Contact Information

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

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

AUSTRALIA:

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

U.K. & EUROPE:

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

NEW ZEALAND:

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

BELGIUM, HOLLAND & LUXEMBOURG:

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

MALAYSIA

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

USA: Ontrack Data International Inc.

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

Ontrack US Offices

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

Germany: Ontrack Data Recovery GmbH.

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

London: Ontrack Data Recovery Europe Ltd.

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

Why Should You Become a Registered Vet User.

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

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

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

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

Command Line Switches

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

Long-form command line options

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

Scanning

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

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

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

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

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

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

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

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

/fast - scans entry point of each file.

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

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

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

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

Actions

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

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

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

Reporting

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

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

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

Miscellaneous

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

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

/cancel - default, allow cancelling of the scan.

/nocancel - disable cancelling of the scan

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

Contents of Virus Information

The on-line virus information is broken down into a number of more manageable topics;

Information on a Specific Virus

Software Problems that are not viruses

General Virus Information

Different Types of Viruses

Vet Sales and Technical Support contact details

If your question has not been answered by this help system please try the Cybec web site WWW.VET.COM.AU or the Vet Technical Support department. These help systems are regularly improved due to customer input. Any comments or suggestions would be most welcome, please Email **support@Vet.com.au** or mail to your closest Vet distributor.

Viruses and Windows

If an infected program is run before Windows is opened, the virus appears to operate normally. In our tests, Jerusalem infected WIN.COM, but did not infect Windows applications. When a DOS file infected with Jerusalem was run from Windows, Windows helpfully reported: *Your Pop-up program has been loaded, and you may activate it as you would normally*. However the virus was apparently not able to infect other files and was not found in memory by VET. We got the same message and result when we ran a file infected with AntiCad, but it did manage to infect the Master Boot Record. When we ran Windows with *Frodo* already installed, or attempted to run a file infected with *Frodo* from Windows, the system crashed. Some viruses (eg *Junkie*) will cause Windows to report a message about not being able to use 32-bit disk access when it has been previously able to.

Windows files have a dummy .EXE header which gives a message about loading Windows if you try to run them under DOS. If you do so and the PC is infected, this header will become infected. Jerusalem and its descendants will destroy the file in the process, but most viruses will not have any effect on the program's operation under Windows. If Windows files do become infected, Vet will detect and remove the virus in the normal way.

Sabotage

By now, most large organisations have been hit by viruses, but far more data is still destroyed by careless, incompetent or malicious users. You can reduce the risks from careless and incompetent users by education and by using well designed software, but it is much harder to prevent sabotage. The best protection against both sabotage and mechanical failures is to establish and use good backup procedures. Proprietary backup programs enable you to take a quick snapshot of your PC, but unless you immediately restore the data onto a second PC, preferably at another location, the only time you will know if your backup is any use is when it is too late. We strongly recommend that you use COPY, or XCOPY, to copy all vital data to floppies. Check that you can read the files (on another PC) and store them somewhere else. BACKUP, supplied with the PC, is notoriously unreliable and boot sector viruses will ruin most proprietary backup disks if they infect them.

More Information

There are many potential sources of virus information but not all can be relied upon as being accurate and unbiased. Here are some reliable sources of information:

1. Virus Bulletin

21 The Quadrant
Abingdon Science Park
Oxfordshire, OX14 3YS
United Kingdom

This publication is owned by Sophos Ltd, publishers of Sweep Anti-Viral software, and it provides accurate technical information on viruses. Vet's Roger Riordan is a member of the Virus Bulletin's Advisory Board and in June 1995 Jakub Kaminski was appointed as Virus Bulletin's Technical Editor. Virus Bulletin can be obtained on a subscription basis from your Vet distributor.

2. Secure Computing

West Coast Publishing Limited
William Knox House
Britannic Way, Llandarcy
Swansea, SA10 6EL
United Kingdom

This monthly journal provides good quality technical articles and information on new viruses. Vet's Roger Riordan is a frequent contributor to this magazine.

3. Computer and Security

Elsevier Advanced Technology
PO Box 150
Kidlington
Oxford, OX5 1AS
United Kingdom
Email: j.meyer@elsevier.co.uk

This journal contains many papers on the subjects of computer viruses and security. For research purposes, this is a very valuable resource.

4. VIRUS-L / comp.virus

The *Frequently Asked Questions* (FAQ) document is available by anonymous ftp from **ftp.cert.org**

This is a USENET newsgroup, also available as a mailing list, on the Internet. For information about it, as well as much useful information, see the FAQ file. Many of the well-known anti-virus researchers use this to exchange much useful information.

Viruses and Anti-Social Software

Unfortunately there are as many misfits among computer users as anywhere else and over the last few years, a wide range of anti-social software has appeared. This software surreptitiously interferes with the user's computer, without the perpetrator having to gain direct access to the computer. Software of this type can be divided into three main groups:

- Worms
- Trojan Horses
- Sabotage

If users are have problems executing a program, it may not always be a virus infection. Some other possible causes are:

- Bugs
- Invalid Boot Sectors

There are also a number of hoax viruses that keep circulating on the internet. If you receive an email warning about a new virus it may be that it is actually a hoax. For a list of the common hoaxs click here.

Worms

A *worm* is a program that has been written to replicate through a network of computers and unlike a virus, does not need a carrier program in order to multiply. The main difference between a worm and a virus is that a worm actively tries to infect other computers, whereas viruses rely on the users to spread them, albeit inadvertently. Worms haven't been a threat to PC networks in the past since none existed of sufficient size or uniformity, however the growth of the Internet and the greater availability of common applications for it may change this.

Trojan Horses

A *Trojan Horse* is a malicious program that hides inside a legitimate program, as in the soldiers in the wooden horse of Troy. There are lists of programs known to contain Trojan Horses, but the best protection is to be very careful to obtain all your software from reputable sources. The only way to prove that a program does not contain a Trojan Horse is to do a total disassembly and this is impractical for any but the most trivial program.

Validation programs, such as VCRC, calculate Standard Cyclic Redundancy Codes for any file and validation data is available for many Shareware products. If the validation data for a file does not match the published values, the code has been tampered with after the final release.

Viruses

In biology, a virus is a small particle of living material which is not capable of breeding by itself, but which has sufficient genetic material to enable it to enter a living cell and subvert the active processes of the cell so that the cell replicates the virus, producing new particles of virus which can attack other cells. An example is the Ecoli virus which infects humans.

By analogy, a *computer virus* is a program which attaches itself to another program, but modifies the action of that program so that the virus is able to propagate. There are thousands of viruses which differ widely in the types of program they infect, the way they propagate and in the side effects that they have. Some are extremely destructive while others are relatively benign. Viruses can be classified in several different ways, but the most common way is to classify them by what they infect:

How Viruses Work:

Choice of Vehicle

In principle, any program could serve as a vehicle for a virus, but for a virus to propagate effectively it must attack a program which is both common and likely to be swapped between users. Some viruses are specific and attack a single program, while others have more catholic tastes and attack a wide range of programs.

Common vehicles are:

1. DOS boot sector
2. Master boot record
3. Executable files (eg those with COM and EXE extensions)
4. Files containing an executable code (eg Word or Excel documents containing auto-macros).

It is also possible to design viruses which infect device drivers and batch files. Both types of virus exist, but neither is common.

Boot sector viruses are fairly easy to design and were probably the first to appear. They are relatively inconspicuous (if they don't display messages etc.) but are also easy to keep out of your system. Viruses which infected executable files soon followed and now there are multipartite viruses which infect both program files and boot sectors.

Some viruses alternate between boot sector and programs. This makes them harder to study, as it is impossible to generate test files without infecting a hard disk.

Propagation Mechanisms

If a virus is too aggressive in its efforts to propagate, it will be conspicuous by causing excessive disk activity, but if it is too coy it will probably not infect many files. There are two main classes of infection mechanism:

When a program infected with a *direct infector* is run, the virus actively searches for a file or files to infect. It may search the current drive or directory, or selected directories, such as the directories specified in the PATH. It then loads the infected file and runs it. Direct Infectors do not remain in memory and they are not very common, as the infection mechanism is not very efficient and the additional disk activity is obvious, especially when all files are already infected.

When a program infected with an *indirect infector* is run, the virus installs itself in memory, usually redirects one or more interrupts and then runs the original program. Most indirect infecting program viruses infect every file which is loaded for execution and some infect every executable file which is loaded for any reason.

Boot sector viruses usually act like indirect infectors when infecting floppy diskettes and like direct infectors when infecting hard drives.

Location in Memory

Program viruses which use DOS Function 31h to go resident, stay in low memory and other programs use the memory above them. Viruses which modify the memory allocation chain usually move themselves to the top of normal memory and set the top of memory marker down. Boot sector viruses normally occupy the top of memory. A few viruses move themselves to the top of memory, but do not reserve any memory to protect themselves. These cannot be detected by checking the available memory, but most large programs will crash the system when they overwrite the virus. The EDV virus searches for memory in the system area (0A000:0000h - 0F000:FFFFh). There are many programs that use this area now and it is likely that this virus will also crash many systems.

A few viruses have tried to find other hiding places. The Troi family install themselves in the top half of the Interrupt Table and others hide in the DOS buffer area.

Stealth

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

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

Encryption

Virus scanners generally detect a virus by looking for a sequence of instructions or template characteristic to it. Some viruses are encrypted, usually by some simple procedure like XORing each byte with a key chosen at random for each new copy. These viruses are detected by looking for the decryption procedure at the start of the virus.

Warheads (also known as Payload)

Some viruses exist just to propagate, others have *payloads* or *warheads*. This can be the display of a taunt (eg *Your Computer is now Stoned!*) or it may interfere with the operation of the computer in an amusing, irritating, or destructive manner. Generally a virus will propagate more widely if its warhead doesn't activate immediately; the payload is usually triggered on some event, or after a certain amount of time. It is unwise to deliberately trigger a virus's warhead.

Bugs

The opportunities for testing viruses are limited and it is impossible to recall faulty products, so most viruses have bugs. These may reduce the viability of the virus or make it more obvious, but often they make the virus unintentionally destructive when they interact with another program (or virus!) or a non standard piece of hardware. On a number of occasions infections with normally trivial viruses have become disasters because a bug in the virus has interacted fatally with the PC's particular configuration. Some viruses betray themselves by causing Critical Error Messages when they try to infect a write-protected disk.

Invalid Boot Sectors

A normal boot sector contains a parameter table specifying the number of tracks, heads and sectors, size of sectors, numbers of FATs and so on. This takes up bytes 0bh to 1ch and includes the media descriptor byte. This was originally intended to indicate the type of disk, but most programs don’t use it. Many viruses (including Brain, Computer Ogre and Stoned) overwrite the parameter table. The results are unpredictable and apparently depend on the size of the disk, the last disk read, the DOS version and possibly the BIOS. MSDOS doesn't usually seem to mind with 360K disks, but will often refuse to read other size disks, or will not find some or all files.

Type of Viruses

There are many different viruses loosely grouped into families. Each of these families is explained below;

- Boot Sector Viruses
- File Viruses
- Boot Sector and File Viruses
- Parasitic Viruses
- Companion Viruses
- Overwriting Viruses
- Polymorphic Viruses
- Macro Viruses

Boot Sector Viruses

The Boot Sector viruses can only infect your system if you boot from an infected disk. However, the disk does not have to be a system disk to transfer the virus. A major weakness of the IBM PC in its most common configuration, is that it will always first try to boot from drive A. If you never boot your PC from a floppy disk you are generally safe from boot sector viruses, but even booting with a floppy disk inadvertently left in drive A can infect your PC. So always check the floppy drive is empty before switching on or rebooting your computer.

As the boot program is very short, it cannot contain both the virus and the original boot program and the virus has to make sure that it is run first. Therefore, when a virus infects a new disk, it has to store the original boot program (and often most of the virus as well) somewhere else on the disk and then put its own installation procedure in the boot sector. Some viruses simply move the boot sector to a fixed place, trying to choose somewhere which won't be too obvious. The Stoned virus puts the old boot sector at the end of the directory where it won't be noticed unless the disk contains more than 96 files in the main directory (on a 360K disk). The Yale virus occupies the last sectors of the last track and will only be noticed if the disk is completely full, while the Den Zuck virus formats an extra track on the disk above the normal last track (where it is completely inaccessible to any normal procedure and to most disk editing utilities).

Other viruses look for an unused cluster on the disk, put themselves in it and then mark the cluster(s) used as bad, so that MSDOS will not try to use them for something else. On a normal disk, the loss of capacity is insignificant, but if the disk has a non standard data structure the virus may overwrite something vital when it writes to an apparently empty cluster.

If a virus also infects hard disks, the process is similar but the virus can infect either the Master Boot Record or the DOS boot sector. On normal hard disks, Sector 1 (the MBR) is the only sector used on Cylinder 0, Head 0 and many viruses store themselves in the empty sectors. Unfortunately these sectors are not empty on some non-standard PCs, and infecting them may have dire consequences.

File Viruses

Also called *program viruses*, these generally 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. There is a greater number of file viruses than boot sector viruses, but boot sector virus incidents are far more common.

File viruses can be further divided into Parasitic Viruses, Overwriting Viruses, Companion Viruses and Linking Viruses.

All of the above can use some of the following techniques Stealth, Encryption or Polymorphism.

Multipartite (Boot Sector and File) Viruses

These viruses infect both boot sectors and files. This generally makes them far more effective in propagating, since they can be spread by booting from an infected disk, or by running an infected file, and thus there is more chance of being infected. The Junkie virus is an example of a common multipartite virus; it has been prevalent in Australia for the last couple of years.

Parasitic Viruses

Parasitic viruses are those that attach themselves to files in order to propagate. They generally keep most of the file intact and either add themselves to the start (prepending viruses) or end of the file (appending viruses). COM files are easiest to infect, as they are simply loaded directly into memory and execution always starts at the first instruction. Thus a virus can simply insert its self at the beginning of the file. Then when the file is run, the virus is loaded before the actual program. This is how early viruses infected .COM files. The infection process is quicker if the virus is appended to the file but this causes some complications, as the first few bytes of the file must be saved and replaced with a jump to the virus and the virus is not at a fixed offset from the start of the code segment.

While .COM files cannot be longer than 64 kilobytes, .EXE files can be of any length (provided they will fit in memory), but the file structure is more complex. The program can be built up from a number of segments and the file has a header which specifies the size of the program, the segments used and how they are to be linked together and where execution is to start. When a virus infects an .EXE file, it must save the original contents of the header, copy itself to the end of the file and modify the header so that the virus is loaded as part of the file and executed first.

Once virus writers had learned how to handle .EXE files, most found it easiest to treat .COM files in the same way. Thus many viruses put the virus at the end of both .COM and .EXE files. Many files contain empty space and some viruses exploit this by overwriting it with their own code, so that they don't change the length of the file. At least one virus (*Command Bomber*) comes in several sections, which are inserted at various locations in the file.

Companion Viruses

If you try to run a program without specifying a file extension, the system will always try to find and execute the .COM program first and if it cannot be located then .EXE file will be called next. Companion viruses make use of this to provide an infection mechanism which does not modify the original file in any way. These viruses only infects .EXE files and do so by writing a companion .COM file with the same name. Then, when the user runs an infected program, the .COM file containing the virus is run. It looks for another .EXE file to infect, then loads the requested .EXE file and runs it. An example of a companion virus is the *AIDS II* virus.

Overwriting Viruses

Most viruses are careful not to destroy the infected file, but overwriting viruses overwrite part of the infected file, so that it will no longer operate. However, this makes these viruses extremely obvious, so they are unlikely to spread far. The Zeroto-0, or Australian 403 virus, is of this type. When an infected file is run, the virus searches for an uninfected .COM file and replaces it with a 403 byte file which only contains virus. The original file is destroyed, so infected files appear to run, but do nothing.

Polymorphism

Polymorphism is an advanced form of encryption in that the key changes all the time, rather than staying the same. Typically, in polymorphic viruses, the decryption procedure will use three or four registers and each is chosen randomly from the set of registers available. Additionally, the procedures often include variable numbers of randomly chosen instructions which do nothing, but act as inert fill, or noise. Writing procedures to detect these viruses is more difficult than using a template, but the viruses are also much harder to write and there are not many of them, even though engines are available to add polymorphism to a normal virus. The main problem with polymorphic viruses is that detection is more difficult and less reliable, and it is not practical to disinfect files that have been infected.

Macro Viruses

The majority of macro-viruses are written in WordBasic which is used for the Microsoft range of products, most notably MS Word. MS Word is available on a number of platforms and in a number of languages giving a greater variety of environments where macro-viruses can propagate. People copy, edit and share Word documents more often than sharing a floppy disk, this allows macro viruses to spread faster than other varieties of viruses. Macro viruses also use the growing popularity of attaching Word documents to E-mail and downloading files from the Internet as additional vehicles to infect many more computers.

They arrive attached to a spreadsheet or document, when the file is opened it will transfer from the document to the application template. Any new or existing file that is saved will have the virus inserted into it. The virus will spread to other files via a variety of methods, the most common is the File | Save As sequence which is used to save file or by using Save As to save a different version of an existing file.

By default Macro viruses (including the Excel macro viruses) will automatically be detected and cleaned by the resident protection.

How To Find Information About A Specific Virus

This help file does not contain information on every virus, it only contains information on each of the families of Viruses that have been detected by Vet users. If you wish to check if a specific virus is detected by this version of Vet please open the VIRUSES.HLP file in your Vet directory. (Normally C:\Vet\Viruses.hlp)

The easiest way to find information is to check the index;

For Vet95 or VetNT users select Index (above), Find, Next>, Finish and enter the name of the virus.

For Vet for Windows 3.1x users select Search (above), Find, Next>, Finish and enter the name of the virus.

1099

1099 is a file virus which infects .COM and .EXE files, adding 1099 bytes to their length. It contains a dangerous payload including corrupting of CMOS date and contents of MBR on a hard disk.

ABCD

ABCD is a boot sector virus which infects the Master Boot Record on a hard disk and the DOS Boot Sector on floppies. The virus is 6 sectors long and keeps its code encrypted even while active in memory. The virus decrypts parts of itself when it needs to execute certain procedures and encrypts them as soon as the execution flow reaches another subroutine.

The virus name is derived from its signature on the infected disks; all infected boot sectors contain the word 0ABCDhex located at offset 017Bhex. The virus hides the copies of the original boot sectors; the original MBR is stored on cylinder 0, head 0, sector 2 and the original DBS is stored on the last cylinder, head 0, sector 1.

Symptoms of infection with ABCD are that amount of available memory decreases by 4K and there is additional disk activity while accessing new floppies.

The ABCD virus contains a random payload targeting a specific set of files with the following extensions: ‘DBF’, ‘PRG’, ‘FOX’, ‘LSP’, ‘MEM’, ‘SCR’, ‘MAS’, ‘PLM’, ‘ASM’, ‘PRO’, ‘PAS’, ‘C’, ‘BAK’ and ‘LST’.

Alfons.1344

Alfons.1344 has been seen extensively in the wild in Israel and is thought to originate there. It has been used by one of our competitors on a “virus test disk” which they give to prospective customers to assess their program: since users now have access to this virus, we believe that it may soon appear in the wild here.

Alfons.1344 is a memory resident, file infector which infects .COM files, adding 1426 bytes to their length where it is a prepending infector, and infecting .EXE files, adding 1344 bytes to their length where it is an appending infector.

It contains an encrypted message, as follows:

> *ALFONS!*
>
> *synchonizing drive C: (Do not interrupt this operation!)*
>
> *Done*

Alfons.1344 contains a nasty warhead which is activated if the virus infects a PC on Sunday the 1st of the month, or Monday 2nd, Tuesday 3rd etc, up to Saturday 7th. It may overwrite the hard drive of the PC.

Angelina

Memory-resident boot sector virus based on the Stoned virus. It contains, but does not display, the message:

> *Greetings for Angelina!!!/*
> *By Garfield/*
> *Zielona Gora*

Anthrax

On the 17th of each month, the computer beeps or clicks on every keypress.

Anthrax initially just infects the Master Boot Record of the hard disk. After the PC is booted from the infected hard disk, the virus becomes memory resident and infects files also. Anthrax was uploaded together with other viruses to many bulletin board systems in New Zealand.

It contains the text

> *ANTHRAX*
>
> and
>
> *(c)Damage, Inc*.

Anti CMOS

Infected floppies become unbootable and systems with non standard MBRs may crash after infection.

This virus infects boot sectors of hard and floppy disks. The original Master Boot Record (hard disk) and the DOS boot sector (floppy disks) are not stored anywhere. When active in memory, Anti-CMOS decreases the amount of available memory by 2 kilobytes and redirects interrupt 13H. There are two known variants, one is meant to change the CMOS date and the other to play a tune. Neither of these effects have been triggered in any incidences in the wild.

Anti EXE

Infects the boot sectors on hard disks and floppies. Saves original Master Boot Record to hard disk or a hidden buffer in memory. Anti-exe also corrupts certain EXE files when read. A stealth virus which occupies 1 K of memory. The payload is executed as a 3 in 256 chance. It has been suggested that the target of this virus is a Russian anti-virus program.

AntiCAD (also known as Plastique, Taiwan 3 or Invader Family)

Anti-Cad infects boot sectors and .COM and .EXE files. Periodically it plays a tune and if the Ctrl, Alt and Del keys are pressed simultaneously during the tune, or if ACAD.EXE is referred to, the virus deletes information on drives A-D and modifies the CMOS setup information. This family of viruses includes the Plastique 5.21 and Invader viruses, which were some of the first to infect both boot sectors and files. They infect the boot sector of any disk referred to and any file opened. They load themselves into top of memory if loaded from the boot sector and in low memory if loaded from a file.

They use the top of memory if loaded from the boot sector, but in low memory if loaded from a file. Plastique 5.21 first issues a warning not to run ACAD.EXE. In some circumstances they may also disable disk writes.

VET identifies them variously as AntiCad, Invader, Taiwan 3, or Taiwan 3A.

Anxiety.(family) (also known as Win95 and Harry.B)

There are a number of variations of this overwriting virus including .poppy and .Harry.

Once a Windows 95 system has been infected the virus will be loaded into memory and will wait for .exe files to be opened, so that it can infect them.

This virus infects Windows95 PE (Portable Execution) files and has been detected in Germany, Finland, USA and Australia.

As this virus has overwritten part of it's host file and not saved the area of the file that it now occupies it is not possible to return infected files to working order.

Australian 403 Virus

This is a direct acting, overwriting virus that destroys infected files. A stupid virus, of interest only because it's thought to have been written in Sydney. Replaces infected files with 403 byte files only containing virus.

Autumnal.3072

Autumnal.3072 is a Multi-partite virus.

Symptoms of Autumnal.3072 include the amount of available memory decreasing and additional disk activity while executing new files.The virus received its name from the message contained in its code:

Ver 4.00 (C) Copyright Autumnal Water Corp. 1991

Vet version 9.24 will detect and clean Autumnal.3072

Azusa

This is a potentially serious virus because it corrupts the Master Boot Record but it does not save the original. It may crash systems with a non standard MBR and there will be no copy to put back if you have not previously saved one. On every 32nd boot from an infected disk, it will disable the parallel and serial ports. The original boot sector is written to track 40, regardless of disk size and files may be corrupted on high density disks.

Baran.3294 & .4968

This file virus is polymorphic and encrypted. Once it is memory resident it will infect .EXE and .COM files. It can also display the message:

Gwader to baran!

BARA3294

Barrotes

If the virus becomes resident on the 5th of January, it displays the message *Virus BARROTES pro OSoft* and coloured bars across the screen. It then overwrites the master boot record of the hard disk, causing the hard disk to be inaccessible.

This is a memory resident, parasitic virus, capable of infecting both EXE and COM files (including command.com). Barrotes is not a stealth or polymorphic virus, and therefore is simple to detect.

Better World (also known as Fellowship)

Increases file lengths by between 1019 and 1027 bytes. Decreases amount of free memory by 2048 bytes. It contains the text:

This message is dedicated to
all fellow PC users on Earth
Towards a better tomorrow
and A Better Place to Live In.

The first time an infected file is executed, the virus installs itself as a memory resident program in low system memory and takes control of interrupt 21h. Then it infects any .EXE file run and appends itself to the infected program.

Another virus based on the Better World virus is known. It has a number of changes, including the addition of this message:

This message is dedicated to
all fellow PC users on Earth
Do NOT provoke the INTROVERT
ALSO the security here stinks

BIOS.2048 (also known as Meta)

The Bios virus is parasitic file virus which infects .EXE and .COM files. In .EXE files, the virus code is placed at the end of the file and in the infected .COM files, virus inserts itself at the beginning of the programs. All infected files become 2048 bytes longer. Symptoms include File length growth and continual system reboots

Bios is a memory resident virus and while active in memory it takes 8,336 bytes. The virus contains an encrypted message:

“Mr. Watshira Sae-eu KMIT_NB Date 12/28/1990 BIOS”

Black Monday

Formats the hard disk the 2nd time an infected file is run on a Monday. A relatively unsophisticated albeit damaging virus that infects .COM and .EXE files. It includes the text *Black Monday.*

BootEXE 451

No obvious symptoms or known warheads.

The BootEXE.451 virus is a multipartite Master Boot Sector and EXE file infector. It contains an encrypted message **Stalker** inside the virus. After an infected EXE file is run the virus will infect the Master Boot Sector. On the subsequent boot of the machine it will become memory resident, checking for any read/writes on EXE files. It will then alter the files header to allow the execution of the virus before the actual file is run.

Boza (V32)

The virus was written in Australia by a member of the VLAD group but it was first discovered in England. The Boza virus targets files of PE (Portable Executable) format. This format is used by Windows 32-bit systems such as WindowsNT and Windows 95. The new virus is a non-resident, direct infector.

When an infected file is run the virus infects up to three .exe files in the current subdirectory. On the 31st day of a month, when there are no more files to infect, the virus displays a message box with the text:

'The taste of fame just got tastier!

VLAD Australia does it again with the world's first Win95 Virus

From the old school to the new..

Metabolis, Quark, Darkman, Automag, Antigen, RhinceWind, Quantum, Absolute Overlord, CoKe'

Another message, visible in the virus body, but not displayed, reads:

'Please note: the name of the virus is

[Bizatch] written by Quantum of VLAD'

The virus infects by adding a new section named '.vlad' and modifying the program's entry point in order to start the execution from the virus code. Additionally Boza uses one of the reserved locations in the PE header (offset 4chex) for storing its signature (F00DHex). The infected files are bigger than originals by 3192 bytes, but occasionally the virus corrupts the files it infects.

VET version 8.50 detects files infected with Boza ('/f' switch or 'full scan' option is recommended). Because of potential file corruption, users are advised to replace all suspect files with the clean originals.

Boot 437

The Boot 437 virus is memory resident and infects boot sectors of hard and floppy disks. Loss of files on high density disks (and less commonly, on other diskettes) is a symptom of this virus. There is a bug in the infection routine and on 1.44 Mb disks, the old boot record is stored in cluster 3, overwriting any data contained there. This is not an intentionally destructive; the virus actually tries to calculate the last sector in the root directory.

Brain (also known as Pakistani, Ashar or Dungeon Virus)

Brain infects 360 Kb floppy disks only, marking three clusters as bad and changing their volume label to *(C) Brain*. It uses 7 kilobytes of memory. Brain is of interest only because it is believed to be the first successful PC virus written. It will only run on PCs with an 8088 or 8086 microprocessor.

Brasil

This boot sector virus is memory resident. On hard disk infections, the original Master Boot Record is moved to sector 3, and on floppy disks the DOS boot sector is moved to the last sector in the root directory. After the hard disk has been infected for a certain amount of time, the message *Brasil Virus!* is displayed and random data is written to the hard disk.

Bravo

This is a boot sector virus infecting the Master Boot Record on hard disks and the DOS boot sector on floppy disks. It overwrites the Master Boot Record with the string *Bravo* when its payload is triggered.

Bua.2263

This virus probably originated from the USA. It is a trivially encrypted, non-resident COM infector. File length increase is nominally 2263 bytes but can vary. The virus itself expands with each infection and when size and a counter reach a certain point the first payload is triggered. The first payload is non destructive and is best described as *Phallic Animation*; displayed on screen with the message "**Big Caibua"**. When the second trigger point is reached, the second payload is activated. This includes reformatting of drive C, and deleting and corrupting of existing files and directories.

Bunny
A simple boot sector virus, based on the Stoned virus code.
Contains the word *BUNNY.*

Bupt.9146

This is a harmless boot sector virus infecting the Master Boot Record on hard disks and the DOS boot sector on floppies.

The virus contains a message:

> *Welcome to BUPT 9146, Beijing!*

Burglar.1150

Burglar.1150 is a memory resident, appending file virus which infects .EXE files only It contains two plain text messages which read:

AT THE GRAVE OF GRANDMA and BURGLAR/H.**

and the latter is displayed, flashing, if it happens to be 14 minutes after any hour when the virus has infected a file.

One unusual point is that unlike other file infectors which keep a copy of the original header information somewhere in them, Burglar.1150 keeps an encrypted copy of this information, meaning that the recovery procedure must decrypt the .EXE header before replacing it.

ByWai

ByWai is a polymorphic, memory resident, encrypted virus which infects all executable files. It is a linking virus, infecting files without modifying any of the targeted programs. The ByWai virus infects a program by changing the pointer to the first cluster (this value is stored in the directory entry) and redirects it to the virus code. As a result all infected files seem to start from the same sector on a disk, ie files are cross-linked.

ByWai creates a working file called CHKLIST .MS that is 2048-bytes long and has the Hidden, System and Read-only attributes set, in the root directory of an infected disk. This is similar to the files created by Microsoft Anti Virus but they are clearly visible in a directory whereas the files created by ByWai are hidden. The virus contains encrypted messages *<by:Wai-Chan,Aug94,UCV>* and *The-HndV.* It triggers if the year is 1996 or later, if the day of the month is equal to the doubled month number plus 2 (ie 4 January, 6 February, etc). The virus will then display in scrolling text

TRABAJEMOS TODOS POR VENEZUELA!!!

(Spanish for *Let's all work for Venezuela*) and plays a tune.

Cascade (also known as Autumn or Blackjack Virus)

This encrypted virus infects .COM files, adding 1701 or 1704 bytes to their original size. Random characters fall until they hit the character below so that eventually all the characters on the screen are piled up at the bottom. Cascade is primarily a nuisance and does not cause any damage to the data. So if you are editing a file when the characters begin falling, you should save the file and resume editing it after you've removed the virus from the computer.

Chaos.1241

This is a memory resident, parasitic file infector which infects .COM and .EXE files, increasing their length by 1244-1259 bytes for .EXE files and by 1241 bytes for .COM files. It contains a very destructive payload which, when triggered, overwrites 9 sectors on side 0 of the current disk, starting at cylinder 39 and working downwards. If the infection occurs on 13 September, after 4 cylinders have been damaged, the virus displays the encrypted message:

I see, I come, I conquer...Trojan horse -CHAOS v2.0 by Faust

The warhead is triggered once a month but the exact day depends on the month and year. In 1995 the dates are August 8, September 13, October 10, November 11 and December 12. In 1996 they are January 18, February 19, March 20, May 5, June 7, July 8, August 9, September 13, October 11, November 12 and December 13.

Clone

Your PC is Cloned!! displayed on screen on April 1st.

If an infected file is run on April 1st, the message “Your PC is Cloned!!” will be displayed before the program is run. Clone is a **companion virus** which “infects” .EXE files by creating a hidden .COM file with the same name. Because of the way COMMAND.COM searches for programs, the hidden .COM files will be run instead of the users' programs. These load the virus into memory and it then loads and runs the original program. The virus does no deliberate damage and the original files are not altered in any way. Companion viruses have never proved very successful and Clone is not expected to pose a significant threat.

The companion files have the **hidden, system** and **read only** attributes set and are 833 bytes long. They contain the following messages at the end.

Your PC is Cloned!!

Clone Virus ver 2.0 .. (c) Cataclysm 1992 Sydney, Australia

....To Create and Mutate....

Disinfection is simply a case of deleting the companion files. However, this can only be done after the PC has been booted from a clean disk (so that the virus is not active) and using an appropriate utility to clear the **Read Only** attribute.

CNTV.2630

Cuban New Technology Virus 2630.

This encrypted file virus will randomly insert the instructions to decrypt and run the virus within the .EXE or .COM file. This virus has a warhead that will display the message “Cuban New Technology Virus” once every hour on the 7th day of any month.

Computer Ogre (also known as Disk Killer)

This is a boot sector virus with an extremely nasty warhead. It marks three unused sectors bad and stores the main body of the virus and the original boot sector in them. On hard disks it replaces the DOS boot sector, which it stores in the unused space following the Partition Table. If the computer is not turned off for 48 hours, the virus is activated and writes garbage over the entire hard disk.

On high density disks the virus correctly marks an unused sector bad, but then stores itself elsewhere. Sometimes it overwrites a program and if this happens, it may trigger if the program is run instead of waiting 48 hours. It may not work correctly and may not destroy the hard disk, but don't count on it. It contains the text:

> *Disk Killer -- Version 1.00 by COMPUTEROGRE*

Da Boys

The virus infects the DOS Boot Sector of hard and floppy disks. It doesn't save the original sector, but it is well written and the infected system disks are still bootable.

Infected boot sectors do not contain the usual messages, but the text 'DA'BOYS' (the Dallas Cowboys) can be seen instead. When active in memory, the virus occupies the usually unused space in the region 0:021D hex to 0:031F hex and it redirects the interrupt 13 hex (low level disk access).

Because part of the boot sector has been destroyed and there is no way of knowing exactly what has been destroyed it is necessary to follow these steps to remove the virus and return the boot sector to working order.

For Floppy disks:

Accept Vet’s offer to replace the boot sector with a known clean boot sector

For Hard Disks:

Boot with a system disk that has the same version of DOS as the operating system that is on the PC. From the DOS prompt type SYS C: and select <Enter>. (This will overwrite the system files that have been damaged by the virus, removing the virus, and repairing the files to working order)

Dark Avenger

Overwrites random sectors of hard disk at random times.

This is a particularly nasty virus since it does not make itself known until it has caused a fair amount of damage. If the victim backs up regularly using only a small number of disks, it is likely that they will all be infected before the virus is noticed. Dark Avenger calls the BIOS code directly rather than redirecting interrupts, so interrupt-monitoring software will not detect it. The virus infects .COM and .EXE files.

Den Zuk (also known as Ohio and Search)

This virus, which was written in Indonesia, comes in several versions. It writes an extra track (No 40) with non-standard sector numbering and stores the original boot sector in this track, starting at sector 33. When it infects a disk, it searches for the Brain virus and removes it if it is present and updates older versions of itself (known as Ohio). It interrupts the Ctrl-Alt-Del combination and displays the text *Den Zuk* in big purple letters. This virus will not run on most PCs and has never been common.

Die Hard

On Tuesday 3, 11, 15 or 28 of any month, Die Hard (also called *Die Hard 2*) may prevent writing to opened files and display an *SW Error* message instead. If the video mode is changed to mode 19, it displays *SW* in big colourful characters. If files with extensions .PAS or .ASM (Pascal and Assembly language files) are opened or closed, Die Hard overwrites the first 256 bytes with the code which when compiled displays D1hex A5hex on the screen.

Die Hard infects .COM and .EXE files, using tunnelling and stealth techniques. It installs itself in the last memory block (MCB) and takes about 10 kilobytes of memory. Files are infected when they are loaded, opened, closed or renamed. It infects .COM files between 24bytes and 57345 bytes, and .EXE files between 24 bytes and 448K as long as the first file opcode isn't E8 hex. It doesn't infect IBMDOS.COM or IBMBIO.COM and requires 192K extra memory. Die Hard increases the length of infected files by 4000bytes and redirects interrupts 0, 1, 8, 10hex, 13hex, 21hex, 22hex, 24hex and 40hex. It contains the encrypted message:

SW Die Hard 2

Dir II

No obvious symptoms or effects.

The Dir II virus is a 1024 byte linking virus from Bulgaria. It infects COM and EXE files in each directory. Its infection process involves linking a single cluster which contains the virus code to each infected file. It preserves the original location of the start of the file in an encrypted form within the directory entry, which means the files aren't altered in any way and can be accurately and completely recovered. It should be noted, that if any other parasitic virus is on the same disk, the scanning program will not find it until the Dir-II infection has been removed. See ByWai virus

DiskWasher

This is a boot sector virus based on the Stoned virus code. It contains a dangerous payload; it formats the hard disk after 5000 infections and displays the text (with heart characters at start and end):

From DiskWasher with love

Dudley

Increases file lengths by between 1200 and 1250 bytes. Causes delay in loading files from floppies.

This virus was first reported on 15th February 1993. It is highly infectious, encrypted and moderately polymorphic. It contains the message:

<[Oi Dudley!][PuKe]> .

Although Dudley does no intentional damage and is quite inconspicuous, it may disrupt Windows programs execution.

EDV

This is a boot sector virus infecting the Master Boot Record on hard disks and the DOS boot sector on floppy disks.

This is a particularly destructive virus. It was one of the first viruses to use high memory, but if it isn't available it uses conventional memory. It infects the hard disk as if it is a floppy, so it will immediately destroy some data by overwriting it with the original boot sector. It overwrites the system area of the hard disk(s) after infecting six floppies, thus making them unusable.

ECO (also known as Bleah.C)

This is a Boot sector virus infecting DOS boot sectors on floppies and Master Boot Record on hard disks. The virus uses stealth techniques so that while resident in memory, it controls access to infected boot sectors and returns a copy of the clean, original boot sector when a user tries to read the actual contents of the infected boot sector.

Edwin

Discovered in the wild in the UK in early 1997. Edwin is a boot sector virus infecting Boot Sectors on floppies and DOS Boot Sectors on hard disks. The virus is memory resident, when active in memory it takes 2K from the Top Of Memory (the amount of available memory decreases by 2K). Edwin is two sectors long, storing the rest of its code on track zero (cylinder 0, head 0, sectors 4 and 5) in case of a hard disk and in the last two sectors of the root directory in case of a floppy. As a result, systems using track zero on the hard disk to store the valid code or data will crash if infected with Edwin. On floppies up to 32 files may be lost after infection.

The virus assumes that DBS on a hard disk is located at cylinder 0, head 1, sector 1 (true in most cases) so non-standard systems may experience unpredictable behavior.

The virus keeps the code of the original Boot Sector but stores it in two chunks. The original DBS has to be reconstructed from the infected sectors and 80 bytes saved in the rest of the virus code. Additionally the offset of the virus code inside an infected Boot Sector varies from one system to another.

Exebug

Exebug is a stealth boot sector virus infecting the Master Boot Record on hard disks and the DOS boot sector on floppy disks. The first time the system is booted from an infected diskette, the Exebug virus will install itself resident in memory (using 1 kilobyte) and infect the hard disk's master boot sector. The original master boot sector will be moved to the last sector of side 0, Cylinder 0 of the hard disk. The virus then saves its own instructions over the original master boot sector. The virus changes the boot sequence in the CMOS setup and sometimes overwrites the header of EXE files with a code corrupting the hard disk.

Fairz (also known as Khobar)

This is an encrypted, memory resident file virus which infects EXE and COM files, adding approximately 2083 bytes to the size of infected files. It contains the messages:

> *This is an [illegal copy] of Keypress virus remover*
>
> *System Halted* and *Eternal Fair.*

FAT Avenger

FAT Avenger is a boot sector virus which infects the DOS boot sector of floppy disks and the Master Boot Sector of hard disks. It is 4 sectors long and hides the majority of its code in cylinder 0, head 0, sectors 3-5 of hard disks and in the last cylinder, head 1, sectors 3-5 of floppy disks.

When active in memory, it takes 3Kb from top of memory.

The second sector of the virus contains a plain text message:

> *THIS PROGRAM WAS WRITTEN IN INDIA (c) 1993 FAT AVENGER*
>
> *PS. this program is not meant to be destructive.*

Finnish Sprayer

This is a boot sector virus infecting the Master Boot Record on hard disks and the DOS boot sector on floppy disks. On March 25th, the virus will overwrite random sectors of the partition and display on a grey screen:

> *FINNISH SPRAYER.1. Send your painting -358-0-4322019 (FAX), [Aija]*

The fax number listed is that of the Finnish House of Parliament.

FiveVolts.2659 (also known as Tequila.5volts.2659and 5volt4)

FiveVolts.2659 is a variant of the Tequila virus but unlike the original Tequila, it is not multi-partite. It tries to avoid infecting files which start with WIN, CHKDSK and BACK. It contains the plain text:

> *This is a beta version of the '-5 Volt' virus. A final and error free one will never follow because I've got enough viruses. Now a message to the programmers of Turbo Anti Virus: You do a dangerous play with INT 21h in your TSAFE utility. It took me quite a long time to make the virus compatible with TSAFE. Please use clean programming technics [sic] in your next version. Today it's a Saturday and a big party with a lot of TEQUILA takes place! Wow!! Greetings to the US Army in Iraq.*

FITW.7918

FITW.7918 (which stands for Fart In The Wind) is a polymorphic, multi-partite virus infecting .EXE and .COM files as well as boot sectors. FITW has a particularly nasty payload: on an infected system, if the day is Monday and the date is 1st, 3rd, 5th, 7th or 9th of any month, it will intercept Int 09h, disabling a soft reboot (Ctrl-Alt-Del). At the same time, random data is written to the local hard disks, and as keys are pressed, the following message, (rather than the keys pressed) is displayed:

> *The “FartStorm” coded by Demon Emperor >Sig hello to*
>
> *Cmoskiller&Xorboot< Are you wild? Hey don't... wait...*
>
> *let us talk... No? Be off lame f*ckhead!*

Flip

This polymorphic virus infects COM files, EXE files and the Master Boot Record of hard disks. On the 2nd day of any month, its payload is triggered; the screen appears *flipped* or upside down on computers with EGA or VGA displays.

Form

It is a boot sector virus infecting the DOS boot sector on hard drives and floppy disks. On the 18th day of any month, the speaker of the infected system may emit a clicking noise.

On the active partition of a hard disk, Form replaces the boot sector, moves the original DOS Boot Sector to the last sector and the rest of the virus code into the preceding sector. When it infects a floppy disk, Form hides the original DOS Boot Sector and its own code in two unused clusters, marking them as bad. Form decreases the amount of available memory by 2Kb and redirects interrupts 13h (low level disk access) and 9h (keyboard). A message can be found in the second part of the virus code:

> *The Form-Virus sends greetings to everyone who's reading this text. Form doesn't destroy data! Don't panic!*
>
> *Fuckings go to Corrine.*

Frodo (also known as 4096 or Stealth Virus)

Frodo slowly and randomly cross-links (and therefore corrupts) files by modifying the FAT. It is supposed to overwrite the hard disk if it is run on or after 22 September of any year, but because of a bug it doesn't and the PC merely hangs.

Frodo is an encrypted virus of 4096 bytes that uses sophisticated stealth techniques to hide itself. After an infected file has been opened, the virus disinfects it, and then re-infects the file when it's closed. This makes it more difficult for anti viral programs to detect the virus. The virus also uses a technique called 'tunnelling' to access the system in a way which is not detectable by most 'watchdog' software.

Gingerbread.2774

This stealth, multi-partite virus first appeared in Sydney in 1993 and contains the following encrypted message:

> *You can't catch the Gingerbread Man!!*
>
> *Bad Seed - Made in OZ*

The Gingerbread virus is not deliberately destructive, but causes loss of data on some PCs (eg Olivetti M24s) and the stealth techniques can cause clashes with some applications software.

The virus infects .COM and .EXE files, increasing the length by about 2773 bytes. The virus is highly infectious and incorporates a variety of stealth techniques which will probably fool most integrity checkers, unless the PC is first booted from a clean DOS disk.

The author has gone to extreme lengths to hide the virus and the code is very convoluted. However, the result is rather like a bank with elaborate locks on the front door, but none on the back door and the virus is readily detected and removed.

Green Caterpillar

After this virus has infected your PC, it waits 2 months before displaying the green caterpillar. This crawls across the screen from the top, moving left to right, line by line, and disappears when it reaches the bottom. As the caterpillar passes any characters on the screen, it moves them 8 spaces to the left and turns them yellow. This virus is a nuisance but does no deliberate damage. There are many variants of this virus, all doing similar things but with small changes to the code.

Each time a directory is examined, the virus looks for a file to infect. It adds 1583 - 1591 bytes to infected files.

Helloween

This virus was found in Europe in 1992 but has been found in Australia. It does no deliberate damage. Once in memory, Helloween will look for a date of 1 November. If successful, it displays a message in Czech about a heavy metal band called Helloween. The virus is unlikely to become common as it is not very well written.

Holiday

On 3rd March, if the virus is active in memory, it displays:

ATTENTION!
I'm very sorry, today is my holiday.
So, I can't serve you, cause I want to play on your computers.
DON'T TURN OFF YOUR COMPUTER UNTIL TOMORROW,
OR YOUR DATA WILL BE LOST!!!
I'll be back to serve you tomorrow.
Thank You,
AAA

When the system date changes to 4th March, it displays:

Thank You for playing, see you...
Please, hit ENTER!
before rebooting your PC

Holiday is a memory resident, parasitic file infector which infects COM and EXE files, decreasing available memory by 2912 bytes. Infected COM and EXE files become about 2900 bytes longer, and the text messages are clearly visible within them

Hooters.4676

Believed to have originated in New Zealand, Hooters.4676 appears to have spread via some of the Internet alt.binaries news groups. The virus is a direct file infector which encrypts the files it infects. It is very easy to determine if you have the Hooters virus as a file of zero length will sit in the root directory of your hard disk calling itself HOOTERS.EXE.

Hooters.4676 is an encrypted virus written in the high level language. It is classed as a Parasitic, Prepending, directfile infector .It contains the text:

"Wow - you've found the hidden message
(like it's hard!) Made in Auckland, New Zealand,
in 1996 Contains the greatest saying of all time
Dedicated to the few truly great pairs of
lucious hooters."

Symptoms of infection with Hooters include file growth by 4676 bytes longer, it displays the message (above or below), and it deletes the files: "anti-vir.dat" and "chklist*".

When an infected file is run, the virus searches for and infects one program. Then it copies the original hosts to the specially created file HOOTERS.EXE, decrypts and executes it. Next, Hooters.4676 deletes the HOOTERS.EXE file and returns to the operating system. All infected files start with characters ZM.

When there are no files to infect, the virus may display the message:

"Hooters, hooters, yum, yum, yum. Hooters, hooters
on a girl that's dumb - Al Bundy".

Ignorant

This encrypted, stealth, multipartite virus is not deliberately destructive, but overwrites the last four sectors on floppies and four sectors on track zero of the hard disk, causing some loss of data under certain circumstances. The virus was probably written in Brisbane, Australia and contains the message:

> *Ignorance is Strength*
>
> *Freedom is Slavery*
>
> *War is Peace*, and
>
> *[1984] by [T.L.N<.>N.K.]'93!*
>
> *THiS iZ iNFeCTiON #00000012!*
>
> *Greetz RS/NuKE!"*

Version V109 of the anti-virus software **SCAN** has been trojanised with this virus (ie an earlier version of SCAN has been taken, infected with a virus and uploaded to bulletin board systems with the name SCANV109

Int12

This virus is difficult to recover from as it is an overwriting boot sector virus. Normally boot sector viruses will insert themselves so that they are the first thing run when the boot sector is activated, they store the code that they have displaced so that the boot sector will continue to function normally. This is not the case with over writing viruses, they insert themselves and do not save the data that they have over-written.

Because part of the boot sector has been destroyed and there is no way of knowing exactly what has been destroyed it is necessary to follow these steps to remove the virus and return the boot sector to working order.

For Floppy disks:

Accept Vet's offer to replace the boot sector with a known clean boot sector.

For Hard Disks:

Boot your computer with a system disk that has the same version of DOS as the operating system that is on the PC. Next, type the command SYS C: and select <Enter>. (This will overwrite the system files that have been damaged by the virus, removing the virus, and repairing the files to working order).

Invisible.2926, 3223

This slightly polymorphic boot sector virus will attempt to infect .EXE and some .COM files as well as the master boot record.

When triggered it will display the lyrics of a song and produce a noise from the PCs speaker. The trigger is randomly activated but will become more likely the longer the PC remains infected. Some files may also have some data overwritten.

Lyrics displayed:

I'm the invisible man,
I'm the invisible man,
Incredible how you can
See right through me.
I'm the invisible man,
I'm the invisible man,
It's criminal how I can,
See right through you"

The following text is not displayed but is inside the virus:

The invisible Man - Written in SALERNO (ITALY),
October 1992. Dedicated to Ester: I don't know
how or when, but I will hold you in my arms again"

IVP.Flipper

IVP.Flipper is a parasitic, appending, fast direct infector, infecting files with extensions .EXE and .COM (it avoids infecting COMMAND.COM). The virus attaches its code at the end of files increasing their length by 872 bytes.

When an infected program is executed, the virus infects all .EXE and .COM files in the current directory/subdirectory and then it tries to do the same in the parent directory.

When all files are infected the virus displays the message:

'Flipper is in a blender

Eeeekk !!!! Eeeeekkk!!

Eeeeeeeeeeeeeek!!'

The speaker emits 'dolphin like' sound effects and after a few minutes it invokes the print screen routine (Int 5). Additionally, because of a bug, the binary code of the virus may be sent to the console (meaningless ASCII characters are displayed on the screen). The virus does not contain other payloads.

IVP.Scroll (aka Alias: IVP.630)

After infecting files in the current directory, the virus changes the default directory to the parent directory and repeats the whole infection procedure. When the root directory is reached the virus' payload is triggered - it scrolls the contents of the screen, horizontally from right to left and does it for a few seconds.

Then the virus displays its message:

Hello world! This is the Scroll Virus!

I hope you enjoy it (NOT!)

Ciao!
[IVP]

As the last step the virus passes control to and executes the original program.

Symptoms: .EXE files grow in size, screen effects, messages.

IVP.Scroll is a File, parasitic, appending, direct infector

IVP.Scroll is a non-resident virus infecting .EXE files. When an infected program is run, the virus searches the current directory for all files with the extension 'exe' and infects them by appending its code to the end of files. Infected programs grow by 630 bytes. Additionally they are marked by the word 4747h (string 'GG') located at the offset 0010h (initial value of SP in the exe-header).

Hoax- These are not real viruses

Currently it is NOT possible for you to be infected by just opening your Email and reading it. It IS possible to be infected if the email has a file attached to it and you attempt to open/run the file and you don't have your Vet Resident Protection loaded.. If you receive files attached to email and attempt to open them they will be AUTOMATICALLY scanned by Vet provided you have resident protection loaded (Open Vet and select Options | Resident Protection | Enable to check that it is on).

If you have turned resident protection off then save the file(s) to a directory, open Vet and scan the files before opening them.

A hoax is a message, typically distributed via email or newsgroups, that is written to deliberately spread fear, uncertainty and doubt. Hoaxes prey on the lack of technical knowledge and goodwill of all those that receive a hoax. Generally, hoaxes are warnings about threats to your computer that do not actually exist.

Most of the hoaxes (not all) are just variations of the same basic idea: they warn that if you read an email with a particular subject, a virus will be activated that will destroy your data. The fact is that simply reading an email message cannot activate a virus, regardless of what the subject is. Reading an email message does not involve the execution of any sort of program, which is a prerequisite for any sort of malicious software to activate. It should be noted that attachments to email messages such as programs or Word documents could potentially contain a virus or other malicious program. None of the hoaxes warn against this real threat, they only warn you of nonexistent email threats!

Another very common characteristic of a hoax is that it asks you to forward the warning on to as many people as possible. This is how the hoax "spreads" itself. If you receive any form of message that asks you to forward it on to others, you should check out the accuracy of the message before forwarding it on to anyone else, otherwise you may help perpetuate a hoax.

How can you check a message for accuracy? You can check a hoax web page to see if it is a known hoax, or you can ask your Anti-Virus or security software vendor. Vet technical support are happy to help you identify possible hoaxes.

The following is a list of email hoaxes that users of Vet Anti-Virus Software commonly report to Vet's technical support staff.

Good Times
Join The Crew
Penpal Greetings
Irina
Deeyenda
AOL4FREE
Naughty Robot

The following is a list of other hoaxes that are known to Vet but are only rarely reported.

Returned Email
Free Money
Budweiser Screensaver
YUKON3U.mp
Hackingburgh
Yahoo Crack and Logic Bomb Hoax
Win a holiday

Jerusalem (also known as Friday 13th Virus)

After the computer has been infected for half an hour, a gray rectangle is displayed at the centre left of the screen. The rectangle is about 35mm wide and 15mm high, ie roughly the size of a matchbox. The computer also slows down noticeably. Programs run on Friday 13th of any year will be erased.

Jerusalem is memory resident and infects .COM and .EXE files (except for COMMAND.COM). It doesn't check to see if it has already infected each .EXE file, presumably due to a bug. The effect of this is that .EXE files grow, taking longer to load each time.

The virus damages WordPerfect, INGRES, Windows and programs linked with early versions of the Phar Lap Linker. Jerusalem virus may crash Netware networks, which use the same function call to control the print spooler.

Jerusalem was one of the first successful program viruses and there are many viruses derived from it. It is highly infectious and is thus fairly common.

Joshi

Joshi is a relatively harmless boot sector virus. If you boot from an infected floppy on the 5th of January in any year, you are prompted to type "Happy Birthday, Joshi" before you can continue using your computer. The virus does no deliberate damage, however, it may destroy some data on floppy disks.

June 4 (also known as Bloody)

Displays message: *Bloody! Jun. 4, 1989*

This virus is based on the Stoned virus code. After you have booted from an infected disk 128 times, the message is displayed on every 32nd boot. Bloody causes very obvious excessive disk activity. The MBR is stored in Head 0, cylinder 0, sector 6.

Junkie

This is a very common, multipartite virus. The only known payload of Junkie is that it disables VSAFE (the memory resident part of Microsoft Anti Virus). The virus contains two messages, which aren't displayed:

Dr White - Sweden 1994

Junkie Virus - Written in Malmo ... M01D

When an infected file is executed, Junkie infects the Master Boot Record of the hard disk and does nothing else. The next time after rebooting from an infected hard disk, the virus installs itself in memory and then infects every executed or open .COM file and the boot sector of every new floppy disk accessed (except 360K 5.25" disks). The virus code is 3 sectors long. Infected files grow in length by about 1300 bytes. When active in memory, Junkie decreases the amount of available memory by 3Kb and redirects interrupts 13 hex (low level disk access) and 21 hex (DOS). The original MBR is hidden in cylinder 0, head 0, sector 4 and the original DOS Boot Sector is hidden in cylinder 79, head 1, sector 8 on 720K and 1.2M floppies or in sector 16 on 1.44M floppies.

Jumper

Is a memory resident boot sector virus which has been detected and cleaned by Vet customers in the past.

Kampana (also known as Telefonica or Spanish Telecom)

This is a family of multipartite, encrypted viruses which infect .COM and .EXE files, the Master Boot Record on hard disks and the DOS boot sector on floppy disks. After a certain number of boots from an infected disk, the disk sectors are erased and the virus displays the text:

> *Campaña Anti-TELEFONICA (Barcelona)*

Kaczor.4444 (Also known as Pieck)

Kaczor is believed to have been written in Poland in 1995, and took nearly a year to be seen outside of Europe. The virus is a Master Boot Record infector as well as an .EXE file infector. It will increase the size of an infected file by 4,444 bytes, but when active in memory will hide this change in size from the user.

Kaczor is a Memory-resident, multi-partited, stealth virus .

Kaczor (which is Polish for “Duck”) is often named “Pieck” for reasons shown below. It infects the MBR on the harddisk when an infected file is run, and goes memory resident next time the computer is booted. It then infects every .EXE file executed or accessed from any floppy disks. If an infected file is found on the hard disk the virus actually disinfects it.

Symptoms of infection with Kaczor are .EXE file growth; file date/time seconds = 62; decrease in available free memory; master boot record altered; file allocation errors.

Kaczor is a stealth virus, so all changes to the MBR and files can not be seen by the user. On March 3rd every year the virus displays the message “`Podaj haslo ?`” - which means “Password?” in Polish. The correct password is “`PIECK`”, and if entered the message “`Pozdrowieniadla wynchowankow Pieck'a`” will be displayed (Greetings to Pieck’s students). All other answers will cause the virus to display “`Blad`” (which is Polish for “Error”), and then render the computer unbootable.

Keypress (also known as St Leo's)

This is a family of parasitic memory-resident viruses. After the virus has been present for some time, every ten minutes a string of keyboard interrupts is issued. Any key hit during this period will repeat many times and soon overload the keyboard buffer (typically causing beeping). There are a lot of viruses that are based on the original Keypress virus. Some of them contain dangerous payloads, including overwriting hard disk sectors.

This virus appeared in Melbourne in late 1990. It was once fairly common.

Krsna.7720 (also known as Krsna.7750 and Krsna.7786)

Krsna.7720 has spawned great debate amongst the anti-viral fraternity regarding both its name and its official length. The message which it contains:

> *"HD Euthanasia" by Demon Emperor: Hare, Krsna, Hare, Hare...*

has given rise to suggestions that it should be named Euthanasia, Hare or Krsna. It is encrypted three times and its pure virus length, without decryptors is 7610 bytes, but if the two non-chaning decryptors are included, the length is 7720 bytes.

Krsna.7720 infects the MBR on the hard disk and DOS boot sectors on floppies. It infects .COM and .EXE files and when active in memory, takes 9Kb from top of memory.

Payload: on 22 August and 22 September, Krsna.7720 will display the message above and will overwrite or corrupt data on all hard disks on the system. The other two versions corrupt the hard disk and have a slightly different message.

Larry

The virus payload displays the text:

> *Larry on a Screen.*

This virus is a resident .COM and .EXE file infector which includes a counter which is decremented each time a program is infected. When the counter reaches zero, the above message will be displayed. It does no deliberate damage and is so unreliable that most users would realise something was wrong even before they got the message.

Lemming

Disables the resident scanner of the Thunderbyte Anti Virus package.

The Lemming virus is a memory resident file infector that originated and is common in Australia. It appends 2160 bytes to both COM and EXE files, although there is a variant which appends 2144 bytes.

The virus targets an anti viral product called Thunderbyte Anti Virus; it disables the resident scanner if it has been installed on the infected computer. It also searches for files containing the strings: TBAV, TBSCAN, NAV, VSAFE and FPROT. These are filenames of anti-viral products, so it presumably avoids infecting them to avoid alerting their internal checking procedures. It contains the encrypted message:

> *The Rise & Fall of ThunderByte - 1994 - Australia*
>
> *You Will Never Trust Anti-Virus Software Again!!*
>
> *[Lemming]*

Leprosy

Overwrites start of files, destroying them. When an infected file is run, the virus looks for six files to infect, then gives message *Program too big to fit in memory*. When there are no files to infect it announces itself. Students at the Royal Melbourne Institute of Technology patched this with a message about RMIT, infected a copy of McAfee's anti virus program SCAN and uploaded it to various bulletin boards. Infected programs must be replaced.

Little Brother

This is a companion virus. When an infected file is run, the virus is loaded into memory, and from then on, when any EXE files are run, a COM file with the same filename is created. When the user tries to run an EXE file, the virus is loaded and executed instead.

The original virus creates COM files that are 307 bytes long and contain the text *Little Brother*.

Little Brother.321 is a variant which creates COM files of 321 bytes.

Little Brother.349 creates COM files that are 349 bytes long which have the Hidden, System and Read-Only attributes set. If an infected file is run on the first Tuesday in November when major elections are held in the USA, the message:

DID YOU VOTE SHITHEAD?

is displayed and the computer beeps several times.

Little Red

On December 26th (Mao Tse Tung's birthday) the virus plays a tune called Liu Yang He (or Liu Yang River). On September 9th (the day Mao Tse Tung died), a patriotic song called Dong Fang Hong (The East is Red) is played. The tunes will only be played if the system date is set at 1994 or later. On the specified dates, the tunes will start an hour after the virus is activated and will then play continually. There are no other effects, although in one of our tests, the virus damaged COMMAND.COM and thus prevented the computer from booting, and using the DIR command causes obvious additional disk activity. For example on an XT, it took over twice as long to display a file directory when the virus was active.

Presumably of Chinese origin, this is a resident file infector with limited stealth capabilities. It infects all files loaded by the DOS function 4B (Load and execute) and one .COM or .EXE file on each use of the DIR command. The virus increases file lengths by 1465 bytes although these increases are not visible by using the DIR command from DOS while the virus is in memory.

Loren

Loren contains the encrypted message:

> *Your disk is formatted by the LOREN virus.*
>
> *Written by Nguyen Huu Giap.*
>
> *Le Hong Phong School *** 8-3-1992*

When twenty files are infected in a single session, the virus attempts to format cylinder 0, head 0, on drive C. If this fails, it then tries drives A and B. If it succeeds in formatting any drive, it gives the message above and resets the counter. A low level format will normally be needed to recover affected hard disks and IDE drives may have to be returned to the agents for repair.

Loren infects all files opened for execution and all .COM and .EXE files when the DIR command. is issued. Files are increased by 1387 bytes although this isn't apparent from a file directory. Anyone who regularly uses DIR (or a similar program using DOS Fns 11 and 12) is likely to be hit almost immediately they become infected, but the other users will probably not notice the virus immediately.

Macgyver

A sample of this virus was given to the Vet developers at the Melbourne PC Show on August 10th, 1993. It plays a tune continuously if the month is March or later, the date ends in a 5 and it isn't the day on which the PC was first infected. The virus contains an encrypted message (which doesn't seem to be displayed):

[MACGYVER V1.0 Written by JOEY in Keelung. TAIWAN 1992]

The virus infects .EXE files, adding 2803 bytes to them. It uses stealth and tunnelling techniques and has a sloppy infection mechanism, causing it to infect many Windows files. When an infected file is run the virus uses the normal DOS TSR call to go resident. It hooks Ints 8 and 21, and subverts a number of DOS function calls. All .EXE files opened will be infected, but the increase in length will be hidden from DIR.

Maltese Amoeba

This polymorphic file virus infects .COM and .EXE files. The virus overwrites the boot sector on the 21st of March with a new boot sector containing the poem *Auguries of Innocence* by William Blake and a tirade against the University of Malta. This causes the system to crash, and there is also a technicolour display.

Megabug.546

Increases file lengths by 546 bytes. Decreases available memory.

This virus infects .COM files, adding itself at the end. When an infected program is executed, the virus installs itself in memory and then attempts to infect every .COM file called by the Load & Execute function (int 21H, function 4b00h). Megabug.546 is encrypted with a random key and contains the encrypted message:

V.C.M-MEGABUG

Megabug uses Int 91h and will therefore crash any system also using this interrupt.

Memorial (AKA Win95.Memorial, Memorial.12314, Memorial.7783)

Although it has several serious bugs, Memorial has been reported to be in-the-wild in Northern Europe. Memorial is a 'memory-resident' Windows 95 virus, the first of its kind in-the-wild. It operates a Windows 95 VxD, called Clint.VxD, and infects DOS COM and EXE files, and Win32 PE (Portable Executable) files. The virus can disable many Windows 95 anti-virus programs, including VET Anti-Virus Software, by deleting or changing registry settings.
Memorial also contains the following message, which it will display on the 10th April:

> *Clinton Haines Memorial Virus by Quantum/VLAD and Qark/VLAD*
>
> *Clinton Haines, also known as Harry McBungus, Terminator Z and Talon*
> *died of a drug overdose on his 21st birthday, April the 10th, 1997.*
> *During his time as a virus writer he wrote the No Frills Family, X-Fungus, Daemon and 1984 viruses. He was a good friend to VLAD and so we write this virus in his honour. We hope it's good enough to do him justice.*
>
> *VLAD Remembers. Rest in Peace*

Michelangelo

Michelangelo is a variant of the Stoned virus, but displays no messages. If the computer's date is set to the 6th of March (Michaelangelo's birthday) in any year, the virus overwrites the first 256 cylinders (track 0) of the hard disk. These cylinders include the Master Boot Record, the partition information, both copies of the FAT, the root directory and a large amount of data (files). Unless you have copies of this system information (eg on a reference disk created by VET) or consult a data recovery company, your hard disk will be unusable and need to be reformatted. On floppy disks, it overwrites the same directory entries as Stoned. Michelangelo was the subject of world wide media hysteria in 1992, but was discovered in Melbourne in February, 1991.

Micro Cops

This boot sector virus was designed to propagate until February 92 without showing itself, but will now go off within an hour of booting the PC from an infected disk. It overwrites the MBR, clears the screen and displays the message:

Using unauthorised program - Micro Cops

After this it will not be possible to boot from the hard disk or access files on it.

Because of the lethal nature of this virus, all infected PCs have probably already been hit, but there will no doubt be infected floppies around for some time.

Mongolian

The virus originated in Mongolia in 1992, it has symptoms of lots of disk activity and a message displayed on May 30th.

This is a fairly primitive, but destructive virus. If the PC is switched on on May 30th the virus overwrites the first 17 sectors of each partition on the hard disk, and then overwrites the Master Boot Record. Finally it displays the message:

> *Mongolain Virus VERSION 1.00*
>
> *Mongolian Brain Co.Ltd 1992*
>
> *Today is birthday of my babby!!!*

Moloch

Moloch is a memory resident, stealth, polymorphic, encrypted, boot sector virus which infects the Master Boot Record on hard disks and the boot sector on floppy disks. It contains the text:

> *OH-MY-GOD! Moloch (TM) is here! Moloch is*
>
> *trademark of SquiBoyz*

It hooks Int 13H and tries to find the entry point to the BIOS to avoid detection by resident anti-virus programs. It does not appear to contain any warheads and the message is not displayed.

Monkey

Stealth virus that encrypts and hides the original Master Boot Record, overwriting the partition table.

This virus originated in Europe in December 1993 and is based on the Stoned virus. Monkey has no known warhead, but if you boot from an uninfected system disk you won't be able to access the hard drive from DOS. It is currently common in Australia.

When Monkey infects a hard disk, it stores the encrypted (XORed with a constant) MBR in cylinder 0, head 0, sector 3 and then copies itself to cylinder 0, head 0, sector 1, overwriting the partition information. Monkey is a stealth virus and when active in memory it hides its presence on a disk by returning the original MBR when the user tries to read cylinder 0, head 0, sector 1. The original DOS Boot Sector is hidden in the last sector of the root directory (floppies only) and can therefore cause the loss of up to 16 directory entries. When a new floppy is accessed on an infected system, the chance that Monkey will infect its DOS boot sector are 1:4. There is a second variant, Monkey 2.

Mummy 1.2

Mummy 1.2 is a memory-resident file virus infecting .EXE programs. This virus has a destructive warhead which writes garbage characters over the first 63 logical tracks of disk from which the file was loaded. This will usually destroy the first copy of the File Allocation Table and on small disks may also destroy the second copy of the FAT and possibly also the root directory.

The virus examines all files opened. It infects .EXE files (increasing their size by 1399 bytes) and decrements a “D-Day” counter when it finds an already infected .EXE file. When the counter reaches zero, the warhead is detonated. The maximum delay is quite short and many users will be hit within a few days of becoming infected.

Natas

Natas is a memory resident, multipartite, polymorphic stealth virus. The virus infects the Master Boot Sector as well as COM and EXE files. It formats the entire hard drive if the virus detects a debugger, or on a one in 512 chance on loading from an infected disk. The virus contains 2 internal text strings; *'Natas'* and *'BACK MODEM'*.

No-Frills

This is a memory-resident file virus. Infected files contain the following text:

No Frills by Harry McBungus-

No Frills originated in Australia in 1992. It infects .COM and .EXE files when they are opened, executed or copied, increasing their size by 813 bytes. It will infect COMMAND.COM.

One Half

One Half infects program files and the Master Boot Record of hard disks. Once the MBR is infected, each time the PC is booted it encrypts two cylinders of the hard disk, starting from the last cylinder of the last DOS partition. When more than half the hard disk has been encrypted it will give a message on every 4th day and wait for a key to be hit. The message reads:

> *Dis is one half.*
>
> *Press any key to continue...*

The virus uses stealth techniques and is not detected in the boot sector while the virus is in memory. Also, the encrypted cylinders are decrypted when the user accesses them so the damage will not be noticed until the virus is removed. All cylinders are encrypted with the same key.

One Half is common in the USA and also Europe. It is quite a nasty virus, as it is highly infectious and has a nasty warhead. It is also known as Free Love.

Ozterm

Ozterm is highly infectious and has a nasty warhead. It was common in New South Wales in 1993. However, it appears to have some bugs (or may have been deliberately mangled) and it is not clear when the warhead will be triggered, or even if it will be triggered at all. If it **is** triggered, both copies of the File Allocation Table (which specify where all the files are stored) on the current drive will be overwritten. The virus contains a number of encrypted messages, most of which include the text *THE TERMINATOR* or *TERMINATED* and all infected files end with the string *TERMINATOR* (unencrypted).

The virus infects all files loaded for execution using the DOS load and execute function as well as all .COM and .EXE files opened **or** for which attributes are set. Therefore, if you scan for the virus using a scanner which does not recognise Ozterm, you will infect all files checked. In addition, since, resetting the attributes is normally the last thing done after disinfecting a file, any attempt to remove the virus while it is active in memory will be thwarted. Ozterm also contains a boot sector infector which is designed to infect the DOS boot sector of every disk accessed, but it appears that this is never activated.

Ozzie.426

This virus was found in the wild in Australia in mid 1997.

It is a direct COM file infector that spreads very fast. When it infects a sub directory it will infect all files in directories above it until it reaches the root directory.

If an infected file is run when the number of seconds on the system clock is 59 it will trigger the payload.

Once triggered it will display the following message in the middle of the screen. The message will also change colour.

> "*" OZZY "*" = Yeew duh-Mee it Reeel!! [KR]"

This virus does not have any payloads that will deliberately cause damage to your PC files.

Padded

This is a non-resident file virus. No messages are given, there is no warhead and the only intention of the virus is to spread itself. As the infection spreads, the virus takes longer and longer to find an uninfected .COM file to infect and its presence becomes increasingly obvious. The name Padded has been given to this virus, due to the large amount of excess code present. It was discovered by Roger Riordan in January 1992.

Padded is a non-resident direct infector which only infects .COM files of less than 63946 bytes in length, adding 1589 bytes to the file size. When an infected file is run, the virus searches the current drive for an uninfected .COM file. It begins searching in the root directory and scans sub-directories to a depth of 9 levels. It runs the original program when it has found a file to infect, or has checked all .COM files on the drive.

ParityBoot

Parity Boot contains two minor payloads. Parity Boot intercepts Ctrl-Alt-Del and then simulates a memory parity error. The second payload can be triggered on every call to int 9 (keyboard). The message *PARITY CHECK* is then displayed and the computer is halted.

The virus is one sector long and infects the master boot record of hard disks, and the DOS boot sector of floppy disks. When it infects floppies it hides the original DOS Boot Sector in the last sector of the root directory. It treats 1.44M diskettes as if they are 1.2M. Parity Boot takes 1Kb from top of memory and redirects interrupts 13 hex (low level disk access) and 9 hex (keyboard). There are two known variants of this virus which differ in location of the hidden original MBR on the infected hard disk: cylinder 0, head 0, sector 0E (variant A) or sector 9 (variant B).

Pathogen

This is a resident, highly polymorphic virus which infects COM and EXE files. If the virus reaches a certain number of generations and on any Monday between 5 and 6pm, the virus writes random data over the hard disk and displays:

> *Your hard disk is being corrupted, courtesy of PATHOGEN!*
>
> *Programmed in The U.K. (Yes, NOT Bulgaria!)*
>
> *[C] The Black Baron 1993-4.*
>
> *Featuring SMEG v0.1: Simulated Metamorphic Encryption Generator!*
>
> *'Smoke me a kipper, I'll be back for breakfast.....'*
>
> *Unfortunately some of your data won't!!!!!*

Ping Pong (also known as Italian Virus)

Ping Pong is activated if a disk access is made exactly on the half hour. A diamond character then bounces diagonally around the screen rebounding off the edges and off certain characters. It is extremely annoying but is intended to be harmless. Whilst Ping Pong is active, you cannot replace the boot sector - it either prevents you writing to it or it immediately re-infects it.

The original boot sector and most of the virus are stored in the first free cluster. It marks this as bad (on the first copy of the FAT only), so that DOS will not try to use it. It infects disks on every active drive and will even infect non-bootable partitions on the hard disk (eg drive D:). The virus contains a POP CS instruction which won't run on 80286s and higher machines, thus the virus is probably almost extinct.

Rainbow

This was first reported in New South Wales. It is a memory resident multipartite virus that infects the Master Boot Record of hard disks, the DOS boot sector of floppy disks and all executable files. Rainbow only saves parts of the original MBR and it adds 2351 bytes to executable files, infecting such files when they are run.

Rainbow does not appear to have any warhead. However, it is quite well *armoured*. When it infects a hard drive, it points the partition table back on itself, creating a *recursive partition*; with boot disks higher than MS-DOS version 4, this will cause the PC to hang if you attempt to boot from a clean system floppy.

Rauser.250 (also known as MAAIKE)

The Rauser.250 is a companion file virus. It infects .EXE files but it doesn't change the contents of the infected files. The virus takes advantage of the DOS system which always try to execute programs with a .COM extension first, if no file extension is specified.

For every infected .EXE program, Rauser.250 creates a 250 byte-long hidden .COM file and copies itself into the file. Rauser.250 is a memory resident virus and while active in memory it occupies 507 bytes.

On a random basis it fills the whole screen with the text: “*Maaike I Love You*!” in green flashing characters on a red background.

The virus originated in the Netherlands and has been uploaded onto different BBSs as a hacking utility.

Ravage (also known as Dodgy)

Like many other boot sector viruses, Ravage copies itself to cylinder 0, head 0, sector 1 of the hard disk, and moves the original boot sector to another part of the disk. When active in memory, the virus decreases the amount of available memory by 1K. The virus intercepts Interrupt 13H, as well as Interrupt 8, 21H, 2FH, and 40H.

Ravage's payload is date triggered. However, this date is generated randomly each time the PC is rebooted, so, on one occasion it could be the 12th March, while on the next boot-up it could be the 26th October. When the current date of the computer matches Ravage's randomly generated date, the virus displays the message:

"RAVage is wiping data! RP&muRPhy"

Next, Ravage overwrites the first 14 sectors on side 1 of every cylinder of the 1st physical hard disk.

Ripper

Ripper infects the Master Boot Record on hard disks and the DOS Boot Sector on floppies. It is intentionally destructive and dangerous. When active in memory, it will corrupt data in the writing buffer on a random basis, so that the damage caused accumulates over a period of time. Ripper hides the original MBR in cylinder 0, head 0, sector 9 and the original DOS Boot Sector on floppies in cylinder 0, head 1, sector 3 (360K disks) or sector 5 (720K disks). Ripper infects double density disks only and up to 32 directory entries may be lost. When active in memory, it decreases the amount of available memory by 2Kb and redirects interrupt 13 hex (low level disk access). It contains the encrypted message:

FUCK'EM UP!

() ack Ripper

Rusty Bug.5330 (AKA HLL.5330 and HLLP.5330)

This is another member of the family of high level language viruses. Its fast spread is mainly due to the amount of files the virus tries to infect in one go. In addition, the virus always chooses to infect the user's most frequently accessed files (located in the directories listed in the PATH statement).

RustyBug.5330 prepends itself to a victim file by replacing the first 5300 bytes of the original program with the virus code and moving the original code to the end of the file. To make disinfection difficult, the virus encrypts all of the code relocated to the end of the file. The virus is a fast, direct infector which propagates very quickly. It infects both .COM and .EXE (starting with 'MZ') files, searching for its potential victims through a current subdirectory and also subdirectories listed in the PATH statement.

Payload: The virus does not appear to have any destructive payloads. Randomly (a probability of 1:200), the virus displays a moving star-field, a similar effect to one of the Spanksa viruses. The picture itself shows white dots of different intensity and speed moving from the right to the left side of the screen. This animation disappears after a button is pressed.

Sampo

May display the message:

> *SAMPO Project X*
> *Copyright (c) 1991 by*
> *Sampo X-Team - All rights reserved.*
> *University of East Manila*

Sampo infects the Master Boot Record on hard disks, hiding the original in cylinder 0, head 0, sector 0Eh. Similarly it infects the DOS boot sector on floppies, hiding the original in the last cylinder, head 1, sector 5. Sampo is six sectors long. When active in memory it takes and occupies 6Kb from top of memory. It incorporates stealth techniques so that if an attempt is made to read the boot sector from an infected disk, Sampo returns a copy of the original sector. When a clean disk is accessed, the virus infects it and then returns the original sector. If it can't infect the new clean disk (for example, if it is write-protected), it returns a copy of the Kampana virus. When the user write-enables the disk in order to clean the virus, Sampo infects it with its own code and returns a copy of the original clean boot sector. It contains an encrypted message which it tries to display on 30 November, in the top right hand corner of the screen, surrounded by a double border.

Satanbug

This highly polymorphic, harmless virus infects COM and EXE files, but seems to do no deliberate damage. The virus contains the text:

> *Satan Bug - Little Loc*

Satria

Satria is a memory resident boot sector virus that probably originated in the USA. Satria uses no stealth techniques, is 1 sector long and will set the Top of Memory down by 1 Kb when in memory.

When an infected computer is booted on the 4th of July Satria displays the characters:

> *I <HEART> U* (where HEART is the heart symbol)

It contains two strings that are not displayed: *My Honey B'day* and *SATRIA*. These are not encrypted and they are therefore clearly visible in the boot sectors of infected disks. As far as we can determine Satria does not contain a warhead.

Satria.B is a new variant based on the original Satria code. It does not save the original Master Boot Record anywhere on a disk and it re-infects floppy disks that are already infected. A picture similar to that displayed by Satria.A is displayed every time a PC is booted from an infected diskette.

Shin

Shin contains the encrypted message:

[DarkElf]v2.0 Shin

and it does not seem to contain a warhead. It has been found in the wild at a Melbourne university.

Shin is a memory resident, stealth, boot sector virus residing in the last 3 Kb of the Top of Memory. It infects the Master Boot Record on the hard disk and the boot sector on high density floppy disks only. The virus code in the boot sector is encrypted using a slightly variable encryption procedure. It is also quite a large virus, using 4 sectors.

Shifter

Keys seem to occasionally not work, computer resets, messages displayed about formatting the hard disk.

Shifter is a multipartite .EXE and Master Boot Record infector. When you run an infected file, it infects the Master Boot Record and when you next boot it installs itself in memory.

It is a relatively poor infector but has several tricks to annoy users which are enabled after periods of 10-15 days. These include lost keys, programs refusing to run and messages about formatting the hard disk. This seems to be a bluff and no damage is done. (During this time, random sectors are read so that the disk light stays on.)

Slow (also known as Sydney or Zerotime)

If the system date is set at 1991 or later, every second file closed has its date and time set to zero. This is seen in a directory listing as midnight of either 1980 or 1900. The EXE file corruption is due to the virus not distinguishing between COM and EXE files properly, and thus infecting them incorrectly.

This encrypted virus is memory resident and infects .COM and .EXE files when they are executed (except for COMMAND.COM). The zeroing of the date/time seems to designed to disrupt automatic backup procedures and self-aging applications. On every 150th day, the virus may generate a mutant strain using a different signature. When a file is infected, there may be a delay before the warhead is activated.

Spanz

Spanz is a direct file infector from Malaysia infecting .COM files in the current directory and all subdirectories included in the path variable. It contains the text:

*INFECTED! *SPANZ**

Spanska.1120.A (Also known as NoPasaran1)

This is an encrypted, appending, direct infecting file virus. Spanska targets .COM files, but avoids infecting COMMAND.COM. When an infected file is executed the virus searches for and infects up to 7 clean files. The payload, activated at 22 minutes past every hour (in a gap of 30 seconds), displays a black screen with the text: "Remember those who died for Madrid. No Pasaran! Virus (c) El Gato 1996" and two burning torches in both bottom corners of the screen.

Squawk

The most obvious and annoying symptom of this virus is the loud squawk the PC emits when infected. The virus does not set the frequency of the timer (which determines the tone) so the pitch of the squawk will depend on the last value set. This will usually be the normal beep but there are indications that it may sometimes be supersonic. The virus causes many software programs to crash.

It contains the text:

> *Nguyen Van Cuong - Saigon IBM company.*

Squawk is memory resident and when an infected file is run, it issues a call to see if it is already in memory. If it is not already resident, it sets the top of memory down and copies itself to the top of memory. It redirects Int 21 to a handler in the virus and then loads and executes the original file. The infection procedure adds 852 bytes to both .EXE and .COM files. The virus can infect Read Only files and restores the file date, time and attributes. However, it does not set up a critical error handler, so you will get a “Write error...” message if it attempts to infect a write-protected floppy.

Stardot 789 (also known as AMZ.789)

This is a non-resident virus infecting .EXE and .COM files, adding 789 bytes to infected programs. On September 24th, the virus erases the FAT sectors of all logical drives. The virus contains the string: *AMZ*

Stoned (also known as Marijuana or New Zealand)

Occasionally gives the message *Your PC is now Stoned* if you boot from an infected floppy, otherwise it is generally harmless unless you have a non-standard hard disk. The virus can destroy some directory information on high density floppies but lost files are relatively easy to retrieve.

Stoned is a memory resident boot sector virus that infects hard disks and floppy disks used in drive A. When Stoned infects the MBR of the hard disk, it moves the original to cylinder 0, head 0, sector 7. This is unused on most PCs, but is part of the File Allocation Table on some PCs causing data to become inaccessible. A great number of viruses (including Michelangelo) have been derived from it.

On floppy disks, the directory entries overwritten are:

360K	97-112	720K	65-80
1.2M	33-48	1.44M	17-32

Stoneheart.1490

This is a memory resident polymorphic file virus. It is quiet choosey about which files it will infect, it will only infect EXE files that are greater than 4096 bytes long, do not contain any digits in the filename, have headers less than or equal to 200h, and whose names don't end with the letter 'F' or begin with 'AID', 'AVP', 'PRO', 'SCA', 'EXT', 'WEB', or 'F-'.

Stoneheart also employs some unusual tricks, deliberately making proper detection and cleaning difficult. (i.e. when it finds a file that meets the strict infection criteria, it encrypts the first 512 bytes of the original program code d places the encryption key inside the encrypted virus body (which makes disinfection harder. Vet will detect and clean StoneHeart in memory.

Stonehenge

Stonehenge is a boot sector virus, related to the Marijuana or Stoned virus, but much more primitive; hence its name. Stonehenge will destroy copy-protected games etc. which require the user to boot from a floppy and will destroy the FAT in non-standard PCs such as the Olivetti M24. Otherwise it should not do any serious damage. It was first discovered in Australia, by Roger Riordan, in February of 1992.

The only obvious symptom is that the PC will hang with both A and C drive lights on, if booted from an infected floppy. Disk access to drive A will be slower than normal, but this may not be obvious. If the virus infects a PC already infected with any of the Stoned variants, the hidden copy of the MBR (Master Boot Record) will be destroyed and the PC will become unbootable.

Sunday

On any Sunday, displays the message:

> *Today is Sunday! Why do you work so hard*
>
> *All work and no play make you a dull boy!*
>
> *come on Let's go out and have some fun!*

There are several variants, some damage files or the FAT.

Every Sunday at approximately half-hour intervals the message appears. The virus contains instructions to delete every program as it is executed, however due to a bug in the virus this doesn't happen.

This virus was reported in mid 1990, but is not very common. It appears to have been derived from the Jerusalem virus. File sizes increase by approximately 1,626 bytes. There are 5 other variants, which have different sizes and triggers. Some of these have been modified so that the virus DOES delete files.

Tai-Pan

Tai-Pan (also known as *Whisper*) is a memory resident, parasitic .EXE file infector which increases file lengths by 438 bytes. It contains the string *Whisper Presenterar Tai-Pan*, which is clearly visible in infected files (no encryption is used). The virus contains no other payload and does no deliberate damage. However, it spreads quickly and unobtrusively and it can have infected a lot of files before being noticed.

Tanpro.524

Tanpro.524 is a pre-pending file which keeps an encrypted copy of the original file beginning within the virus code. This means that to disinfect files, the original bytes need to be decrypted.

Tanpro.524 contains the plain text string:

(c)tanpro'94

implying that the virus was first written in 1994.

It infects .EXE and .COM files.

Tau (also known as Sepultura)

Tau is a fairly trivial boot sector infector that was first reported in South Australia. If you boot your computer from an infected floppy disk, Tau will infect the master boot record of the hard disk. Booting from an infected hard drive disk load the virus into memory, reducing the Top of Memory by 1 kb. Tau does not infect 720 kb diskettes.

Tau does no deliberate damage, but if you boot an infected PC from anything but an infected 360 kb disk, the virus will infect the PC and then crash it (due to a bug in its code).

Tequila

Four months after the first infection of the hard disk, Tequila displays the message:

Execute; mov ax, FE03 / int 21 - Key to go on!

If the above program is typed in and run, another message is displayed:

Welcome to T.TEQUILA's latest production.

Contact T.TEQUILA / P.O. Box 543 / 6312 St'hausen

Switzerland

Loving thought to L.I.N.D.A.

Beer and Tequila forever!

When an infected file is executed, Tequila infects the Master Boot Record on the hard disk and copies the rest of its own code and the original MBR to the last 6 sectors of the partition. The next time the system is rebooted from an infected disk, the virus installs itself in memory taking 3 K from the top of memory, and infects .EXE files when they are executed, increasing their size by 2468 bytes. It uses stealth techniques when in memory, and is encrypted with a randomly variable decryption algorithm. It is no longer very common.

Tiny_Family.133

Tiny_Family.133 is an appending file infector which just infects .COM files: it installs itself into the low memory area

It is a simple memory resident virus which belongs to the family of short memory resident file infectors and is related to the Ghost virus. In fact, older copies of VET detected it as Ghost.

It contains no warheads and is thought to be harmless.

Tonya (also known as Skater)

Tonya is a resident .COM file infector that adds 971 bytes to infected files. A message will be displayed if the display is switched to text mode after a specified number of calls have been made to DOS. This normally occurs when the user exits from a program using a graphics mode, like Windows. As programs differ greatly in the number of calls they make to DOS, and as the user may not use many graphics programs, the delay is variable. The message below is displayed at the bottom of the screen and it remains there when the screen is scrolled. The message is encrypted and cannot be seen in infected files

> *I love Tonya Harding,*
>
> *The best womens Figure Skater in history.*
>
> *Now Tonya,*
>
> *Do that triple axle and kick Kristi Yamaguchi's arse*
>
> *- Australian Parasite -*

The virus is not deliberately destructive and the very obvious message means it is not likely to become common.

Trakia

The most outstanding feature of the virus is its replication rate; it installs itself into memory and intercepts int 21H, infecting files which are loaded for execution, opened, renamed or which have their attributes reset. It will therefore rapidly manage to infect large numbers of files.

Trakia is a parasitic file virus which infects .COM and .EXE files attaching itself to the end of them and increasing the length of .COM files by 1070 bytes (Trakia 1070) or by 570 bytes (Trakia 570) and .EXE files by up to 1086 bytes. It seems the virus does no deliberate damage and displays no messages. If you have a write-protected floppy disk in the A or B drive and Trakia 1070 tries to infect it, you may find that it causes the PC to hang.

Tremor

This is a memory resident and polymorphic virus from Germany. Tremor contains two different payloads which occur at random intervals. The first (and more common effect) is the display of the following message on a cleared screen:

> *-=> T.R.E.M.O.R was done by NEUROBASHER*
>
> */May-June '92, Germany <=-*
>
> *-MOMENT-OF-TERROR-IS-THE-BEGINNING-OF-LIFE-*

The computer then pauses for a few seconds and allows normal operation to continue. The second effect is that the screen *shakes* slightly and then halts the PC.

Tremor contains a number of tricks to bypass or disable resident versions of various anti-viral software programs, in particular the anti-viral software supplied with MS-DOS version 6. It is not deliberately destructive but certain low level tricks may interfere destructively with other software. Tremor is not common in Australia, but has been common in Europe.

Troi Two

This memory resident virus contains the words

TROI TWO

but they are never displayed. It was discovered by Roger Riordan in June 1992. The virus is extremely unreliable and crashes under some versions of MSDOS. The virus does no deliberate damage and is too obvious to present much of a problem.

Until May 1st 1992, this virus simply ran the original program. Now however, it issues a hello call and if it gets the right reply, it copies itself to the second half of the interrupt table. If the file extension is .EXE, it reads the file header into a work area on the stack. It then copies itself to the end of the file, adding 512 bytes. It clears the attributes and restores the file date, but it does not trap critical errors.

Trojector.1561 (also known as Athens)

Trojector 1561 is fairly common in the United Kingdom; it was first found at Manchester University. It is a memory resident file virus which appends itself to .COM and .EXE files adding exactly 1561 bytes to their length. Trojector 1561 uses stealth techniques and is encrypted. It is a memory resident file virus which appends itself to .COM and .EXE files adding exactly 1561 bytes to their length. Trojector 1561 uses stealth techniques and is encrypted.

Trojector 1561 is closely related to another virus called *Athens.*

TVPO.3464

This multipartite virus can infect DOS, Windows 3.1x and Windows 95 (NE and PE) .EXE and .COM files. It has Stealth routines to hide the fact that it has loaded itself into memory and infected files.

It adds 100 years to the date stamp for when the file was created

TVPO.3783 (also known as DS, DS.3783) a variant of TVPO.3464

Twin Peaks (also known as Burger.1310)

Displays:

> *Welcome to Twin Peaks. Your PC now has the Twin Peaks virus.*

This virus is an overwriting direct infector which overwrites the first 1310 bytes of infected files before issuing the above message. After this, the infected program usually crashes, locking up the system. The virus has not been analysed in detail but appears to start searching the root directory of drive C. It only infects .COM files and is capable of infecting read-only files. When all files in the current directory are infected, it searches sub directories.

It is not known where Twin Peaks originated, but the sample received was down loaded from a Melbourne Bulletin Board in 1992 and was contained in a file named MIPS.COM.

Vienna

The Vienna family includes many non-resident viruses that infect .COM files, including COMMAND.COM. One out of every six programs which Vienna selects will not be infected. It will change the first five bytes of an infected file, which on execution may cause the system to do a warm boot. This virus is also known as 648, Lisbon, DOS 62.

Usually the Vienna virus will infect a file and set the seconds in the file's time attribute to 62. Infected files will have a file length increase of 648 bytes with the virus being appended to it. Some infected files are not repairable and will need to be replaced. This is a very poor infector and would never have got far, except that the source code for this virus was published in a book. This has resulted in many variants, and this is a fairly common virus.

V Sign

V Sign is a boot sector virus that infects the Master Boot Record on hard disks and the DOS boot sector on floppy disks. After infecting 64 diskettes it displays a 'V' shaped sign on the screen using block graphics and then halt the computer. The virus does not store the original boot sector anywhere, but instead stores 38 bytes of the boot sector within its own code (which is eventually overwritten). It has a slight similarity to the Stoned virus, although unlike the Stoned virus has no problems infecting high density 3.5" disks.

V3SCAN

V3SCAN contains the internal string "*V3SCAN*" and infects .EXE and .COM files unless they begin with "V3" or "SCAN", perhaps to avoid infecting certain anti-virus programs, as a detection delay mechanism. Otherwise, it is harmless, contains no payloads and is not considered to be of particular concern.

VCL (Virus Creation Laboratory)

VCL is an attempt by a virus writer to create a ‘User Friendly’ package that will allow even novice computer users to create their own viruses. VCL allows a user to pick from menus to determine the infection type, encryption and to select from a nasty array of warheads. Once the options are selected it will produce either assembler code or a .COM file (which can then be inserted into programs or projects).

On a lighter note, the writer has also added a warning to expressly forbid the disassembly of his code for the purposes of scanning for viruses created by the package.

W Boot (also known as Stoned NSW)

W-Boot is also known as Stoned.NSW since it is a variant of Stoned and was found in New South Wales in early 1993. It infects the Master Boot Record on hard disks and the DOS Boot Sector on floppies. It has no known visible effects or payloads. The virus is one sector in length and places the original Master Boot Record in sector 7 on hard disks and in the last entry of the root directory on floppies. It occupies 1K of memory and possesses stealth capabilities.

Wanderer.1209 (aka KSTmo.1209)

This file virus targets .EXE and .COM files except for command.com (infecting comman.com may corrupt your PC and draw attention to the virus. This virus uses stealth techniques to evade detection. Once run the virus will be memory resident in low memory and will begin infecting any clean .EXEs and .COMs that are run.

Wanderer.1756 is a variant of this virus.

X-Fungus

John Bonham-September 20, 1980

-LED ZEPPELIN-

On the 20th. of September of any year X-Fungus displays the above message up to 5 times, pausing in between each. Some time after this the PC will lock up and any work in progress at the time will be lost. A Queensland student claims to have written the virus, and source for this virus and its earlier versions have been available on various bulletin board systems. So far the earlier versions have not been found in the wild.

After the X-Fungus virus becomes memory resident, it will infect all executable files that are opened, even files being accessed for renaming or copying. The virus adds about 1425 bytes to infected files, and spreads fairly quickly, especially on networks.

Xtac

May display the text:

> *good news! you have just been*
>
> *smitten by XTAC - lyndon siao, usc - tc*

Xtac is a memory resident file infector which infects COM and EXE files appending 1564 bytes to the file. It may corrupt COMMAND.COM, so that the PC will no longer boot properly. It was discovered in March 1993 at a Melbourne university.

Yale (also known as Alameda and Merritt Virus)

This is a memory-resident boot sector virus which infects only floppy disks. It infects diskettes in drive A on the Ctrl-Alt-Del key sequence.

This early virus stores the boot sector in cylinder 39, sector 8, but does not mark it as bad, therefore if the disk is full some data will be overwritten. It uses 1 kilobyte of memory and hooks interrupt 9. Whenever the user uses the Ctrl-Alt-Del key sequence, the virus fakes a warm boot and infects the disk in drive A if it is not infected. It was never common and may be extinct now, particularly since it cannot run on computers with 80286 or higher processors.

YMP

Have a Nice Day (c) YMP

is displayed on 1st of month

YMP is a memory resident boot sector virus from Europe. If you boot from an infected floppy, YMP will infect the Master Boot Record and will occupy 2 K of memory. When the PC is rebooted, YMP will infect any floppy in drive A on read or write access.

YMP does not save the original MBR, but it does not alter the partition information. YMP contains no warhead or payload and appears to be fairly harmless. However, it saves the boot sector on floppies in one sector so it may overwrite 16 files, causing data loss.

Zerotime 2

This is a variant of the Slow virus. It is a memory resident virus that has been trivially modified to avoid detection, but seriously compromised in the process. The dates on files are altered, infected .COM files probably won't work and .EXE files are infected multiple times.

See also Zerotime 3

Zerotime 3

This variant of the Slow or Zerotime virus was found at a New South Wales school in 1992. The changes made are trivial and should not have any effect on the operation of the virus.

See also Zerotime 2

Zibbert.1268

This is a memory resident, file virus that infects .COM files by appending the viral code to the target file.

The virus has a warhead will activate between July and December on Tuesdays and Thursdays. Once activated any printed character of As or Qs will be replaced with a space.

Zibbert.1315

This is the same as Zibbert.1268 except that it can also infect .EXE files.

Agent.A (aka NOP.A)

Was found in the wild in Australia in mid 1997.

This document will infect your Normal.DOT when the AutoOpen macro is run during the opening of the document. If calculator is active at the time of infection a dialog box will appear with the message “eher is HG tnegA”

This virus will not intentionally damage files on your PC.

Macro names: AutoOpen, Agentgh

Anti-Concept

This macro virus seems to have been written to remove the Concept macro virus. It will automatically be triggered when you attempt to open any file infected with Anti-concept. Once activated it will look for and remove any macros called AAAZAO, AAAZFS, FileSaveAs, FileSave, FileNew, FileOpen, and PayLoad from the Word template Normal.DOT. It will also display a message “Your system may or may not be clean. Please close, clean and open it AGAIN”

Macro names: FileNew, AutoOpen, FileSave, FileSaveAs

Atom

When an infected file is opened, the virus checks normal.dot to see if it is already infected. If not, each of the virus macros is copied to normal.dot. The virus then checks to see if it is the 13th of December and if so attempts to delete every file in the current directory.

The virus replicates to documents through File/Open and File/SaveAs. When the user opens a new file the virus immediately copies itself to the file and saves it. When the user saves a file using File/SaveAs the virus copies itself to the file. Before saving, it checks to see if the seconds on the system clock equal to thirteen and if so the file is protected with the password 'ATOM#1'. If the file is already infected and the virus tries to set the password, a WordBasic error occurs.

Macro names: Atom, AutoOpen, FileOpen, FileSaveAs

BadBoy.B

Found in the wild in Australia in early 1997. The virus replicates as an infected document is opened and as documents are saved. As it infects the global template (NORMAL.DOT) and removes 3 items from the default Word menus: Tools/Macro, Tools/Customize and File/Templates. On the 18th or 20th day of the month, if a file is opened by an infected system a message box pops up with the caption "Mack daddy", the text "Bad Boy, Bad Boy, What u gonna do" and a single 'OK' button. If the user clicks the button a second message pops up entitled "the Gangsta Rappa" with the text "What u gonna do when they come for you" and a single 'OK' button. BadBoy.B does not intentionally cause any damage, apart from renaming the Word menus Tools/Macro, Tools/Customize and File/Templates.

Macro names: AutoOpen; FileSaveAs; BadBoy

Bandung

WordMacro.Bandung originated in Indonesia and like many other Word macro viruses, is a variation of WordMacro.Concept.

It replicates by infecting normal.dot when an infected document is opened, copying each of its macros to the global template. It then infects clean documents as they are saved with either File/Save or File/SaveAs.

WordMacro.Bandung has a pseudo stealth mechanism which disables both the Tools/Macro and the Tools/Customise menu items. If a document is infected and the user selects either of these menu options nothing will happen. Other media sources have described a payload which is triggered when the user selects either of these menu options, involving a message box saying "Fail on step 29296 ", and each letter 'a' in the current document being replaced by '#@'. This is in fact wrong, as this particular payload can never be triggered.

The virus does have a working and quite dangerous payload which is triggered when the user starts Word, but only if the date is the 20th or later in any month, and the time is after 11am. When triggered the virus deletes the contents of each directory on C drive, excluding the root directory (c:\), WINDOWS, WINWORD or WINWORD6, recursing three directories deep. It then creates a file in the root directory called PESAN.TXT containing a message from the author written in Indonesian, describing the damage done and the date and time the files were deleted.

Macro names: AutoExec, AutoOpen, FileSave, FileSaveAs, ToolsCusomize, ToolsMacro

Boom

This virus was written for the German version of Word, and doesn't replicate fully with the English version. Document files may infect the English normal.dot, but the infected normal.dot cannot spread the virus further.

The virus replicates when a file is opened and through Datei/SpeichernUnter. When a user opens an infected document the virus checks normal.dot to see if it is already infected. If not, it copies itself to normal.dot and runs the AutoExec macro. When a user using the German version of word saves a file using Datei/SpeichernUnter (File/SaveAs), the virus checks the file to see if it is already infected and if not, copies itself to the file and saves it.

The AutoExec macro sets a Word timer to run the System macro at exactly 1:13:13pm (13:13:13). If Word is running at this time, the System macro is automatically launched. The AutoExec macro is automatically run by Word at startup, so if a copy of Word is infected, this timer will be set every time Word starts, even if the user has not yet done anything.

The System macro contains the virus payload. It will only do anything if the date is after February 1996, and it is the 13th day of the month. Each of the menus are renamed as follows, although it only works for the German version of word and if the menus have all the default German names:

Datei (File) to "Mr. Boombastic", Bearbeiten (Edit) to "and", Ansicht (View) to "Sir WIXALOT", Einfügen (Insert) to "are", Format to "watching", Extras (Tools) to "you", Tabelle (Table) to "!", Fenster (Window) to "!" and ? (Help) to "!".

The message "Mr. Boombastic and Sir WIXALOT : Don`t Panik, all things are removeable !!! Thanks VIRUSEX !!!" is then displayed 5000 times on the statusbar.

A new file is created and the messages "Greetings from Mr. Boombastic and Sir WIXALOT !!!", "Oskar L., wir kriegen dich !!!" and "Dies ist eine Initiative des Institutes zur Vermeidung und Verbreitung von Peinlichkeiten, durch in der Öffentlichkeit stehende Personen, unter der Schirmherrschaft von Rudi S. !" are inserted. The file is then printed and closed.

The virus then resets all the menus to normal and removes the message from the statusbar.

Macro names: AutoExec, AutoOpen, DateiSpeichernUnter, System

CAP.A

This is a multi lingual macro virus which has no ‘destructive’ payload.

CAP will remove the Macro and Customise from the Tools menu, and also Macro from the File menu.

The virus is multi-lingual as it uses the names of the menu items as the names for the macros. As the menu item names change with each different version of Word, its macro can be created in any language. By mid 1997 it has been found in English, German, Dutch and Taiwanese versions of Word.

The following message is in the programming code:

> C.A.P.: UnVirus Social. Y ahora digital.
>
> “jacky Rwrty” (jpn3rty@hotmail.com)
>
> Vemezuela, Maracay, Dec1996.
>
> P.D. Quehaces gochito? Nunca seras
>
> Simon Bolivivar. Bolsa!

The Spanish used in this message is quiet poor but appears to refer to somebody connect with Digital in Venezuela. It also says that you can smoke hash, but you will never be as good as Simon Bolivivar.

Macro names: ToolsMacro, FileTemplates, CAP

Colors.A (also known as Rainbow)

This virus replicates through all of its macros except AutoExec and macros. Saving a file with either File/Save or File/SaveAs or creating a new file with File/New will infect the document. Opening, closing, creating or saving any file will infect normal.dot, as will exiting Word or selecting Tools/Macro from the menu.

The AutoExec macro is run automatically by Word at startup, but it contains no macro code.

If the user tries to view the macros via Tools/Macro, normal.dot will be infected but the Tools/Macro dialogue box does not pop up. Therefore, to manually delete this virus the Template Organiser must be used. To access the Template Organiser it must be installed on the toolbar with Tools/Customise and clicked from there.

The macros macro contains no main code, but has common sub-routines used by each of the other macros except AutoExec.

Each macro except AutoExec calls a sub-routine which eventually triggers the virus payload. A counter is incremented and stored in win.ini under the section [Windows] with the name 'countersu'. Every 300th call to the sub-routine it randomly changes the Windows desktop colours

See also Colors.B

Macro names: AutoClose, AutoExec, AutoOpen, FileExit, FileNew, FileSave, FileSaveAs, macros, ToolsMacro

Colors.B (also known as Rainbow)

This virus is a variation of the Colors.A virus. It contains the same macros as Colors.A and all except FileNew and AutoOpen are exactly the same.

The AutoOpen macro from Colors.B is actually the AutoOpen macro from Concept, an older virus. This would indicate that at some stage a user had a document infected with firstly Colors.A and then Concept, but when Colors.A replicated into the user's normal.dot it copied Concept's AutoOpen macro. This has little effect on the virus' behaviour, only that the virus no longer infects normal.dot when an infected file is opened.

The FileNew macro from Colors.B is almost identical to FileNew from Colors.A, only one line is removed. Removing the line made no difference to its behaviour.

The Colors.B virus has exactly the same payload as Colors.A.

Macro names: AutoClose, AutoExec, AutoOpen, FileExit, FileNew, FileSave, FileSaveAs, macros, ToolsMacro

Concept (also known as WW6Macro and 'Prank' Macro)

Concept is widely accepted as the first macro virus and appears to have been written to prove the concept that it was possible to write a virus in an applications (i.e. Word's) macro language.

There are five different macro names in the Concept virus, but only four of them are in an infected document or normal.dot at any time. Infected documents don't have FileSaveAs and an infected normal.dot doesn't have AutoOpen. AAAZAO and AAAZFS are merely copies of AutoOpen and FileSaveAs respectively.

The virus infects normal.dot when an infected document is opened. During the first infection, the virus displays a message box with a faulty counter in it. It is supposed to count the number of times normal.dot has been infected, though the counter is buggy, and never counts higher than one. It is stored in winword6.ini in the [Microsoft Word] section with the name 'WW6I'.

The virus infects documents through File/SaveAs, by simply copying itself to the file before saving it.

The PayLoad macro contains no macro code, only a message declaring "*That's enough to prove my point".*

See also Anti-Concept
See also Concept.French

Macro names: AAAZAO, AAAZFS, AutoOpen, FileSaveAs, PayLoad

Concept.French

This is a French version of Concept. The virus has been modified to work with the French version of Word and contains the macro FichierEnregistrerSous instead of FileSaveAs. The virus otherwise behaves exactly the same as the original version of Concept.

Macro names: AAAZAO, AAAZFS, AutoOpen, FichierEnregistrerSous, PayLoad

Date (also known as Anti-DMV)

This virus replicates when a document is opened. Before infection it checks the date, and only continues if it is prior to June 1996. Obviously this virus is no longer as great a threat as it once was, though if a user's system time is incorrect (and earlier than June in a year earlier than 1996) the virus may still spread.

After infection the virus deletes the AutoClose macro if one exists. The reason for this is not known, it may be targeting another virus or an anti-virus product.

Macro names: AutoOpen

Defender

Defender.A is a new virus discovered by Cybec in Australia recently. It is unusual because it professes to be an anti-virus tool (it is based on the outdated Microsoft tool ScanProt), yet it replicates and therefore is a virus itself. It copies itself to the global template when an infected file is opened, and infects documents as they are saved with File/SaveAs. It also searches for other macros on the system (such as the Concept macros AAAZAO and AAAZFS) and notifies the user before deleting them. Defender.A will block the Tools/Macro menu item requesting a password before the user may use the usual Tools/Macro dialog box, using the file name as the password.

Macro names: Module1, Module2, Defender, FileOpen, FileSaveAs, ToolsMacro, Defend, Module3, Module4, AutoOpen

Demon.A

This macro virus will remove ALL macros from the macro menu in Word 6 and 7 (by removing all of the macros the virus hopes to remove some of the simpler anti-virus software). The virus will also edit the FileSaveAs and AutoClose items from the menus and convert them to macros, this is a common method used by virus writers to get users to trigger the virus. If you select File then SaveAs from the Word menus it will check to see if there is a macro by this name, if there is it will be run. Provided the macro still saves the file users are unlikely to note the extra time that it takes to perform the file save.

The virus is unusual in that it will continually reinfect itself to modify the random name of two of the macros.

If you have a document called “Dark Master Calling” the virus will identify itself by displaying a message box with;

“Winword Hidden Demon is happy to see it’s master!!!

”This file is infected with Winword DEMON”

Macro names: FileSaveAs, AutoClose, Two randomly nameed macros

Divina

This virus is very similar to Date and is quite likely by the same author. It also has only one macro, AutoClose, and Divina may be the virus that Date targets when it deletes AutoClose.

Although it is similar to Date, Divina is much larger. It does not have the date restriction Date enforces and will replicate at any time of the year. The virus replicates as a document is closed and if the time when the user closes the file is exactly 30 or 45 minutes after the hour, the virus attempts to infect every document in the default template directory with the extension '.dot'. If the user has their time format setting to 24 hour 'hh.mm' and it is ten past ten in the morning ('10.10') then the virus also attempts to infect every document in the current directory with the extension '.doc'.

If it is the 21st of May and between 10 and 20 minutes after the hour or between 40 and 50 minutes after the hour then a payload is launched. A message box entitled "zio Massimo " displays the text " . . . . . DIVINA IS THE BEST! . . . . . .". All the open files are then saved. The virus pauses and beeps before displaying another message box entitled "Virus 'DIVINA' in esecuzione" with the text "Oggi è il compleanno di Divina: devi far festa! Non continuare o verrà formattato il disco rigido...". It then causes Windows to shut down completely.

If the first payload didn't qualify, another may be launched. If on any day it is exactly 17 minutes past the hour a message box entitled "Massimo " displays the text " . . . . . ROBERTA TI AMO! . . . . . .". The virus pauses and beeps and displays another message box entitled "Virus 'ROBERTA' is running" with the text "Hard Disk damaged. Start antivirus ?". The message box (like all previous message boxes) has only one button labelled 'OK'. The virus then saves all open files and pauses and beeps again. A message box entitled "Virus stopped" displays the text "Exit from system and low level format are recommended.". Another pause/beep combination follows before a final message box entitled "Microsoft Windows" displays the text "Exit from System ?". The inevitable pause and beep follows before Windows is shut down.

The pauses make the virus seem like it is actually doing something, though both payloads are quite harmless unless the user follows the 'advice' and performs the low-level format.

Macro names: AutoClose

DMV

DMV stands for Document Macro Virus. This virus was (supposedly) written in late 1994, before macro viruses were found in the wild. It was written and documented only as an example of the potential danger macro viruses pose. The original documentation of the virus explains the Document Macro Virus concept and outlines the steps a virus takes when infecting documents.

The virus replicates when a document is closed. At each stage of the infection a message box pops up informing the user of the virus' actions, and is blatantly obvious as it performs the infection.

Macro names: AutoClose

Doggie

This virus is fairly simple. Documents are infected when opened, or saved with File/SaveAs. When a document is infected by the AutoOpen macro a message box pops up displaying the text ‘Doggie’. The Doggie macro is never called.

Macro names: AutoOpen, Doggie, FileSaveAs

FormatC

This is not a virus, but a trojan horse. The AutoOpen macro simply contains two lines of code that when run, will unconditionally format drive C. It doesn't try to replicate itself at all and is therefore not a virus. Even if it did replicate, it wouldn't get far once the hard disk had been formatted.

Macro names: AutoOpen

Friendly

This virus attempts to be effective in both the English and German versions of Word although it doesn't work to it's fullest potential in the English version. Bugs prevent it from replicating in the English version of Word, and many WordBasic errors are reported while the virus tries to replicate. The virus does replicate in the German version of Word.

It tries to achieve bilingual infection by simply carrying an English version and a German version of itself, thus the relatively numerous macros. Both versions of the virus are very similar but not identical.

The virus replicates to normal.dot when an infected document is opened. It checks a flag in win.ini under the section [friends] called 'author'. If it is 'Nightmare Joker' then it assumes normal.dot is already infected, otherwise it copies each of the macros to normal.dot. It then attempts to drop an executable file virus using the debug program in the c:\dos directory using a script. c:\autoexec.bat is modified to run the virus at next boot up.

For both English and German users, documents are infected many ways. When the user creates a new document, opens a document, or saves a document it will be infected. When Word exits the open document is infected. For the German version only, a document is infected when it is closed. Also for the German version only, the executable file virus is dropped (again) when a document is saved with Datei/Speichern (File/Save).

The Cancel macro and its German equivalent Abbrechen are never called.

The ExtrasMacro and ExtrasMakro macros pop up two message boxes each, both saying the same thing in English and German respectively. The author of this virus was German and mistakenly named ExtrasMacro as a direct translation of ExtrasMakro, instead of ToolsMacro. Therefore, in the English version the macro is never called.

In ExtrasMacro the first message box is entitled "Hello my friend!" and contains the text "You can't do that!". The second is entitled "<< Friends >> Virus" with the text "I'm very anxious!".

The first message box in ExtrasMakro is entitled "Hallo mein Freund!" with the text "Du kannst das nicht tun!" while the second, called "<< Friends >> Virus" contains "Ich bin sehr ängstlich!".

In both versions, opening a new document will call the talk macro, as will the English versions of FileOpen and FileSaveAs.

The talk macro is run only once. After it has finished it modifies win.ini, setting the option under [NJ] called 'info' to 'update'. Each time the talk macro is called it checks this flag and does not continue if 'update' is found.

It then interacts with the user. Firstly, it determines which version of Word the user is running. If the default currency for the system is 'DM' then the virus assumes it is a German version. If the default currency is not 'DM' then the virus assumes it is an English version. Based on these assumptions it then displays a series of message boxes in the corresponding language.

For English users the first message box is entitled "Hello my Friend!" with the message "I´m the << Friends >> Virus and how are you? Can you give me your name, please:". A prompt appears on the status bar saying "My name is: " and the user must type their name to continue. A second message box pops up displaying "Hello *name* I have a good and a bad message for you! The bad message is that you have now a Virus on your Harddisk and the good message is that I´m harmless and useful. Press OK!". A third message box then pops up with the text "If you don´t kill me, I will insert a programme in your AutoExec.bat thats your Keyboard accelerated. Please *name* don´t kill me. Goodbye!"

For German users the first message box is entitled "Hallo mein Freund!" with the message "Ich bin der << Friends >> Virus und wie heißt du? Gib doch bitte anschließend unten deinen Namen ein:". A prompt appears on the status bar saying "Mein Name ist: " and the user must type their name to continue. A second message box pops up displaying "Also *name* ich habe eine gute und eine schlechte Nachricht für dich! Die schlechte Nachricht ist, daß ich mich auf deiner Platte eingenistet habe und die gute ist, daß ich aber ein freundlicher und auch nützlicher Virus bin. Drücke bitte OK für Weiter!". A third message box then pops up with the text "Wenn du mich nicht killst, dann füge ich ein Programm in deine Autoexec.bat ein, daß deine lame Tastatur etwas auf Touren bringt. Also *name*, gib dir einen Ruck und kill mich nicht. Goodbye!"

Macro names: Abbrechen, AutoExec, AutoOpen, Cancel, DateiBeenden, DateiNeu, DateiÖffnen, DateiSchließen, DateiSpeichern, DateiSpeichernUnter, ExtrasMacro, ExtrasMakro, Fast, FileExit, FileNew, FileOpen, FileSave, FileSaveAs, Infizieren, Talk

Goldfish

Goldfish was first found in late 1996 and is thought to have been written in Australia.

Goldfish replicates by using the AutoOpen and AutoClose macros when an infected document is opened or closed. The payload has a one in five hundred chance of triggering when the infected file is opened or closed. When triggered it will displaying a dialog box with the following message:

> GoldFish
> I am the GoldFish,
> I am hungry, feed me.

You will not be allowed to continue until you enter one of the following words: fishfood, worms, worm, pryme or core.

Macro names: AutoOpen, AutoClose

Guess (also known as Phantom)

Guess is unusual in that it acts as a companion virus, rather than a direct infector. It creates a template and associates it with the document, and then infects the new template. Every time the document is loaded, the associated template is also loaded along with the virus. Deleting the virus is simple; the associated template should be deleted, and the original document need not be modified.

Guess has many simple payloads based on a random number generated at run time. These 'symptoms' can be the font size reducing by one, the sentences "The word is out.", "The word is spreading." and "The Phantom speaks..." sent to the printer, the sentences "Sedbergh", "is CRAP" and "The word spreads..." sent to the printer, any of the sentences "This school is really good. NOT", "We all love Mr. Hirst.", "Mr. Hirst is a great bloke", "M.R.Beard", "This network is REALLY fast.", "Hi sexy!", "Who's been typing on my computer?", "Well helloooo there!" or "Guess who?" inserted into the current file, or the file closing upon being opened. One of these actions need not happen every time though.

Macro names: AutoOpen

Hot

This virus has only four macros, but when it replicates it renames them, hence the many macro names. An infected document will contain the macros AutoOpen, InsertPBreak, DrawBringInFrOut and ToolsRepaginat. When it is opened it infects normal.dot, copying each macro to the global template. InsertPBreak is renamed to InsertPageBreak, DrawBringInFrOut is renamed to AutoOpen, ToolsRepaginat is renamed to FileSave and AutoOpen is renamed to StartOfDoc.

Documents are infected when they are saved with File/Save. Each macro is copied to the document, and renamed back; StartOfDoc to AutoOpen, FileSave to ToolsRepaginat, AutoOpen to DrawBringInFrOut and InsertPageBreak to InsertPBreak.

The InsertPageBreak macro is there solely to allow the virus to check if normal.dot is already infected.

When normal.dot is infected the virus stores the date of infection plus fourteen days in the winword6.ini, under the section [Microsoft Word] with the name 'QLHot'. Then, when a clean document is opened, the virus checks this value. If the value isn't there, it sets it to the current date plus ten days. If the value is later or equal to today then the virus does nothing. If the value is earlier than eleven days ago then the value is reset to today plus six days. In all other cases the virus may launch a payload. It generates a random number between 1 and 6 inclusively, and if today plus the random number is equal to the stored value then the virus checks for the existence of the file c:\dos\ega5.cpi. If it does exist then the file is saved and closed. If it doesn't exist, all the text is wiped from the document and it is saved.

Macro names: AutoOpen, DrawBringInFrOut, FileSave, InsertPageBreak, InsertPBreak, StartOfDoc, ToolsRepaginat

Hunt.A

This macro virus has been known to infect several German versions of Word.

When Hunt infects a PC it will copy itself into the startup path as winword.dot. It will replicate without using wither macrocopy or Nomal.DOT, dateinew bases a new document on the template winword.dot so it can only replicate suing FileNew. Hunt will infect English versions of Word but will then not be able to replicate. It contains no payload apart from displaying the following mesage:

One - you look the target

Two - you bait the line

Three - you slowly spread the net

And four - you catch the man

Macro names: AutoOpen, Dateineu, Extrasmakro

Hunt.B

This macro virus has been known to infect several German versions of Word.

Hunt.B is able to reconstruct the startup path if it has been cleared. The Datainer macro will create a new document. In Hunt.A the document would contain 'Catch the man'. This version clears the new document that it creates.

Macro names: AutoOpen, Dateineu, Extrasmakro

Hunt.C

Similar to Hunt.B except that it is Polymorphic.

When an infected document is opened there will be a one in twelve chance that it will pick up one of the infected macros and will randomly insert a variable setting command. This version will not display the 'Catch the man' message that was in Hunt.A.

Macro names: AutoOpen, Dateineu, Extrasmakro

Imposter

This virus is a heavily modified version of Concept. It contains two macros, though they are renamed when copied, hence the three different macro names.

An infected document contains the macros AutoClose and DMV. When an infected document is closed, the virus checks normal.dot for a copy of the DMV macro and FileSaveAs macro. If neither are there it copies both macros to normal.dot, renaming AutoClose to DMV and the original DMV to FileSaveAs. It then displays a message box with the text “ DMV ”.

The virus infects documents when they are saved using File/SaveAs. It simply copies the macros to the file and renames them back; DMV to AutoClose and FileSaveAs to DMV.

Macro names: AutoClose, DMV, FileSaveAs

Hybrid.B

This macro virus has been known to infect several English versions of Word.

The AutoClose macro belongs to the Scan.DOC virus protection macro set. The virus will replicate every time AutoOpen or FileSaveAs is run. This virus does not have any payloads. The AutoClose macro effectively does nothing. This virus has been corrupted at some point and will generate errors due to the absence of some of the original macros.

Macro names: AutoOpen, AutoClose, FileSaveAs

KillDLL

This virus is very simple and quite destructive. It replicates when a document is opened, copying itself either to or from normal.dot. Every time it replicates it deletes every file matching *.d?? in the c:\windows\system directory.

Macro names: AutoOpen

LbyNJ (also known as Sex)

This virus is German and only replicates with the German version of Word. It was written similarly to Friendly and is most likely by the same author. It is also very similar to Xenixos, and may be based on Xenixos code (or vice-versa).

The virus replicates to normal.dot when an infected document is opened. It checks if a value in win.ini under the section [Compatibility] named 'LBYNJ' is equal to 0x0030303. At no stage does the virus set this value nor is it a default setting, so the check always returns false. The virus also makes sure the macro Telefonica is present in the document before copying each of the macros to normal.dot. It then passes control to the Telefonica macro.

The virus replicates to documents when they are created or opened, or when the user exits Word. When a document is opened control is passed to the Telefonica macro.

The Telefonica macro (like the Fast macro from Friendly and the Drop macro from Xenixos) attempts to drop an executable file virus using the debug program in the c:\dos directory. There is a bug in the macro code though, and the attempt is always unsuccessful.

When the user prints a document, if the current time is within ten seconds after the minute the words "Lucifer by Nightmare Joker (1996)" are appended to the file and also printed.

Macro names: AutoExec, AutoOpen, DateiBeenden, DateiDrucken, DateiNeu, DateiÖffnen, Telefonica

Laroux (also know as Excel Macro Virus)

Laroux is the first Macro virus to infect Excel spreadsheets and is a pretty innocuous virus, more like a proof of concept than an attempt to do deliberate damage. Written in VBA (Visual Basic for Applications), Laroux can only infect spreadsheets created by Excel versions 5 and above.

Laroux infects Excel spreadsheets by storing itself in the Personal.xls workbook and attempts to infect other workbooks when they are opened. Laroux takes control of the system by creating the Personal.xls workbook in the Excel startup directory. This is done automatically when an infected workbook is opened. By writing itself to the startup directory, the virus ensures that it is loaded automatically every time Excel is started, allowing it to infect other workbooks by copying itself to the workbook and hiding the sheet (called “laroux”), which contains the virus code.

It will often cause Excel to display a macro error message. Excel users can also detect it by using Tools/Macro to check for the two virus macros “auto_open” and “check_files”. If they both exist, the virus is present.

Laroux will not be able to infect any system where the Personal.xls workbook already exists. Excel automatically creates this workbook when users record their own macros, so many systems are already protected against infection from this virus.

LOX

This macro virus has been found in several English versions of Word.

This virus has many trigger and payloads. i.e. the time that you exit a word document. The most obvious payload is that it can replace spaces “ “ with the infinity and null characters. Any infected document will not let you save the document with a .DOT extensions (it must have .DOC)

Macro names: WordDe, AutoExec, AutoOpen, FileOpen, FilePrint, FileSaveAs, WordSu

MDMA

MDMA.A

This macro virus has been found in all English versions of MS Word.

Macro names: AutoClose

MDMA.B

This is a corruption of MDMA.A (some of the warheads have been corrupted)

MDMA.Q

Slightly corrupted version of MDMA.A

Mess

The virus has a number of different payloads, however none are destructive. For example, if you are working on a Word document just before midnight (23:59:59), the MESSA macro is triggered. This macro produces 100 beeps, moves to the beginning of the currently opened document, and inserts the following text:

> *THE 'V' WARNING MESSAGE*
> *Sorry to interrupt You. I think You are tired,*
> *because You have worked until midnight.*
> *so I suggest You to go to bed now and*
> *tomorrow You could work harder than this day.*
> *Kota Pelajar, Yogyakarta.*

Mess.A is unusual in yet another way: if the user presses CTRL+ALT+SHIFT+K,K, the 'TheVWarning' macro is activated. This macro 'takes care' of all Mess.A macros and added menu items, and removes everything except itself. It then "rewards" the user with a series of beeps and the following message:

> *Congratulations you have found the keywords of this macro virus*

Some of the following macros will be found in the document and some will be found in the normal.dot template.

Macro names: AutoExec, AutoOpen, FileOpen, FileSave, FileSaveAs, POO, EOP, ESA, ESAA, BEEPER, MESSA, README, INFO, TheVWarning, WATCH, NIZ, CROM, PLT, CUS, CUST, WEV, Organizer, ToolsMacro, FileTemplates, ToolsCustomize, ToolsCustomizeToolbar, ViewToolbars, OEX, OOP1, OOP,

Muck

This macro virus has been known to infect all English versions of MS Word.

This virus will sometime display the work ‘MUCK’ when infecting a document, it has no other warheads.

Macro names: AutoOpen, FileSave, AutoNew, AutoExit, FileSaveAs and AutoClose

Muck.B

Same as Muck.A

Muck.H

Same as Muck.A except that AutoClose and AutoExit are empty and AutoNew has been corrupted to a benign “Inter office communications” macro. No payload.

Muck.K

Same as Muck.A except AutoOpen and AutoClose have been modified and call a non-existent macro.

AutoExit deletes some files from C:\Msoffice\Templates\OEP-Dial.DOT and WordInfo.DOT.

This is a corruption of Muck.A and can give lots of errors. No deliberate payload.

Muck.P

Same as Muck.A except AutoClose, AutoExit and AutoNew have been substituted with non viral utility macros.

It will still delete some add-ins and customisations and will also display errors due to the macros listed above not containing viral code.

Nop (NOP.A aka Agent.A, NOP.C aka TADAII & RV01)

This virus has two macros; an infected document contains AutoOpen and Nop, while an infected normal.dot contains DateiSpeichern and Nop.

The virus infects normal.dot when an infected document is opened. It copies both macros to normal.dot and renames AutoOpen to Nop and the original Nop to DateiSpeichern (FileSave).

The virus then spreads to documents as they are saved, simply by copying the macros and renaming them; Nop to AutoOpen and DateiSpeichern to Nop.

NOP.A:

The only payload for NOP.A is if the windows calculator is running the virus will bring up a massage saying "…eher si HG tn eya"

NOP.C:

Has no payload except that it replaces the file extension .SAP to .SÁP

NOP.I:

Targeted at a particular system, this virus is designed to move files into a different user's share directory. (This version of NOP has been customised to steal Word files over a LAN).

NOP.M:

This version will infect English version of Word but is only able to successfully propagate when it has infected a German version of Word. Once Word is infected the virus display fake error messages (in German). It will also change command.com to commmand.com, and io.sys to iio.sys.

Macro names: AutoOpen, Nop, DateiSpeichern, FileSave, QV01, FichierEhregistrer.

NikNat.A

This macro virus has been known to infect all version of Word that are in the English language. It will create a hidden directory C:\EvaHzy2. When using Windows 95 it will drop a bitmap picture of a model into the hidden directory.

On October 23rd it substitutes the picture for the wallpaper used by Windows 95.

Macro names: Evahzg, Tclosean, AutoCLose, ToolsMacro, FileTemplates

Npad (various versions)

All 50 variants (to mid 1997) are not deliberately destructive. (But this does not mean that future versions will also be harmless)

Macro names: AutoOpen,

Nuclear.A

This virus infects normal.dot when an infected document is opened. Documents are then infected as they are saved with File/SaveAs or as they are opened.

The Payload macro is called when a document is opened. It tries to delete some DOS system files on the 5th of April, but always fails due to a bug. The DropSuriv macro is called when normal.dot is infected. It attempts to infect the PC with an executable file virus, but it also has bugs, and fails. So, fortunately, both these destructive payloads are defunct.

The virus does have a less dangerous payload. If, as the user prints a file, the current time is between the 56th and 59th second after the minute the virus inserts the text “And finally I would like to say:” and the text “STOP ALL FRENCH NUCLEAR TESTING IN THE PACIFIC!” at the end of the document, and is printed with the rest of the original document.

See also Nuclear.B

Macro names: AutoExec, AutoOpen, DropSuriv, FileExit, FilePrint, FilePrintDefault, FileSaveAs, InsertPayload, Payload

Nuclear.B

This virus is a cut down version of Nuclear.A. It is the same in all respects, except it does not attempt to infect the PC with the executable file virus when normal.dot is infected. It still tries and fails to delete the DOS system files when a document is opened.

Macro names: AutoExec, AutoOpen, FilePrint, FilePrintDefault, FileSaveAs, InsertPayload, Payload

Paycheck (Version B and C)

Paycheck.B and Paycheck.C are very similar to each other, having slightly different macros and corruptions. Both viruses will display a message in Indonesian on the 25th of any month as Word is started. The FileSaveAs and ToolsMacro macros are both corrupted and produce errors if the user tries to access the File/SaveAs and Tools/Macro menu items. Paycheck.B's ShellOpen macro is a conversion to Indonesian of the ShellOpen macro from Microsoft's ScanProt tool, while Paycheck.C's ShellOpen macro is the same macro but not converted to Indonesian. Neither virus has a dangerous payload.

Macro names: AutoExec, AutoOpen, FileOpen, FileSave, ShellOpen, FileSaveAs, ToolsMacro.

Pheeew (also known as Nl or Concept.Nl)

This is a Dutch virus and replicates only with the Dutch version of Word. It is very similar to Concept and contains messages that are also found in the Nuclear viruses.

It replicates in a similar way to Concept. When an infected document is opened it copies itself to normal.dot. IkWordNietGoed1 is a copy of AutoOpen and IkWordNietGoed2 is a copy of BestandOpslaanAls (FileSaveAs). The AutoOpen macro is found only in infected documents, and BestandOpslaanAls is found only in normal.dot.

Then when a document is saved with Bestand/OpslaanAls (File/SaveAs) it is infected. Unlike Concept, Pheeew has a destructive payload. After the virus infects normal.dot it displays a message box entitled "GOTCHA" with the message "Important!". It then displays another message box entitled "FINAL WARNING!" with the text "STOP ALL FRENCH NUCLEAR TESTING IN THE PACIFIC" and two buttons labelled 'Yes' and 'No'. If the user chooses 'No' the virus deletes all the files in the c:\dos directory. It also attempts to delete all files in the c:\ directory but fails due to a bug.

The Lading macro, like the Payload macro from Concept, contains no code, only the messages:

STOP ALL FRENCH NUCLEAR TESTING IN THE PACIFIC

*** WARNING ***

You're computer could be killed right now!

Thanks to you and me it's still ok!

Next time will be worse!

*** PHEEEW! ***

STOP ALL FRENCH NUCLEAR TESTING IN THE PACIFIC

Macro names: AutoOpen, BestandOpslaanAls, IkWordNietGoed1, IkWordNietGoed2, Lading

Polite

This virus is very simple. It replicates to normal.dot when an infected file is closed, and as it does so it displays a message box entitled “Activization” with the text “I am alive!”.

Documents are infected when they are saved with File/SaveAs, but only with the users’ permission. A message box pops up after the FileSaveAs dialogue box with the title “Propagation of the virus”, the text “Shall I infect the file ?” and two buttons labelled ‘Yes’ and ‘No’. Only if the user selects ‘Yes’ will the virus infect the document.

Macro names: FileClose, FileSaveAs

Safwan

This macro virus uses the AutoOpen macro to infect the Normal.DOT template. Once the master template (Normal.DOT) has been infected Safwan will use the FileOpen and System32 macros to infect further documents. Safwan uses stealth tactics by encrypting the code in the macros so that users can't open and edit them.

The only Warhead/Payload is that if you attempt to open an uninfected document on October 10th a message box will display the following message;

Happy Birthday

Is it you birthday today?

Macro names: AutoOpen, FileOpen, System32

ShareFun

When a document infected with ShareFun.A is opened, the virus will randomly call the ShareTheFun macro which saves the infected document to the root directory as “doc1.doc”. If the PC is running MS Mail under Windows, ShareFun.A will then select 3 recipients from the address book and mail them a message titled “You have GOT to read this“ with the infected document as an attachment.

Cybec has not received any confirmed reports of ShareFun.A, but the latest version of VET can detect and clean the virus.

Macro names: AutoExec, AutoOpen, FileExit, FileOpen, FileSave, FileClose, ToolsMacro. FileTemplates and ShareTheFun.

Showoff

This macro virus replicates when the AutoOpen or AutoClose macro is used to open or close a document. It has an active payload that will display the following message on the 11th and 13th of any month “Ra ono we, U can delete this mess later”. A dialog may also appear and display the following essage:

> Watch this!
>
> To one of us, Peace!
>
> Puff!
>
> Happy Birthday!

See also Showoff.G

Macro names: AutoCose, AutoOpen, Show, CFXX

Showoff.G

This is similar to the original but it also carries a file virus in the SHOW macro which will infect and begin replicating once it is released. This variant uses a modified AutoExec macro to replicate and has a destructive warhead that will delete system files on C: drive. The payload is only released on the 13th of any month.

See also Showoff.A

Macro names: Organizer, AutoExec

Smiley

This macro virus is thought to have been written in Germany and will only work ‘properly’ on German versions of Word. It replicates when the AutoOpen macro is run on file opening.

It has a stealth mode and many different payloads that do not work, as well as two payloads that do work. Under certain conditions the lines will be added to the Autoexec.bat which will format C: drive when you next reboot. Another working payload will add text to the end of files created with the German version of word.

Macro names: AutoOpen

Sofa.A (Excel macro virus)

Sofa is a microsoft excel macro virus, which works on excel5. It is an older virus, not seen in the wild until now. It has no destructive payload, but does make its presence felt in other ways.

It will change the caption of Excel to “MicroSofa Excel”. It consists of two worksheets, both hidden. One has the actual virus (name is 11 spaces) and the other has the source code stored in a standard excel worksheet (name 12 spaces). The virus dumps the source from the 12spaces sheet into a file called setup.gru and then copies it into any document it wishes to infect. It saves itself as book.xlt in the XLSTART directory, which is often at c:\msoffice\excel\xlstart. To remove the virus run Vet over all of the infected files and pay particular attention to ensure that the master template is cleaned.

When Sofa.A successfully infects an Excel file it will display the following deceptive message;

File successfully repaired!

Worksheet names: (12 spaces), Setup.gru, Book.xlt

Switcher

When Word is started it will check your computer's clock, if the seconds equal 00 (a one in sixty chance), the virus will attempt to delete a file from the following groups:

\msoffice\excel*.xls
\access*.mdb
\msoffice\access*.mdb
\windows*.grp
*.hlp

When an infected document is closed, it will also check the system clock and if the second's value is between 0 and 9 on your PC's clock (a one in six chance), Switcher.A will randomly select 2 numbers that appear in the document and switch them.

In addition, if a user selects either FileTemplates or ToolsMacro, a message will appear stating "Configuration conflict - menu item is not available."

Macro names: AutoExec, AutoOpen, FileOpen, FileSave, AutoClose, FileClose, FilePrint, FileSaveAs, ToolsMacro, FileTemplates

Terror.A

This macro virus has been found in several German versions of MS Word.

Inside the macro it has the word ‘Terror’ repeated over and over but there is no payload. It will not work on English versions of Word as it uses a German WordBasic command.

It contains only one macro: AutoOpen.

Macro names: AutoOpen

Wazzu

This virus replicates when a new document is opened, and Wazzu has a payload that modifies the file every time it is opened. There is a one in five chance that the virus will select a word in the document at random and move it to an equally random position in the file. There is also a one in four chance that the virus will insert the text “wazzu ” in the document at a random position.

See also Wazzu.BC
See also Wazzu.CH

Macro names: autoOpen (not AutoOpen)

Wazzu.BC

A variant of the Wazzu virus is of particular interest to Cybec as it is the first virus to specifically target VET in its payload. This is not a threat, rather a sign that VET is now considered by many (including the virus writers) as a one of the main anti-virus software products.

Wazzu.BC replicates as the original Wazzu.A virus does; as an infected file is opened, the virus copies itself to the global template (normal.dot). As a file is opened by an infected Word system, the virus copies itself to the fresh file. All of this is achieved by one macro, autoOpen.

Wazzu.BC is a particularly interesting virus to Cybec because of its payload. Every time an infected file is opened, the virus attempts to rename the c:\vet directory to c:_____.____, thus potentially disabling VET.

This action is fairly obvious though, since under Windows 3.1 the screen will go black temporarily, and under Windows 95 a window performing the rename is left open. The virus may also insert words such as ‘waffle’, ‘zoom’, ‘kill’ or ‘mum’ into the current document at random places, or simply swap random words around.

Macro names: autoOpen (not AutoOpen)

Wazzu.CH

Wazzu.ch is quiet dangerous. When an infected document is opened, the virus copies the macro to the original template (usually normal.dot). From then on, every document that is opened will have its contents removed before the user has a chance to see it. The way to save the contents from permanent deletion is to close the document and when asked “Do you wish to save the changes to this document” select No. The file will then keep the original contents.

Macro names: AutoOpen

Xenixos (also known as Xos and Nemesis)

This virus is German, and will not replicate fully with the English version of Word. It will infect normal.dot, but not spread any further form there.

Xenixos is very similar to both Friendly and LbyNJ. It infects normal.dot when an infected file is opened. Each of the macros are copied across, then Dummy is copied another three times, and renamed to AutoClose, AutoExit and AutoNew. All the 'Bak' macros are then copied from their respective original macros. A total of twenty four macros make up the virus when is resides in the global template.

The virus infects documents as they are saved with Datei/Speichern (File/Save) and Datei/SpeichernUnter (File/SaveAs). In both cases, if the current system time is more than forty five seconds after the minute as the document is saved, the file is protected with the password "xenixos". If it is presently May then the line "@echo j|format c: /u >nul" is appended to c:\autoexec.bat. If the document is saved using Datei/SpeichernUnter in March the virus attempts to drop an executable file virus using the debug.exe utility. Fortunately the macro has a bug and the file virus is never launched.

When a document is printed, if the time is presently less than thirty seconds after the minute, then the words "Nemesis Corp." are appended to the document beforehand.

If the user tries to use the Extras/Makro (Tools/Macro) from the menu a message box entitled "Fehler" pops up with the text "Diese Option ist derzeit leider nicht verfügbar.", effectively disabling the Extras/Macro dialogue box.

Macro names: AutoClose, AutoExec, AutoExecBak, AutoExit, AutoNew,AutoOpen, AutoOpenBak, DateiBeenden, DateiBeendenBak, DateiDrucken,DateiDruckenBak, DateiDruckenStandard, DateiDruckenStandardBak, DateiÖffen, DateiÖffnenBak, DateiSpeichern, DateiSpeichernBak, DateiSpeicherneUnter, DateiSpeichernUnterBak, Drop, DropBak, Dummy, ExtrasMakro, ExtrasMakroBak

Frequently Asked Questions

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

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

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

Installation Problems

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

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

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

4) Why do I have to update at all?

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

6) How do I make a reference disk?

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

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

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

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

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

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

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

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

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

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

Why do I have to update at all?

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

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

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

How do I make a reference disk?

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

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

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

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

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

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

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

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

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

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

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

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

To fix the clash with Mcafee Anti-Virus:

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

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

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

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

Viruses

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Vet deleted my infected files instead of repairing them.

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

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

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

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

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

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

If Top of Memory has gone up

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

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

If Top of Memory has decreased

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Resident Protection (Vet-Res) problems

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

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

For further information call Vet Technical Support

Error Messages

1) Repair was abandoned or Unable to perform repair?

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

3) VET.EXE appears to have been damaged.

4) System files appear to have been damaged.

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

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

7) VET.CFG is corrupted or missing!

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

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

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

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

Repair was abandoned or Unable to perform repair.

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

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

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

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

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

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

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

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

VET.EXE appears to have been damaged

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

System files appear to have been damaged

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

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

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

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

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

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

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

VET.CFG is corrupted or missing!

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

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

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

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

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

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

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

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

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

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

What are the return codes for DOS Vet?

Install Error Codes

1 User quit the Vet scan before it was finished

2 Reference disk may be invalid

4 Install abandoned by user

8 Vet reported errors (Error level 8 or up)

16 Vet reported a fatal error

32 Install failed

Scanning Error Codes

1 User quit the Vet scan before it was finished

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

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

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

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

32 Virus found in the hard disk boot sector

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

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

General

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

2) Am I protected while using the Internet?

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

4) What are exotic viruses?

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

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

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

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

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

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

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

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

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

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

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

Am I protected while using the Internet?

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

What is packed with <propriortorial compression algorithm>?

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

What are exotic viruses?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Glossary

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

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

CARO (Computer Antivirus Research Organisation)

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

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

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

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

OEM (Original Equipment Manufacturer)

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

OLE2 (Object Linked and Embebed language version 2)

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

VBA5 (Visual Basic for Applications version 5)

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

VxD (Virtual Device Driver)

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

Stealth

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

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

What is Vet_Res (Vet Resident Protection)

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

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

What is a TSR? (Terminate and Stay Resident)

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

File Viruses

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

File viruses can be further divided into the following groups:

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

Parasitic Viruses

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

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

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

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

Companion Viruses

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

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

Link Viruses

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

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

Macro Viruses

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

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

Multi-Partite Virus

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

Encrypting Virus

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

Polymorphic Virus

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

DAME or MTE (Dark Avenger Mutation Engine);

TPE (Trident Polymorphic Engine);

SMEG (Simulated Metaphoric Encryption Generator).

Trojan Horse

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

Worm

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

Warheads (Also known as Payload)

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

Heuristic Detection

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