner menu choice.
5 Follow the on-screen prompts.

WWW

http://www.safe.net - VirusNet updates, security software

FTP

ftp://ftp.safe.net/pub/safetynet - ftp to ftp.safe.net and go to the /pub/safetynet directory

CompuServe

go cis:safe and enter the Safetynet section

BBS

201-467-1581 (28800,n,8,1)

E-Mail Support

support@safe.net

Mailing Address

Safetynet Technical Support
140 Mountain Ave.
Springfield, NJ 07081
United States of America

Phone Numbers

201-467-0465 (Support)
201-467-1611 (Fax)

Quit

When the you exit out of VirusNet you have the option of saving the changes that were made, this includes everything from the type of scan to the display settings.

To save the changes make sure the check box next to Save changes is checked to disgaurd the changes make sure that the box is not marked.

Table of Contents

DOS Version

To load the DOS version of VirusNet run VNDOS from the /VN directory at a DOS prompt. For guidence on how to use VirusNet for DOS open the help file associated with it.

Command Line Operation

Secure and Heuristic scans can be run in command-line mode by running the VN.EXE program directly. When run in command-line mode, the scanner will display its results and exit to DOS with an Errorlevel code after the scan is completed. Command-line operation is ideal for use within batch files and is especially powerful when used with the VirusNet scheduling utilities.

Syntax: VN [Drive, Directory, File or Volume] [Options]

Path Specifications

Drives are specificed as the drive letter followed by a colon, for example VN C: would scan drive C. More than one drive can be listed, as long as the drives are separated by spaces.

Directories and files are specified using DOS syntax. For example, VN C:\DOS will scan the \DOS directory on drive C, while VN C:\DOS\CHKDSK.EXE will scan just the CHKDSK file in the C:\DOS directory. More than one location can be scanned by separating each entry with a space. To scan an entire drive, just specify the drive letter as in the example in the previous paragraph.

On many networks, the network drive can be scanned by providing the name of the server and volume. The syntax is usually in the form \\SERVER\VOLUME. For example, if you have a server named OCTANE and want to scan its SYS drive, type the following command:

```
VN      \\OCTANE\SYS
```

If the above method does not work in your environment, network volumes can be scanned by providing the drive letter of the volume. For example, VN F: will scan the entire drive F. If you intend to scan the entire network drive, make sure that the drive letter is mapped to the root of the drive, not to one of its sub-directories.

Command-Line Scanner Switches
Command-Line Examples
VirusNet Errorlevel Return Codes

Command Line Scanner Switches

Command-line Scanner Switches

The available command-line options are:

/ALL

Specifies that all files should be searched, not just normal “executable” files.

/ANALYZE

Performs a heuristic analysis instead of a signature-based scan.

/APPEND

Used with /REPORT. Append the report to an existing file.

/AUTO

May be specified with /DELETE or /DISINF so VirusNet will not request permission before deleting or disinfecting. If only /DELETE or /DISINF is given, it will ask if the file should be disinfected (or deleted).

/DELETE

Used only with the Secure Scan. Deletes all infected files by overwriting them and then deleting their entry from the directory.

/DISINF

Disinfect whenever possible — deletes first-generation samples and files destroyed by overwriting viruses. It will never delete a file that can be disinfected. This switch does not work with the /ANALYZE switch.

/EXT=

Specify up to ten filename extensions to scan by default. Each extension must be separated by a period.

For example: VN /HARD /EXT=COM.EXE.SY

/HARD

Scans the entire hard disk.

/LIST

Produce a report of all files checked, not just those which are infected.

/MULTI

Scan multiple diskettes.

/NET

Scans any network drives found.

/NOBOOT

Don't scan for boot sector viruses.

/NOBREAK

Disables ESC during scanning.

/NOFILE

Don't scan for file viruses. If /NOFILE is used, it implies /NOPACKED and /NOUSER as well.

When combined with the /HARD and /NOBOOT setting, the VN will just scan memory for a virus infection. This fast test can be used in a network login script to check if workstations have an active virus infection. It is recommended to run the VN.EXE scanner from a directory that has Read and Execute privileges only to prevent the VN.EXE program from becoming infected.

For example: VN /HARD /NOFILE /NOBOOT

/NOMEM

Skip the memory scan. The first time a scan is performed, memory will not be scanned for viruses. Use this option only if you are receiving memory virus errors from the scanner and you ARE ABSOLUTELY SURE that there is no memory virus.

Important! Skipping the memory scan when there are certain advanced viruses in memory can result in every program on your computer becoming infected.

/NOPACKED

Do not search inside packed files. By default, VirusNet will search inside packed executables (DIET, PKLITE, LZEXE).

/NOSUB

Scan the specified directory path only without scanning its subdirectories.

/NOWRAP

Do not wrap text in the report.

/OLD

Do not display the “This version of the program is rather old” message. It is not recommended that this switch be used since updates designed to fight new viruses are being worked on constantly.

/ONLY

When used with /ANALYZE, it will make VN.EXE perform ONLY a heuristic scan.

/PAGE

Used to pause screen output.

/REPORT=filename

Sends the output to a file in addition to displaying it on the screen.

/SILENT

Generates no screen output at all - useful if you want to run the program from a batch file, and only check the return code.

Command-Line Operation
Command-Line Examples
VirusNet Errorlevel Return Codes

Command Line Examples

VN C:

Scan the boot track and files on drive C: along with memory. Its progress will be displayed on the screen, including identifying any viruses by name, but no viruses will be removed.

VN C: /PAGE

Same as above except the screen report will pause when every full page is displayed.

VN C: /REPORT=VIRUS.RPT

As above, but findings will be sent to the screen and to a VIRUS.RPT file created in the current directory.

VN C: /REPORT=VIRUS.RPT /APPEND

As above, but any existing VIRUS.RPT file will be appended with the new scan information.

VN C: /DELETE

Scans drive C:, the boot track and memory. If a virus is found, you will be asked if you want to delete the infected file.

VN C: /AUTO /DELETE

As above, except automatically deletes (by overwriting and then deleting) files that are infected. You may wish to combine this option with /REPORT to have a permanent copy of the scanner result.

VN /HARD

Scans all hard drives, boot tracks, and memory for viruses. Will issue a screen report but will not disinfect any infected files.

VN /HARD /AUTO /DISINF /REPORT=VIRUS.RPT

As above, but will automatically disinfect any infected files, delete those that it cannot disinfect, and issue a report to a VIRUS.RPT file.

VirusNet Errorlevel Return Codes

The VN.EXE scanner uses the following exit codes, which can be checked with the ERRORLEVEL command from a batch file.

0 Normal exit - nothing found

1 Abnormal termination - unrecoverable error. This can mean any of the following:
DOS version 1.x was used (VirusNet requires DOS 2.0 or higher)
The report file (specified with /REPORT=) could not be created. ENGLISH.TX0 or SIGN.DEF corrupted or not present.
The VN.EXE program was run from a diskette, and the diskette then changed.

2 Selftest failed - program has been modified.

3 A Boot/File virus infection found.

4 Virus search string found in memory.

5 Program terminated with Control-C or ESC.

6 At least one virus was removed. This code is only meaningful if the program is used to scan just a single file.

7 Insufficient memory to run the program.

8 At least one suspicious file was found, but no infections.

Command-Line Operation
Command-Line Scanner Switches
Command-Line Examples

Table of Contents

Using the Spectrum Scanner

The Spectrum Scan feature of VirusNet enables you to run VirusNet automatically without any user interaction unless a virus is found. It gives you the freedom to decide what VirusNet scans for, what drives to scan and when to scan. If a virus is found the Spectrum Scanner will prompt you with the option to disinfect, delete, rename or ignore the infected file.

To get started with the Spectrum Scan feature immediately, just follow these simple steps:

1 Select the Spectrum Scanner option from the VirusNet desktop.

2 Decide what to scan (Program Files, All Files, Memory Only) and whether or not you wish to have the boot sector scanned

3 Select the drive(s) you what VirusNet to scan from the list shown.

4 Tell VirusNet when to run. You may have it run on Windows startup or in a specified amount of time from the last scan, or after a period of system inactivity.

5 When you have defined all the options according to your specific needs you can click on the Scan Now button to scan the system immediately.

6 The final step is to click on the OK button. This will activate all of your settings and will scan the system according to your selections.

What to Scan

The Spectrum Scanner gives you the option to scan program files, all files, or to scan only memory. Memory will be scanned once before any files are scanned.

What Drives to Scan

You should normally configure the Spectrum Scanner to scan all workstation hard drives. Only the system administrator should scan all network hard drives because the user will only be able to scan the directories and files that they have rights to.

When to Run

You can configure the Spectrum Scanner to run on Windows startup, After a specified period of inactivity, or during a specified time interval.

If a Virus is Found

A message box will appear if a virus is found on your system. You will then be prompted to decide what VirusNet should do. You have the following options...

- Disinfect - this is the option that should be used in most cases. If the file can not be disinfected VirusNet will delete it.
- Delete - deletes the infected file by overwriting them and then deleting them their entry from the directory.
- Rename - will rename the infected file by replacing the first letter of the extension with a “V.” COMMAND.COM changes COMMAND.VOM if infected with a virus.
- Ignore - ignores the infected file and leaves it active on the machine.

If multiple viruses were found on your machine the scanner will prompt you for every infected file with the same options listed above.

Index

Technical Support

Updates and Technical Support

We have tried to make VirusNet as user-friendly and helpful as possible. If you run into a problem during its installation or use, please browse through the section in the manual covering that topic. You'll often find a tip or suggestion to guide you along that was learned from a previous customer. If you have found a problem or situation that is not covered in this documentation, contact our technical support department. You will quickly get in contact with a courteous, knowledgeable expert on our software.

Disclaimers

Disclaimer
Safetynet, Inc. makes no warranties as to the contents of this documentation and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Safetynet, Inc. further reserves the right to alter the specifications of the program and/or the contents of the manual without obligation to notify any person or organization of these changes.