How to Use Vet

When you run the Vet program, the initial window that appears will display both the Browser and the Reports windows.

When you select one of the menus a drop-down menu will display further options. A brief description of the menu options associated with the command or icon appears in the Status Bar (bottom left) of the Vet screen.

These options explain the various activities associated with the use of these windows.

Introduction to the Browser window

Introduction to the Report window

How to set the defaults

Vet Application Functions

Selected from the top left corner of window, this function offers the standard Windows commands **Restore**, **Move**, **Size**, **Minimize**, **Maximize** and **Close** (which has a Hot Key ALT F4).

Restore, **Minimize** and **Close** operate when the Vet window is full size. All the commands except **Restore** operate when the Vet window is less than full size.

Toolbar Buttons

The Vet program uses standard Windows icons, buttons (*i.e. Minimize, Maximize, Cascade,* and *Close*), slider bars, and menu commands such as **File**, **Edit** and **Help**. Menu commands, icons and buttons specific to Vet usage are explained below.

When you position the cursor above a toolbar button without selecting the button, a help text will appear in a small pop-up window beside the button.

Select the options below for information on;

Move up button

Large Icon button

Small Icon button

List button

Details button

Change options

Go button

Stop button

The Move Up Button

Select this button to move to the parent directory of the directory currently displayed.

The Vet Button

Select this button to scan the selected item(s) using Vet. If no item(s) have been selected, then Vet will prompt you to specify a path and then to try again. The results of the scan will be noted in the Report window and the second, third and fourth panels at the bottom of the Vet window will note the number of files scanned, the number of scanned files found to be infected and the number of scanned files suspected of being infected.

The Stop Button

Select this button to stop the scanning process. The Report window will note that the operation was interrupted. The second, third and fourth panels at the bottom of the Vet window will note the number of files scanned before the scan was interrupted, the number of scanned files found to be infected and the number of scanned files suspected of being infected.

The Large Icons Button

Select this button to display large icons in the Browser window. Either specific or generic icons may be displayed, depending on the file they refer to and the **All Icons** option under the View menu .

The Small Icons Button

Select this button to display small icons in the Browser window. Either specific or generic icons may be displayed, depending on the file they refer to and the All icons option under the View menu .

The List Button

Select this button to display the list of files, folders or drives in the Browser window. Either specific or generic icons may be displayed, depending on the file they refer to and the View menu .

The Details Button

Select this button to display the list of files, folders or drives in the Browser window along with their various details such as type, size, and date last modified. Selecting the title of one of these details sorts the window according to that category of information. Selecting the same category again will reverse the order of details.

This option uses the small icons associated with each item. Either specific or generic icons may be displayed, depending on the file they refer to and the View menu

What the Vet | Window menu does

To activate any menu item press both the <ALT> key and the first letter of the menu required. To select an option from the menu, press both <Shift> and the letter that is underlined in the option. (once the menu is displayed the arrow keys can be used to navigate to the selected menu option)

i.e. Select an item(s) with the mouse, press down both the <ALT> and <F> keys to activate the File menu, then both <Shift> and <V> to run the scan.

Select the options below for information on;

- File
- Edit
- View
- Options
- Window
- Help

The File Menu

Vet: Scans the selected item(s). If no item(s) have been selected, then Vet will prompt you to specify a path and then to try again. The results of the scan will be noted in the Report window and the second, third and fourth panels at the bottom of the Vet window will note the number of files scanned, the number of scanned files found to be infected and the number of scanned files suspected of being infected.

Stop: Stops the scanning process. The Report window will note that the operation was interrupted. The second, third and fourth panels at the bottom of the Vet window will note the number of files scanned before the scan was interrupted, the number of scanned files found to be infected and the number of scanned files suspected of being infected.

Exit: Quits the Vet application.

The Edit Menu

Cut: Standard Windows command (Ctrl X. This command can be used to cut sections of the log file for storage on the Clipboard.

Copy: Standard Windows command (Ctrl C). This command can be used to cut sections of the log file for storage on the Clipboard.. Such item(s) can be then pasted to a Word document.

Paste: Standard Windows command (Ctrl V). For use with the **Cut** and **Copy** commands.

Select All: Selects all files, folders or drives displayed in the Browser window if it is the active window. Selects all the text in the Report window if it is the active window.

Invert Selection: When the Browser screen is active this will invert the previous selection. That is, if one or more files, folders or drives were previously selected, this command will select the remaining files, folders or drives to the exclusion of those previously selected.

The View Menu

These options will alter the way the icons and information about files is presented in the browser window. The first four options are mutually exclusive. That is, selection of one will cancel the previous selection.

Large Icons: Displays large size icons in Browser window.

Small Icons: Displays small size icons in Browser window.

List: Displays list of files, folders or drives in Browser window.

Details: Displays details (e.g. Name, Size, Type, Date Last Modified, Total Size, Free Space) of files, folders or drives in Browser window.

Arrange Icons: Directory contents can be arranged by Name, Size, Type and Date of last modification. (Depending on the option **All icons** either specific or generic icons may be displayed.)

All icons: Switches the Browser display between generic and file specific icons.

Refresh: Cancels the selection of any item(s) in the Browser window. Also checks to see if there have been any changes to the items displayed in the Browse window (it will update the list if there have been any new files added, removed or any other changes made to the directory that is currently displayed).

The Options Menu

Program: Selecting this menu item opens the Program dialog, which allows changes to the default settings for every subsequent scan. Program dialog

Resident Protection: Selecting this item opens the Resident Protection dialog, which allows changes to the way the resident protection operates Resident dialog

Alerting : Selecting this item opens the Alert Properties dialog, which can enable, disable and configure the sending of an Email message when a virus is detected. See Alerting for further details.

Options Wizard: Selecting this item will run the configuration wizard. For further details on the Installation/Configuration wizard please select the on-line help button that is on each dialog of the wizard. Options Wizard

Password Protect Options: Many system administrators have asked that we provide password protection to stop unauthorised alterations to the Vet configuration so this feature has been added to Vet95 and VetNT. The password protection can be enabled by selecting Options | Password Protect Options and entering a password. This option can also be set while configuring a network installation so that the password will be the same on every workstation that is updated from the server.

NOTE: The password that is entered is case dependant, so an “a” is not the same as an “A”.

See Password protection for further details.

The Options Wizard

Please select the Wizard Option that you want more information on.

Scanning Options

For more information Click here

Scan File Types

For more information Click here

Program Virus Detection Actions

For more information Click here

Macro Virus Detection Action

For more information Click here

Reporting Options

For more information Click here

Boot Sector Scanning

For more information Click here

Memory Scanning (Vet95 only)

For more information Click here

Vet Start-up Options

For more information Click here

Progressive Scan

For more information Click here

An Index of all the Resident Protection options

For more information Click here

Resident Protection Components

For more information Click here

Resident Floppy Disk Boot Sector Protection

For more information Click here

Resident File Monitor Options

For more information Click here

Resident File Infection Actions

For more information Click here

Resident Macro Infection Actions

For more information Click here

Resident File Monitor Reporting

For more information Click here

Virus Alerting

For more information Click here

SMTP E-Mail Configuration

For more information Click here

Out-of-date Warning

For more information Click here

The Window Menu

Report: Selecting this option will activate the Report window.

Browser: Selecting this option will activate the Browser window.

The Help Menu

Help Topics:	Accesses Vet On-line Help
DOS VET:	Accesses On-line Help for DOS Vet Users
Virus Information:	Accesses The Virus Encyclopaedia. For a full list of the Viruses detected by this version of Vet select Start | Programs | Vet anti-virus for Windows | Viruses Specifications or select VIRUSES.HLP from your Vet directory.
About:	This dialog will always contain the version number of your current copy of Vet. Provided the name of the registered user, the name of the registered company and the Vet customer number were entered during installation, these details will also be displayed in this box.

How to use the Vet Browser Window

The Vet Browser window can be used to view the contents of folders, directories, drives, and to select items for scanning.

To open (display the contents of) a folder, directory or drive that is in the Browser window, double-click on the item or press <Enter> if the item has already been highlighted. If you do this on a file it will be scanned.

Press the "Level Up" toolbar button to move to the parent directory of the directory currently displayed.

How to select files in the browser window

How to start scanning the selected files

Selecting the File, Folder, Directory or Drive for Scanning

To select an item in the Browser for scanning, click it with the mouse.

Multiple items can be selected by using standard Windows95 actions with the <Shift> and <Ctrl> keys. All items in the Browser window can be selected by using the **Edit** | **Select All** command.

If you select individual files to be scanned they will be scanned.

If you select directories or drives, only the files with extensions in the executable list will be scanned.

For further information on the list of files considered executable click here.

How to start scanning the selected files

How to Start a Scan

Once item(s) have been selected for scanning, any of the following actions will initiate the scan:

1. pressing the Vet toolbar button;
2. selecting the **File** | **Vet** menu item;
3. pressing the right mouse button and selecting the Vet option in the pop-up menu;
4. pressing the <Enter> key if item(s) are highlighted;
5. double-clicking a file icon.

Results of the scan are displayed in the Report window and also written to the log file. (see the **Options** | **Program** | **Reporting** menu for the name of the log file). Depending how the item(s) for scanning where selected, one of the following options will have occurred;

1. If the Browser window is active when a scan is started:
1. If the Report window is active when a scan is started:

If the Browser Window is active when the scan is started:

Item(s) that have been selected in the Browser window will be scanned.

The Browser window will be active immediately after item(s) have been selected.

If no item(s) are selected and a scan is started Vet will not know which item(s) to scan and will put up a message box prompting you to select a file, folder or drive in the Browser window and then to try again.

If the Report Window is active when a scan is started:

Vet will not know which item(s) to scan and will put up a message box prompting you to select item(s) and then to try again.

This will happen even if an item has been highlighted in the Browser box.

Click on the Browser icon to make it active then try again

About the Report Window

The report window displays the results of scans. The Options | Program | Scanning menu allows changes to the types of files scanned (either all files or executables only) and also allows sub-directories to be scanned.

The Options | Program | Reporting menu can set the report window to show all files scanned or only those that are infected or suspected. Checking the tick box **Cumulative report** causes the report window to show the results of the current scan after the results of the last i.e. causes a log. Not checking the box will cause the report window to be cleaned before the results of a scan are displayed.

How to use the Vet Report Window

The Report window displays the results of scans done in the current session.

The various options possible while using the Report window are described below;

1. Text can be cut or copied to the Clipboard using the **Cut**, **Copy** and **Paste** commands. Text from the Clipboard can also be pasted back to the Report window using the same commands;
2. All the text in the Report window can be selected for cutting or copying using the **Edit** | **Select All** command;1. Text can be cut or copied to the Clipboard using the **Cut**, **Copy** and **Paste** commands. Text from the Clipboard can also be pasted back to the Report window using the same commands;
3. The results that are displayed in the Report Window can also be emailed. See the Options menu for further details.
4. The names of the files that have been scanned can be displayed in the report window. Either *all* of the file names scanned can be displayed or *only those that are suspected* of having a virus can be displayed. This option can be set under the Options | Program | Reporting menu

How to Edit the Defaults (Options | Program menu)

The Program dialog is opened by selecting **Options** | **Program** from the menu. It provides an opportunity to change the Vet default options for Scanning, Actions, Reporting, Boot Sectors and Memory. Each option can be examined by selecting the appropriate tab at the top of the window. The processes involved in adjusting the default settings are detailed below;

NOTE: Set **All files** and **Full Scan** if you suspect that you may have a virus or you have just had a virus – it may find infected overlay files with obscure extensions that the **Executable Only** test may not test, as well as any non-executable files the virus has corrupted by trying to infect.

Select the options below for information on:

Scan Options

- Fast scan or full scan
- Include subfolders
- Show network drives
- Skip renamed files

File Types

- File Types to scan

Reporting

- Reporting when a virus is found
- Suppress 'Out-of-date' warning

Program Viruses

- Infected program files
- Suspect program files

Macro Viruses

- Infected document files

Boot Sectors

- Scan boot sectors plus options

Memory (For Vet95 Only)

- Resident memory checking

Start-up

- Start-up Scan
- How to customise the Start-up Scan

The Tools Menu

The Tools menu (<Alt> T) allows a template or reference disk to be created for each disk drive. A template is a copy of the current boot sector. Vet can compare the saved copy of the template with the current template to determine if changes have occurred. The reference disk stores copies of the templates to a floppy disk.

The re-installation of an old template can cause files to be lost if the drive structure was changed after the template was made. For this reason the ability to re-install templates (emergency functions) are protected with a password.

NOTE: New templates will be required if more drives are added, the partitions of current drives change or the operation system is updated.

Record Templates

Record Reference Disk

Emergency functions

Emergency password

Change Password

How to Record Templates

The tools menu allows a template to be created for each local hard disk drive. Vet will check that the template matches the current boot sector as part of the first scan of any session.

A dialog will display all of the drives available. Click on each drive (or use the space bar and arrow keys) to select the drive(s) that you wish to make templates for.

Options:

OK:	A template for each of the selected drives is made and stored in Vet.
Cancel:	No templates are made.
Help:	Displays this help screen.

Record Reference Disk

Emergency functions

Emergency password

Change Password

How to make a Reference Disk

A reference disk can be made to store copies of the current templates. These templates can be re-installed at a later date if the drive has been corrupted by an unrecoverable virus.

Insert a blank formatted disk, or preferably a system disk, into the floppy drive. (If you do not have a new disk see NOTE: below)

Select the floppy drive that will produce the reference disk by using the arrow keys or selecting from the scroll-down menu. Enter a caption in the Identification field (<Shift> I) so that copies of the current template(s) can be recognised at a later date. As a default, the Identification field type-in box will store the time and date that the templates are created.

This disk should now be kept in a safe place.

NOTE: To format a new disk insert it into the floppy drive, in Explorer click the drive, then click the right-hand mouse button. Select Format, Full and Start.

Record Templates

Emergency functions

Emergency password

Change Password

Emergency Services

The re-installation of an old template can cause files to be lost if the drive structure was changed after the template was made. For this reason the ability to re-install templates is protected with a password .

When the correct password has been entered the Emergency Services dialog will appear. Select the local hard drives that you wish to verify then select <Enter> to begin the comparisons. As each of the drives are checked a dialog will appear with the results of the comparison.

> **If** a drive template was not created, a dialog will confirm that no comparison is possible. It is only possible to check local hard drives.
>
> **If** the Boot sector, DOS and large IDE template attributes match the current drive configuration, select the OK button to begin the next comparison.
>
> **If** the template does not match the current drive configuration, Vet will offer to replace it with the original template.
>
> **YES:** Loads the original template over the current configuration.
>
> **NO:** The template remains the same and is not replaced.

Record Templates

Record Reference Disk

Emergency password

Change Password

How to change the Emergency Functions Password

For security reasons the password should be changed periodically.

To change the emergency password;

1. Enter the current emergency password in the Current Password type-in box
2. Enter the new password in the New Password type-in box
3. Re-enter the new password in the Confirm New password type-in box
4. Select the OK button

Record Templates
Record Reference Disk
Emergency functions
Emergency password

How to use the Report File Dialog

This dialog allows the user to define the location of the log file. The file structure can be navigated and new files/folders can be created as required.

This dialog is accessed from the **Options** | **Program | Reporting** menu command and pressing of the **Browse** button. It enables you to browse for alternate files to use as the log file or to create a new file in a chosen directory.

NOTE: As the log file has to be able to be edited in DOS the name must NOT contain spaces; unprintable characters or contain directory names longer than eight characters.

Toolbar buttons used in this window are explained below:

Up One Level	Press the "Level Up" toolbar button to move to the parent directory of the directory currently displayed.
Create New Folder	Used to create a new folder in the folder, directory or drive displayed in the Report File window.
List	Select this button to list the files, folders, directories and/or drives available. The *List* and *Details* buttons are mutually exclusive.
Details	Select this button to display the details (type, size, and date last modified) for the files, folders, directories and/or drives available. The *List* and *Details* buttons are mutually exclusive.

The **File name** type-in box allows the name for a new log to be entered

Save as type changes the type of file to be displayed.

Save & Cancel Buttons

Virus in Memory

The **Virus in memory!** dialog will immediately appear if a virus is detected in resident memory. The first function performed by Vet when a scan is activated is to check resident memory for viruses.

Resident memory (RAM) is checked for viruses at the start of each Vet session (i.e. when the first scan is requested Vet will check resident memory and then check the item(s) requested for scanning.)

Vet is normally installed to scan each time a machine is booted (started) and the memory will automatically be the first item checked. If Vet is started from the desk top and the **Options | Program | Memory** menu option is enabled the resident memory will be checked before the first scan is performed.

Options:

Yes A message will confirm if Vet has disabled the virus(es). If it has not been possible to disable the virus call Vet Customer Care

Once Vet has dealt with the virus in memory it will automatically check the boot sectors of all hard drives. See below.

No Check the **Help | Virus Information** menu for details on virus payloads. **WARNING:** If the virus present on your computer has a "payload" it may severely damage your files(s) and drive(s).

Details The Detail of viruses in memory dialog will display the number, name and memory location of the virus(es) that have been found.

Help Displays this help page.

Details of the Virus(es) in memory

This dialog will be displayed when the **Details** option is chosen on the Virus in memory dialog.

This dialog displays the number, name and memory location of the virus(es) that have been found in resident memory.

Selecting the **OK** button will close the dialog and return to the Virus in memory dialog.

Virus in memory dialog

If Vet finds a Hard Disk Boot Sector Virus

Vet checks drive boot sectors if the **Options | Program | Boot Sectors** menu has the *Scan boot sectors* option enabled and the infected drive is scanned.

If a virus is detected the Repair infected boot sector? dialog will be displayed. This will display the name of the drive and the type of virus found. It will also display options to repair the boot sector (if it is possible to repair it).

Options:

Yes Vet will display the Make a Rescue Disk dialog. A rescue disk can be made to store copies of the current file structure. The structure can be re-installed at a later date if the drive is corrupted by an unrecoverable virus.

No The fact that the virus has been found will be recorded in the log file.

WARNING: If the virus present on your computer has a "payload" it may severely damage your files(s) and drive(s). Check the **Help | Virus Information** menu for details on virus payloads.

Help Displays this help page.

YES - Make a rescue disk

Payloads and Warheads

The first virus writers were content with proving that they could write a virus, but now most add a PAYLOAD or WARHEAD. This may be in the form of a message put to the screen or it may be something that interferes with the operation of the computer in an ‘amusing’, irritating or destructive manner.

With warheads, there is a conflict between the desire to show off and the need to be inconspicuous so that the virus will propagate widely. This is usually achieved by making a warhead wait a certain amount of time or wait for an unusual event, so that the virus does not declare itself until it has had a chance to propagate.

WARNING: It is unwise to deliberately trigger a virus’s warhead. There are often variations and revisions made to viruses. Viruses that have been harmless in the past may have been modified to cause substantial damage. Some people cannot resist the temptation to run a virus and the consequences of doing so can be disastrous.

How to make a Rescue Disk:

A rescue disk can be made to store copies of the current boot sector. The current boot sector can then be re-installed at a later date if the virus has corrupted the original boot sector and it is unrecoverable. This dialog is activated by selecting **Yes** in the *Repair infected boot sector?* dialog.

Insert a blank formatted disk in the floppy drive. (If you do not have a new disk see NOTE: below). Select the floppy drive that will produce the reference disk by using the arrow keys or selecting from the scroll-down menu. Enter a caption in the Identification field (<Shift> I) so that the rescue disk can be recognised at a later date. As a default, the Identification field type-in box will store the time and date of the disks creation.

NOTE: To format a new disk check that the disk can be written to (i.e. the hole in the top, right side of the disk is open), insert it into the floppy drive, in Explorer click the floppy drive once, then click the right-hand mouse button. Select **Format, Copy system files only** and **Start**.

STOP! As soon as the rescue disk is created **it will be infected** with the virus and has the potential to infect other PCs. Do not use this disk in any other PC.

Options:

Yes The rescue disk will be created allowing Vet to recover the current boot sector if the original has been corrupted by the virus. Once the disk is created, Vet will check to see if the original boot sector is recoverable and will display the Ready to replace boot sector? dialog.

No The virus will be removed. If the original boot sector can be found and it has not been corrupted Vet will display the Ready to replace boot sector? dialog. If the original boot sector has been destroyed by the virus Vet will display the Master boot record damaged dialog.

Help Displays this page.

Ready to replace boot sector?

Master boot record damaged

If the original Boot Sector has been corrupted:

If the virus has damaged or destroyed the original boot sector, Vet will display the Master boot record damaged dialog. This allows the option of installing of a standard boot sector which will recover the drive for almost all systems. But there is no guarantee that it will work for yours. If the installation fails to recover the drive, the rescue disk (if one was created) can be used to reverse the cleaning process. Call Vet Customer Care

NOTE: If a standard boot sector is installed on a non-standard drive, the drive will be corrupted and all files may be lost. A rescue disk can reverse the cleaning process and re-install the infected (but functional) boot sector.

Options:

YES Installs a standard boot sector.

NO The fact that the virus has been found will be recorded in the log file.

Installing the Boot Sector:

At this point the original boot sector (or a standard replacement if the original was not recoverable) is able to be installed as the boot sector for the hard drive.

NOTE: If a standard boot sector is installed on a non-standard drive, the drive will be corrupted and all files may be lost. A rescue disk can reverse the cleaning process and re-install the infected (but functional) boot sector.

Options:

YES Replaces the boot sector.

NO The fact that the virus has been found will be recorded in the log file.

“Replace Floppy Boot Sector?” dialog

Vet checks floppy boot sectors if the **Options | Program | Boot Sectors** menu has the *Scan boot sectors* option enabled and the infected drive is scanned.

If a virus is detected the Repair infected boot sector? dialog will be displayed. This will display the name of the drive and the type of virus found. It will also display options to replace the boot sector (if it is possible to repair it).

Options:

Yes Vet will replace the existing boot sector with a standard floppy boot sector.

No The fact that the virus has been found will be recorded in the log file.

WARNING: If the virus present on your floppy has a “payload” it may severely damage your files(s) and spread to other drive(s) and floppies. Check the **Help | Virus Information** menu for details on the amount of damage this virus can cause.

How to remove File Viruses

File viruses will be automatically, if the *Options* | *Program* | *Action* tab has been set to Clean infected files. Other possible options are to automatically delete or rename the file. Whichever option is selected, the name of the virus and the name of the infected files will be written to the log file.

When a scan is performed on a group of files the file name of the infected file(s) along with the name of the virus and the action Vet has taken will be displayed in the Vet Report window. By default only those files that are infected will be displayed. All the files scanned can be displayed if the Vet Options | Program | Reporting *All files scanned* option is selected

How to clean Word97 documents

Word97 has a different file structure to the documents created by Word 6 or Word 7. This new structure (VBA5) requires a different method for detecting and cleaning the Word97 viruses.

The good news is that all of this is now transparent to you the user!

Vet95 and VetNT can automatically detect and clean all Word97 macro viruses as well as the Laroux Excel macro virus.

On Demand Scanning Default Settings

These default settings determine how Vet will perform a scan when you start Vet and scan a file, directory or drive. To alter these defaults select the Options | Programs menu item.

Scanning:
Fast scan is on. For further information click here..
Include sub-folders is on. For further information click here.
Skip renamed files is on. For further information click here.
File types to scan is set to Files of these types BIN, COM, DLL, DOC, DOT, DRW, EXE, OVL, SYS. The list of default extensions on your computer can be returned to the default list by selecting the default button. For further information click here.

Actions:
Infected program files is set to clean. For further information click here.
Suspect program files is set to report only. For further information click here.
Infected document files is set to clean. For further information click here.

Reporting: For further information click here.
Filenames reported is set to Infected or suspect files only
Cumulative report is on. The default name of the log file is C:\VET\VET_LOG1.
Suppress the out-of-date warning is off

Boot Sectors: For further information click here.
Scan boot sectors is on
Replace bad boot sectors is on
Check for large IDE driver is on (this option is only available in Vet 95)
Treat as a bad boot sector is set to known virus only

Memory: (Not available in Vet NT until version 9.50) For information click here.

Enable memory scanning is on

Resident Protection Default Settings

By default resident protection is enabled when Vet is installed. To alter any of these settings select Options | Resident Protection. For more information click here.

Floppy Boot Sector: For information on the this option click here.
Consider the boot sector bad if it contains a known virus
Replace any boot sector considered bad is on

File Monitoring: For information on this option click here.
Monitoring executing programs is on
Monitoring opening files is on
Monitoring closing files is (off for VetNT but on for Vet95)
Action for infected files is set to clean file
Action for suspect files is set to report and deny access
Scan type is set to Fast (for Vet95 only)
The full scan check box is not selected (for VetNT only)
Beep on detection is off (for Vet95 only)
Invisible mode is off (for Vet95 only)
Write log file is off (There is no default name for the log file) (for Vet 95 only)

Macro Monitoring: For information on the this option click here.

Clean infected documents is on (for Vet95 only)
Action for infected documents is Clean documents (for VetNT only)

The OK/Save and Cancel Buttons

OK/Save Closes the dialog and saves any changes or selections that you have made.

Cancel Closes the dialog without saving any changes or selections.

Resident File OK and Cancel Buttons

OK Closes the Resident Protection Options dialog A summary of the current settings will be displayed Selecting **OK** will save the changes that have been made.

Cancel Closes the Resident Protection Options dialog without saving any changes or selections that you have made in this dialog box.

Web Update & Technical Support from the Internet (Australian customers only)

This option will allow Australian registered users (of Vet95 and VetNT) who are connected to the Internet to access our update and technical support areas on the Cybec Web page via the Web Update and Technical Support menu option. Simply select Start | Programs | Vet Anti-virus for Windows 95/NT | Web Update & Tech Support. This starts an Internet session and connects you to the two main areas of the Vet Web site.

The “Get Vet Now” button will display a menu with the latest versions of Vet. You will be required to enter the customer number and the surname on the subscriber card to get access to these upgrades.

The “Technical Support” button links you into the lists of Frequently Asked Questions. There is a new set of FAQs produced for each release (so any known bugs and their work-arounds can be viewed, anytime and anywhere!).

The Vet web site and FAQs can be accessed by anyone. See the Contact list for details.

Password Protecting Your Vet Setup

Many system administrators have asked that we provide password protection to stop unauthorised alterations to the Vet configuration, so this feature has been added to Vet95 and VetNT. The password protection can be enabled by selecting Options | Password Protect Options and entering a password. This option can also be set while configuring a network installation so that the password will be the same on every workstation that is updated from the server.

NOTE: The password that is entered is case dependant, so an “a” is not the same as an “A”.

How to print out all of the on-line information for the installation wizard

Select the print button above to print out the following list of all the information screens in Options | Options Wizard.

Password

The password can be invoked by either selecting **Options** | **Password protect options**, or **Tools** | **Emergency.**

Options | Password protect options:

This feature is in Vet95 and VetNT because many system administrators asked that we provide password protection to stop unauthorised alterations to the Vet configuration. The password protection can be enabled by selecting Options | Password Protect Options and entering a password. This option can also be set while configuring a network installation so that the password will be the same on every workstation that is updated from the server.

The password protection of the Options menu can be disabled by selecting Options | Password Protect Options and entering the correct password. (The password protection for the Tools | Emergency menu is not affected by disabling the Options menu password).

Tools | Emergency:

The re-installation of an old template could cause files to be lost if the drive structure was changed after the template was made. For this reason the ability to re-install templates is protected with a password.

The Emergency Password dialog will appear when the **Tools | Emergency** functions menu is selected. It prompts for a password to allow access to the emergency options, and will continue to prompt until the correct password is entered.

NOTE: If no password was set when Vet was installed the default password **VET** will be used. Enter the password then select OK

The password entered is case dependant, so an “a” is not the same as an “A”.

Scan Type

Full Scan: Causes Vet to examine every byte of a file when checking it for viruses. This will increase the time Vet takes to check your files and disks and is only recommended when you have had (or suspect you may have) a virus. You can choose either Full Scan or Fast Scan but not both.

Fast Scan: Causes Vet to examine the entry point and selected areas of a file when checking it for viruses. This is the preferred mode for routine checking of your files and disks as it is both an extremely fast and extremely accurate check for viruses. You can choose either Full Scan or Fast Scan but not both.

Include subfolders

Skip renamed files

Show network drives

Include Subfolders/Skip renamed files/ Show network drives

Include subfolders: Causes Vet to check the subdirectories or subfolders of the current directory or folder.

Skip renamed files: Causes Vet not to check those files which have been renamed by Vet during previous scans. Renaming will occur if the default in **Options | Program | Actions** is set to Rename and a suspect file is found. The file extension will be changed so that the first letter will be an underscore. So .exe will become ._xe.

Show network drives: If your PC is attached to a network and this option is enabled the network drives will be displayed (and can be scanned) in the Browser.

Enabling this option will also cause files that are stored on network drives to be scanned by the resident protection before they are used by the PC.

File Types to Scan

All files: Causes Vet to check *every* file it encounters for viruses. You can choose either All files or Files of these types, but not both.

Files of these types: Causes Vet to check files that it considers to be executable (or 'runable'). By default Vet considers files with
the .XLS, .XLT, .BIN, .COM, .DLL, .DRV, .EXE, .OVL, .DOC, .DOT and .SYS extensions to be executable. You can choose either All files or Executable only but not both.

Add: Allows you to add to the list of file extensions Vet will consider executable. With the advent of Macro language viruses, it is now possible for a file with any extension to contain a virus that can infect your PC. Selecting this button causes an input window to appear. You then have the opportunity to enter the new file name extension in the type-in box.

Delete: If you select a file extension from the displayed list and press this button, the file extension will be removed from the list that Vet considers executable.

Default: Restores the default list of file extensions Vet considers executable. (.XLS, .XLT, .BIN, .COM, .DLL, .DRV, .EXE, .OVL, .DOC, .DOT and .SYS extensions)

Add Vet to 'right-click' menus for these file types: If this option is selected and you are using MS explorer (or other navigation tool) you can select a file, directory or drive, right click the mouse button, and Vet will scan your selection.

Infected & Suspect Program Files:

The following mutually exclusive options are available for actions dealing with infected files.

STOP! If you chose for files to be **Clean**ed and a file has been infected with an overwriting virus , Vet will offer to ignore, rename or delete the file, as no disinfection is possible. By default Vet will offer to delete the file.

Report only: Causes Vet to report, but not attempt to clean, infected files.

Clean: Causes Vet to attempt to disinfect virus-infected files, returning the files to working order. If the file has been infected by an overwriting virus, Vet will **Delete** the file, as no disinfection is possible

Rename: Causes Vet to change the first letter of the extension of any file infected with a virus to an underscore '_' (.EXE becomes ._XE). This allows you to keep the file for further examination, without the risk of accidentally running it.

Delete: Delete causes Vet to delete irreversibly any file that it finds has been infected with a virus. The file is first overwritten with 'D's and then set to zero length, so no recovery of the deleted files is possible.

STOP! Use this option with caution, as there is no possibility of recovering files deleted in this manner.

Suspect Program Files:

The following mutually exclusive options are available for dealing with files suspected to contain a virus.

Report only: Causes Vet to report, but not attempt to clean, infected files.

Rename: Causes Vet to change the first letter of the extension of any file suspected of infection with a virus to an underscore '_' (.EXE becomes ._XE). This allows you to keep the file for further examination, without the risk of accidentally running it.

Delete: Delete causes Vet to delete irrevocably any file that it finds has been infected with a virus. The file is first overwritten with 'D's and then set to zero length, so no recovery of the deleted files is possible.

STOP! Use this option with caution, as there is no possibility of recovering files deleted in this manner.

Overwriting Viruses

Most viruses are careful not to destroy the infected file, but overwriting viruses overwrite part of the infected file, so that it will no longer operate. However, this makes these viruses extremely obvious, so they are unlikely to spread far.

The Zeroto-0, or Australian 403 virus, is of this type. When an infected file is run, the virus searches for an uninfected .COM file and replaces it with a 403 byte file which only contains the virus. The original file is destroyed, so infected files appear to run, but do nothing.

Suspect Program Files:

The following mutually exclusive options are available for dealing with files suspected to contain a virus.

Report only: Causes Vet to report, but not attempt to clean, infected files.

Rename: Causes Vet to change the first letter of the extension of any file suspected of infection with a virus to an underscore '_' (.EXE becomes ._XE). This allows you to keep the file for further examination, without the risk of accidentally running it.

Delete: Delete causes Vet to delete irrevocably any file that it finds has been infected with a virus. The file is first overwritten with 'D's and then set to zero length, so no recovery of the deleted files is possible.

STOP! Use this option with caution, as there is no possibility of recovering files deleted in this manner.

Infected Document Files:

The following mutually exclusive options are available for dealing with documents or spread sheets that contain a macro virus.

Windows97 has a different file structure to the documents and spreadsheets created by earlier versions of Word and Excel. This new structure (VBA5) requires a different method for detecting and cleaning the viruses.

The good news is that all of this is now transparent to you the user!

Vet95 and VetNT can automatically detect and clean all Word97 macro viruses as well as the Laroux Excel macro virus.

Report only: Causes Vet to report, but not attempt to clean, infected files.

Clean: The file will be cleaned, and if possible, returned to working order.

Reporting

This dialog controls what will be displayed in the Report window and written to the log file.

All files scanned: Causes Vet to display on a separate line the name of each file it tests (which in turn causes the name of every file tested to be written to the log file, regardless of whether it had a virus or not). This is useful in explicitly identifying which files are *not* infected (Vet uses a separate line for each infected file).

Infected or suspect: Causes Vet to report on a separate line the name of each file it finds to be suspected or infected.

The *All files scanned* and *Infected or suspect* options tell Vet which file names are to be listed in the Report window. These two options are mutually exclusive.

Write log: The name of the log file to which all scan results are written is displayed in the type-in box. The location of the log file can be changed using the Browse button to select an existing file or allow the entry a new file name.

Cumulative report: If this option is enabled the results of each scan will be stored cumulatively in the log file. If it is NOT enabled the log file will be cleaned and overwritten each time a scan is performed.

Limit log size to: Once you perform a scan and the file becomes larger than (the default) 32Kb it will automatically be truncated by removing the oldest information first.

Suppress 'Out-of-date' warning

NOTE: As the log file has to be able to be edited in DOS the name MUST NOT contain: spaces, unprintable characters or contain sub-directory names longer than eight characters.

Display 'Out-of-date' Warning

Around four months after you have installed the latest copy of Vet it will display a message to let you

know that it is now out of date and to remind you to load the next upgrade. If you are not able to load the next upgrade this option allows you to disable the message.

Boot Sectors

This dialog sets up the defaults for the treatment of boot sectors.

Scan boot sectors Allows Vet to scan boot sectors. Turning this option off causes all the other options in this dialog box to become inactive.

Consider a boot sector bad if it contains: The following options tell Vet how to define a bad boot sector; The first option gives adequate protection, whilst the last gives an extremely high level of protection. The three levels of protection are mutually exclusive. i.e. only one can be chosen.

Known viruses only Causes Vet to consider a boot sector bad only if it contains a known virus.

Invalid boot sector or known virus Causes Vet to consider a boot sector bad if it contains an invalid boot sector or a known virus.

Unknown or invalid boot sector, or known virus

STOP! Replacing unknown boot sectors may cause problems with some backup programs and copy-protected software. You should only use this setting if you are aware of the potential problems. Please call the Vet support line if you have any questions. Causes Vet to consider a boot sector bad if it contains an unknown or invalid boot sector or a known virus.

Replace bad boot sector Causes Vet to replace bad boot sectors. Vet will always warn you before replacing a boot sector.

Check for large IDE driver To determine if a large drive is present Vet uses direct port I/O to read the Extended Boot sector. This will not work on all PCs. The **Check for large IDE driver** allows users to disable this test if it causes problems on their system. This option is not available in VetNT.

Memory (for Vet 95 Only)

Enable Memory Scanning

This dialog enables Vet to monitor resident memory for viruses.

If another anti-viral program is running it may cause false alarms as virus templates may be detected from the other program.

Start-Up

This option allows you to configure how Vet will perform the scans that are performed when you start or reboot your computer.

Run Vet automatically when Windows starts up

This option will enable or disable the Start-up scan option.

Start-up Command

Perform progressive scan (recommended)

This will enable a progressive test which will begin the next test where the last one finished, thus, over a period of days/weeks the entire hard drive will be checked.

Customised Start-up command

This option allows you to configure your own scan using the Vet command line switches.

A summary of the option that you have selected will be displayed at the bottom of the dialog.

The Configure Progressive Scan button allows you to modify the way the progressive scan is performed.

Command Line Switches

Command line switches can be used by selecting **Start | Run…**, typing in the full path and filename (ie. C:\VET\VET95 or C:\VET\VETNT) and adding any of the command line switches that are listed below.

The following switches are available:

Long-form command line options

All options are able to be abbreviated providing the abbreviation is unambiguous and three or more characters in length.

Scanning

/display=full - default, display the main GUI.

/display=progress - show a progress meter of the scan.

/display=notify - hide the progress meter unless infection detected.

/display=none - do not show anything. (replaces /&)

/ext - specify a list of extensions to scan.

Multiple extensions can be delimited like so: /ext=”exe,dll,sys” or

/ext=exe,dll,sys;

/ext=* - scan all files

/ext - scan the default extensions. (replaces /.=)

/resume - begin scan from where the last scan to use /maxfiles ended.

/resume now resumes a user-aborted scan also. (replaces /P)

/maxfiles - specify the number of files to scan. eg.

/maxfiles=1000 (replaces /M=)

/memoryscan - scan memory.

/nomemoryscan - do not scan memory.

/bootscan - scan the boot sector(s).

/nobootscan - do not scan the boot sector(s). (replaces /!S)

/renamed - scan renamed files (*._??).

/norenamed - do not scan renamed files. (replaces /!V)

/fast - scans entry point of each file.

/full - scans every byte of each file. (replaces /F and /!F)

/sub - includes subdirectories in the scan. (replaces /R)

/nosub - does not include subdirectories. (default)

/progressive - triggers the progressive scan (options defined within the program).

/autoscan - equivalent to /progressive (redundant as of 9.60)

Actions

The Action options will specify one of the following values...

clean, rename, reportonly, delete

/infected= - specify the action to be taken on infected files.

/infected=clean

/infected=rename

/infected=delete

/infected=reportonly (replaces /!C, /U, and /Z)

/suspect= - specify the action to be taken on suspected infections.

/suspect=rename

/suspect=delete

/suspect=reportonly (replaces /O, and /Y)

/macro= - specify the action to be taken on infected documents.

/macro=clean

/macro=reportonly

Reporting

/report= - specifies how much information is to be output.

Current available values are:

/report=infected - report only infected files.

/report=all - report all files scanned show all files scanned. (replaces /E)

/logfile - use the default log filename.

/logfile="filename" - specify a log filename.

/nologfile - do not write to a log. (replaces /L and /L=)

Miscellaneous

/exit - VET is to exit on completion of the scan. (replaces /X)

/help - print the command line help. The current /? switch will be kept as it is a fairly standard option.

/cancel - default, allow cancelling of the scan.

/nocancel - disable cancelling of the scan

Any path or logfile name specified on the command line that contains any of the following characters MUST be enclosed in quotes = ; - / (and white space)

Progressive Scan Properties

This dialog allows you to configure how the start-up scan will be performed and what will be reported.

Display

Progress of the scan: This will display Vet and show you the details as the scan is performed.

Nothing unless infected: Vet will not appear unless it has found a problem with a file.

Number of Files to Scan

First boot: This is the number of files that will be scanned when you first start your PC for the day.

Reboots: This is the number of files that will be scanned if you re-boot your PC throughout the day.

Log File

Write log file: By selecting this option you can either select the browse button to specify the name of the log file, or you can type in the path and file name that you wish to call the log file.

Allow Cancellation of Progressive

If this option is NOT selected (NOT ticked) you will not be able to stop the scan until it is finished.

Options | Resident Protection

The Vet suite includes memory resident programs to automatically check files and floppy disks for viruses. Settings for these programs are controlled by this dialog.

The Resident Protection Options dialog is initiated by selecting **Options** | **Resident Protection** from the menu. Each of the dialogs can be entered by selecting the appropriate tab at the top of the dialogs.

Enabling

More information

Floppy boot sectors

More information

File Monitoring

More information

File virus action

More information

Macro virus action

More information

Reporting

More information

Enabling

Enable resident floppy disk boot sector protection

You can configure the floppy disk protection by selecting Options | Resident protection | Floppy Boot Sectors. Resident floppy protection settings

Enable resident file monitor (file & macro protection)

This will allow Vet to automatically check files, documents and spreadsheets for viruses as they are accesses by Windows.

File monitoring

File virus actions

Macro virus actions

Floppy Boot Sector

This dialog controls the checking of floppy boot sectors for viruses. You may choose the level of protection required from the three (mutually exclusive) options. The first option gives adequate protection, whilst the last gives an extremely high level of protection. These options will also contain a message to note if this option is currently loaded.

A known virus Causes Vet to consider a boot sector bad only if it contains a known virus. This is the default level of protection.

An invalid boot, sector or known virus Causes Vet to consider a boot sector bad if it contains an invalid boot sector or a known virus.

An unknown or invalid boot sector, or known virus This option causes Vet to consider a boot sector bad if it contains an unknown or invalid boot sector or contains a known virus.

STOP! Replacing unknown boot sectors may cause problems with some backup programs and copy-protected software. You should only use this setting if you are aware of the potential problems. Please call the Vet support line if you have any questions.

Replace any boot sector considered bad Causes Vet to replace bad boot sectors. Vet will always warn you before replacing a boot sector.

File Monitoring

This dialog controls which events will trigger Vet's automatic file monitors to scan files. There are three events where files may be monitored for viruses. You may enable as many of these options as you wish as they are not mutually exclusive.

An infected file may trigger more than one of the following options. A warning will be issued from each of the options that is activated, so it is possible for a single infected file to create multiple warnings.

Monitor Activation

If the file is infected with a virus it may activate as soon as the file is opened (macro viruses normally infect normal.dot when the infected file is opened). For this reason Opening will automatically be enabled when you select either Executing or Closing if you are using Vet95. VetNT can be fully configured and will allow any configuration to be set by the user.

Executing programs If a virus is found when a Windows application is run the resident protection will prevent the file from running. If the resident protection only suspects a virus is present you will be given the choice of whether or not to run the file.

Opening files Files with extensions specified in the *File types to scan* box of the Options | Program | File types menu are checked for viruses on opening. If a virus is found, you have the option of proceeding.

Closing files Files with extensions specified in the *File types to scan* box of the Options | Program | File Types menu are scanned for viruses on closing. If a virus is found the filename and the name of the virus will appear in the Report window and the log file if it is enabled.

Scan Type

Fast Scan: Causes Vet to examine the entry point and selected areas of a file when checking it for viruses. This is the preferred mode for routine checking of your files and disks as it is both an extremely fast and extremely accurate check for viruses. You can choose either Full Scan or Fast Scan but not both.

Full Scan: Causes Vet to examine every byte of a file when checking it for viruses. This will increase the time the resident protection takes to check your files and disks and is only recommended when you have had (or suspect you may have) a virus.

Scan Network Files

The resident protection can be configured to scan all files that are passed to, or are copied from, the network drive by enabling the Options | Resident Protection | File Monitoring | Scan Network Files. Once this is set every file that is moved to or from the network drive, as you go about your daily business, will be checked for viruses.

File Virus Actions

Action - Infected Files

Report only: Causes Vet to report, but not attempt to clean, infected files.

Report & deny access: Causes Vet to report when an infected file is detected and to lock the file so that it may not be used by other programs.

Clean file: Causes Vet to attempt to disinfect virus-infected files, returning the files to working order. If the file has been infected by an overwriting virus, Vet will delete the file, as no disinfection is possible

Action - Suspected Files

Report only: Causes Vet to report, but not attempt to clean, infected files.

Report & Deny access: Causes Vet to report when an infected file is detected and to lock the file so that it may not be used by other programs.

If this option is viewed form the Vet program is will also have a note to indicate if the option is currently loaded and active.

Macro Virus Actions

By default Vet macro monitoring will check documents and spreadsheets for macro viruses.

A message is included on the bottom of the dialog to let you know if the macro resident protection is currently loaded.

Action - Infected Documents

Select on of the following options to determine what the macro resident protection will do when it detects a Word or Spreadsheet document that is infected with a virus.

Report Only

> Causes the macro resident protection to report when a virus is detected but not attempt to clean the file. Vet will still allow the document to be used so it is likely that the virus will infect your PC. We recommend you do not use this option.

Report and Deny Access

> When an infected document or spreadsheet is detected Vet will report that a virus has been found and not allow you to access the file.

Clean Document

> When an infected document or spreadsheet is detected Vet will remove the virus, return the file to working order and allow access to the file.

Reporting

Write log file

> Selecting this option will cause a log file to be written when suspect or infected files are detected by the resident file protection. The log file will record the filename and path of any infected files, and results of Vet's attempt to clean the files.

SMTP E-Mail Alerting

This dialog allows you to configure the details of the SMTP email message that will be sent when a virus is detected. At the end of the report that is produced during an on-demand scan (when you open Vet and start scanning files), there is a summary of the results. If a virus has been found this summary will be copied into the body of a mail message and sent to the address in the TO: field below.

If all of the fields are grey Email alerting has not been enabled on the Alerting.

Mail Configuration:

> **Mail Server:** The is the Name or TCP/IP address of your mailserver. Please call your Network Administrator if you are unsure what to enter.
>
> **From:** Enter your email address. This is so that when the email is sent it is easy to work out which PC it has come from.

To: Enter the email address of your computer support person that you want the message sent to.

Subject:

This is the Subject line in the email message that will be sent.

Test (send e-mail):

This will send a test message to the person specified in the TO: field. This button is designed to allow you to test that the details you have entered will work when a virus is detected.

Alerting

This dialog allows to enable/disable the sending of an Email message when a virus is detected. (Currently email messages can only be sent via SMTP mail protocol)

On-demand scanner:

By selecting (ticking) the “Alert administrator via e-mail when virus found” option you can send an Email when a virus is detected after you have opened Vet and started scanning files. You must also configure the SMTP Email tab with the details required to send the message.

Resident Protection: (Only available in Vet for Windows NT version 9.5x)

By selecting (ticking) the “Display message box when virus found” option you will be notified if a virus is detected by the resident protection as you go about your daily tasks.

You must also configure the SMTP Email tab with the details required to send the message.

Confirm Configuration Selections

This dialog will display a list with all of the options that the installation intends to install Vet with. If you wish to change the settings; select the <Back button until you see the dialog with the option that you wish to change, modify the option and then select Next> until the Confirm Configuration Sections dialog is once again displayed. Select the Finish button to accept the configuration and complete the installation.

Contact Information

The developers of Vet have always aimed to provide straightforward software that will operate in the background until a virus attempts to infect and damage your PC.

To become a Registered Vet User talk to our sales department or fill in and return the registration card to your nearest Vet supplier.

AUSTRALIA:

Cybec Pty Ltd,
1601 Malvern Rd, Glen Iris 3146, Victoria, Australia. ACN:007229361
Melbourne Customers Phone Support 9825 5656 (8:30 AM to 6:00 PM)
Non Melbourne Phone Support 1800 807 062 (8:30 AM to 6:00 PM)
Fax (+61) 03 9886 0844 Email support@vet.com.au Web: http://www.vet.com.au
Phone Sales 1300 364 750 Email info@vet.com.au

U.K. & EUROPE:

Vet Anti-Virus Software Ltd,
342 Glossop Road, Sheffield, S10 2HW, England.
Phone (+44) 0114 275 7501 Fax (+44) 0114 275 7508
Email support@vetavs.co.uk
Web www.vetavs.co.uk

NEW ZEALAND:

Vet Anti-Virus Software Ltd,
Level 4, 10-12 Scotia Place, Auckland, NZ.
P.O. Box 7429, Wellesley Street, Auckland, NZ
Phone(+64) 9 309 3281 Fax (+64) 9 309 3287
Freecall 0800 838 691
Email sales@vetavs.co.nz

BELGIUM, HOLLAND & LUXEMBOURG:

Data Results Nederland BV
Industrieweg 30, NL-4283 GZ Giessen, The Netherlands
Phone +31 (0)183 449944 (Support: 08:30 to 17:30)
Fax +31 (0)183 449045
Email support@dataresults.nl
Web www.dataresults.nl

MALAYSIA

Vet Anti-Virus Software Sdn Bhd
21-3A Jalan SS 23/15, Taman SEA, Petaling Jaya, 47400 Selangor, Malaysia.
Phone (+60) 03 705 1103 (8:00 AM to 7:00 PM MST)
Fax (+60) 03 705 1203
Email info-asia@vet.com.au

USA: Ontrack Data International Inc.

6321 Bury Drive, Eden Prairie, MN 55346
Phone: General: (+1) 800 872 2599 Sales: (+1) 612 937 5161 Support: (+1) 612 937 2121
Facsimile: (+1) 612 937 5815
Email: sales@ontrack.com
WWW: http://www.ontrack.com

Ontrack US Offices

Los Angeles: 940 South Coast Drive, Suite 225, Costa Mesa, CA 92626
Toll Free: (+1) 800 872 2599 Phone: (+1) 714 641 0530
San Jose: 2001 Gateway Place, Suite 750 West, San Jose, CA 95110-1013
Toll Free: (+1) 800 872 2599 Phone: (+1) 408 573 9592
Washington DC: 2000 Corporate Ridge, 8th Floor, McLean, VA 22102
Toll Free: (+1) 800 872 2599 Phone: (+1) 703 821 8101

Germany: Ontrack Data Recovery GmbH.

Germany: Ontrack Data Recovery GmbH
Phone: Toll Free: 00 800 10 12 13 14 Sales: +49 (0)7031 644 150
Facsimile: +49 (0)7031 644 100
Email: sales@ontrack.de
WWW: http://www.ontrack.com

London: Ontrack Data Recovery Europe Ltd.

The Pavilions, 1 Weston Rd, Kiln Lane, Epsom, Surrey KT17 1JG England.
Phone: Toll Free France: 0 800 90 72 42 Toll Free Europe: 0 800 24 39 96
Office: (+44) 0 1372 741 999 Tech Support (+44) 0 1372 747 414
Facsimile: (+44) 0 1372 747 074
Email: WWW: sales@ontrack.com http://www.ontrack.com

Why Should You Become a Registered Vet User.

This copy of Vet provides protection against all viruses that are known to be in the wild at the time of production. Unfortunately new viruses and new varieties of existing viruses appear on an almost weekly basis. Registered Vet Customers get a comprehensive solution for protection against viruses.

The services and benefits of becoming a registered Vet customer depend on the country where Vet was purchased. Services that are commonly offered are listed below.

1) A full set of user manuals - comprehensive installation and usage details (manuals are available in some boxes of Vet, from the Web site and are also on Vet CDs)
2) Additional installation options for networks and systems administrators
3) Access to the Vet internet web site and Bulletin board service - used to provide updates and general virus information
4) Free unlimited Email and phone support (See the Contact page for the support hours)
5) 48 Hour fixes - If you discover a new virus that Vet does not clean we will provide a solution within 48 hours of receiving a copy of the virus
6) Employee Protection - Any company holding a Vet site licence, that is a licence to install Vet on every PC in the work place, may allow all employees to install Vet on their home-use computers, free of charge.
7) On Site Support - Charges normally apply, but we are committed to supporting our registered Vet users

So, please return the registration card with the appropriate fee or talk to your local Vet sales team.

Command Line Switches

Command line switches can be used by typing in the full path and filename (ie. C:\VET\VET95 or C:\VET\VETNT) and adding any of the command line switches that are listed below.

Long-form command line options

All options are able to be abbreviated providing the abbreviation is unambiguous and three or more characters in length.

Scanning

/display=full - default, display the main GUI.
/display=progress - show a progress meter of the scan.
/display=notify - hide the progress meter unless infection detected.
/display=none - do not show anything. (replaces /&)

/ext - specify a list of extensions to scan.
Multiple extensions can be delimited like so: /ext="exe,dll,sys" or
/ext=exe,dll,sys;
/ext=* - scan all files
/ext - scan the default extensions. (replaces /.=)

/resume - begin scan from where the last scan to use /maxfiles ended.

/resume now resumes a user-aborted scan also. (replaces /P)

/maxfiles - specify the number of files to scan. eg.
/maxfiles=1000 (replaces /M=)

/memoryscan - scan memory.
/nomemoryscan - do not scan memory.

/bootscan - scan the boot sector(s).
/nobootscan - do not scan the boot sector(s). (replaces /!S)

/renamed - scan renamed files (*._??).
/norenamed - do not scan renamed files. (replaces /!V)

/fast - scans entry point of each file.

/full - scans every byte of each file. (replaces /F and /!F)

/sub - includes subdirectories in the scan.
/nosub - does not include subdirectories. (replaces /R)

/progressive - triggers the progressive scan (options defined within the program).

/autoscan - equivalent to /progressive (redundant as of 9.60)

Actions

The Action options will specify one of the following values...
clean, rename, reportonly, delete
/infected= - specify the action to be taken on infected files.

/infected=clean
/infected=rename
/infected=delete
/infected=reportonly (replaces /!C, /U, and /Z)

/suspect= - specify the action to be taken on suspected infections.
/suspect=rename
/suspect=delete
/suspect=reportonly (replaces /O, and /Y)
/macro= - specify the action to be taken on infected documents.
/macro=clean
/macro=reportonly

Reporting

/report= - specifies how much information is to be output.
Current available values are:
/report=infected - report only infected files.

/report=all - report all files scanned show all files scanned. (replaces /E)

/logfile - use the default log filename.
/logfile="filename" - specify a log filename.
/nologfile - do not write to a log. (replaces /L and /L=)

Miscellaneous

/exit - VET is to exit on completion of the scan. (replaces /X)

/help - print the command line help. The current /? switch will be kept as it is a fairly standard option.

/cancel - default, allow cancelling of the scan.

/nocancel - disable cancelling of the scan

Any path or logfile name specified on the command line that contains any of the following characters MUST be enclosed in quotes = ; - / (and white space)

Frequently Asked Questions

Over the years the Cybec support team has compiled a considerable database of support questions. This appendix lists the more common ones, along with their answers.

To make finding questions easier, they are grouped into like categories. Please take the time to read this appendix before ringing Cybec for advice as you may already have the answer you need.

Installation Problems

Viruses

Resident Protection

Error Messages

General

This appendix also contains the common error messages that Vet may display, and what they mean. If Vet reports an error that you do not understand, and which is not listed here, please contact Cybec for advice.

Installation Problems

1) When I run Install, the screen display shows strange border characters and symbols

2) I missed installing one update. Do I have to install the intervening copy of Vet before I install this one?

3) Do I have to delete my previous copy of Vet before I install this one?

4) Why do I have to update at all?

5) When I ran install, it prompted me to delete an existing copy of Vet in a different directory. Should I accept?

6) How do I make a reference disk?

7) I did a Standard Vet installation, but whenever I run Vet the Emergency option on the front screen is disabled. Did I do something wrong?

8) I used Master to configure an automatic installation, but when it runs I get the message 'Unable to copy C:\VET\VET.EXE to C:\VET\VET.EXE', and then the PC hangs.

9) Vet is reporting that the Vet configuration file is damaged or missing. Do I have to reinstall Vet?

10) I have just installed/updated Vet95 and when I reboot and Windows 95 doesn't start properly. What went wrong?

When I run Install, the screen display shows strange border characters and symbols

Install (and Vet) reprogram some of the extended text characters for border, tick, mouse and icon characters. If your screen is in graphics mode, these characters are not reprogrammed, making the display a little odd. This won't cause any problems, but you can avoid it altogether by running ‘INSTALL /D’ to turn off the special characters.

I missed installing one update. Do I have to install the intervening copy of Vet before I installing the latest one?

No. You only ever need to install the latest version of Vet you have. Every Vet disk we distribute is self contained (it holds all the information necessary to install that copy of Vet onto your PC).

Do I have to delete my previous copy of Vet before I install this one?

No. Install actually looks for a previous copy of Vet, and if it finds it will preserve the existing Vet configuration. This not only speeds up the installation process; it also saves you having to recreate your Vet configuration every time you get a new copy.

Why do I have to update at all?

Vet is a scanner based anti-virus product. This means it is constantly being updated to detect and clean new viruses. Even when new copies of Vet don't look any different, they will always detect and clean more viruses than their predecessors. It is for this reason that you should always let a new copy of Vet do a full check of your disk when you install it, and you should try to install every update you receive.

When I ran install, it prompted me to delete an existing copy of Vet in a different directory. Should I accept?

Probably. Early versions of Install would place Vet in whatever directory you happened to be in when you ran Install; it is probably one of these copies Install has found. Check the directory name where the existing copy is located, if you are sure you don't want Vet there, accept. Install will only delete the Vet files (nothing else in the directory will be touched).

How do I make a reference disk?

There are several reasons why you might want to make a reference disk:

- If I skipped that step during Install? or
- mis-typed my name in the User ID field or
- updated my version of DOS, and now every time Vet runs it warns me my Master Boot Record has changed or
- add a password to Vet if I didn't enter one when I installed it?

All four of these questions are concerned with the customisation of Vet to your PC, and are solved in the same way. To 're customise' Vet to your PC, from the Vet Main Menu select Configure | Record System Data. This option prompts you for a password, allows you to alter the User ID, gives you the option of creating a reference disk for your PC and causes Vet to update its configuration file with copies of the current Master Boot Record, DOS Boot Sector and CMOS save information. It will also update the Top of Memory and Load Address values in the Edit Setup | Daily Test | Advanced Features screen.

I did a Standard Vet installation, but whenever I run Vet the Emergency option on the front screen is disabled. Did I do something wrong?

No. This is the default if you run a Standard Installation. If you want to enable the Emergency option, either run a Custom Installation or use Record System Data from the Configuration menu, and enter a password when prompted.

I used Master to configure an automatic installation, but when it runs I get the message 'Unable to copy C:\VET\VET.EXE to C:\VET\VET.EXE', and then the PC hangs.

If the rest of the installation process worked OK, you have probably set the Reference Directory to the same directory as the Install to: directory, causing Install to try to copy Vet over itself. Run Master again and set the Reference Directory to somewhere else (it may be left blank)

Vet is reporting that the Vet configuration file is damaged or missing. Do I have to reinstall Vet?

No. Vet is perfectly capable of generating a new configuration file for itself if the old one has been deleted or damaged in some way. Vet checks the integrity of the configuration file every time it is run, and will offer to create a new one if there is a problem. Simply accept this offer and follow the prompts.

I have just installed/updated Vet95 and when I re boot Windows 95 doesn't start properly, what is wrong??

There are several possibilities, the most common reason is that another anti-virus product (Mcafee) has already been loaded onto you machine and is in conflict with Vet95.

If this is not the problem please contact Cybec for advice.

To fix the clash with Mcafee Anti-Virus:

1.) Reset your computer and press F8 when you see the message "Starting Windows 95..."

2.) This will bring your Setup Menu. Select SAFE MODE (normally third on the list).

3.) From safe mode select the Control Panel and Add/Remove Programs. A number of programs will be displayed, select Mcafee and press the Remove button.

Once Mcafee has been removed from your machine is will return to working order.

Viruses

1) Vet cleaned a virus infection from my PC, but now it is saying that some files may have the same virus it has just cleaned. Are they infected or not?

2) Vet cleaned my files of a virus, but Windows still isn't working properly.

3) Vet deleted my infected files instead of repairing them.

4) When I ran a Full Test, Vet reported a virus in the file 386SPART.PAR or WIN386.SWP.

5) Every time I reboot, Vet tells me that my Top of Memory has changed.

6) Can I get a virus from my CMOS? Can a virus hide in video memory? The printer buffer? Can a virus survive in memory from a cold boot from a clean floppy? Did a lady really have baby spiders hatch out of her neck?

7) When I ran Vet to check my floppy disk, it reported 25 Files, No files were checked. Why didn't Vet check any files?

8) When I boot from my hard drive, Vet finds a virus in memory, but when I boot from floppy it doesn't find any viruses at all on the hard drive.

9) I upgraded to DOS 6 and now Vet says my boot sector has changed.

10) Vet found and disabled XXX virus in memory. It then found the same virus again at almost the same location. If it's already disabled it, how can it find it again?

11) I copied a disk, then ran Vet and it claimed that XXX virus was active in memory.

Vet cleaned a virus infection from my PC, but now it is saying that some files may have the same virus it has just cleaned. Are they infected or not?

Probably not. What you are probably seeing is a ‘dead body’ - a file with a little bit of the virus code still attached to it. It may also be a file that was incorrectly infected, so that the virus wouldn’t ever run. In either case, the safest course is to replace the file with a known clean copy (preferably from the original program disk).

Generally, when a file virus infects a file, it writes its code to the end of the file, and places a jump instruction at the start of the file to ensure that code is executed first. If the amount of code added to the end is variable, Vet may not know exactly where to cut the file, and leaves a small amount of virus attached to the end. The file is no longer infected, but when you run a Full Test Vet may still find it. (A Full Test simply looks at every byte of the file. The default test is an Intelligent Test, which ignores such cases, as the virus is not actually active.)

Vet cleaned my files of a virus, but Windows still isn't working properly.

This is almost certainly because the virus wasn't aware of the Windows New Executable file structure, and has overwritten part of the file as a result. In such a case, Vet can remove the virus, but not restore the code the virus has destroyed. The only option is to replace the damaged files.

The Vet log file records all files that were infected, so it may be possible to do a selective restore of the damaged files.

Vet deleted my infected files instead of repairing them.

This is almost certainly because the files were infected with an overwriting virus. Such viruses do not save the original program code, so no restoration is possible. Replace them with known clean originals.

The other possibility is that you have selected Delete Infected Files in the Handling of Viruses screen for your Vet setup.

When I ran a Full Test, Vet reported a virus in the file 386SPART.PAR or WIN386.SWP.

This is your Windows permanent swap file. What has happened is that a virus has been active in the section of memory Windows memory manager wrote out to disk. Vet will not be able to clean this. You can either delete the file and let Windows regenerate it, or run Windows for a while - the warning should go away as Windows overwrites it.

Every time I reboot, Vet tells me that my Top of Memory has changed.

There are a number of reasons this might happen, and two directions the change may have occurred in.

If Top of Memory has gone up

1. Have you altered your PC's CONFIG.SYS? Some device drivers set Top of Memory down, and removing one (or changing how it runs) may cause this to change.
2. Did you install Vet to an infected PC, or from a command shell instead of the DOS prompt? If there was a virus active in memory when Vet was installed, it almost certainly would have set Top of Memory down. Now that Vet has removed it from the PC, it has gone back up to the correct value. Shelling out of some programs also leads to a decrease in what DOS reports as Top of Memory.

If either of these is the case, exit to DOS, then run DOS Vet and select Configure | Record System Data to record the current Top of Memory.

If Top of Memory has decreased

1. You may have a new virus that Vet doesn't know about. If you suspect this is the case, see the Help Topics on-line help system for details on how to proceed.

However, it is much more likely that you have altered the PC's CONFIG.SYS. See If Top of Memory has gone up.

Can I get a virus from my CMOS? Can a virus hide in video memory? The printer buffer? Can a virus survive in memory from a cold boot from a clean floppy? Did a lady really have baby spiders hatch out of her neck?

No, No, No, No and probably not. These are all Urban Legends. A virus has to be run to become resident in your computer's memory. The CMOS, video memory, and printer buffers are all data storage areas - even if virus code were placed there, it would never be run. And nothing survives in memory from a cold boot. The only thing to watch is that your boot sequence is A, C, so that you are really booting from the floppy. (And of course that you don't have the resume option selected if you are using a laptop that supports this feature). As for the spiders, like the Wrestling, I believed it was real when I was a kid, but these days ...

When I ran Vet to check my floppy disk, it reported “25 Files, No files were checked.”Why didn’t Vet check any files?

By default Vet only checks program files (i.e. files you can run). If you want Vet to check every file on the disk, select Test ALL File Types from the Edit Setup | Current Test | Test Procedures screen.

When I boot from my hard drive, Vet finds a virus in memory, but when I boot from floppy it doesn't find any viruses at all on the hard drive.

Are you running VSAFE, the memory resident component of Microsoft Anti-virus? This program keeps its search strings unencrypted in memory, so that once it is loaded almost any other anti-virus product will report that some virus is active in memory. You don't have a virus - what you are seeing is an incompatibility. We would suggest removing VSAFE.

If the virus Vet reports is Flip Boot, it is almost definitely due to VSAFE. We have not had a valid report of this virus - every single instance has been due to the incompatibility described above.

I upgraded to DOS 6 and now Vet says my boot sector has changed

It has! Run Record System Data from the Configure menu to teach Vet the new boot sector. You should also make a new reference disk.

Vet found and disabled XXX virus in memory. It then found the same virus again at almost the same location. If it's already disabled it, how can it find it again?

Vet uses two different techniques to find viruses - if the location is virtually identical, it is probably finding the same virus using each method. It is also quite possible for more than one copy of a virus to be in memory at the same time. Usually only one copy will be active, but Vet will disable them all, just in case.

Although Vet can safely disable most common viruses, it is always safest to switch your PC off and reboot from a clean, write-protected system disk before you run Vet. This is one reason why we advise you to use the /S option when you format the disk used for the Vet Reference Disk when you install Vet.

I copied a disk, then ran Vet and it claimed that XXX virus was active in memory.

When you read or copy a file or a disk, DOS first loads the relevant sectors into buffers. In most older systems these are in low memory and if you run Vet (or most other scanning programs) after you have accessed an infected file, Vet may find the virus left behind in a buffer. Vet cannot tell whether or not the virus is active, so assumes it is, but, unlike most other programs, Vet is able to disable the virus so that it can finish its job. Always kill any virus Vet finds in memory. If it is only in a buffer it is harmless, but no harm will be done if you kill it.

Resident Protection (Vet-Res) problems

There is resident protection for DOS Vet and for the Vet 3.1x interface. Which one should I use??

The resident protection with Vet for Windows 3.1x is better than Vet_Res due to the “multi tasking” of windows, so please use the resident protection that is in Vet for Windows 3.1x in preference.

For further information call Vet Technical Support

Error Messages

1) Repair was abandoned or Unable to perform repair?

2) Loading address or top of memory has changed. Do you want to continue?

3) VET.EXE appears to have been damaged.

4) System files appear to have been damaged.

5) VET.DAT is corrupted or missing! Re-install Vet from your latest update disk ASAP! Without this file Vet can only find the common viruses.

6) There is not enough memory to load PolySearch. Vet will only be able to find common viruses.

7) VET.CFG is corrupted or missing!

8) Vet has not been installed for this PC. Would you like to install Vet now?

9) Vet can't rename this file. Do you want to delete it?

10) Error has occurred, or virus found. Do you want to keep a log?

11) What are the Error Codes returned by DOS Vet?

Repair was abandoned or Unable to perform repair.

Typically Vet will report this when it is unable to repair an infected (or altered) Master Boot Record or DOS Boot Sector.

On a hard disk this may be because the Master Boot Record is ‘protected’ either by third party software or hardware, or a BIOS option. If you are unsure how to alter BIOS boot protection, please call your supplier or Cybec for advice. It must be disabled to allow Vet to repair the MBR. If it is due to third party hardware or software, refer to their manual for advice.

On a floppy disk, you may get this message because the disk is write protected. Un-write protect the disk and run Vet again to allow the repair.

This message may also appear because the user has selected No or Cancel when Vet was offering to repair an infected (or changed) Boot Sector or file. Run Vet again and read the prompts carefully to accept the repair option.

Loading address or top of memory has changed. Do you want to continue?

When Vet is installed, it customises itself to the PC, recording the current Top of Memory in the Vet configuration file, VET.CFG. By default, Vet only checks this value during the Daily Test (run when the PC boots). If the value has changed, Vet will complain, giving the above message.

If Vet reports a change in Top of Memory, but does not report that a virus is active in memory, it is possible you have a new virus that Vet doesn't recognise. However, it is far more likely that you have changed your system configuration. A number of device drivers (run from your CONFIG.SYS) can cause a change in the Top of Memory - if you know you have just modified this file (installing software can modify it), this is the probable cause.

If Top of Memory has actually increased (Vet will report 'was' and 'is' values) it is definitely not due to a virus. If you know the change is due to changes you have made, run Configure | Record System Data to 'teach' Vet the new Top of Memory. If you can see no reason for the change, ring Cybec for advice.

VET.EXE appears to have been damaged

The main Vet program file, VET.EXE, has failed its integrity check. This may be due to a problem with the disk, but it is most likely that a virus has infected it and is interfering with Vet's attempts to clean itself. Reboot from a known-clean write-protected system disk, and run Vet from your original distribution disk (or your reference disk) to clean the PC.

System files appear to have been damaged

This message indicates that COMMAND.COM (the PC's command processor) has been modified since Vet was installed to the PC. This may be due to a virus, a disk error, or a valid change (such as updating your DOS version).

If you know it is not due to a valid change, the safest course is to replace the file with a known clean copy. If it is due to a valid change, run Configure | Record System Data to 'teach' Vet the new command processor.

VET.DAT is corrupted or missing! Re-install Vet from your latest update disk ASAP! Without this file Vet can only find the common viruses.

VET.DAT is Vet's data file containing templates for all the exotic viruses. Vet can still operate without this file, finding and cleaning all the viruses listed in the Boot Sector and File Viruses sections of the Vet specification, but you should restore the file VET.DAT from your latest Vet disk as soon as you can (you may simply copy this file to the Vet directory).

There is not enough memory to load PolySearch. Vet will only be able to find common viruses.

PolySearch is a statistical algorithm that allows Vet to search for thousands of viruses in a single pass. When Vet is run, it creates the PolySearch table in memory. If there is not enough memory to do this, Vet will still run, finding and removing all the viruses listed in the Boot Sector and File Viruses sections of the Vet specification, but it will not be able to find any of the viruses listed in the PolySearch section of the specification.

The most likely reason for this is that the user has ‘shelled out’ from some other program to run Vet. Exit the program instead, then run Vet again.

VET.CFG is corrupted or missing!

VET.CFG is the Vet configuration file, that holds details of your Vet setup and customised information about your PC. The fact that this file is corrupted or missing could indicate a security breach - i.e. someone may have deliberately deleted it, or a virus targeted against Vet may have removed it.

Vet is able to regenerate the Vet configuration file, but you should investigate why it was deleted.

Vet has not been installed for this PC. Would you like to install Vet now?

You are running a copy of Vet that was copied to your PC rather than installed to it. Select Yes to customise Vet to the PC.

Vet can't rename this file. Do you want to delete it?

If Vet finds an infected file and you have selected the Rename option in Handling of Viruses, Vet will attempt to change the first letter of the file's extension to a 'V'. If a file of this name already exists, Vet will be unable to rename the current file. It thus offers to delete it instead.

If you accept the delete option, Vet will irrevocably overwrite the file and zero its length. Recovery will not be possible. If you choose not to delete the file, you will be leaving a virus infected file on your PC that may be executed.

Error has occurred, or virus found. Do you want to keep a log?

If Vet detects an error (a virus, or some change in the PC's environment), and you have not specified a log file, Vet will stop and offer to write a log.

The log file is a useful record of what went wrong on the PC, and what action Vet took to correct it. Select Yes to write a log file, No to continue without a log of what has occurred.

What are the return codes for DOS Vet?

Install Error Codes

1 User quit the Vet scan before it was finished

2 Reference disk may be invalid

4 Install abandoned by user

8 Vet reported errors (Error level 8 or up)

16 Vet reported a fatal error

32 Install failed

Scanning Error Codes

1 User quit the Vet scan before it was finished

2 Unable to access disk/open file. Often caused by scanning an empty floppy drive

4 The boot sector, Loading address, or Top of memory has changed

8 Virus found in memory (and disabled) or VET.EXE is corrupted

16 Virus found in a program file or a floppy disk boot sector

32 Virus found in the hard disk boot sector

64 Program Virus or floppy boot sector virus found but not fixed

128 Hard disk boot sector not fixed, OR Fatal virus in memory, OR Unable to fix hard disk, OR Virus found but not repaired, OR an error has caused Vet to quit.

General

1) Vet says that my Master Boot Record (MBR) or DOS Boot Sector (DBR) has changed. What does this mean?

2) Am I protected while using the Internet?

3) What is packed with <propriortorial compression algorithm>?

4) What are exotic viruses?

5) How can I tell that automatic protection is installed in Win 95?

6) I have 4 (8,16...256)MB of RAM, but Vet says I have 640K

7) Vet thinks my machine is clean, but says I have only 639K.

8) When I run Vet it says it is out of date.

9) I ran <generic brand> DISK EDITOR and found strange messages on the end of all my files.

10) Everytime I turn on my PC Vet starts up and runs a scan. How do I turn it off?

11) I need to disable Vet as I need to load some new software. How do I turn it off?

Vet says that my Master Boot Record (MBR) or DOS Boot Sector (DBR) has changed. What does this mean?

When Vet reports that the MBR or DBR has changed, it is comparing a snapshot of this information that was taken when you installed Vet, to the current MBR and DBR. Changes may occur when a new operating system is loaded onto the PC.

Also, if you install Vet to a PC that was already infected with a boot sector virus and clean it, Vet will report the boot sector has been changed.

This problem can be fixed by selecting the Configure | Record System Data option from the DOS Vet main menu. Windows 3.x users will need to run DOS Vet to update this option.

Am I protected while using the Internet?

Yes. After you have installed Vet and rebooted your PC, every time you turn on your PC the Vet Resident Protection is loaded into memory. Files can be down-loaded to you PC with any browser. When you attempt to use any file it will be checked for viruses.

What is packed with <propriortorial compression algorithm>?

Many software manufacturers ship their software using compressed files that automatically decompress themselves when the file is run. Vet is able to check the compressed file as it is loaded but is not able to check the decompressed file(s) before they are run. While software manufacturers are normally very vigilant in checking software before it is distributed, it is possible for such a file to contain a compressed virus. If your PC is continually being reinfected by the same virus after you have cleaned the entire drive, it may be because of one of these files. This is why Vet includes an option to report self-extracting files.

What are exotic viruses?

Vet distinguishes between “in-the-wild” viruses (viruses that have been reported from a genuine infection) and “exotic” viruses - viruses we have in our collection, but which we have never seen reported as infecting uses. If Vet says a file “may have” virus X, please send a sample of the file to Cybec. If it is a genuine infection, a removal procedure will be added to Vet and the virus will be upgraded from “exotic” to “in-the-wild” status.

How can I tell that automatic protection is installed in Win 95?

Run Vet95, then select Options | Resident Protection. The box at the bottom of each Resident Protection tab reports the current status of that component of the Resident Protection.

I have 4 (8,16...256)MB of RAM, but Vet says I have 640K.

Vet only reports on the top of Conventional Memory, which stops at 640K. Vet checks explicitly for the few viruses that are able to load into upper memory.

Vet thinks my machine is clean, but says I have only 639K.

Some programs which are installed as device drivers reside at the top of memory, so that the remaining memory is less than expected. Memory managers are a prime example.

When I run Vet it says it is out of date.

Vet records the date when it was installed and warns you if you go on using it after you should have got an update. If you are using an out-of-date version of Vet we strongly advise you to install the latest version to get the maximum possible protection.

It is also possible that your PC's clock is not set correctly. Type 'DATE' and check that it returns the correct value.

I ran <generic brand> DISK EDITOR and found strange messages on the end of all my files.

Something odd happens, the user goes delving with his favourite disk editor and finds garbage or suspicious messages on the end of all his files. What is more, it changes when he or she copies a file to another location. “HELP! VIRUS!” Thankfully, no. MSDOS always allocates an integral number of whole clusters, but the file hardly ever fills the last cluster and the remaining space normally contains random rubbish.

Everytime I turn on my PC Vet starts up and runs a scan. How do I turn it off??

Many users asked for Vet95 to conduct a scan when they start their PC each day. The option to do this has been added to version 9.40 and later. During the installation you will be asked if you would like this option enabled. Once enabled, the Start Up test will scan all executable and document files on the boot drive every time the computer is started.

You can stop the scan at any time by selecting the STOP button from the Vet.

To permanently stop this scan being started select Start | Settings | Taskbar. When the Taskbar dialog appears select the Start Menu Programs tab and the Remove button. Select the Startup Directory, then Vet95 Antivirus and select the Remove button.

I need to disable Vet as I need to load some new software. How do I do it?

This is a dangerous thing to do. When you are loading new “shrink-wrapped” software people tend to believe that the software must be clean because it is direct from the software manufactures. This is not the case. Everytime you load files onto your PC you should have the resident protection running to catch viruses.

If you have tried to load a piece of software and Vet has refused to let you:

1) If the software is on a CD, send it back. Viruses cannot be removed from CDs.

2) If the software is on disks, check that they are write enabled and allow Vet to remove the virus before installing the software.

3) If the resident protection is clashing with the new software. Open Vet and select Options | Enable Resident Protection. Click the check boxes so that they do not have a tick in them and select OK. Close Vet and reboot your PC.

When you have finished loading your software you MUST reverse the process and put a tick in each box to re-activate the resident protection.

Glossary

Unfortunately the computer industry uses a lot of technical terms that the general public has difficulty understanding. Below is a list compiled from customer enquires, if the word or term that you are interested in does not appear below please see the Frequently Asked Questions list or call Vet technical support.

AV short for Anti Virus
CARO short for Computer Anti-virus Research Organisation
Companion viruses
DLL short for Dynamic Link Library
DBR short for DOS Boot Sector (DBR)
Encrypting Viruses
Exotic viruses
File Viruses
GUI short for Graphical User Interface
Heuristic Detection
In the wild
Link viruses
Macro viruses
MBR short for Master Boot Record (MBR)
Multipartite Viruses
NCSA short for National Computer Security Association
OEM short for Original Equipment Manufacture
OLE2 short for Object Linking and Embeding language Version2
Payload
Packed with X
Parasitic viruses
Poly-Morphic Viruses
Reference disk
Resident Protection
Stealth
Trojan Horse
TSR (Terminate and Stay Resident)
VBA5 short for Visual Basic for Applications version 5
Vet_Res
VxD short for Virtual device Driver
Warheads
Worms

CARO (Computer Antivirus Research Organisation)

An informal world wide group of anti viral researchers. If a new virus is found by any of the companies that the researches work for, samples are forwarded to the other members. This allows protection to be built into Vet and other anti viral products before the virus gets to Australia. (Cybec will also forward samples of new Australian viruses to all other members to protect computer users overseas.)

DLL (Dynamic Link Library)
A collection of small programs that can be loaded and used by other programs.

GUI (Graphical User Interface)
A GUI product is one that allows you to “point and click” rather than typing in commands.

NCSA (National Computer Security Association)
A U.S. company that provides quality assurance ratings for products. Vet is NCSA accredited.
For further information see http:\\www.ncsa.com.

OEM (Original Equipment Manufacturer)

This is a mini version of Vet that is often loaded onto new PCs so that when the customer buys a new PC it is guaranteed not to have a virus on it. OEMs are timed to expire after about three months and customers are encouraged to buy a full copy of Vet with regular updates for the latest viruses.

OLE2 (Object Linked and Embebed language version 2)

This language is used to provide the macro functions for MS Word 6.0 and 7.0 documents. The language has been changed in Word97 (MS Word 8.0) to VBA5.

VBA5 (Visual Basic for Applications version 5)

This is the macro language used in Word97 documents. The macro language used for Word 6.0 and 7.0 was OLE2.

VxD (Virtual Device Driver)

When you install a new device into your PC you also need to install a driver so that the operating system can communicate with the new device. A Virtual device driver lets the operating system communicate with a software as if it were a physical hardware device.

Stealth

A virus using stealth techniques takes active measures to hide its presence. For example if you read the boot sector of a disk infected with the Brain virus while it is active, it shows you the original boot sector, not the infected one. Frodo infects files, but the infection cannot be detected while it is active, as it disinfects files before it lets you read them. DIR will show the correct file lengths and programs that monitor checksums will report that infected files have not been modified. Frodo does not trap any interrupts, but instead modifies DOS itself so that monitor programs do not detect any unusual activity. However, these tricks make the virus extremely finicky and it will not run on some PCs and many infected programs will crash.

A few viruses have gone to such lengths to hide themselves that they are called Armoured viruses. The best known of these is the Whale virus. This research virus is multiply encrypted and only decrypts each section immediately before use and then re-encrypts it using a different key. The whole virus is further encrypted, using one of a number of alternative encryption procedures, chosen at random, so that there is no single signature to search for. However, like all armoured vehicles, it is extremely cumbersome and slows an infected PC down so much that it is immediately obvious.

What is Vet_Res (Vet Resident Protection)

When Resident protection is loaded it will automatically check files and floppy disks for viruses as you go about your daily work. Resident Protection is loaded every time you start your PC, unless you specifically requested that it not be loaded during installation.

The level of protection can be modified from the Resident Protection dialog. See the on-line Help topics in your version of Vet for further details as the method for altering these settings is different for each operating system.

What is a TSR? (Terminate and Stay Resident)

VET_RES is a resident (TSR) version of VET. It loads itself into memory when you boot (start) your computer and does not stop checking until the PC is turned off. Vet_Res is a memory resident scanner that offers a number of levels of active virus protection. Unless a virus is discovered, VET_RES is invisible in operation and relatively cheap in memory use, as it works in conjunction with VET, which it invokes if a virus is discovered. VET_RES uses the same search strings as basic VET (ie. It does not look for exotic viruses) and requires only between 7 and 26K of memory to operate. There is (of course) a cost to this added protection. TSRs not only reduce available memory - they can also clash with other TSRs, causing the PC to hang, or behave in an unpredictable manner.

File Viruses

Although there are a lot of different ways of grouping and classifying viruses, we can say that file viruses are those viruses which spread via files that are either executable or contain executable components.

File viruses can be further divided into the following groups:

- Parasitic viruses
- Companion viruses
- Link viruses
- Macro viruses

Parasitic Viruses

These represent the majority of all file viruses and they spread by modifying the code of executable programs. A parasitic virus attaches itself to an executable file and changes its contents in order to activate itself as soon as the operating system tries to execute an infected program.

Since there are a few ways in which a virus can attach its code to another file, we can subdivide still further, into overwriting, appending, prepending and inserting viruses. An overwriting virus simply overwrites the beginning of the file so that the infected file doesn't change its length but it no longer runs. Because of their destructive nature, overwriting viruses are relatively easy to detect and are not very common.

Appending and prepending viruses add their code to the start or the end of the file (respectively) and redirect the entry of the infected program to the start of the virus code. In that way infected programs increase in length but since the virus can pass control to the original program, the difference between executing a clean and an infected file is hard to notice.

Inserting viruses place their code (in one or more blocks) inside infected programs. They can search for an unused area (eg headers of .EXE files) or split the files and add their code in between the blocks of the infected file.

Companion Viruses

These take advantage of the DOS system's feature related to the sequence of loading and executing programs. If the file specified for execution has no extension, the system always tries to execute fname.COM, then fname.EXE and at last fname.BAT. A companion virus infects .EXE file by copying itself to a file with the same name but with .COM extension and.' usually hidden attributes. If the user enters the fname command, the file fname.COM (ie the virus) will be executed first.

A companion virus doesn't modify the infected program and usually passes control to the original .EXE file, but once detected it is easy to clean - you simply delete the relevant .COM file.

Link Viruses

These infect programs by changing information in the directory structure and modifying the file pointers, so every infected program starts at the same location (usually the last cluster on the disk) which contains virus code. Cleaning disks infected with a link virus requires a specific approach.

Every file virus can incorporate different techniques to improve the infection rate or to avoid detection. Each of the above viruses can be memory-resident, can have stealth capabilities, can use encryption or can use a polymorphic engine.

Macro Viruses

Technically another form of parasitic virus, the thing that makes macro viruses rate a class of their own is that they are transmitted as an executable component in an otherwise non- executable data file. All known macro viruses to date are written in WordBasic (Microsoft Word's macro language) or VBA (the macro language developed for other Microsoft products).

Macros are executable code intended to automate tasks in applications. However the underlying macro language is extremely powerful, and can call out to external programs, making macro viruses potentially quite dangerous. They are also the first "platform independent" virus, in that they will run on Macintosh computers as well as PCs. Another way of looking at it is that they depend on Word as their platform. Macro viruses have rapidly become the most reported viruses in the world.

Multi-Partite Virus

This is a virus that infects both boot sectors and executable files and exhibits characteristics of both boot sector and parasitic viruses.

Encrypting Virus

This is a virus which hides its code or even a whole infected file by encrypting it. The only plain text that can be seen inside an infected file is a decrypting procedure.

Polymorphic Virus

This is a self-modifying encrypting virus. Polymorphic viruses incorporate a special algorithm to create many different-looking copies of the same virus. Every next generation of a polymorphic virus can look slightly or even completely different from the previous one. The majority of new polymorphic viruses use specially designed libraries (engines) containing subroutines to produce different encryption schemes and encryption keys. The most famous polymorphic engines are:

DAME or MTE (Dark Avenger Mutation Engine);

TPE (Trident Polymorphic Engine);

SMEG (Simulated Metaphoric Encryption Generator).

Trojan Horse

This is a program that doesn't replicate and doesn't infect any other executable files and whose execution will result in undesired (often destructive) effects.

Worm

This is a program that distributes multiple copies if itself across the system. The most famous was the Internet Worm, which in 1988 virtually shut down the Internet in the US. It exploited holes in the Unix sendmail and finger programs. information Virus A rumour of a virus that becomes so widespread that its effects are similar to that of a real virus (at least in terms of system resources being used). The best known is the Good Times virus.

Warheads (Also known as Payload)

The first virus writers were content with proving that they could write a virus, but later writers have become more ambitious and added a payload. This can be a taunt (Your Computer is now Stoned!) or it may interfere with the operation of the computer in an amusing, irritating, or destructive manner. Again there is a conflict between the desire to show off and the need to be inconspicuous, so that the virus will propagate widely. This is usually achieved by making the payout wait some time or depend on some rather unusual event, so that the virus does not declare itself until it has had a chance to propagate. It is generally unwise to deliberately trigger a virus's warhead; we know of at least one user who was infected with the Michelangelo virus who advanced his system clock to March 6th just to see what would happen and thereby lost the data on his hard disk. Even joke viruses aren't funny when they go wrong on a non-standard PC.

Heuristic Detection

Heuristic or generic scanning is a technique for detecting viruses that instead of using specific virus templates and signatures, performs analysis of virus structure and behaviour. The advantage of Heuristic Detection is that it can catch unknown viruses - the disadvantage is that it requires a high level of user expertise to use it correctly, and is prone to false alarms.

Password

The password can be invoked by either selecting **Options** | **Password protect options**, or **Tools** | **Emergency.**

Options | Password protect options:

This feature is in Vet95 and VetNT because many system administrators asked that we provide password protection to stop unauthorised alterations to the Vet configuration. The password protection can be enabled by selecting Options | Password Protect Options and entering a password. This option can also be set while configuring a network installation so that the password will be the same on every workstation that is updated from the server.

The password protection of the Options menu can be disabled by selecting Options | Password Protect Options and entering the correct password. (The password protection for the Tools | Emergency menu is not affected by disabling the Options menu password).

Tools | Emergency:

The re-installation of an old template could cause files to be lost if the drive structure was changed after the template was made. For this reason the ability to re-install templates is protected with a password.

The Emergency Password dialog will appear when the **Tools | Emergency** functions menu is selected. It prompts for a password to allow access to the emergency options, and will continue to prompt until the correct password is entered.

NOTE: If no password was set when Vet was installed the default password **VET** will be used. Enter the password then select OK

The password entered is case dependant, so an “a” is not the same as an “A”.

Scan Type

Full Scan: Causes Vet to examine every byte of a file when checking it for viruses. This will increase the time Vet takes to check your files and disks and is only recommended when you have had (or suspect you may have) a virus. You can choose either Full Scan or Fast Scan but not both.

Fast Scan: Causes Vet to examine the entry point and selected areas of a file when checking it for viruses. This is the preferred mode for routine checking of your files and disks as it is both an extremely fast and extremely accurate check for viruses. You can choose either Full Scan or Fast Scan but not both.

Include subfolders

Skip renamed files

Show network drives

Include Subfolders/Skip renamed files/ Show network drives

Include subfolders: Causes Vet to check the subdirectories or subfolders of the current directory or folder.

Skip renamed files: Causes Vet not to check those files which have been renamed by Vet during previous scans. Renaming will occur if the default in **Options** | **Program | Actions** is set to Rename and a suspect file is found. The file extension will be changed so that the first letter will be an underscore. So .exe will become ._xe.

Show network drives: If your PC is attached to a network and this option is enabled the network drives will be displayed (and can be scanned) in the Browser.

Enabling this option will also cause files that are stored on network drives to be scanned by the resident protection before they are used by the PC.

File Types to Scan

All files: Causes Vet to check *every* file it encounters for viruses. You can choose either All files or Files of these types, but not both.

Files of these types: Causes Vet to check files that it considers to be executable (or 'runable'). By default Vet considers files with the .XLS, .XLT, .BIN, .COM, .DLL, .DRV, .EXE, .OVL, .DOC, .DOT and .SYS extensions to be executable. You can choose either All files or Executable only but not both.

Add: Allows you to add to the list of file extensions Vet will consider executable. With the advent of Macro language viruses, it is now possible for a file with any extension to contain a virus that can infect your PC. Selecting this button causes an input window to appear. You then have the opportunity to enter the new file name extension in the type-in box.

Delete: If you select a file extension from the displayed list and press this button, the file extension will be removed from the list that Vet considers executable.

Default: Restores the default list of file extensions Vet considers executable. (.XLS, .XLT, .BIN, .COM, .DLL, .DRV, .EXE, .OVL, .DOC, .DOT and .SYS extensions)

Add Vet to 'right-click' menus for these file types: If this option is selected and you are using MS explorer (or other navigation tool) you can select a file, directory or drive, right click the mouse button, and Vet will scan your selection.

Infected & Suspect Program Files:

The following mutually exclusive options are available for actions dealing with infected files.

STOP! If you chose for files to be **Clean**ed and a file has been infected with an overwriting virus , Vet will offer to ignore, rename or delete the file, as no disinfection is possible. By default Vet will offer to delete the file.

Report only: Causes Vet to report, but not attempt to clean, infected files.

Clean: Causes Vet to attempt to disinfect virus-infected files, returning the files to working order. If the file has been infected by an overwriting virus, Vet will **Delete** the file, as no disinfection is possible

Rename: Causes Vet to change the first letter of the extension of any file infected with a virus to an underscore '_' (.EXE becomes ._XE). This allows you to keep the file for further examination, without the risk of accidentally running it.

Delete: Delete causes Vet to delete irreversibly any file that it finds has been infected with a virus. The file is first overwritten with 'D's and then set to zero length, so no recovery of the deleted files is possible.

STOP! Use this option with caution, as there is no possibility of recovering files deleted in this manner.

Suspect Program Files:

The following mutually exclusive options are available for dealing with files suspected to contain a virus.

Report only: Causes Vet to report, but not attempt to clean, infected files.

Rename: Causes Vet to change the first letter of the extension of any file suspected of infection with a virus to an underscore '_' (.EXE becomes ._XE). This allows you to keep the file for further examination, without the risk of accidentally running it.

Delete: Delete causes Vet to delete irrevocably any file that it finds has been infected with a virus. The file is first overwritten with 'D's and then set to zero length, so no recovery of the deleted files is possible.

STOP! Use this option with caution, as there is no possibility of recovering files deleted in this manner.

Overwriting Viruses

Most viruses are careful not to destroy the infected file, but overwriting viruses overwrite part of the infected file, so that it will no longer operate. However, this makes these viruses extremely obvious, so they are unlikely to spread far.

The Zeroto-0, or Australian 403 virus, is of this type. When an infected file is run, the virus searches for an uninfected .COM file and replaces it with a 403 byte file which only contains the virus. The original file is destroyed, so infected files appear to run, but do nothing.

Suspect Program Files:

The following mutually exclusive options are available for dealing with files suspected to contain a virus.

Report only: Causes Vet to report, but not attempt to clean, infected files.

Rename: Causes Vet to change the first letter of the extension of any file suspected of infection with a virus to an underscore '_' (.EXE becomes ._XE). This allows you to keep the file for further examination, without the risk of accidentally running it.

Delete: Delete causes Vet to delete irrevocably any file that it finds has been infected with a virus. The file is first overwritten with 'D's and then set to zero length, so no recovery of the deleted files is possible.

STOP! Use this option with caution, as there is no possibility of recovering files deleted in this manner.

Infected Document Files:

The following mutually exclusive options are available for dealing with documents or spread sheets that contain a macro virus.

Windows97 has a different file structure to the documents and spreadsheets created by earlier versions of Word and Excel. This new structure (VBA5) requires a different method for detecting and cleaning the viruses.

The good news is that all of this is now transparent to you the user!

Vet95 and VetNT can automatically detect and clean all Word97 macro viruses as well as the Laroux Excel macro virus.

Report only: Causes Vet to report, but not attempt to clean, infected files.

Clean: The file will be cleaned, and if possible, returned to working order.

Reporting

This dialog controls what will be displayed in the Report window and written to the log file.

All files scanned: Causes Vet to display on a separate line the name of each file it tests (which in turn causes the name of every file tested to be written to the log file, regardless of whether it had a virus or not). This is useful in explicitly identifying which files are *not* infected (Vet uses a separate line for each infected file).

Infected or suspect: Causes Vet to report on a separate line the name of each file it finds to be suspected or infected.

The *All files scanned* and *Infected or suspect* options tell Vet which file names are to be listed in the Report window. These two options are mutually exclusive.

Write log: The name of the log file to which all scan results are written is displayed in the type-in box. The location of the log file can be changed using the Browse button to select an existing file or allow the entry a new file name.

Cumulative report: If this option is enabled the results of each scan will be stored cumulatively in the log file. If it is NOT enabled the log file will be cleaned and overwritten each time a scan is performed.

Limit log size to: Once you perform a scan and the file becomes larger than (the default) 32Kb it will automatically be truncated by removing the oldest information first.

Suppress 'Out-of-date' warning

NOTE: As the log file has to be able to be edited in DOS the name MUST NOT contain: spaces, unprintable characters or contain sub-directory names longer than eight characters.

Display ‘Out-of-date’ Warning

Around four months after you have installed the latest copy of Vet it will display a message to let you know that it is now out of date and to remind you to load the next upgrade. If you are not able to load the next upgrade this option allows you to disable the message.

This option can be enabled/disabled by opening Vet and selecting Options | Program | Reporting and modifying the ‘Suppress Out-Of-Date option’.

Boot Sectors

This dialog sets up the defaults for the treatment of boot sectors.

Scan boot sectors Allows Vet to scan boot sectors. Turning this option off causes all the other options in this dialog box to become inactive.

Consider a boot sector bad if it contains: The following options tell Vet how to define a bad boot sector; The first option gives adequate protection, whilst the last gives an extremely high level of protection. The three levels of protection are mutually exclusive. i.e. only one can be chosen.

Known viruses only Causes Vet to consider a boot sector bad only if it contains a known virus.

Invalid boot sector or known virus Causes Vet to consider a boot sector bad if it contains an invalid boot sector or a known virus.

Unknown or invalid boot sector, or known virus

STOP! Replacing unknown boot sectors may cause problems with some backup programs and copy-protected software. You should only use this setting if you are aware of the potential problems. Please call the Vet support line if you have any questions. Causes Vet to consider a boot sector bad if it contains an unknown or invalid boot sector or a known virus.

Replace bad boot sector Causes Vet to replace bad boot sectors. Vet will always warn you before replacing a boot sector.

Check for large IDE driver To determine if a large drive is present Vet uses direct port I/O to read the Extended Boot sector. This will not work on all PCs. The **Check for large IDE driver** allows users to disable this test if it causes problems on their system. This option is not available in VetNT.

Memory (for Vet 95 Only)

Enable Memory Scanning

This dialog enables Vet to monitor resident memory for viruses.

If another anti-viral program is running it may cause false alarms as virus templates may be detected from the other program.

Start-Up

This option allows you to configure how Vet will perform the scans that are performed when you start or reboot your computer.

Run Vet automatically when Windows starts up

This option will enable or disable the Start-up scan option.

Start-up Command

Perform progressive scan (recommended)

> This will enable a progressive test which will begin the next test where the last one finished, thus, over a period of days/weeks the entire hard drive will be checked.

Customised Start-up command

> This option allows you to configure your own scan using the Vet command line switches.

A summary of the option that you have selected will be displayed at the bottom of the dialog.

The Configure Progressive Scan button allows you to modify the way the progressive scan is performed.

Command Line Switches

Command line switches can be used by selecting **Start | Run…**, typing in the full path and filename (ie. C:\VET\VET95 or C:\VET\VETNT) and adding any of the command line switches that are listed below.

The following switches are available:

Long-form command line options

All options are able to be abbreviated providing the abbreviation is unambiguous and three or more characters in length.

Scanning

/display=full - default, display the main GUI.
/display=progress - show a progress meter of the scan.
/display=notify - hide the progress meter unless infection detected.
/display=none - do not show anything. (replaces /&)

/ext - specify a list of extensions to scan.
Multiple extensions can be delimited like so: /ext="exe,dll,sys" or
/ext=exe,dll,sys;
/ext=* - scan all files
/ext - scan the default extensions. (replaces /.=)

/resume - begin scan from where the last scan to use /maxfiles ended.
/resume now resumes a user-aborted scan also. (replaces /P)

/maxfiles - specify the number of files to scan. eg.
/maxfiles=1000 (replaces /M=)

/memoryscan - scan memory.
/nomemoryscan - do not scan memory.

/bootscan - scan the boot sector(s).
/nobootscan - do not scan the boot sector(s). (replaces /!S)

/renamed - scan renamed files (*._??).
/norenamed - do not scan renamed files. (replaces /!V)

/fast - scans entry point of each file.
/full - scans every byte of each file. (replaces /F and /!F)

/sub - includes subdirectories in the scan.
/nosub - does not include subdirectories. (replaces /R)

/progressive - triggers the progressive scan (options defined within the program).
/autoscan - equivalent to /progressive (redundant as of 9.60)

Actions

The Action options will specify one of the following values...
clean, rename, reportonly, delete

/infected= - specify the action to be taken on infected files.
/infected=clean
/infected=rename
/infected=delete
/infected=reportonly (replaces /!C, /U, and /Z)

/suspect= - specify the action to be taken on suspected infections.
/suspect=rename
/suspect=delete
/suspect=reportonly (replaces /O, and /Y)
/macro= - specify the action to be taken on infected documents.
/macro=clean
/macro=reportonly

Reporting

/report= - specifies how much information is to be output.
Current available values are:
/report=infected - report only infected files.
/report=all - report all files scanned show all files scanned. (replaces /E)

/logfile - use the default log filename.
/logfile="filename" - specify a log filename.
/nologfile - do not write to a log. (replaces /L and /L=)

Miscellaneous

/exit - VET is to exit on completion of the scan. (replaces /X)

/help - print the command line help. The current /? switch will be kept as it is a fairly standard option.

/cancel - default, allow cancelling of the scan.
/nocancel - disable cancelling of the scan

Any path or logfile name specified on the command line that contains any of the following characters MUST be enclosed in quotes = ; - / (and white space)

Progressive Scan Properties

This dialog allows you to configure how the start-up scan will be performed and what will be reported.

Display

Progress of the scan: This will display Vet and show you the details as the scan is performed.

Nothing unless infected: Vet will not appear unless it has found a problem with a file.

Number of Files to Scan

First boot: This is the number of files that will be scanned when you first start your PC for the day.

Reboots: This is the number of files that will be scanned if you re-boot your PC throughout the day.

Log File

Write log file: By selecting this option you can either select the browse button to specify the name of the log file, or you can type in the path and file name that you wish to call the log file.

Allow Cancellation of Progressive

If this option is NOT selected (NOT ticked) you will not be able to stop the scan until it is finished.

Options | Resident Protection

The Vet suite includes memory resident programs to automatically check files and floppy disks for viruses. Settings for these programs are controlled by this dialog.

The Resident Protection Options dialog is initiated by selecting **Options** | **Resident Protection** from the menu. Each of the dialogs can be entered by selecting the appropriate tab at the top of the dialogs.

Enabling

More information

Floppy boot sectors

More information

File Monitoring

More information

File virus action

More information

Macro virus action

More information

Reporting

More information

Enabling

Enable resident floppy disk boot sector protection

You can configure the floppy disk protection by selecting Options | Resident protection | Floppy Boot Sectors. Resident floppy protection settings

Enable resident file monitor (file & macro protection)

This will allow Vet to automatically check files, documents and spreadsheets for viruses as they are accesses by Windows.

- File monitoring
- File virus actions
- Macro virus actions

Floppy Boot Sector

This dialog controls the checking of floppy boot sectors for viruses. You may choose the level of protection required from the three (mutually exclusive) options. The first option gives adequate protection, whilst the last gives an extremely high level of protection. These options will also contain a message to note if this option is currently loaded.

A known virus Causes Vet to consider a boot sector bad only if it contains a known virus. This is the default level of protection.

An invalid boot, sector or known virus Causes Vet to consider a boot sector bad if it contains an invalid boot sector or a known virus.

An unknown or invalid boot sector, or known virus This option causes Vet to consider a boot sector bad if it contains an unknown or invalid boot sector or contains a known virus.

STOP! Replacing unknown boot sectors may cause problems with some backup programs and copy-protected software. You should only use this setting if you are aware of the potential problems. Please call the Vet support line if you have any questions.

Replace any boot sector considered bad Causes Vet to replace bad boot sectors. Vet will always warn you before replacing a boot sector.

File Monitoring

This dialog controls which events will trigger Vet's automatic file monitors to scan files. There are three events where files may be monitored for viruses. You may enable as many of these options as you wish as they are not mutually exclusive.

An infected file may trigger more than one of the following options. A warning will be issued from each of the options that is activated, so it is possible for a single infected file to create multiple warnings.

Monitor Activation

If the file is infected with a virus it may activate as soon as the file is opened (macro viruses normally infect normal.dot when the infected file is opened). For this reason Opening will automatically be enabled when you select either Executing or Closing if you are using Vet95. VetNT can be fully configured and will allow any configuration to be set by the user.

Executing programs If a virus is found when a Windows application is run the resident protection will prevent the file from running. If the resident protection only suspects a virus is present you will be given the choice of whether or not to run the file.

Opening files Files with extensions specified in the *File types to scan* box of the Options | Program | File types menu are checked for viruses on opening. If a virus is found, you have the option of proceeding.

Closing files Files with extensions specified in the *File types to scan* box of the Options | Program | File Types menu are scanned for viruses on closing. If a virus is found the filename and the name of the virus will appear in the Report window and the log file if it is enabled.

Scan Type

Fast Scan: Causes Vet to examine the entry point and selected areas of a file when checking it for viruses. This is the preferred mode for routine checking of your files and disks as it is both an extremely fast and extremely accurate check for viruses. You can choose either Full Scan or Fast Scan but not both.

Full Scan: Causes Vet to examine every byte of a file when checking it for viruses. This will increase the time the resident protection takes to check your files and disks and is only recommended when you have had (or suspect you may have) a virus.

Scan Network Files

The resident protection can be configured to scan all files that are passed to, or are copied from, the network drive by enabling the Options | Resident Protection | File Monitoring | Scan Network Files. Once this is set every file that is moved to or from the network drive, as you go about your daily business, will be checked for viruses.

File Virus Actions

Action - Infected Files

Report only: Causes Vet to report, but not attempt to clean, infected files.

Report & deny access: Causes Vet to report when an infected file is detected and to lock the file so that it may not be used by other programs.

Clean file: Causes Vet to attempt to disinfect virus-infected files, returning the files to working order. If the file has been infected by an overwriting virus, Vet will delete the file, as no disinfection is possible

Action - Suspected Files

Report only: Causes Vet to report, but not attempt to clean, infected files.

Report & Deny access: Causes Vet to report when an infected file is detected and to lock the file so that it may not be used by other programs.

If this option is viewed form the Vet program is will also have a note to indicate if the option is currently loaded and active.

Macro Virus Actions

By default Vet macro monitoring will check documents and spreadsheets for macro viruses.

A message is included on the bottom of the dialog to let you know if the macro resident protection is currently loaded.

Action - Infected Documents

Select on of the following options to determine what the macro resident protection will do when it detects a Word or Spreadsheet document that is infected with a virus.

Report Only

> Causes the macro resident protection to report when a virus is detected but not attempt to clean the file. Vet will still allow the document to be used so it is likely that the virus will infect your PC. We recommend you do not use this option.

Report and Deny Access

> When an infected document or spreadsheet is detected Vet will report that a virus has been found and not allow you to access the file.

Clean Document

> When an infected document or spreadsheet is detected Vet will remove the virus, return the file to working order and allow access to the file.

Reporting

Write log file

Selecting this option will cause a log file to be written when suspect or infected files are detected by the resident file protection. The log file will record the filename and path of any infected files, and results of Vet’s attempt to clean the files.

SMTP E-Mail Alerting

This dialog allows you to configure the details of the SMTP email message that will be sent when a virus is detected. At the end of the report that is produced during an on-demand scan (when you open Vet and start scanning files), there is a summary of the results. If a virus has been found this summary will be copied into the body of a mail message and sent to the address in the TO: field below.

If all of the fields are grey Email alerting has not been enabled on the Alerting.

Mail Configuration:

Mail Server: This is the Name or TCP/IP address of your mailserver. Please call your Network Administrator if you are unsure what to enter.

From: Enter your email address. This is so that when the email is sent it is easy to work out which PC it has come from.

To: Enter the email address of your computer support person that you want the message sent to.

Subject:

This is the Subject line in the email message that will be sent.

Test (send e-mail):

This will send a test message to the person specified in the TO: field. This button is designed to allow you to test that the details you have entered will work when a virus is detected.

Alerting

This dialog allows to enable/disable the sending of an Email message when a virus is detected. (Currently email messages can only be sent via SMTP mail protocol)

On-demand scanner:

> By selecting (ticking) the “Alert administrator via e-mail when virus found” option you can send an Email when a virus is detected after you have opened Vet and started scanning files. You must also configure the SMTP Email tab with the details required to send the message.

Resident Protection: (Only available in Vet for Windows NT version 9.5x)

> By selecting (ticking) the “Display message box when virus found” option you will be notified if a virus is detected by the resident protection as you go about your daily tasks.

You must also configure the SMTP Email tab with the details required to send the message.

Confirm Configuration Selections

This dialog will display a list with all of the options that the installation intends to install Vet with. If you wish to change the settings; select the <Back button until you see the dialog with the option that you wish to change, modify the option and then select Next> until the Confirm Configuration Sections dialog is once again displayed. Select the Next> button to accept the configuration and complete the installation.

Online Registration For New Customers

If you are installing Vet for the first time and are not yet a registered Vet user you can select “Yes, please register me now” and, provided you have a modem and Internet access, you will be connected to the registration section of the Vet web page. Once you have filled in all the details, select the submit button to send the information to us. Your Vet Customer Number will be displayed. Copy down this number as you will need it to get access to the download area. You can record it by selecting Options | Options Wizard and filling in the Customer Details dialog. Once you have entered your details here you can view them at any time by selecting Help | About...

If you wish to register at a later date then select “No, do not register now” and select Run | Programs | Vet Anti-Virus for Windows | Web Update & Tech Support, then select Online Registration and enter your details when you are ready to register. NOTE: It is not necessary to enter your customer number to successfully complete the Vet installation. It is possible to enter your customer number at a later date by opening Vet and selecting Options | Options Wizard and running through all of the screens till you find the customer details dialog.

Once you have entered your customer number and other details it will be displayed in the About box (Open Vet and select Help | About...).

You will need to know these details if you call the Vet Technical Support department.