VirusScan NT Technical Reference

Overview

✍ *This chapter contains detailed information about VirusScan NT. For a general overview of VirusScan and its most popular features, refer to Chapter 3, "Using VirusScan NT."*

The VirusScan program detects, identifies and disinfects computer viruses by checking memory as well as both the system and data areas of disks for evidence of virus infections. If VirusScan detects a virus, in most cases, it will eliminate the virus and fully restore infected programs or system areas to normal operation.

This chapter presents detailed information about using VirusScan that will be most useful to network administrators and information services staff, particularly in highly-vulnerable environments. The command line options described here offer additional power and control over virus detection and removal.

In addition, VirusScan can also assign validation and recovery codes to files and use those codes to detect and treat infection by new and unknown viruses. If NTScan has stored validation or recovery data for files, it may detect file changes and warn that infection by an unknown virus may have occurred. NTScan can also use the recovery codes to remove new or unknown viruses and restore infected files.

To obtain a list of all the viruses that VirusScan detects, run NTScan with the /VIRLIST option.

System requirements for Scan

VirusScan NT requires Windows NT. VirusScan NT works with Microsoft Network (including Windows for Workgroups) and Novell NetWare. Contact McAfee or your local authorized agent if you do not see your network listed (refer to "McAfee Support," in Chapter 1, "Introducing VirusScan NT").

VirusScan NT is designed to check for pre-existing infections of known and unknown viruses on diskettes, hard, CD-ROM and compressed (NT 3.51 Compact, SuperStor, Stacker, DoubleSpace and so on) disks on both stand-alone and networked personal computers, as well as network file servers.

✍ *To use VirusScan to clean (disinfect) virus-infected files, the CLEAN.DAT file must be present in the same subdirectory as VirusScan. If you do not have the CLEAN.DAT file, first verify whether you should contact your system administrator or information systems staff directly for virus clean-up. Otherwise, you can contact McAfee (refer to "McAfee Support," in Chapter 1, "Introducing VirusScan NT").*

Technical overview

Known virus detection

VirusScan detects known viruses by searching the system for characteristics (sequences of code) unique to each computer virus and reporting their presence if found. For viruses that encrypt or cipher their code so that every infection is different, VirusScan uses detection algorithms that work by statistical analysis, heuristics and code disassembly.

New and unknown virus detection

VirusScan can also check for new or unknown viruses by comparing files against previously recorded validation data. If a file has been modified, it will no longer match the validation data and VirusScan will report that the file may have become infected. Using NTScan with the /CLEAN option and validation options (/AF, /AV, /CF, /CV, /RF and /RV) can use the validation and recovery data to restore infected files.

Note to network users

To use VirusScan on a network drive (or directory), you must be connected to that drive and have read access to it. Some command line options described in this chapter attempt to create, change and delete files. To use these options, you must have sufficient access rights. If you have questions about access rights, contact your network administrator.

Validating VirusScan

VirusScan is supplied on a write-protected diskette that should be secure from infection. We recommend that you update your copy of VirusScan regularly. You can obtain an upgrade from several sources, as described in "Update VirusScan regularly," in Chapter 2, "Installation and Setup."

Before using a new version of VirusScan for the first time, verify that it has not been tampered with or infected by using the Validate program, as described in "Validate VirusScan," in Chapter 2, "Installation and Setup." If your new copy of NTScan differs from the validation data in the on-line documentation file, it may have been damaged. Discard it and obtain a clean copy of NTScan from a known source. Refer to "McAfee Support," in Chapter 1, "Introducing VirusScan NT."

NTScan performs an integrity test when run. This self-check allows NTScan to determine if it has been modified. If NTScan fails its integrity test, a warning message appears and NTScan refuses to run and returns to the command line prompt. You must obtain an undamaged copy before continuing. Refer to "McAfee Support," in Chapter 1, "Introducing VirusScan NT."

✍ *NTScan may report a failed integrity check if you upgrade the data files and attempt an immediate scan. After upgrading the VirusScan data files, shutdown and restart your computer before attempting a scan. For more information, refer to "Update VirusScan regularly," in Chapter 2, "Installation and Setup."*

Running NTScan

NTScan checks files and other areas of the system that can contain computer viruses. When a virus is found, NTScan identifies the virus and the system area or file where it was found. By default, NTScan examines only executable files (.EXE, .COM, .SYS, .BIN, .OVL and .DLL files). These are the files most likely to be infected with a virus. Use the /ALL option to scan all files on your system. Refer to “NTScan Option Descriptions” later in this chapter for more information about the /ALL option.

To run NTScan, launch a Windows 32-Bit Dos Command prompt to display the DOS prompt (C:\).

Use the following syntax for NTScan:

```
ntscan {drives} [options]
```

ntscan launches the application.

{drives} indicates one or more drives to be scanned. You must specify at least one drive to be scanned. If you specify a drive with just the drive letter and a colon (e.g. **ntcan c:**), all its subdirectories will be scanned. If you specify only a back-slash (e.g. **ntscan **), only the root directory of the active drive will be scanned. You can also scan a specific directory (e.g. **ntscan c:\mcafee**).

✍ *If you do not specify a drive to be scanned, NTScan will search for a virus in memory, then return the message “No target for scan was specified!”*

[options] indicates one or more of the NTScan options as listed in “NTScan Command” on page 54.

NTScan Command

List of options

The following table describes the NTScan command line options:

NTScan Command Line Options

Command	Description
/? or /HELP	Display help screen.
/ADL	Scan all local drives (including compressed, CD-ROM and PCMCIA drives, but not diskettes).
/ADN	Scan all network drives.
/AF {*filename*}	Store validation/recovery codes in *filename.*
/ALL	Scan all files, not just standard executables.
/APPEND	Append to, rather than overwrite, the file (used with /REPORT).
/AV	Add validation/recovery data to program files.
/BOOT	Scan boot sector and master boot record only.
/CF {*filename*}	Check validation/recovery codes in *filename*.
/CLEAN	Clean up infections in boot sector, master boot record and files when possible.
/CONTACTFILE {*filename*}	Display message stored in *filename* when a virus is found.
/CV	Check validation/recovery data in files.
/DEL	Overwrite and delete infected files.
/EXCLUDE {*filename*}	Exclude from scan any files listed in *filename* (with /AV).
/FAST	Speed up VirusScan's scanning; may detect fewer viruses.
/FREQUENCY {*hours*}	Set the time frequency with which to scan your system.
/HELP or /?	Display help screen.
/LOAD {*filename*}	Use Scan settings stored in *filename*.
/LOG	Save date and time VirusScan was last run in SCAN.LOG.
/MANY	Scan multiple diskettes.
/MOVE {*directory*}	Move infected files to *directory*.
/NOBEEP	Disable beeps.

NTScan Command Line Options (continued)

/NOBREAK	Disable CTRL-C / CTRL-BREAK during scans.
/NOCOMP	Skip checking compressed executables created with the LZEXE or PKLITE file compression programs.
/NOEXPIRE	Disable data files expiration data notice.
/REPORT {*filename*}	Create report of infected files found during scan in *filename*.
/RF {*filename*}	Remove validation/recovery codes in *filename*.
/RPTALL	Add list of files scanned to the report file (used with /REPORT).
/RPTCOR	Add list of corrupted files to the report file (used with /REPORT).
/RPTERR	Add list of system errors to the report file (used with /REPORT).
/RPTMOD	Add list of modified files to the report file (used with /REPORT).
/RV	Remove validation/recovery data from files.
/SHOWLOG	Display information in SCAN.LOG.
/SUB	Scan subdirectories inside a directory.
/VIRLIST	Display list of viruses detected by VirusScan.

Option details

This section describes each NTScan option in detail.

/? or /HELP

Display list of Scan options.

Does not scan. Instead, displays a list of Scan command line options with a brief description of each. No scanning is performed when these options are specified. Use either of these options alone on the command line.

/ADL

Scan all local drives (including compressed, CD-ROM and PCMCIA drives, but not diskettes).

Scans all local drives for viruses, in addition to those specified on the command line. To scan both local and network drives, use /ADL and /ADN together in the same command line.

/ADN

Scan all network drives.

Scans all network drives for viruses, in addition to those specified on the command line. To scan both local and network drives, use /ADL and /ADN together in the same command line.

/AF {*filename*}

Store validation/recovery codes in file.

Helps you detect and recover from new or unknown viruses. /AF logs validation and recovery data for executable files, the boot sector and master boot record on a hard disk or diskette, in the specified file. The log file is about 95 bytes per file validated. You must specify a *filename*, which can include the target drive and directory (such as D:\VSVALID\VALCODES.VSC). If the target path is a network drive, you must have rights to create and delete files on that drive. If *filename* exists, NTScan updates it. /AF adds about 300% more time to scanning.

To recover from a virus using the /AF information, use the /CF and /CLEAN options together in the same command line. Using any of the /AF, / CF or /RF options together in the same command line returns an error.

✍ */AF performs the same function as /AV, but stores its data in a separate file rather than changing the executable files themselves. For more information, refer to "Detecting new and unknown viruses," in Chapter 5, "Tips and Troubleshooting."*

The /AV option does not store any information about the master boot record or boot sector of the drive being scanned.

/ALL

Check all files, not just standard executable files

Increases system security by performing a more thorough scan. Otherwise, NTScan checks only standard executable files (with .COM, .EXE, .SYS, .BIN, .OVL and .DLL extensions), which are the files most likely to be infected by a virus. If /ALL is specified, NTScan checks all files on the specified drive, which increases NTScan's ability to detect viruses in overlay files but substantially increases the scanning time required. Use this option if you have found a virus or suspect one.

/APPEND

Append to the report file.

Used in conjunction with /REPORT, appends the report message text to the specified report file, if it exists. Otherwise, the /REPORT option overwrites the specified report file, if it exists.

/AV

Add validation/recovery data to files.

Helps you detect and recover from new or unknown viruses. /AV adds recovery and validation data to each standard executable file (.EXE, .COM, .SYS, .BIN, .OVL and .DLL), increasing the size of each file by 98 bytes. To update files on a shared network drive, you must have update access rights. The /AV option adds about 100% more time to scanning.

To exclude self-modifying or self-checking files that might cause false alarms, use the /EXCLUDE option. To recover from a virus using the /AV information, use the / CV and /CLEAN options together in the same command line. Using any of the /AV, /CV or /RV options together in the same command line returns an error.

✍ *The /AV option does not store any information about the master boot record or boot sector of the drive being scanned.*

/BOOT

Scan boot sector and master boot record only.

Scans the boot sector and master boot record on the specified drive(s), but not files or directories on those drives.

/CF {*filename*}

Check validation/recovery codes in file.

Helps you detect new or unknown viruses. Checks validation data stored by the /AF option in filename. If a file or system area has changed, NTScan reports that a viral infection may have occurred. The /CF option adds about 250% more time to scanning. For more information, refer to "Detecting new and unknown viruses," in Chapter 5, "Tips and Troubleshooting." You can use /CF and /CLEAN in the same command line to check validation/ recovery codes and remove any viruses found. Using any of the /AF, /CF or /RF options together in a command line returns an error.

✍ *Some older Hewlett-Packard and Zenith PCs modify the boot sector each time the system is booted. If you use /CF, NTScan continuously reports that the boot sector has been modified even though no virus may be present. Check your system's reference manual to determine whether your PC has self-modifying boot code.*

/CLEAN

Remove viruses from boot sector, master boot record and infected files.

Attempts to restore the boot sector, if infected, and any infected files. Usually, between 10% and 20% of all viruses are not removable; they damage the file they infect beyond repair. If the infected file resides on a network drive, you must have rights to modify files on that drive to clean it. If it cannot restore a file, a message is displayed that identifies the unrecoverable file. To use /CLEAN, the CLEAN.DAT file must reside in the NTScan directory. For more information, refer to "Removing viruses" on page 69.

Use /CLEAN instead of /DEL when you want to restore infected files, not just delete or overwrite them. The /CLEAN option can remove master boot record and boot sector viruses, but the /DEL option cannot. If you use /CLEAN and /DEL in the same command line, NTScan first attempts to disinfect an infected file, then deletes it only if it cannot be repaired. Similarly, if you use /CLEAN and /MOVE in the same command line, NTScan first attempts to clean an infected file, then moves it to the specified subdirectory if the file is unrecoverable.

You can use /CLEAN and /CF or /CV in the same command line to check validation/recovery codes and remove any viruses found. We strongly recommend that you get experienced help in dealing with viruses if you are unfamiliar with anti-virus software and methods. This is especially true for “critical” viruses and master boot record or boot sector infections, because improper removal of these viruses can result in the loss of all data on the infected disks.

✍ *When scanning a network drive using /CLEAN, you must have sufficient rights to update files on that drive.*

/CONTACTFILE {*filename*}

Display a text message (saved in {filename} when a virus is detected.

/CONTACTFILE identifies a file that contains the message string to display when a virus is found. This option is especially useful in network environments, because you can easily maintain the message text in a central file rather on each workstation. Any character is valid except a backslash (“\”). Messages that begin with a slash (“/”) or a hyphen (“-”) should be placed in quotation marks.

/CV

Check validation/recovery data in files.

Helps you detect new or unknown viruses. Checks validation data added by the /AV option. If a file is modified, NTScan reports that a viral infection may have occurred. The /CV option adds about 50% more time to scanning. You can use /CLEAN and /CV in the same command line to check validation/recovery codes and restore infected files. Using any of the /AV, /CV or /RV options together in the same command line returns an error.

For more information, refer to “Detecting new and unknown viruses,” in Chapter 5, “Tips and Troubleshooting.”

✍ *The /CV option does not check the system areas for changes.*

/DEL

Overwrite and delete infected files.

Deletes and overwrites each infected file. Files erased by the /DEL option cannot be recovered (you should generate a report so that you can restore them from backups). Instead of using /DEL alone, we recommend using it in combination with the /CLEAN option to attempt to disinfect an infected file first, then delete it only if the file is unrecoverable. The /CLEAN option can remove master boot record and boot sector viruses, but the /DEL option cannot.

When scanning a network drive using /DEL, you must have sufficient access rights to delete files on that drive.

This option has no effect if the Master Boot Record or Boot Sector is infected, since these are not actually files.

/EXCLUDE {*filename*}

Scan using exception list file.

Allows you to exclude files from /AF validation and /CF checking. Self-modifying or self-checking files can cause a false alarm during a scan. To create filename, refer to “Creating an exception list file for the /EXCLUDE option” on page 79.

/FAST

Speed up scanning.

Reduces scanning time by about 15%. Using the /FAST option, NTScan examines a smaller portion of each file for viruses, although it examines more files overall. Using /FAST might miss some infections found in a more comprehensive (but slower) scan. Do not use this option if you have found a virus or suspect one.

/FREQUENCY {*hours*}

Set the time frequency with which to scan your system.

In environments where the risk of viral infection is very low, use this option to prevent unnecessary or too-frequent scans. The lower the number of *hours* specified, the greater the scan frequency and the greater your protection against infection.

The first time this option is used on a workstation, NTScan creates a hidden file named MCAFEE.FRC in the root directory of drive C. In it, Scan stores the date and time that the system was scanned. Thereafter, whenever this option is used, NTScan checks this file and compares the time elapsed from the last scan with the specified number of *hours*. If *hours* does not exceed the elapsed time, NTScan exits without scanning the system. Otherwise, NTScan proceeds as usual to scan the system and, when finished, updates MCAFEE.FRC with the system date and time.

/HELP or /?

Display list of NTScan options.

Does not scan. Instead, displays a list of NTScan command line options with a brief description of each. No scanning is performed when these options are specified. Use either of these options alone on the command line.

/LOAD {*filename*}

Use NTScan settings stored in {*filename*}.

By default, NTScan loads its internal default settings plus any options specified on the command line. You can store all custom settings in a separate ASCII text file, then use /LOAD to load those settings from that file.

Use a text editor to create the file. You can put all options on the same command line or put each option (with its parameter) on its own line, separated by a hard carriage return and line feed. Use the /LOAD {filename} command line option to perform a scan using the information saved in this file. For example, if you have created a configuration file called FLOPPY.CFG:

```
ntscan /load floppy.cfg
```

The above command line will initiate a scan using its internal default settings plus any options specified in FLOPPY.CFG.

/LOG

Save date and time of last scan.

Stores the time and date NTScan is being run by updating or creating a file called SCAN.LOG in the current directory.

/MANY

Scan multiple diskettes.

Scans multiple diskettes consecutively in a single drive. NTScan will prompt you for each diskette. Once you have established a virus-free system, use this option to check multiple diskettes quickly.

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

```
a: ntscan a: /many
```

Perform the scan from a drive that is not to be removed (i.e. scan A: drive from C: drive or B: drive).

/MOVE {*directory*}

Move infected files to specified directory.

Moves all infected files found during a scan to the specified directory. If you use /MOVE in conjunction with /CLEAN, Scan attempts to restore an infected file first, then moves it to the specified directory only if the file cannot be restored. Using /MOVE and /DEL in the same command line returns an error message.

This option has no effect if the Master Boot Record or Boot Sector is infected, since these are not actually files.

/NOBEEP

Disable beeps during scans.

The PC will not issue "beeps" in the process of scans.

/NOBREAK

Disable CTRL-C / CTRL-BREAK during scans.

Users will not be able to halt scans in progress using CTRL-C or CTRL-BREAK. Use this option in conjunction with /LOG to create a meaningful audit trail of regularly scheduled scans.

/NOCOMP

Skip checking compressed executable files.

Reduces scanning time when a full scan is not needed. Otherwise, by default, NTScan checks inside executable, or self-decompressing, files that have been created using the LZEXE or PKLITE file compression programs. NTScan decompresses each file in memory and checks for virus signatures, which takes time but results in a more thorough scan. If you use /NOCOMP, NTScan does not check inside compressed files for viruses, although it can check for modifications to those files if they have been validated using validation/recovery codes.

✍ *NTScan does not check PKZIP files.*

/NOEXPIRE

Disable data files expiration date and notice.

NTScan will disable the “expiration date” message if the VirusScan data files are out of date. For information about updating VirusScan data files, refer to “Update VirusScan regularly,” in Chapter 2, “Installation and Setup.”

/REPORT {*filename*}

Create report of infected files and system errors.

Saves the output of NTScan to filename in ASCII text file format. If *filename* exists, /REPORT erases and replaces it (or, if you use /APPEND, adds the report information to the end of the existing file). You can include the destination drive and directory (such as **D:\VSREPRT\ALL.TXT**), but if the destination is a network drive, you must have rights to create and delete files on that drive. You can also use /RPTALL, /RPTCOR, /RPTMOD and /RPTERR to add scanned files, corrupted files, modified files and system errors to the report.

For more information about report files, refer to "Configuring reporting options" on page 78.

/RF {*filename*}

Remove validation/recovery codes in file.

Removes recovery and validation data from *filename* created by the /AF option. If *filename* resides on a shared network drive, you must be able to delete files on that drive. Using any of the /AF, /CF or /RF options together in the same command line returns an error.

The validation file can be deleted through DOS instead of using this option. Refer to "Updating validation codes" on page 79 for more information.

/RPTALL

Add all scanned files to Scan report.

Used with /REPORT, adds the names of all files scanned to the report file.

/RPTCOR

Add corrupted files to VirusScan report.

Used in conjunction with /REPORT, adds the names of corrupted files to the report file. A corrupted file is a file that a virus has damaged beyond repair, which typically occurs in 10% to 20% of all viral infections. You can use /RPTCOR with /RPTMOD and /RPTERR on the same command line.

✍ *There may be false readings in some files that require an overlay or another executable to run properly (i.e. a file that is not executable on its own).*

/RPTERR

Add errors to VirusScan report.

Used in conjunction with /REPORT, adds system errors to the report file. System errors include problems reading or writing to a diskette or hard disk, file system or network problems, problems creating reports and other system-related problems. You can use /RPTERR with /RPTCOR and /RPTMOD on the same command line.

/RPTMOD

Add modified files to the VirusScan report.

Used in conjunction with /REPORT, adds the names of modified files to the report file. Scan identifies modified files when the validation/recovery codes do not match (using the /CF or /CV options). You can use /RPTMOD with /RPTCOR and /RPTERR on the same command line.

/RV

Remove validation/recovery from files.

Removes validation and recovery data from files validated with the /AV option, along with the SCAN.LOG file on the specified drive. To update files on a shared network drive, you must have access rights to update them. Using any of the /AV, /CV or /RV options together in the same command line returns an error.

/SHOWLOG

Update and display the contents of SCAN.LOG.

Stores the time and date NTScan is being run by updating or creating a file called SCAN.LOG in the current directory and shows you the date and time of previous scans that have been recorded in the SCAN.LOG file using the /LOG switch. The SCAN.LOG file contains text and some special formatting. To pause when the screen fills with messages, specify the /PAUSE option.

/SUB

Scan subdirectories.

By default, when you specify a directory to scan rather than a drive, NTScan will examine only the files it contains, not its subdirectories. Use /SUB to scan all subdirectories inside any directories you have specified. Do not use /SUB if you are scanning an entire drive.

/VIRLIST

Display the contents of SCAN.DAT.

Shows you the name and a brief description of the viruses that VirusScan detects. To pause when the screen fills with messages, specify the /PAUSE option. Use /VIRLIST alone or with /PAUSE on the command line.

✍ *VirusScan can detect many viruses. This file is over 50 pages in length.*

Saving and using default settings

If you use the same NTScan command line options often, you can save your settings in a configuration file, called DEFAULT.CFG. NTScan will check for the existence of the file specified in {filename} and, if it exists, will use the settings in this file as its default.

Creating a configuration file

Use the following procedure to create a configuration file:

1. Using a word processor or text editor such as Windows Write, create a new file.

2. Put all options on the same command line or put each option (with its parameter) on its own line, separated by a hard carriage return and line feed, as shown in the following examples.

   Sample configuration file with all options on the same command line:
   `c:\user /sub /report d:\virus.rpt /rpterr /append`

   Sample configuration file with each option on a separate command line:

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

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

3. Save the file as “DEFAULT.CFG” in the same directory that NTSCAN.EXE is stored in.

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

Using the configuration file

After creating the configuration file, NTScan will default to the selected drive(s) and command line options specified in the DEFAULT.CFG file. For example:

1. Create the configuration file using the above procedure, ensure that it is saved in the same directory as NTSCAN.EXE and that it is saved as an ASCII or DOS Text file.

2. At the system prompt, type

   ```
   ntscan
   ```

3. NTScan will initiate a virus check using the drives and command line options specified in the file, DEFAULT.CFG. Using the above example, VirusScan will scan the directory “USER” and all its associated subdirectories on the C drive. A report file, called “VIRUS.RPT,” will be saved to the D drive. This report file will also include any errors encountered during the Scan. If “VIRUS.RPT” already exists, VirusScan will add the new information to the end of the existing file.

Removing viruses

Although /CLEAN removes many viruses and restores normal operation, viruses can be harmful and insidious and no anti-virus program can undo all their damage. Usually, between 10% and 20% of all viruses corrupt the files they infect, making them unrecoverable. If the file is infected with an uncommon virus that /CLEAN cannot remove, NTScan notifies you and identifies the filename. Note this filename so that you know what to restore from a backup diskette or tape. If you use both the /CLEAN and the /DEL options, NTScan will first attempt to repair an infected file and, if the file is damaged beyond repair, NTScan will delete it. Deleted files are not recoverable except from backups.

Follow the procedures outlined in "Using DOS Scan to remove a virus" on page 73 to remove boot sector and master boot record (MBR) viruses. Do not use NTScan to remove these viruses.

✍ ***WARNING!*** *Do not attempt to remove a virus using DOS commands (i.e. FDISK, FORMAT, DEBUG).* ***Improper removal of viruses can result in the loss of all data and the use of infected disks.*** *If you are unfamiliar with viruses and virus methodology, you should get experienced help before using DOS commands to remove these viruses. For assistance, contact McAfee technical support or your local authorized agent (refer to "McAfee Support," in Chapter 1, "Introducing VirusScan NT"). For more information, refer to "Using DOS commands to remove a virus," in Chapter 5, "Tips and Troubleshooting."*

Basic principles to minimize damage

These considerations lead to the three important principles:

1. Before running NTScan with the /CLEAN option, back up all of your programs and data.

   Of course, this works best if you back up your files regularly, so that you can restore your files from a backup made before your system was infected. But even a backup from an infected system can be useful for restoring data, because most viruses do not corrupt data. If a program no longer runs after being cleaned, replace it from the original diskettes or from a virus-free backup.

When disinfecting an infected system, it is important to start from a "sterile field," as described in Chapter 2, "Installation and Setup."

2. Before running NTScan with the /CLEAN option, restart your computer from a clean, write-protected diskette.

   Preferably, use the clean anti-virus start-up diskette you created in "Creating a clean DOS start-up diskette," in Chapter 2, "Installation and Setup." And, because running any program can spread the infection:

3. Do not run any programs before running NTScan /CLEAN.

   After restarting your computer, immediately launch a Windows 32-Bit Dos Command Prompt to display a DOS prompt (C:\) and run NTScan following the procedures outlined in Chapter 3, "Using VirusScan NT."

Using NTScan to remove a virus

Before running NTScan to clean up infections:

1. Only use NTScan to remove a virus that has infected files. Do not use NTScan to remove a virus from the master boot record or boot sector. If a virus is detected in the master boot record or boot sector, follow the procedure outlined in "Using DOS Scan to remove a virus" on page 73.

2. Launch a Windows 32-Bit DOS Command Prompt to display the DOS prompt.

3. Run the NTScan program to locate and identify the infections.

4. Back up the files on the infected disks (be sure not to overwrite any previous back-ups).

5. Repeat Step 1.

6. Run the NTScan program with the /CLEAN option to remove infections.

   - Do not run any programs before running NTScan /CLEAN from the Windows 32-Bit Dos Command Prompt.
   - When disinfecting a hard disk, always run NTScan /CLEAN from a write-protected diskette to prevent infection of the NTScan program. When disinfecting diskettes, make sure there is no active virus in memory before running NTScan from your hard disk.

Successful and unsuccessful results

NTScan /CLEAN reports the results of its attempt to remove the virus from each infected file. If a file has several infections, it will report on each.

If viruses were not removed

If NTScan cannot remove a virus, a message similar to the following one is displayed:

```
Virus cannot be safely removed from this file.
```

Make sure to take note of the file name, because you will need to restore it from backups. If you have any questions about how to proceed, contact McAfee technical support or your local authorized agent (refer to "McAfee Support," in Chapter 1, "Introducing VirusScan NT").

If viruses were removed

If NTScan /CLEAN has successfully removed all the viruses, shutdown and restart your computer from the system hard disk or diskette. Scan your hard disks again to make sure they are virus-free. If you suspect that your system was infected from a diskette, run NTScan from your hard disk to examine and disinfect the diskettes you use.

Using DOS Scan to remove a virus

If you detect a master boot record or boot sector virus, you can run DOS Scan with the /CLEAN option to remove the virus. If you are at all unsure about how to proceed once you have found a virus, contact McAfee for assistance (refer to "McAfee Support," in Chapter 1, "Introducing VirusScan NT"). You can also use DOS scan to remove viruses that have infected files on your system.

✍ **WARNING!** *Using DOS commands (i.e. FORMAT, FDISK, DEBUG) from a Windows 32-Bit Dos Command Prompt to remove a virus can result in the* ***loss of all data and use of the infected disks****. If you are unfamiliar with viruses and virus methodology, contact McAfee immediately for assistance before using DOS commands to remove a virus (refer to "McAfee Support," in Chapter 1, "Introducing VirusScan NT"). For more information, refer to "Using DOS commands to remove a virus," in Chapter 5, "Tips and Troubleshooting."*

Restart from a clean environment

Restart your computer from a diskette you know to be virus-free, preferably the original write-protected DOS installation diskette that came with your computer. If you do not have one, get one from someone else; do not use a diskette that might be infected. (If you do not have one, you can create one following the procedure outlined in "Creating a clean DOS start-up diskette," in Chapter 2, "Installation and Setup." but only *after* you have successfully cleaned your system.)

Step	Action
1.	Shutdown your computer. (Do not just reset or reboot since doing this may leave some viruses in your computer's memory.)
2.	Make sure your clean DOS boot (start-up) diskette is write-protected. ▪ For a 3.5" diskette, slide its corner tab so that the square hole is open. ▪ For a 5.25" diskette, cover its corner notch with a write-protect tab. Be sure to use the write-protect stickers provided with your diskettes, not tape.
3.	Insert your DOS start-up diskette in drive A and restart your computer.

4. You should see a DOS prompt (A:\). Do not run any other programs or you risk spreading a virus.

5. Remove the DOS start-up diskette.

Run DOS Scan with the /CLEAN option

Step	Action

1. Insert the diskette containing the DOS version of Scan into drive A. This diskette was included with your VirusScan package. If you downloaded VirusScan NT from the McAfee BBS, run DOS Scan from the directory on your hard drive you downloaded the VirusScan program files to.

2. Make sure your DOS Scan diskette is write-protected.

   - For a 3.5" diskette, slide its corner tab so that the square hole is open.
   - For a 5.25" diskette, cover its corner notch with a write-protect tab. Be sure to use the write-protect stickers provided with your diskettes, not tape.

3. Eliminate the first known virus by searching all files on all local drive(s) (including hard drives, compressed, CD-ROM and PCMCIA drives, but not diskettes) by typing:

   ```
   scan /adl /clean /all
   ```

After typing each entry on the command line, press [ENTER].

Scan keeps you informed of its progress and generally reports virus removed successfully.

- If Scan reports that the virus was successfully removed, refer to "If viruses were removed" on page 72
- If Scan reports that the virus could not be safely removed, refer to "If viruses were not removed" on page 71.

If viruses were removed

If Scan successfully removes all the viruses, restart your computer. Begin the installation procedure again as described in "Installing VirusScan NT," in Chapter 2, "Installation and Setup.". Install will again scan your system and, assuming your system is now virus-free, will install VirusScan.

One common source of virus infection is diskettes. Once you have finished installing VirusScan on your hard disk, use Scan again to examine and disinfect all the diskettes you use, as described in "Rescaning new disks and software," in Chapter 2, "Installation and Setup."

If viruses were not removed

If Scan cannot remove a virus, it will tell you:

```
Virus cannot be removed from this file.
```

Make sure to take note of the filename, because you will need to restore it from back-ups. Run Scan again, this time using the /CLEAN and /DEL options to delete the remaining infected files, as described earlier in this chapter. If you have any questions, contact McAfee (refer to "McAfee Support," in Chapter 1, "Introducing VirusScan NT").

One common source of virus infection is diskettes. Once you have finished installing VirusScan on your hard disk, use Scan again to examine and disinfect all the diskettes you use, as described in "Rescaning new disks and software," in Chapter 2, "Installation and Setup."

Examples

These examples show option settings that can be used with NTScan:

To scan all executable files on drive C:

```
ntscan c:
```

To scan all standard executable files on drive F, a network drive:

```
ntscan f:
```

To scan all executable files on drive A, a floppy drive:

```
ntscan a: /many
```

✍ *NTScan checks the diskette in drive A, then prompts you to insert additional disks to continue checking.*

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

```
ntscan c: /adl /adn
```

To scan all files on drives F, G and H and delete any infected files found (use /CLEAN first to attempt to remove viruses before deleting files):

```
ntscan f: g: h: /del /all
```

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

```
ntscan c: d: e: /av /all
```

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

```
ntscan m: /report d:\infectn.rpt /rptcor /rpterr
```

To scan all files in the directories USER\CRAIG and USER\CHRIS, including their associated sub-directories, on drive E:

```
ntscan e:\user\craig e:\user\chris /sub /all
```

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

```
ntscan c: d: e: /fast /cv
```

To scan one specific file:

```
ntscan c:\command.com
```

Error levels

After NTScan has finished running, it sets the ERRORLEVEL. You can use the ERRORLEVEL in batch files to take different actions based on the results of the scan. Refer to your DOS operating system documentation for more information. Scan returns the following ERRORLEVELs:

ERRORLEVEL	Description
0	No errors occurred and no viruses were found.
1	Error occurred while accessing a file (reading or writing).
2	A VirusScan database (*.DAT) file is corrupted.
3	An error occurred while accessing a disk (reading or writing).
4	An error occurred while accessing the file created with the /AF option; the file has been damaged.
5	Insufficient memory to load program or complete operation.
6	An internal program error occurred.
7	An error in accessing an international message file (MCAFEE.MSG).
8	A file required to run VirusScan, such as SCAN.DAT, is missing.
9	Incompatible or unrecognized option(s) or option argument(s) were specified in the command line.
10	A virus was found in memory.
11	An internal program error occurred.
12	An error occurred while attempting to remove a virus, such as no CLEAN.DAT file found, or VirusScan was unable to remove the virus.
13	One or more viruses was found in the master boot record, boot sector, or file(s).
14	The SCAN.DAT file is out of date; upgrade VirusScan data files.
15	VirusScan self-check failed. It may be infected or damaged.
16	An error occurred while accessing a specified drive or file.
17	No drive, directory or file was specified; nothing to scan.
18	A validated file has been modified (/CF or /CV options).
20	/FREQUENCY option in use.
21-99	Reserved.
100+	Operating system error; Scan adds 100 to the original error number.
102	CTRL+C or CTRL-BREAK was used to interrupt the Scan. (You can disable CTRL+C / CTRL-BREAK with the /NOBREAK command line option.)

Configuring reporting options

The /REPORT {filename} command line option can be used to create an ASCII text file, called {filename}, that we recommend you use to create an “audit trail” of scans and scanning results. If {filename} already exists, /REPORT erases and replaces it (or, if you use /APPEND, adds the report information to the end of the existing file). You can include the destination drive and directory (such as **D:\VSREPRT\ALL.TXT**), but if the destination is a network drive, you must have rights to create and delete files on that drive. Other options for /REPORT include /RPTALL, /RPTCOR, /RPTMOD and /RPTERR.

/RPTALL: Add the names of all files scanned to the report file.

/RPTCOR: Add the names of corrupted files (files that cannot be repaired with the /CLEAN option) to the report file. We recommend you use this setting if you are using the /DEL option so you can later replace deleted files with backups.

/RPTERR: Add system errors to the report file. For more information, refer to “Error Levels” earlier in this chapter.

/RPTMOD: Adds the names of modified files to the report file. Use this option when you are using the validation/recovery options (/CF or /CV).

You can use all these reporting options on the same command line:

```
ntscan c: /report c:\infected.txt /append /rptall /rpt-
cor /rpterr /rptmod
```

The above example would scan the C: drive and save the report file as “INFECTED.TXT” on the C: drive. The report file would include the names of all files scanned, all corrupted files, all modified files and any system errors. If this file already exists, NTScan will add the new information to the existing file.

Updating validation codes

If you install any new software or programs on your system, including a new version of Windows NT, and are running NTScan with the /CF (preferred) or /CV validation options, you need to install validation codes for the new files with NTScan's /AF (preferred) or /AV options.

The quickest way to update the validation codes is to remove all validation codes from the hard disk and then add them back. In other words, first run NTScan with the /RF or /RV option, then run it again with the /AF or /AV option.

✍ *You can also remove validation codes added with the /AF command line option by deleting the validation file. Scan your system to check for viruses, delete the validation file, then run NTScan with the /AF command line option to create a new validation file with current information.*

Creating an exception list file for the /EXCLUDE option

If you set up validation codes using VirusScan's /AV or /AF options, subsequent scans using the /CV or /CF options will detect changes in executable files. This can generate false alarms if the executable files are self-modifying or self-checking (most programs that do this will tell you to turn off your anti-virus software before running them; some of these files are listed below). Therefore, use the /EXCLUDE option in conjunction with /AV to identify such files and exclude them from the validation.

The exception list is an ASCII or DOS text file. If you use a word processor to create it, be sure to save the file as ASCII or DOS Text. Each line in the file contains the path and file name of one file that should not be validated:

```
c:\clipper\bin\clipper.exe
c:\123\123.com
c:\fox\foxprolx.exe
c:\dos\setver.exe
c:\pkware\pklite.exe
c:\pkware\pkzip.exe
c:\pkware\pkunzip.exe
c:\semware\q.exe
c:\swapvol.com
c:\wordstar\ws.exe
```

✍ *Although the /AF option does not add code to any files other than the one specified, using /CF will report changes in self-modifying files as possible infections. Refer to the /RF option in* *"Option details" on page 55* *for more information.*