Introducing Vet

Roger Riordan

Roger Riordan graduated from Melbourne University in 1954. After working at CSIRO, he started Cybec Electronics in 1973 and designed a wide range of industrial equipment. He joined Chisholm Institute of Technology as a lecturer in Electronics in 1983 and wrote the first version of Vet in 1989 when their PCs were infected by the Stoned virus. Vet was distributed to the students as shareware and rapidly spread throughout Australia. At the end of 1989, Roger resigned from Chisholm to work on Vet full time. Vet is now officially installed on thousands of PCs and many major organisations have site licences. VET ANTI-VIRUS now has twenty staff in Melbourne, offices in Adelaide and Sydney, and a number of distributors in other parts of the world.

Roger began programming in FORTRAN in 1966 at CSIRO. He has written many technical papers and holds a number of patents. In 1968 he described the first gyrator using op-amps and designed the *Loop-A-Line*, adopted by Australia and New Zealand Telecom's as standard equipment. Roger is married with three grown up children. He is a lapsed climber and bushwalker and is interested in native plants and the outdoors.

About Vet

Vet is a suite of programs for protecting your computer/s from viruses which if left undetected could damage your data and thus cost you considerable time and money.

Vet originated and is developed and marketed in Australia by CYBEC Pty Ltd. We believe that the success of a computer software product lies in the ability to provide fast, expert product support and to solve any customer problems as soon as they arise. Since much of VET ANTI-VIRUS's business comes from renewals, customer satisfaction is of paramount importance. VET ANTI-VIRUS's response time to a new virus has always been less than 48 hours.

Vet users include several Australian Universities, including Monash, Sydney, Adelaide, Melbourne and the Victoria University of Technology, the University of Manchester, other schools and colleges, including all of the Victorian Colleges of TAFE; many large corporate companies, including ANZ McCaughan, Westfield Shopping Centres, IOOF, Canon, Colonial Mutual Life Australia, Yellow Pages and Australia Post; many government departments including the Department of Food and Agriculture, the Department of Veterans' Affairs, the Department of Primary Industry; finally, a large number of private PC users subscribe to Vet.

About CYBEC

CYBEC Pty Ltd was started in 1989 by Roger Riordan.

Cybec has always aimed to provide straightforward software that will operate in the background until a virus attempts to infect and damage your PC.

Vet Anti-Virus Software is designed and written by Cybec Pty Ltd based in Melbourne Australia.

To become a registered Vet User, simply fill in the application card, attach the appropriate fee and return it to Cybec. Alternatively, talk to our sales department for further information.

Updating Vet

Every registered user of Vet is entitled to quarterly updates for one year. If you bought your copy of Vet from a retail outlet, in order to receive your updates, you will need to fill in and return the registration card (which you will find in the box) so that we know where to send them. Your updates will be supplied to you on the media size that you nominate. You install these in the same way as the original copy of Vet.

Out of Date Message

New viruses are written all the time, and Vet is continually updated to handle these. If the version you are using is out of date, a warning message will be displayed every time you use Vet, reminding you to install the latest update. This message can be disabled by opening Vet and selecting Options | Program | Reporting | Suppress out-of-date warning.

Technical Information

Vet uses the Polysearch algorithm and for each virus looks for a carefully chosen string at a specific location. It checks the boot sectors of floppy and hard disks and automatically removes known viruses. It also checks all executable files on any disk and recovers infected files. Vet contains templates for many common disk boot sectors and when installed on your machine(s) it will recognise the boot sectors for your disks and will detect and rectify any change in them. Recovered files will almost always work correctly, apart from a few cases where the virus has already damaged the file. Vet checks memory for active viruses and disables them. Vet is not memory resident.

Vet_RES Command Line Options

How Vet Works

Generic Virus Detection

Vet offers significant generic protection against unknown viruses. Vet warns the user if changes are detected in the Master Boot Record or if the top of memory has been changed. If such symptoms should appear on your PC at any time, we strongly recommend that you run a Full Scan on your drive if you are still experiencing problems then please contact Vet Anti-Virus for further advice.

Vet Utilities

Vet Utilities are additional programs which provide a number of functions for the user to detect unknown viruses and check their Vet software has not been corrupted.

Vet Utilities include the following:

VERIDISK

Veridisk is used to ensure that the Vet distribution disk has not been damaged. When we prepare the disk, we use a companion program VALIDISK, which calculates CRC checksums for the disk and embeds them in it. When you run VERIDISK, it calculates checksums for each part of a floppy disk and compares them with pre-recorded validation data, if this is present. VERIDISK is provided mainly so that it can be used with HUNT for trapping viruses. VALIDISK, which can be used to add validation data to any disk, is available as a separate product. Please ask for further information if you are interested in this facility.

HUNT

HUNT is a batch program which traps viruses. HUNT runs two programs to act as bait and then runs VERIDISK to see if the disk has been changed. See: Using Hunt

VET_TRAP

This is a program which writes copies of the Master Boot Record, the DOS boot sector and the top of memory to a disk in drive A. It can be used in conjunction with HUNT and VERIDISK to capture new viruses. See: Using Vet_TRAP

VCRC

This is a utility program which generates standard Cyclic Redundancy Checksum (CRC) codes for any file. The standard values of these codes have been published for much shareware and if the CRC codes for a file match the published values, you can be reasonably sure it has not been interfered with. VCRC is useful for verifying that two versions of a file are in fact identical. See: Using VCRC

Cyclic Redundancy Checksum [CRC] Codes

Cyclic Redundancy Checksum Codes were first introduced to check for errors in data transmission. However, their value in other fields was quickly appreciated and they now form an important part of anti-viral procedures. CRCs are signatures calculated using polynomials for each file and are recalculated when the file is loaded into memory before execution. The new value is compared with the standard checksum for this file. If the new checksum is different from the standard checksum, the file has been changed (it is possible that the file has been infected with a virus) and the alarm is raised.

Vet Master Disk

The Vet Master Disk is the original Vet disk you receive in the post from us. It contains the Vet program, the Vet utilities, and document files. You will receive a new Vet Master Disk every time Vet is updated.

MBR (Master Boot Record)

Normally, the first physical sector on a hard disk (track 0, head 0, sector 1) contains the MBR. It contains records of the size, location, and type of each partition on the hard disk. If your MBR is infected by a computer virus and you do not have any anti-viral protection, you may lose all the information on your hard disk.

VCRC

This is a utility program which generates standard Cyclic Redundancy Checksum (CRC) codes for any file. The standard values of these codes have been published for much shareware and if the CRC codes for a file match the published values, you can be reasonably sure it has not been interfered with. VCRC is useful for verifying that two versions of a file are in fact identical. See: Using VCRC

VERIDISK

Veridisk is used to ensure that the Vet distribution disk has not been damaged. When we prepare the disk, we use a companion program VALIDISK, which calculates CRC checksums for the disk and embeds them in it. When you run VERIDISK, it calculates checksums for each part of a floppy disk and compares them with pre-recorded validation data, if this is present. VERIDISK is provided mainly so that it can be used with HUNT for trapping viruses. VALIDISK, which can be used to add validation data to any disk, is available as a separate product. Please ask for further information if you are interested in this facility.

HUNT

HUNT is a batch program which traps viruses. HUNT runs two programs to act as bait and then runs VERIDISK to see if the disk has been changed. See: Using Hunt

VET_TRAP

This is a program which writes copies of the Master Boot Record, the DOS boot sector and the top of memory to a disk in drive A. It can be used in conjunction with HUNT and VERIDISK to capture new viruses. See: Using VET_TRAP

Using HUNT

HUNT is a batch program designed to trap viruses. If you run an infected program on a PC, most viruses will become memory resident and will then infect any program you run. HUNT runs two programs to act as bait and then runs VERIDISK to check if the disk has been changed. To use HUNT, follow these instructions:

1. Use DISKCOPY to make a copy of the Vet Distribution Disk. DO not write-protect the copy, but do not do anything which could write to it (eg using the DOS pipe facility, as in *dir a:*|*more*).

2. Run every program you think could be infected.

3. Put the copy in drive A (or B) and type:

a:hunt or **b:hunt**

4. The programs HERE and HELLO will run and VERIDISK will then recalculate the checksums for the disk.

5. VERIDISK will announce the results

a. **Disk is OK.** or b. **Disk is corrupted.**

If the disk is still OK, it is unlikely that the PC has a virus. However, some more recent viruses only infect files selectively (perhaps one in three, for example) and VERIDISK is unlikely to catch direct action viruses. It is theoretically possible for an active stealth virus to hide from it, so to be quite certain, take the test disk to a PC which is known to be clean and run VERIDISK from a clean disk to check the test disk. **DO NOT run any program from the test disk.** If the test disk does become corrupted, it is likely that you have a virus Vet does not recognise. Label the disk clearly and send it to us with a report of its symptoms etc.

Many application programs write temporary files to the default drive, so don't run any other programs while the HUNT disk is in the drive.

Using VET_TRAP

This is a program which writes copies of the two boot sectors and the top of memory to a disk in drive A. This provides a simple way of saving this information to floppy disk for diagnostic purposes. Do not write these files to a disk you have used (or intend to use) with HUNT. Simply type VET_TRAP and put a blank formatted disk in drive A when requested.

Using VCRC

VCRC generates two checksum values using different formulae for any file or group of files. The results are compatible with those generated by VALIDATE ((C) McAfee Associates) and values of these have been published for much shareware software.

The VCRC command is similar to the Vet command and takes the form:

VCRC [?] [N:] [Path] [Template] [/XX]

where

N is a drive letter eg **A-F**

Path is a directory eg **\bin\bug**

Template is a file specification eg **v*.exe**

XX are options

The options provided are:

R	**R**ecursive.	Search the current directory and all subdirectories.
T	**T**horough.	List all files.

The default is to calculate CRCs for program files only, defined as in VET.

Using Veridisk

VERIDISK is intended to be used in conjunction with VALIDISK, which enables software suppliers to add validation data to any disk. When you run VERIDISK, it reads the entire disk, calculates CRC checksums for each critical area and compares the result with the pre-recorded information, if this is present. This procedure, if run on a clean PC, will pick up any change to a disk made since the validation data was added. VERIDISK is provided so it can be used as part of HUNT to catch viruses. There are two points to remember when using VERIDISK:

i. A correct result only means the disk has not been changed since it was validated. To be quite sure a disk has not been tampered with, the checksums generated should be compared with the original values supplied independently by the maker of the disk.

ii. In theory, an active stealth type virus could modify files on a disk but hide the changes from any program of this type. The manipulation of the system required to do this is so complex that it is very unlikely that such a virus will actually be written.

VALIDISK

VALIDISK is similar to VERIDISK, but can encode validation data onto a disk, so that VERIDISK can validate that the disk has not been corrupted. VALIDISK is available on separate order from VET ANTI-VIRUS.

CMOS

The CMOS (**C**omplementary **M**etal **O**xide **S**emiconductor) memory is actually a 64 or 128 byte battery-backed memory module that is a part of the system clock chip. It stores system configuration data, such as time, date, type of hard disk, type of your floppy disks and memory setup, etc.

Using Vet

Checking Floppy Disks

Select Vet **Disk A** from the Main Menu or you can type Vet **A** from DOS to check a floppy disk in drive A. Similarly select Vet **Disk B** or type Vet **B** to check a floppy disk in drive B.

What Vet does:

i. Vet will show the current date and time, the user-defined message, and the current version of DOS. Vet will check that it has not been corrupted and display a message indicating the result of this check. It will state the level of scan (usually intermediate) and check memory for viruses. During this check it will also report whether or not VET_RES is active.

ii. If all is well, Vet will load the file VET.EXE from the Vet directory and scan it for viruses. If the file is clean, Vet will calculate checksums for it and confirm that these are correct. Vet will state where it is loaded in memory and will check that the top of memory (this is the highest address available to the user's program) is correct.

iii. Vet will read the boot sector, check it for viruses and if it seems okay, compare it with the inbuilt templates and with any templates you added during installation. If Vet recognises the boot sector, it will identify it.

iv. Vet will announce which files it is going to check. By default, Vet will scan program files (.COM, .EXE etc), but it will scan other files if setup to do so. It will always scan floppies recursively, meaning that it will scan all subdirectories of the current directory.

v. Vet will scan the specified files for viruses. It will display the name of each file as it is checked. The names of normal files will only be shown while the files are being checked, but if a file is hidden, or infected, Vet will do a line feed so when it has finished you will usually have a list of files. By default Vet only looks at program files (executable files with extensions such as .EXE or .COM etc.)

You may wish to instruct Vet to look at all file types (a Full Test will achieve this) but this option is not selected by default, as it significantly increases the time taken to check a drive.

Macro Viruses

Macro viruses will automatically be detected and cleaned by Vet for Windows 3.1x, 95 and NT.

Because any application that can use macros needs a higher operating system then DOS it is not possible for viruses to propagate under the DOS environment. From DOS Vet version 9.60 onwards macro viruses can be detected and cleaned while running a DOS Vet scan.

All of the above scans will also detect and clean the macro viruses that infect Excel spreadsheets.

Troubleshooting

Are there certain conditions under which Vet will refuse to run?

Vet will refuse to run at all if:

a. you are using DOS version 1.

b. Vet has been installed and gets the wrong answer when it checksums itself. You will get the message:

   Vet appears to have been corrupted!!!

   Note that Vet can pass this test, even if the Vet file is infected, as many viruses can restore infected files in memory before allowing them to run. This is why Vet also checks the file VET.EXE on the disk.

c. there is not enough memory to run VET. If there is less than about 128K of free memory Vet will not run at all. You will get the message:

   Insufficient memory to run this program!

   If there is less than 240K of free memory, Vet will not be able to set up the data tables used by PolySearch and Vet will do a basic scan. This will detect all the common viruses, but will not find exotic viruses. The type of scan will be announced later.

What happens if Vet cannot find VET.DAT?

The templates for PolySearch are contained in the file VET.DAT. If Vet cannot find this, or it is corrupted, it will say so and will do the basic scan. Vet will announce that it is doing the basic scan, which will detect all common viruses, but which will not check for exotic viruses.

What happens if you have not specified that a log be written?

If Vet finds a virus in memory (or any other serious error occurs) and you have not specified that a log be written, you will be asked if you wish to open a log file.

******* Virus found, or error has occurred; Do you want to keep a log (Y/?):**

If you answer Y you will be offered the default log file. If this is OK, just hit Enter. Otherwise you can specify any file on any drive.

Default log file is shown below; edit, if desired, then hit "Enter".

C:\Vet\Vet_log.TXT

If Vet finds an infected file and you have not already specified that a log be written, you will be prompted to specify a log file before you continue. If you decide not to keep a log, make a list of all the files Vet reports as infected.

What happens if Vet cannot find VET.EXE?

After checking for viruses in memory, Vet will load the file VET.EXE. If Vet has not been installed, it will look for it in the current directory. If it cannot find it, Vet will tell you:

Vet.exe : Couldn't open.

but will go ahead anyway.

What happens if the file is still infected after Vet has cleaned it?

If the file is still infected after you run Vet, it means either that Vet has not removed the virus completely, or that the virus is still active in memory. In either case, you will be warned very strongly against continuing and do so at your own risk.

****** File not restored correctly, or re-infected. You may have virus active**

****** in memory, or non-standard virus. DO NOT PROCEED, if avoidable**

****** MUST YOU continue ? (Y/?):**

If you get this message, rebooting your PC from a clean DOS boot disk will remove any viruses active in memory. After doing so, run Vet again. This should resolve the problem.

What happens if Vet reports that the top of memory has changed?

When you install Vet, it records the top of memory. Almost all boot sector viruses and many file viruses load themselves into the top of memory and then set this down so they will not be overwritten. Vet will compare the top of memory with the recorded value and warn you if they do not match. It will show the previous and new values and ask if you wish to continue.

If the top of memory has changed, but Vet has not already found a virus and you have not installed any new software in CONFIG.SYS, it could mean you have a new virus, so we would strongly advise you to stop and reboot from a clean DOS disk.

Vet does not record its own loading address, as this depends on which TSR programs the user has loaded, but if the loading address changes unexpectedly it could indicate a virus.

Vet reports Restored OK

When Vet has finished, check each infected file to make sure it still works. Some viruses kill some programs, so **Restored OK** only means that the virus has been removed, not necessarily that the program is undamaged and still works. Or, in the classic words; *The operation was successful, but unfortunately the patient died.*

Checking all files

If you find a program virus on your system, you should perform a Full Test. Select this option from the Vet Main Menu, either with the cursor keys or by pressing “T.” This performs a complete check of every byte of every file on all local hard drives. To do a similar scan on a floppy disk, select **Edit Setup** from the Vet Main Menu. Next select **Current Test**, and then **Test Procedures**. Ensure that the options **Full Test**, **Test All File Types** and **Test Subdirectories** are checked, and that the **Check 1st** box is NOT checked. Now when you go back to the Main Menu and select Vet **Disk A** (or Vet **Disk B**), Vet will check every byte of every file on that floppy disk.

Non-Standard Sized Disks

Vet can handle disks with capacities of 360K, 720K, 1.2M and 1.44M. If you have any old disks (such as 180K or 320K) which are not a standard size, copy the files to a normal disk and use Vet to check the copy. If the copy was infected destroy the original AFTER you have verified that the recovered data is good.

If you Vet a non-standard sized disk, Vet may convert it to standard size and the data will be lost. It can usually be recovered, but it is much safer to copy the files to a standard sized disk and scan that, as described above.

Checking Unknown Sized Disks

Occasionally a virus will destroy the size information of a disk and DOS will not know what it was, so Vet will ask you for the disk size. If you are not certain that the disk is a standard size, stop and try to find out before you go any further. Then be VERY careful to give the right answer!

Checking Write-Protected Disks

If Vet tries to replace a boot sector or remove a program virus and the disk is write-protected, Vet will warn you, ask you to write-enable it and then press **Y** if you wish to go on. If you press any other key, Vet will display a warning and continue, but will not try to remove any more viruses on the disk (hence the warning not to use the disk). The warning message is shown as follows:

Boot sector is corrupted; Will replace it.

Disk is write protected; if you want to write to it remove tab & hit 'Y',

otherwise hit any other key:

Could not write ???? DO NOT USE THIS DISK !!!

What happens if Vet cannot fix an infected file?

If Vet cannot fix an infected file (usually because the file has been overwritten and is unrecoverable) Vet will offer to ignore, rename or delete the file. As the file still contains infectious material we recommend that the file be deleted.

What if Vet reports a Read Error?

Vet uses the two DOS Int 21 functions 4E (Find first) and 4F (Find next) to scan each directory. If DOS cannot read a file, function 4F may report incorrectly that there are no more files in the directory, so if Vet reports a read error, check the disk again.

Error Codes

If anything untoward is found, Vet returns error codes which can be checked in batch files using the **If Errorlevel** command. These were introduced primarily for PC support staff in larger organisations. Select the feature *Give Summary of Errors* from *Edit Setup*|<*Test Type*>|*Reporting Results* if using the Vet menu interface, or if you're running Vet from the command line add the **/D** switch to have Vet display error codes returned with an interpretation at the end of the run.

The error codes are:

1	User terminated scan prematurely.
2	Unable to access disk, or open file, (often caused by running Vet with no disk in the floppy disk drive).
4	Loading address or top of memory has been changed.
8	Virus found in memory but killed, or VET.EXE corrupted.
16	Virus found on floppy, or in program on hard disk and fixed.
32	Virus found in hard disk boot sector and fixed.
64	Program virus or floppy boot virus found but not fixed.
128	Error found and run aborted.
or	Hard disk boot sector not fixed.
or	Fatal virus in memory.
or	Unable to fix hard disk.
or	Virus found but not repaired.

These error codes will be combined if more than one type of error is detected. If several disks are tested all errors will be reported.

Vet Command Line Options

Most people find it easiest to configure and run Vet using the menu interface. However, early versions of Vet were command-line driven, and these options are still supported. The same functionality is provided, but command line options could be particularly useful if you are running Vet from batch files.

The Vet command line takes the form:

VET [drive:] [path\] [filename] [switches] [drive:] [path\] [filename] [...]

where

drive is a drive letter

Vet will scan any drive. It will always try to check the boot sector on floppy disks and hard drives, but will only check files on CD-ROMs and network drives.

path is a directory

The path can specify any directory on the drive. An example is \JANE\PROGRAMS

filename is a file specification

The filename can specify any file or group of files using the DOS wildcard characters ***** and **?**.

Examples:

H*.COM specifies all files starting with the letter H and with the COM extension.

E???.* specifies files starting with the letter E with 4 characters in the name and any extension. Files EGGS.TXT and ELLE.COM would be scanned, ERNIE.EXE would not.

switches are command line switches

Drive Letter

Vet will scan any drive. It will always try to check the boot sector on floppy disks and hard drives, but will only check files on CD-ROMs and network drives.

Directory

The path can specify any directory on the drive. An example is \JANE\PROGRAMS

File Specification

The filename can specify any file or group of files using the DOS wildcard characters ***** and **?**.

Examples:

H*.COM would specify all files starting with the letter H and with the COM extension.

E???.* would specify files starting with the letter E with 4 characters in the name and any extension. Files EGGS.TXT and ELLE.COM would be scanned, ERNIE.EXE would not.

Command Line Switches

/A	**A**utomatically Fix Hard Disk Boot Sector
/B(=nnnn)	Check **B**ase Address is [nnnn]
/C	Show **C**ompressed Files
/D	Show Error Codes
/E	List Files Checked
/F	**F**ull (dumb) Scan
/G	Consult the user if virus found
/H(=nnnn)	Check Top of Memory is [nnnn]
/I	Disable ESC
/J	Fill unused memory with diagnostic code
/L(=file)	Write **L**og file to [filename]
/M	Test Memory Only
/N	Do **N**ot Delete Viruses
/O	**O**verwrite Suspect Files
/P(=nnnn)	**P**artial Search Option
/Q	**Q**uery Suspect Floppy Boot Sectors
/R	Search **R**ecursively
/S	**S**how Boot Sectors
/T	**T**est all file types
/U	Rename Infected Files
/V	Verify COMMAND.COM
/X	E**X**it Vet after Check
/Y	Rename Suspect Files
/Z	**Z**ap (Delete) Infected Files
#	Run Vet using Startup Test Configuration
#1	Run Vet using Alternative Test 1 Configuration
#2	Run Vet using Alternative Test 2 Configuration
$	Test All Partitions
~	Force Full Log File (even if no errors).
^	Automatically replace floppy disk boot sector (even if good)
&	Ask no questions (runs Vet invisibly)

Examples of usage:

Vet b:/etl

Vet the disk in drive B, check every file, list the names of all files tested and log the results to the default

file.

Vet c:*.*/rxl=lpt1

Vet boot sectors and all executable files in the root directory and all subdirectories on drive C. Record all output to printer. Exit to DOS when finished.

Vet Base Address Option

This allows you to tell Vet to check that it is loaded at the specified **B**ase address. To find the right value, reboot your PC and when Vet runs, write down the loading address. For example if you got :

VET is loaded at 026E3:0000h

use **/B=26E3**

The option to check Vet's loading address can be changed in the menu interface under the *Edit Setup* option for the various types of tests, under the submenu *Advanced Features*.

Show Compressed Files

When run with this option, Vet will notify the user of any executable files that it finds that have been compressed. There are various utilities like PKLite, LZEXE, etc., which compress executable files so that they require less disk space. If these files have been infected BEFORE being compressed, Vet won't be able to detect the virus. If the files have been infected AFTER compression, Vet will find the virus as normal. To check compressed files aren't infected internally, you must uncompress the file yourself (using PKLite, UNLZEXE, UNP or a similar utility) and then check the file using Vet.

Vet Specify Top of Memory Option

Specifying the top of memory is useful if you have a number of optional configurations for your PC. (Vet will not check Top of Memory if you specify H=0).

The option to check the top of memory address can be changed in the menu interface under the *Edit Setup* option for the various types of tests, under the submenu *Advanced Features*.

Logging Vet Output

Because of the way Vet displays filenames as they are checked, you cannot get a satisfactory record of infected files by hitting Ctrl_P before running Vet. However the L option permits you to record the output in a tidy form.

The default error log file is **C:\VET\VET_LOG.TXT**, but you can specify a different path and name, either during installation, or in the Vet command. If you ask for a log, the log will always be written to **C:\VET\VET_LOG.$$$** (or other filename, as specified). If an error occurs, this will then be copied to the end of the file **C:\VET\VET_LOG.TXT** (or the file you have specified). If this is already longer than about 40K, the oldest part will be discarded before the new log is added.

Thus if anything goes wrong, you will have a record of what happened even if you run Vet again after it has cleaned up the problem.

If you just want to print the results of a run, you can specify

L=LPT1 [This is printer 1.]

Checking Your Hard Disk

If you have installed Vet correctly, your hard disk will be checked every time you boot your PC, but you can check it at any time. To do this, simply type Vet from the DOS prompt to load the Vet Menu. Then highlight one of the following options with mouse or cursor keys, and press Enter or click the mouse button to select the option:

Hard Disks:	Checks the hard disk/s
VET Drive:	Check specific file/s, drive/s and/or directory/directories
Full Test:	Runs a full check on all local hard drives

Running Vet from a Floppy

Vet will reliably detect almost all known viruses even if they are active when Vet is run, but many experts insist that you can only check your PC reliably if you have booted it from a clean floppy. With many packages it is difficult to check floppies if you have booted from a floppy, as they repeatedly load files from the source disk. But when you run Vet, it loads the two files VET.EXE and VET.DAT and then makes no further reference to the source disk.

This means that if you want to be as safe as possible, you can easily boot your PC from your Vet Reference Disk, run Vet from it to check your hard disk and then check as many floppies as you like, with no risk of any virus getting a chance to interfere. Notice that Vet always checks the copy of VET.EXE in the Vet directory, even if you have booted from a floppy, and as this is checksummed, any infection will be detected.

Vet Reference Disk

The Vet Reference Disk is the disk which contains all the most important information about your PC, such as the copy of your hard disk's boot sector and Master Boot Record. The Vet Reference Disk is created when you install Vet on your PC using the Standard Installation. You will need a floppy disk which fits into your bootable drive (usually drive A). Then:

1. Make a DOS Boot Disk (format a disk with the system files added)
2. Install Vet using the Standard Installation

Making A DOS Boot Disk

When you bought your PC, you probably received MSDOS installation disks and if you have any reason to suspect your PC may have viruses you should reboot from disk one of these before running Vet. If you don't have this disk or some other bootable disk, make yourself a system disk (see below). Then check that you can boot from it and access drive C. Note that you can only boot up from a disk in drive A, not B. Write-protect it and put it where you can find it when you need it. It is a good idea to make a second disk with copies of your AUTOEXEC.BAT and CONFIG.SYS, and important utility programs so that you can boot from that floppy and get your PC set up as you like it in case anything goes wrong with your hard disk.

Making a System Disk

At the DOS prompt, type the following command:

format a:/s [Enter]

For more details of the DOS format command, refer to the MS-DOS User's Guide.

For the Microsoft Windows user, you can use the File Management Utility in the Windows Main Menu. For more details on how to use it, refer to your Windows User's Guide.

Corrupted Files

Occasionally a virus will try to infect a file, but will corrupt it instead. The file will still operate correctly and if you do an intermediate scan Vet will say it is clean, but if you do a full scan, it will find the virus and say the file *may be* infected. `Dumb` scanners from other suppliers may also report that the file is infected. Don't be alarmed if this should happen; it does not mean that Vet is faulty, but it is advisable to reinstall the corrupted program from the master disk.

A similar effect can occur if you set up a database on a PC which has had a major infection. Data files often contain large sections which are not initialised and if one of these happens to contain part of an infected file which has been deleted, a full scan may report that the file is infected. Such an infection does not pose any risk and will disappear as more data is entered into the file. Windows swap files are another possible source of such false alarms.

Packed Files

Vet cannot detect viruses in compressed files (eg .ARC or .ZIP). Unpack the files and then check them. Vet cannot check self-loading packed files generated by programs like EXEPACK and LZEXE. If a virus infects one of these files after it has been packed, Vet will find and fix it in the normal way. However, if a file is infected with a virus and then packed, the packing program may well disguise the virus, so Vet (and most other scanners) will not find it. If this occurs, the virus will escape and infect other files in the normal way, when the packed file is run. Vet will detect and flag files packed with the following programs;

Diet, Exepack 1, Exepack 2, Ice, Lzexe, Pklite, ???Pack.

We cannot guarantee either that this list is inclusive, or that Vet will detect all versions of these programs. The program ???Pack is used by Microsoft and appears to be an unpacking program, but has not been analysed. Packed files on floppies will always be flagged, but will only be shown on the hard disk during installation, or if you use the **/C** option. If you know of any program of this type which Vet does not detect, please let us know and if possible give us a sample of a packed file.

You are certain to have a number of these files on your hard disk. If you have had them for any time and no other files on your machine are infected, they will almost certainly be safe, as any virus would long since have escaped and been found.

Files packed with these programs are unlikely to be accidentally infected before they are packed and the only real risk comes from people who deliberately infect files, then pack them and upload them onto bulletin boards. So if you download a program from a bulletin board and find it is packed with LZEXE, etc., treat it carefully. If possible, run it on a PC which has nothing important on it, then run HUNT or run some other programs and see if the size of any of the files has changed.

Disabling Viruses

When you run Vet, the program searches memory for active viruses. When you read or copy a file or a disk, DOS first loads the relevant sectors into buffers which are often in low memory, so if you access an infected file and then run a scanning program, Vet may find the virus left behind in a buffer. If Vet finds a virus in memory, we advise you to reboot from a clean DOS disk (most other programs demand that you do so), as there is always a risk of finding a non-standard strain. However, if you cannot find a clean DOS disk, Vet can disable most of the common viruses if it finds them in memory, so that it can safely remove the virus from infected programs.

When Vet does this, it only disables those parts of the virus that could interfere with the clean-up process. It is not possible to remove the virus from memory and Vet does not bother about harmless activities (such as Ping Pong's bouncing ball). If you do let Vet clean up files after finding viruses in memory, you **MUST** always reboot after Vet has finished and Vet your PC again.

If you think your PC is clean, but Vet finds an active virus after you have copied a suspect file, or Vet reports that a virus is in memory, but cannot find any infected files, the virus is probably only in a buffer, but always disable it in case it is active. If the virus is only in a buffer, it is not dangerous, but no harm will be done if you disable it. If the PC locks up when you disable a virus, it probably means you have found a mutant strain, so reboot from a clean disk and start again.

If Vet finds a virus such as 4096 which does not seem to be active, it will insert an endless loop into the virus so that if it is active, but has not been found because it is a mutant strain, the PC will lock up harmlessly.

Recovering Files Hidden by Stoned Virus

On floppy disks, the Stoned (Marijuana), Korea and Michelangelo viruses and a number of related viruses overwrite part of the directory when they save the old boot sector. This may cause files to be lost, especially on higher capacity disks. Vet erases the resultant erroneous directory entries, but cannot restore the lost files. However, when the virus has been removed it may be possible to recover the lost files by putting the disk in drive A and giving the DOS command:

CHKDSK A:/F

CHKDSK will generate a file with name **FILE00n.CHK** for each entry that was overwritten. Inspect these to identify them and then rename them. They will be rounded up to the next 512 bytes and this may cause problems with a few programs. If so, use a suitable editor to remove the excess. This normally works with 360K disks, but may not work with other sizes.

WARNING

> **If you attempt to erase any bogus files, or run CHKDSK before you remove the virus, you will not be able to recover the lost files**.

Vet on Networks

Networks provide the potential for file viruses to spread extremely quickly. In general, network operating system security is better than that offered by DOS - but only if the network is correctly administered. Vet is able to check and clean DOS and Windows files on network operating systems. The following topics are of interest:

Viruses and Networks

Networks provide the potential for file viruses to spread extremely quickly. In general, network operating system security is better than that offered by DOS - but only if the network is correctly administered. Vet is able to check and clean DOS and Windows files on network operating systems.

Workstations

Workstations may be infected by both boot sector and file viruses. Workstations fall into three categories, with different sensitivities to boot sector viruses depending on how they are booted.

i. Normal PCs booting from the hard disk.

These will become infected with boot sector viruses if anyone boots from an infected floppy. The virus will not be able to propagate over the network (unless, like AntiCad/Plastique, it is also a program virus), but will infect every floppy put into the workstation.

ii. Diskless workstations booting from a floppy.

If someone boots from an infected floppy, the workstation will become infected but will not be able to access the network and the virus will be removed when someone reboots. However, if the official boot disks become infected, the virus will again be able to infect all disks inserted. These disks must be write-protected and should be checked frequently. Access to them (by students etc) should be controlled carefully to minimise the risk of sabotage.

iii. Diskless workstations booting from ROM etc.

These cannot be infected by boot sector viruses, unless the boot image file is infected. In such a case it will be necessary to create a new boot image file.

Any workstation running an infected file will become infected. Depending on security, the virus may be able to infect DOS and Windows files that are stored on the network. From that point on, anyone running such an infected file will be infected.

In general, if the user has write access to a file and he or she runs the file from an infected PC, the file will be infected regardless of where it is in the network. This means that if the access permissions are not controlled carefully, viruses can very quickly infect large numbers of programs throughout the network.

The File Server

The file server normally has a different operating system and is not directly susceptible to PC viruses. However, if it's based on a PC with the normal PC BIOS, it can become infected if someone boots from a disk infected with a partition sector virus, such as Stoned. It is very important to check every disk which is brought anywhere near the file server and to ensure that the file server is in a secure environment.

Program viruses cannot infect the file server itself, but files on it appear to the users as normal DOS files and program viruses will try to infect these files in the normal way. If the permissions are set up correctly, they should not be able to infect files on the server, but if there are any holes in the security, the virus will find them. Two common weaknesses are:

i. Anyone having write access to the file server must be very careful that they only use a clean workstation. A number of infections in school systems have been caused by teachers using the nearest PC to upload new assignments etc. without first rebooting it to ensure no file viruses are active.

ii. Students may attempt to bypass access controls on the file server so that they can upload games, pirated software etc. Some systems have fairly obvious loopholes and once students find them, it will not be long before viruses follow them in.

One major infection on a large corporate network was caused by a supervisor logging in as supervisor to re-install Windows from a workstation on which it had crashed inexplicably. The new copy promptly crashed again, as did every copy of Windows on the site. The workstation (which was new and had not been checked before it was connected) was infected with Dark Avenger. When the supervisor logged in, it infected the **LOGIN** program and then infected all the other workstations. If you have supervisor access, it is extremely important that you do not use it for your normal work and that you only log in as supervisor from a PC which is known to be clean.

There is a saying in Unix circles, that

> *"It is impossible to corrupt a properly administered UNIX network"*

but

> *"There is no such thing as a properly administered UNIX network.*

Our experience suggests that this applies equally to PC networks.

Vet on the File Server

While setting up the permissions correctly, and being sure to check your machine for viruses before logging in with supervisor privileges, are major steps in keeping viruses off the network, the following extra precautions will also increase protection against viruses.

1. Rename login.exe and create a batch file on the user's machine which runs Vet when login is called. Test the error level returned by Vet - if it is zero then call the renamed login script; otherwise refuse to run login.
2. Rename ATTACH.EXE and create a batch file to run Vet on the user's workstation and check the error code returned;- if zero, call the renamed attach program, otherwise refuse the operation. Unfortunately this will not prevent remote users attaching to your server from an infected machine.
3. Load VET_RES from the same batch file that is running the login script (see 1 above), so that whenever a user is logged in, every file they run will be checked for viruses before it is allowed to run.

Common Questions

These are the more common questions that VET ANTI-VIRUS's Technical Support staff are asked. If your question isn't listed below, please contact us.

Top of Memory or Master Boot Record has changed

This warning message will be displayed after installing some new software (eg Windows 95) or after having removed a virus. To update Vet's records of the top of memory address and Master Boot Record, load the Vet menu by typing Vet at the DOS prompt, select *Configure,* and select *Record System Data*. Enter or confirm the user message when prompted, and select whether or not you'd like to make a Reference disk. You will be returned to the Configuration menu and Vet's records will have been updated.

Not all files were checked

By default only standard executable files are checked, ie those ending with extensions BGI, BIN, COM, EXE, OVL, PIF, SYS, DOC, DOT, XLS, XLT, and XTP. To add another extension to the files that Vet considers to be executable, load the Vet Menu by typing Vet at the DOS prompt, select *Configure*, and then *Edit Extension List*.

If you want to check all files you can select either *Full Test* or select *Edit Setup* from the Vet Menu and for the appropriate test-type, set the testing procedure to *Test All File Types*.

Vet reports that it is out of date

New viruses appear every day, and Vet is upgraded continually to address this. Major updates are sent out every three months, and if the version that you are using is more than six months out of date according to the system date, a warning message will be displayed every time that Vet is run. If for some reason you wish to disable this warning (eg your system clock doesn't work), load the Vet menu (type Vet from the DOS prompt), select *Configure*, then select *Global Functions*, and enable the *Don't Warn if Obsolete* option.

Vet detects the Flip virus in memory

If Vet is detecting the Flip virus in memory **only**, it is almost definitely a false alarm caused by the presence on the system of another anti virus package's resident scanner. Flip is a boot sector virus but its signature is one of those commonly left unencrypted in memory by certain anti-virus packages. The easiest way to resolve this is to disable the resident scanner (or TSR) of the other package.

The virus keeps coming back!

There are a few possible reasons that this could happen. Firstly be sure that the virus has been removed from all files and all floppy disks. If you are using caching the virus may continue to be detected in memory but nowhere else until the cache buffers are flushed. Similarly the virus may continue to be detected in the Windows swap file (386SPART.PAR) after its been removed from everywhere else. In both these cases the virus is not active and is not a cause for concern.

Some PCs have a BIOS or Setup option for Virus Protection. If this is enabled, Vet won't be able to fix the infected boot sector. Having the option enabled is a good extra measure of virus protection but don't rely on it by itself, and disable it temporarily to remove any boot sector viruses. Some PCs have programs for changing their Setup information stored on their own partition. If the virus has infected this partition, it will keep infecting the main partition every time you run the Setup utility. Contact VET ANTI-VIRUS if this happens as removing the virus from the Setup partition requires a different procedure than usual.

VET_RES detects an unknown virus

Load the Vet menu (or use the Vet Windows interface) and scan the floppy disk in question. It will probably report that the boot sector is **Unknown but seem okay**. If this only happens on one or a few disks, it would indicate only that they've been formatted with a non standard program. If this happens on all your disks, it suggests the presence of an unknown virus and you should send a sample to VET ANTI-VIRUS for analysis.

There’s a virus in only one file

If the file is one being used for caching of some type (eg the Windows swap file 386SPART.PAR) and you have had a virus recently, this means that the virus is not active but parts of it are still present in the buffer file. You can either delete the file and let the caching software recreate it, or simply ignore the message about the virus and after a short amount of time, the buffer will be flushed and a virus will no longer be found in that file.

If a virus is reported in a file that isn’t used in caching you should contact VET ANTI-VIRUS; it is more than likely a false alarm otherwise the virus would have infected other files as well.

Why's the Emergency option disabled?

If you didn't set a password when you installed Vet, the Emergency option will be disabled. You can run Vet from the Reference disk **for that PC** in order to use the Emergency option.

When I run Windows it says VET_RES is not active.

This message is displayed if VET_RES is not resident in memory. Check to see that VET_RES is being loaded in the AUTOEXEC.BAT file, and when booting check what message VET_RES is displaying. Note that if you run Windows the first time that you install Vet before re-booting, this message will appear as the installation program updates the startup (AUTOEXEC.BAT) file which won't be loaded until the computer is re-booted.

Protecting Your PC

If your PC is clean and you never put data on it from anywhere else, you can never get a virus on it. This would not be practical, so your PC is always at risk; everytime you buy a new software package, copy files from a friends disk, or download a new utility from a bulletin board system or the Internet. The three main ways in which you can catch a virus are:

Booting from an Infected Floppy

Running an Infected Program

Having your PC Serviced, or Buying New Hardware or Software

There are a number of ways in which you can minimise the risk of a virus infecting your PC:

Good Housekeeping

Checking New Disks

Symptoms of Viruses

Catching Viruses.

Booting from an Infected Floppy

Any disk you receive from anyone else, or have ever put into anyone else's PC, could have a boot sector virus on it and infect your PC when you boot from it.

This is probably still the most common way of getting a virus. As long as you don't know a disk is safe, whether or not it is bootable, your computer may be at risk. Sooner or later you will forget to check drive A is empty before you switch on or hit RESET, and the virus will be in. If you have seen the message *Non-system disk or boot error...* it means you have booted from a floppy which may have infected your PC.

Running an Infected Program

Any program you have received from anyone else, whether on a floppy, or downloaded from a bulletin board system, or transmitted in any other way, and any program you have run from a disk (that was not write protected) in any one else's PC, could be infected and could infect your PC the first time you run it. Remember, too, that ANY program (including any .BAT file) you have received from a suspect source, could contain a Trojan Horse.

Having Your PC Serviced, or Buying New Hardware or Software

Always backup your PC before having it serviced. Many PCs have been returned from service infected with a virus. Your PC is constantly at risk from viruses and unless you always maintain your vigilance, sooner or later it will become infected. If you have school age children, the risks are increased markedly, as schools are commonly plagued with computer viruses. Fortunately keeping viruses out is not difficult and is largely a matter of good housekeeping.

Good Housekeeping

Prevention is much better than cure. Accept disks only from reputable sources and keep all disks containing programs (as opposed to data) write-protected if you have to use a suspect computer. Check all new disks, and disks used in any other computer before using them in your own PC. Back up frequently and make sure you have a current backup before testing any new software.

The following rules will greatly reduce the risk to your system.

i. Format your disks on your own computer.

ii. If you have to use any other computer, put all the programs you will need on one or two disks beforehand and write-protect them, so you won't get program viruses.

iii. Wherever possible verify any outside computer is clean before using it. If you find a virus, report it to the owner/supervisor. Don't use Vet to clean someone else's PC without first obtaining their permission to do so.

iv. Whenever you want to use a disk that has been used in another PC, use Vet to check that it is clean. Vet will recognise all disks formatted on your PC (and on many other machines using common versions of DOS). If the boot sector on any of your standard disks has been changed, replace it, as it may have a virus.

v. Be wary of programs which require you to boot from the floppy disk.

vi. Try to ensure all your programs come from reputable sources.

vii. Ensure you haven't left a disk in drive A before rebooting (and also when you leave the computer unattended).

viii. Remember that as long as you have a disk in your PC that you do not know is safe, your system is at risk. Never run any program from any disk which is not known to be safe and be very wary of using experimental software when you have a suspect disk in drive A. Remember that a PC can be re-booted at any time, as a result of a power surge, a program crash, or even malicious software.

ix. If you have children at school, find out if the school uses any anti-viral software. If not, suggest that they consider installing VET. Alternatively give us the details and we will contact them. It is much better to have the viruses removed at the school rather than from your home PC.

Checking New Disks (Floppies AND CDs!)

Whenever you get a disk from anyone else, assume that it could be infected. There are many well documented cases where major software suppliers have sent out infected disks, hardware manufacturers have supplied infected setup or demonstration disks with their hardware and magazines have given away infected bonus disks. If you replace any boot sector that Vet doesn't recognise, you cannot get a boot sector virus. DO NOT, however, replace the boot sector on any of your master disks, backup disks, or copy protected programs.

i. Whenever you buy a new program, or borrow a program from someone else, check that the disks are write-protected before you put them into your computer.

ii. Check the disk with Vet. If you find a virus NOTIFY THE SUPPLIER AS SOON AS POSSIBLE. If the disk is infected, or Vet does not recognise the boot sector, copy all the files to a new disk to make a working copy and work from this. Check the working copy and replace the boot sector if Vet does not recognise it. Label any infected master disk very clearly and put it away in a safe place.

iii. List the directory (including any hidden files) and if possible make an index so you know what all the files on the disk do.

iv. Be wary of any hidden files.

v. Do not TYPE READ.MEs: use LIST or similar programs.

vi. List all .BAT files before you run them.

vii. Read the documentation. In 1989 medical workers throughout he world were sent an AIDS Information Disk. The accompanying Licence Agreement asked for a large licence fee and contained (in very fine print) the most draconian threats. It specifically warned that if you did not honour the agreement it would prevent you using your computer. However the disk just said Put in drive A: and type 'A:INSTALL'. A number of victims did so and discovered that the program did exactly what the licence agreement promised.

Symptoms of Viruses

A virus has to use the back door to get at the operating system and inevitably there will be occasions when a particular virus will be incompatible with some program and will crash the system, or scramble data or files. However, almost all programs have bugs (regardless of price) and will crash if you find some unexpected combination of commands and/or data; disks are mechanical devices and inevitably wear out; and users do occasionally hit wrong keys or use the wrong commands. So if you have random crashes or files disappear or become corrupted, you COULD have a virus, but the trouble is more likely to be caused by faulty hardware, software, or fingers.

The operation of the common viruses is well understood and many of the effects reported in popular accounts of viral attacks could not have been caused by the virus involved. There is nothing like a virus (or the suspicion of a virus!) to stimulate the imagination.

Some of the more common symptoms of viruses are:

i. More disk activity than usual. The attempts by a virus to infect disks can cause obvious delays, especially if a disk is write-protected.

ii. Odd messages (Your PC is now Stoned) or odd things happening to the screen (Ping Pong, Cascade, Jerusalem).

iii. You get fatal I/O messages when you try to read a write-protected floppy and a virus tries to write to it.

iv. The computer runs slowly, or erratically (Jerusalem).

v. Files grow in size or load more slowly (Jerusalem).

vi. Your PC starts to play tunes (AntiCad/Plastique, Yankee Doodle). DO NOT hit Ctrl-Alt-Del. To be safest, switch off immediately.

vii. The dates of files change. If programs you bought last year are dated last, week you know you have a virus.

viii. The keyboard locks up or suddenly spits out a long string of characters when you hit a key (KeyPress).

ix. Programs which formerly ran, complain that there is insufficient memory or become too long to load.

x. The available memory or the top of memory is reduced inexplicably.

xi. The PC cannot read from, write to, or format high density floppy disks (Azusa, Michelangelo and many other boot sector viruses).

Catching Viruses

If you suspect a PC may have a virus but Vet does not find anything, there are several things you can try.

i. Boot from a clean DOS boot disk, then do DIRs of your DOS program disk and of the DOS directory. Compare the lengths and dates of the matching files. If a number of files on the hard disk are longer by a consistent amount or have recent dates, they are probably infected with a virus. Copy several of them to a floppy and send it to us, along with details as to what has changed, other symptoms of the virus etc. (But beware of programs which add a signature to files - these have caused many users to panic. If a file still works, but has grown by less than about 500 bytes, it is most unlikely it has a virus.)

ii. Make a copy of the Vet distribution disk, run a selection of programs you suspect are infected and then run HUNT. If the disk becomes corrupted, it has probably caught a virus (unless you've accidentally written to it!)

iii. If you have any reason to suspect you have a new (or rare) virus PLEASE talk to us before you destroy it. We have had several reports of destructive, but apparently unknown viruses, where the victim has rung us after reformatting all their disks. As a result we can't do anything about it till someone else has suffered from it.

How Vet Works

Vet performs the following functions:

Vet checks itself in memory to ensure it has not been damaged.

- It checks to see if any known viruses are present in memory. If it finds any viruses, it disables them.
- It checks the file VET.EXE for viruses, disinfects it if it is infected, and verifies it has not been corrupted.
- It scans the boot sector(s) and all files on any drive specified for known viruses.
- It removes any viruses it finds.

Vet has inbuilt templates so it can recognize most common boot sectors.

Vet can replace any suspect floppy disk boot sector, so that you can be certain you will not get a boot sector virus.

When you install Vet on your PC, it records the boot sectors of your hard disk and your floppies so that it can detect any change in them and if necessary it can restore them from the recorded copies. It also records the normal Top of Memory, which most boot sector viruses (and many program viruses) change.

Once installed on your PC, Vet runs automatically every time you boot your computer, running a quick check to ensure it is virus free.

The sections below describe some of VET's main technical features. This knowledge will help you use Vet to the best advantage and will assist you in evaluating the claims of other suppliers of anti-viral software.

Security

Intelligent Scanning

Dumb Scanning

The PolySearch Algorithm

How does Vet Detect Viruses in Memory?

How does Vet Detect Boot Sector Viruses?

If Vet finds Viruses on Your PC

Running VET

Security

There are two distinct problems in protecting any software. The first is to ensure that what you are getting is what you expected and the second is to ensure that it does not become corrupted in use.

1. Getting Vet to You

As Vet is distributed on disk, the risk of damage in transit is significant, but the risk of deliberate corruption is relatively small. Thus the security measures are primarily designed to detect accidental damage. After the Master Disk has been written, the program **VALIDISK** is used to calculate checksums for each section of the disk and these are embedded on the disk. Notchless disks are used to minimise the chances of their becoming infected or accidentally overwritten. If you wish to check the Master Disk is okay, run VERIDISK

2. Protecting Vet on Your PC

When you install Vet, the following precautions are taken:

As the Vet files are loaded into memory, they are rounded up so that they exactly fill an integral number of clusters on the hard disk. This eliminates the danger of left over virus being found in the unused space in the last cluster of the file (but it does mean the new Vet files are usually longer than the originals).

3. Protecting Vet in Use

Ideally you should always reboot your PC from a clean disk before you run any anti-viral software, but we know that this is seldom done, so we have done everything we can to ensure that Vet can be used safely, even if your PC is infected with a virus. To this end Vet takes the following steps.

Vet decrypts itself and then recalculates its inner checksums. If these do not match, it means that the file is damaged and Vet refuses to run at all.

If there is sufficient memory to run PolySearch, Vet will load the file VET.DAT, containing the viral data and check that it has not been corrupted. If this is OK, Vet will do an intermediate or full scan, as requested. If there is insufficient memory, or Vet can't find VET.DAT, or it is corrupted, Vet will do a basic scan only. This will find nearly all the common viruses.

Vet scans memory for known viruses. It first looks sequentially for a number of common viruses. If Vet finds a virus, it will always warn you against continuing, but it can safely disable most of these viruses and if it can, it will ask if you wish to do so. If there is no virus, or you decide to continue anyway, Vet will then look for a large number of exotic viruses, using the PolySearch algorithm. Vet cannot disable these and will advise you to abort, but will continue if you insist.

Vet loads the file VET.EXE from the Vet directory and checks it for viruses. If it is infected, Vet will disinfect it (and check it again, as described below). It will then calculate the outer checksums for the file and verify them. If they do not match, Vet will warn you that the file has been corrupted, but will go on anyway.

If a virus is active when Vet is run, VET.EXE will usually become infected. This series of checks is designed to ensure that Vet will always clean itself up before it does anything else, so that it will not re-infect your PC the next time you run it.

4. Vet**'s Inbuilt Security**

If a file is infected and Vet has fixed it, Vet will check it again, but this time will do a full scan, to make certain no trace of virus remains. If PolySearch finds a virus on the second pass this will be simply stated and the file will be counted as Not fixed. If this should happen, the file is probably corrupted and the program should be re- installed.

If Vet finds a normal virus on the second pass, it will again be removed and the file will be checked again. If it is again infected, Vet will strongly advise you to desist.

How Does Vet Detect Viruses in Memory?

When Vet scans memory, it first looks for common viruses, then uses PolySearch to look for exotic viruses. If you have booted from an infected disk or an infected file has previously been run, the virus will be active in memory. Vet will display the name of the virus, e.g.:

Junkie virus already in memory at 098B:0A95h

If Vet can disable the virus, it will display:

Vet can kill this, but we strongly advise you to reboot from a clean DOS Boot

Disk & start again. MUST YOU continue?

If Vet can't disable the virus in memory, Vet will display:

!!!!TaiPan virus already in memory at 098B:0A95h

Note the **!!!!** which indicates that Vet cannot disable the virus in memory.

Vet will then display the message:

We strongly advise you to reboot from a clean DOS Boot

Disk & start again. MUST YOU continue?

In all cases, it is best to answer *No* at the prompt and reboot from a clean DOS Boot Disk and then run Vet to clean the virus. However if you don't have a clean DOS Boot Disk and Vet says it can disable the virus in memory, you can proceed and in most cases Vet will disable it from memory so you can then clean the virus from the infected drive.

If Vet finds Viruses on Your PC

When Vet finds viruses in your PC, Vet will often find the virus in several locations. PolySearch uses different templates and there are usually two copies of some. If the virus is found by PolySearch, the name will be preceded by **!!!!** and it may use a different name. Vet will disable these without further query.

How does Vet Detect Boot Sector Viruses?

Vet will check the disk's boot sector for viruses. If Vet finds a boot sector virus it will report the name of the virus. In most cases Vet will be able to find the original boot sector and replace it. However not all boot sector viruses save the original boot sector, and in these cases Vet can replace the infected sector on floppy disks with a standard non-bootable one, which contains a short program to display the following message if you try to boot from it:

Cannot boot from this disk; Insert correct disk and strike any key.

If the boot sector is an unknown type, Vet it will ask whether you'd like to replace it. This could indicate an unknown virus or it might just have been formatted using a non standard program. It normally does no harm to replace it (although you will no longer be able to boot from the disk).

Don't replace the boot sector on original software, copy protected software, proprietary backup disks, or disks which are not a standard size. If you have any doubts, either copy all the files to another disk, or use DISKCOPY to copy the disk and replace the boot sector on the copy.

Intelligent Scanning

Most scanners are **DUMB** scanners. This means they load the whole of each file into memory and then search the whole file for each template. However, every virus runs before it permits the original program to be loaded. This means that if a file is infected, the first instruction executed must always be part of the virus and so if we choose templates near the start of the virus, we need only load a relatively small block around the initial entry point and we can look for each virus at a specific location in this block. Scanners using this technique are called **INTELLIGENT** scanners. Vet has always used this technique.

Some viruses have been designed to hide from intelligent scanners, by making the initial instructions jump all over the place before they reach the decrypting procedure. Vet decodes the first instruction and checks if it jumps outside the initial block. If it does, Vet loads another block at the next location and repeats the procedure. By default, Vet will do an intelligent scan and will detect all but a handful of exotic viruses

Dumb Scanning

Occasionally, a file will become corrupted and viral code will be attached to it (but not activated) or inserted randomly into a file. For example 4096 sometimes writes part of itself to a sector chosen at random and this can be inserted into any type of file. There is also a version of Dark Avenger which has been crudely patched to hide from a particular scanner with the result that it infects .COM files normally, but does not patch .EXE file header when it infects them so that the virus is not activated. If you find any infected files on your hard disk, we advise you to do a **FULL**, or DUMB, scan of all files, to detect any corrupted files of this type. This will also detect a few exotic viruses Vet does not currently find in the normal mode.

We also advise doing a FULL scan if you suspect you could have a virus, but the normal scan does not find anything

File or Program Viruses

These attach themselves to executable files and are grouped according to the class(es) of program they infect. They can be extremely infective and are much harder to counter than boot sector viruses because of the wide range of potential targets. Most viruses are of this type, but surprisingly, boot sector viruses are still more common and are involved in more viral incidents.

The PolySearch Algorithm

Conventional scanning techniques involve looking for each virus in turn. As the number of viruses has grown, this has become progressively slower and there have been many predictions that scanning would become completely impractical. To enable us to keep up with the flood of new viruses, we developed the PolySearch Algorithm which will enable Vet to scan for the thousands of viruses expected in the next few years, without significantly degrading the performance.

PolySearch is a radically new scanning algorithm using statistical methods to scan for a large number of viruses simultaneously. It is extremely fast and its speed is almost independent of the number of viruses being searched for. At present we are looking for about 600 distinct templates, but we don't expect the speed to fall noticeably until this reaches 10,000. However, the statistical tables used in PolySearch and the data to describe all these viruses, require a substantial amount of memory and at present Vet requires about 200K of free memory to run PolySearch.

Running VET

VET is safe, quick and easy to use and does not interfere with the normal operation of your PC. To start Vet from the DOS prompt, type:

Vet

The Vet Main Menu will be displayed. By default, Vet is configured as follows:

- to perform an **intelligent** check, ie it looks for specific viruses in specific locations
- to check **executable** files only, rather than every file
- to check the disk recursively, ie the current directory and all its subdirectories
- to automatically clean any viruses it finds
- to record the results of the check in a file C:\VET\VET_LOG.1

Each time you run Vet, the first time it actually checks something, Vet will check itself in memory, it will check for any viruses in memory, it will check if VET_RES(2) is loaded, it will report its own loading address and the current top of memory and finally check VET.EXE for viruses. From the Main Menu, the most useful options are:

Vet Disk A	Check the disk in drive A for viruses
Vet Disk B	Check the disk in drive B for viruses
Hard Disks	Check all hard disks for viruses
Full Test	Check all files on all disks for viruses.

Running an Uninstalled Version of Vet

You can run an uninstalled version of Vet from the Vet Master Disk simply by typing Vet from the DOS prompt (when the current drive is that with the Vet Master Disk in it). The Vet Main Menu will appear, from which you can select which drive or directory you would like to check.

Checking Hard Disk Boot Sectors

1. If you are checking drive C, Vet will read the Master Boot Record, followed by the DOS boot sector and check them for known viruses. If Vet finds a virus, it will offer to remove it. Otherwise Vet will compare them with the copies saved during installation and will warn you if they do not match.

2. If Vet finds a known boot sector virus, it will look for the hidden copy of the original boot sector. If there is no hidden copy or it appears corrupted, Vet will advise you to run **Emergency** which can put back the copies made during installation. If Vet has not been installed, or you can't find your Reference Disk, Vet can write a generic Master Boot Record. This will normally work, but we cannot guarantee it.

Checking Floppy Disk Boot Sectors

1. If you are checking a floppy, Vet will read the boot sector and check it for viruses. If it appears clean, Vet will calculate two checksums for it and compare these with lists of checksums for known boot sectors. If it finds a match, the boot sector will be identified. Otherwise you will be advised to replace it.

2. If Vet finds a virus on a floppy, it will look for the original sector if it knows where the virus has hidden it.

3. Vet will check the recovered boot sector to see if it has a virus. If so, it will repeat the preceding step, up to a maximum of five times.

4. If Vet cannot find a boot sector it recognises is clean, or if you ask it to replace an unknown boot sector, it will write a standard non-bootable boot sector. Thus we can guarantee that Vet will never put back a corrupted boot sector if it finds a virus.

Checking Files

1. Vet will start checking files in the specified directory. If you have specified a recursive scan or you are checking a floppy, Vet will change to each subdirectory as it finds it. When it comes to the end of a subdirectory, Vet will return to the level above and continue searching it. As a result, the order in which Vet checks files is unpredictable.

2. As Vet finds each file, it checks if it matches the list of files to be checked.

3. If the file is to be checked, Vet will load one or more blocks for an intelligent scan, or the entire file for a full scan. Vet then calls the testing procedure.

4. The test procedure calls the checker. This looks for specific viruses, then calls PolySearch to look for exotic viruses.

5. If a virus which can be removed is found and this is permitted, the removal procedure is called.

6. If a virus has been removed, the checker is again called, but this time a full scan is always done. If the file is again infected, you will be warned strongly against continuing as it means there is something wrong with the restoration procedure and if you continue, you could infect all files.

As VET.EXE is the first file checked, this sequence minimises the danger of Vet spreading a modified virus through your hard disk.

7. When all specified files have been checked, Vet will ask if you wish to check another disk.

8. When you have finished, Vet will announce the results of the run and return an appropriate error code to DOS.

Repairing Files

Ideally you should **REINSTALL** any infected file from the master disks, but this is often a major undertaking. For this reason we have gone to a lot of trouble to ensure that Vet will reliably repair files infected with most of the common viruses. Because Vet is an intelligent scanner, it will always find the last virus on a file first, and because the detection and repair facilities are designed to go together, mixed or multiple infections will not confuse it.

In contrast, packages in which the detection and cleaning facilities are separate will often get confused by multiple or mixed infections and destroy the file instead of restoring it. This applies particularly to packages in which you must tell the cleaning facility which virus to remove.

VET has an excellent reputation for repairing files reliably, but many viruses will destroy some files, so we cannot guarantee that a repaired file will still actually work.

When Vet identifies a virus it can repair, it goes through the following steps:

1. If it has not already done so, it will load either the entire file or the last 64K into a buffer.

2. If the virus is encrypted and the recovery information is in the encrypted section, it will decrypt it.

3. If the virus is at the start of a .COM file, Vet will copy the original file down to the start, overwriting the virus.

4. If the virus is at the end of a .COM file, Vet will recover the initial section.

5. If the file is a .EXE, Vet will restore the original header information.

6. Vet will fill the tail containing the virus with zeroes.

7. Vet calls the detection procedures to see if there is another virus. If the result is positive these steps are repeated until all viruses are removed.

8. Vet writes the entire file back to disk so that the virus is overwritten and then truncates the file to the correct length.

9. Vet then reloads the file from disk, and checks it again, but this time it does a full scan (provided enough memory is available). If a common virus is again found it is removed again, and then the whole process is repeated. If the file is infected on the third pass the user is strongly advised to seek expert help. This is extremely improbable, and would only occur if a non standard virus were either not being removed correctly, or had not been disabled, and was re-infecting the file after it had been cleaned.

Some viruses do not record the original length of the file and the new file will often be a few bytes longer than the original. This is quite safe, but some programs will detect the change in length and refuse to run and most integrity checkers will report that the file is still corrupted.

Deleting Files

If you want Vet to automatically delete infected files, load the Vet menu and select the *Edit Setup* option, then the appropriate test-type (eg *Startup Test*), then *Handling of Viruses*. Enable the *Delete Infected Files* option. The corresponding command-line option is ***/Z.*** With this enabled, Vet will overwrite and then delete any infected files. The *Delete Suspect Files* or /O option causes suspect files to be deleted. Both these options remove any trace of the virus from the hard disk and it is **NOT** possible to recover the files deleted. Renaming the files is a safer method.

We do our best to avoid generating false alarms, but it is not always easy to choose a template which never occurs in legitimate programs, especially if the virus has been written in a High Level Language. We try to avoid false alarms by checking each version on a wide range of commercial software, but it is clearly impossible to test more than a small sample of the software in use throughout the world.

Renaming Files

If you want Vet to automatically rename infected files, load the Vet menu and select the *Edit Setup* option, then the appropriate test-type (eg *Startup Test*), then *Handling of Viruses*. Enable the *Rename Infected Files* option. The corresponding command-line option is **/U.** The first letter of the file extension will be replaced with **V**, so FRED.EXE will be renamed FRED.VXE and so on. If you use *Rename Suspect Files* or **/Y**, files with exotic viruses will be renamed, but files with common viruses will be repaired or deleted as usual.

Boot Sector

In both the floppy disks and hard disks, the logical sector 0 is known as the *boot sector.* The boot sector contains all of the critical information regarding the disk's characteristics. If your boot sector is damaged, you will lose all the information on the disk.

Vet Installation

Installing your Vet Updates

When you receive your new Vet update, we encourage you to install it without delay. Install the updated version in the same way as the original copy of Vet. Whilst at the C:\> prompt, put the disk you received in drive A and type "A:install" or put the disk into drive B and type "B:install".

When installing an update, Vet will already have most details from the original installation, but you may alter any of them you choose to or just hit Enter to accept the existing details.

If you have entered templates for non-standard disks, these will also be copied. If you select a custom installation, you will be asked if you wish to continue to use the existing templates.

If you only have a few PCs, we recommend the full re- installation as the new INSTALL program may put additional files or other valuable information onto the Vet Reference Disk. (It also reduces the chances of the Reference Disk being lost, corrupted or out of date when you need it!).

Network Installation

Vet will work with all popular network software and can check files on both the workstations and the file server.

If the workstations have hard disks, Vet should be installed on them in the normal way. Vet can be used to check the workstation before logging into the network and also to check files on the server.

Network supervisors must be very careful to check their workstation before they log in as supervisor. Once they are logged in, any virus which is present will gain full access rights and will usually spread rapidly through the system. For the same reason supervisors should never log in as supervisor, unless they have to do a job requiring supervisor rights.

If you have diskless workstations Vet should be installed on the server, using the Network Install option.

INSTALL will not attempt to take copies of the file server boot sectors, or record the top of memory and will not attempt to modify AUTOEXEC.BAT or CONFIG.SYS. We suggest you install Vet to the file server to a directory where users can access it before they have logged in if possible. Vet will not try to check boot sectors on the workstations, or complain about changes in top of memory.

Installing VET_RES

VET_RES is a resident version of Vet, written originally for use in schools, colleges etc. where it is not always possible to ensure that all floppy disks are checked. However, VET_RES has proved very popular and is now offered as the default TSR for all applications.

VET_RES can be installed automatically during the standard installation procedure or added afterwards using the following procedure. The INSTALL program automatically copies VET_RES.EXE to the same directory as Vet (the Vet directory, if you have followed the standard installation procedure above) and all you need to do is to activate it by putting the appropriate command into AUTOEXEC.BAT; *ie C:\VET\VET_RES.EXE* If no options are specified, VET_RES will be installed with the default options.

VET_RES Command Line Options

The VET_RES command line takes the form:

Vet_res [options]

The following options may be specified:

- **/R** Remove VET_RES from memory.
- **/S** Sleep. Disable VET_RES, but do not remove from memory.
- **/F** Fatal. Don't replace or repair infected boot sectors.
- **/M** Minimise memory usage.
- **/N** No overlays, ie don't check overlays.
- **/P** Protected. If specified, VET_RES cannot be disabled or removed from memory.
- **/0** Replace all unknown, suspect or infected boot sectors.
- **/1** Replace all suspect or infected boot sectors.
- **/&** Hidden operation (don't display messages)

Standard Installation

The standard installation is designed to enable non-technical users to install Vet on their PCs with a minimum of effort. The Vet files will be installed in a directory Vet, which will be added to the PATH specification in AUTOEXEC.BAT. A command to run Vet will be placed immediately after the PATH command. The resultant installation will be satisfactory for the vast majority of users, but if you are technically literate, or know that your PC is non-standard, you may prefer to use the custom installation procedure. We recommend that you do the normal installation even if you know your PC is infected, unless you are unable to access the hard disk. In this case it MAY be possible to recover the hard disk.

When you receive Vet, carry out the following steps:

1. Ensure that the disk you receive (the Vet DISK) is write-protected. (And tell us if it isn't - something has gone wrong!)
2. Format a new floppy disk in drive A using your normal procedure. Format it with the /S option to add the system files. (The disk capacity does not matter, but we suggest you use 360K or 720K disks to save time.) If you normally use preformatted disks, use one of them. This disk will become the Reference Disk for this PC. Put it aside for the moment.
3. If you normally operate through a menu system, exit to DOS.
4. Put your Vet disk in drive A (or B if it won't fit in A) and type

   a:install [or **b:install**]
5. The Vet Installation Program will load. Select **Standard.**
6. VET will ask for a message of up to fifty-eight characters identifying your computer. An example might be: *Sales Department 486* or *Joanne's PC*. The message that you choose will be displayed every time you run Vet and should uniquely identify the PC from any others you use.
7. INSTALL will create the directory C:\VET and write the Vet configuration file (VET.CFG) to it. It will then copy the Vet program files into the C:\VET directory.
8. INSTALL will next ask if you wish to create a reference disk. We recommend you do this, using the bootable disk created in step 2. Clearly label this disk and keep it in a safe place, it will be invaluable if your hard disk is ever damaged or CMOS settings changed.
9. INSTALL will prompt you as to whether or not to install VET_RES. Select yes if you wish to enable the resident scanner.
10. Finally Vet will ask whether you would like to check the hard disk. Select **Yes** in case a virus has already infected your system.

Installing Vet to an Infected PC

If Vet discovers a virus during installation, the first warning will probably be a message that **XXX virus** is active in memory. If you get any message of this type, proceed as follows.

When the installation is finished, reboot the PC and see if Vet reports that the PC is now clean. Don't worry if it reports that the top of memory has changed or that one of the boot sectors appears to have changed. Format another new Vet Reference Disk and repeat the installation procedure. (This will ensure that your Vet installation holds the correct values for your PC and that your Vet Reference Disk is also clean.)

If your PC is still infected, reboot from a clean DOS disk, run Vet from the distribution disk and clean your hard disk, then re install Vet when your PC is clean.

DO NOT destroy the first Reference Disk until you are certain your PC is clean and is working properly. If anything were to go wrong during the installation or clean up, the information on this disk could be invaluable in recovering your data. This disk will probably be infected, so label it clearly and reformat it when you are certain all is well.

If Vet found a virus during the installation, it is very important to do a complete cleanup. It is usually difficult (if not impossible) to discover where you got the virus from and how long you've had it. If you have had a virus for any length of time, most of your disks will probably be infected. Look in all your boxes, drawers and the dark recesses of your office and get all your disks together. Vet **them all,** regardless of where you got them or how long you've had them. If you have a lot of disks, use some way of marking those you've Vetted (eg put a coloured label on the clean disk as you take it out of the machine). You only have to miss one to reinfect your PC.

Make sure that all your proprietary software disks are write-protected. If any of them are infected, copy them using DISKCOPY or copy all the files to a clean disk. Vet the copy and then write-protect it. Label the infected master disk with a very obvious warning and put it away in a safe place. Practise on some of your less important disks first and check they still work before you do the important ones. Watch out for old disks which may be non-standard sizes.

If I have just cleaned a virus from my disks, what else do I need to do?

If you have had a virus infection on your PC, we always recommend that you do a Full Scan of your PC from the Vet Main Menu.

If you've had a boot sector virus, check that you can access all partitions (read the directories for drive C (and D if you have one) and list a few files from each to check that all is well).

If you have had a virus for any length of time, you can be sure that most of your floppy disks will have become infected. If you have a lot of floppy disks to clean, it is a good idea to place some sort of tag on the disk so that you know which ones you have done.

Try to find out where the virus came from and warn anyone else who has used your PC that they may have caught the infection.

Vet normally has no difficulty removing the common viruses, but occasionally something will go wrong. The most likely causes of failure are:

a. The Disk Manager software used by Mitac (and the Setup option *Virus Protection*) prevent you from writing to the Master Boot Record when Vet tries to remove a boot sector virus. Therefore, if you have booted from drive C and Vet has found an apparently good replacement sector but announces that it could not write when you ask it to replace the virus, reboot from a clean system disk in drive A and start again.

b. For some reason a boot sector virus has infected your PC twice, so that the recovered sector is also infected.

c. Your hard disk is so badly corrupted that DOS cannot find the system files, or a vital sector has been erased or damaged.

d. Someone has used a disk editor, or an old version of Vet set up for another PC, to remove a boot sector virus and has put back an incompatible partition table.

If Vet cannot restore your PC and you haven't made a Reference disk, you have several options.

a. Seek expert advice. It may be possible to repair your system using a utility program such as Norton Disk Doctor. It may also be possible to remove DOS boot sector viruses by booting from a clean DOS system disk and giving the command:

   sys c: (if the virus has infected the DOS boot sector)

   or

   fdisk/mbr (if the virus has infected the Master Boot Record)

   However these commands can be extremely dangerous, and their use is not recommended unless you know exactly what you're doing.

b. Run FDISK followed by FORMAT C:/S. WARNING: this will destroy all files so make sure that you have backed them up first.

Installing Vet on a PC with No Hard Drive

If you wish to install Vet on a PC with no hard disk, use the following procedure:

1. Format a new floppy disk, as described in Standard Installation.
2. Select drive A. (Type "**A:**" then hit **Enter**.)
3. At the A:\ >prompt type

   install

   INSTALL will ask if the PC has a hard disk. Answer **N**. The installation will follow the same steps as in the normal installation but will not attempt to write to the hard disk or to update AUTOEXEC.BAT or CONFIG.SYS.
4. When the installation is complete, copy VET.EXE and VET.DAT from your new Vet Reference Disk to your working boot disk and edit your AUTOEXEC.BAT and CONFIG.SYS if required.
5. After you have edited your working boot disk, put it in drive A and hit **RESET**. Confirm that your PC starts up again correctly.

Custom Installation

The standard installation is designed for the non-technical user, and provides an easy-to-install and generic solution. It will provide a good level of protection and assumes the user has no special requirements for their Vet software.

If you have a basic understanding of MSDOS and would like a higher (or different!) level of protection, or know your system is non-standard in some way, you should request the custom installation. This prompts the user at every step and allows modification of the settings from the default values.

For a custom installation, use the following instructions as a guideline and choose the options desired.

The following is just an example and assumes that you are installing from drive B and writing the Reference Disk to drive A.

1. Format a blank floppy disk as a bootable disk, using **FORMAT A: /S**
2. Put your Vet disk in the appropriate drive and from a DOS prompt, type:

   a:install
3. Select **Custom** from the Install menu.
4. The Custom Install menu will be displayed. The following menu choices are available:

VET Directory	to specify the directory to install Vet to.
Enter User ID	allows you to enter a message identifying your PC.
Global Functions	is for setting up which features of Vet you want enabled.
Default Log Files	lets you specify what log files Vet will write for each of its tests.
Enter Password	allows you to enter a password to protect VET.
Okay	Installs Vet according to the options you have configured
5. The Install program will copy the required files into the Vet Directory and prompt you to make a Reference disk.
6. INSTALL will prompt you as to whether or not to install VET_RES. Select yes if you wish to enable the resident scanner.
7. The Install program will then display what changes Vet requires to be made in the AUTOEXEC.BAT, WIN.INI and SYSTEM.INI files. You can either accept these, or modify the files yourself.
8. Finally Vet will ask whether you would like to check the hard disk. Select **Yes** in case a virus has already infected your system.

The default Error Log File

The default Error Log File is:

C:\Vet\Vet_log.TXT

(If you have chosen to install Vet in a different directory this will be shown in the path.) If you are happy with this just hit Enter. However, you can use any name and put the log file in any directory on any drive if you wish: if so, edit it accordingly.

Vet will offer to edit your AUTOEXEC.BAT

If during the installation procedure you choose not to allow Vet to update your AUTOEXEC.BAT, Vet will remind you at the end of the installation procedure that you must update it yourself by including the line:

[Vet\] Vet c:\ [path] / [options]

Refer to Vet **Options** for more information on these.

If you allow Vet to automatically update it, it will revise the path command to include the Vet directory. It will show you the new command and ask your approval. You can edit this if you wish. Hit **Enter** when you are happy with it. If the existing path command is more than about 70 characters long, INSTALL will add a second line to extend the path.

Master Installation

It is possible to automate the installation/upgrading of Vet to all workstations attached to the server, or to create a Master floppy disk to install a pre-configured version of Vet onto multiple PCs. The following describes the procedure required:

1. Log on to the server with sufficient rights to create a directory and files in the area you intend to place the master copy of Vet. Select **Master** from the Install menu to access the *Master/Network Install Overview Menu.*
2. Select **Master Directory** to specify where the master copy will be installed on the server.
3. Select **Enter Data** to specify where the automatic installation will place Vet (typically this will be C:\VET), and to personalise this copy of VET.
4. You can select **Set Options, Global Functions, Default Log Files** and **Enter Password** if you wish to configure Vet yourself rather than using the default values.
5. Select **Okay** from the *Master/Network Install:Overview* menu and the master copy will be installed.
6. To install Vet on individual PCs, you must run the INSTALL file from the master copy. On a network, this may be automated by modifying the system login script. On a Novell network, copy VET_NEW.BAT, VET_INST.BAT and VET_INST.DOC to the master directory, edit VET_INST.DOC appropriately and add the following line to the system login script:

   #command /c f:\apps\Vet\Vet_new.bat f:\apps\Vet c:\Vet

END!!!

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 6:30 PM EST)
Non Melbourne Phone Support 1800 807 062 (8:30 AM to 6:30 PM EST)
Fax (+61) 03 9521 0727 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

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) Quarterly Vet upgrades mailed to you to protect against new viruses
2) A full set of user manuals - comprehensive installation and usage details
3) Additional installation options for networks and systems administrators
4) Access to the Vet internet web site and Bulletin board service - used to provide updates and general virus information
5) Free unlimited Email and phone support (See the Contact page for the support hours)
6) 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
7) 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.
8) 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.