1008 Virus

Alias: Suomi, Oulu
Type: Resident .COM infector
Length: 1008 bytes
Symptoms: COMMAND.COM increases in size, stack errors occur in operating system, computer stops during booting

The 1008 virus is encrypted and possibly originates from Finland. It becomes resident in the memory and infects COMMAND.COM immediately, so that every .COM program subsequently started is also infected. The enlargement of the infected files cannot be detected when the virus is active in the memory.

12-Ticks (Trojan horse)

This Trojan horse replaces the master boot record of a hard disk with one of its own. The program "rides piggyback" on the hard disk test supplied by Core and may be called CORETST, CORETnnn etc. The modification of the boot record is easily identified from the following text in the master boot record:

SOFTLoK+ V3.0 SOFTGUARD SYSTEMS INC
2840 St. Thomas Expwy,suite 201
Santa Clara,CA 95051 (408)970-9420

12-Tricks, so-called because of the number of tricks it performs, attempts in various ways to get at the original entry point in the hard disk BIOS in the ROM. When it finds this entry point, it can modify the master boot record without having to watch out for resident guard programs. From this modified master boot record, 12-Tricks copies approx. 200 bytes to a rarely used area of the interrupt table when the computer is restarted. The advantage of this is that it does not have to become resident via the operating system and it does not draw attention to itself by a reduction of the 640KB area.

12-Tricks installs one of twelve different routines when the system is restarted. These may include delays and gradual changes to the FAT.

1253

Type: Resident .COM infector
Length: 1253 bytes

This virus becomes resident in the conventional way and infects every loaded .COM file. The following code can be found in the fourth to the sixth byte of an infected file:

V-1

On 24th December of each year, the virus overwrites the entire data medium with a repetitive pattern of nine records. This may lead to uncontrolled floppy disk activities in non-accessed drives.

1260

Alias: V2P1
Type: COM infector
Length: 1260 bytes
Similarities: Wiener

Heavily encrypted virus which infects at an extremely fast rate.

405

Type: Overwriting, non-resident .COM destroyer
Length: 405 bytes

The 405 virus is easy to detect, as it simply overwrites the first 405 bytes of the files it infects. The infected programs are usually rendered unusable as a result and have to be replaced. Program files smaller than 405 bytes are increased to 405 bytes once infected.

4096

Alias: 100 Years, IDF, Stealth, Frodo, Century
Type: Resident .COM and .EXE infector
Length: 4096 bytes

A thoroughly nasty piece of work. This virus tries to become resident by eluding the operating system, and reserves space for itself at the upper end of the main memory. This reduction of the main memory space is not reported in the BIOS. Using the single-step procedure, the virus latches on to the lowest level of the operating system and thus even gets round any 'watchdog programs' which may be installed. The virus has various techniques for concealing its presence, including a highly arbitrary lengthening of the MCB chain. Any attempts to access the virus cause it to disappear again immediately in order to cover its tracks. It infects everything it can lay its hands on, making a bee-line for COMMAND.COM in particular. The 4096 also infects files both during loading and opening. The virus 'remembers' which files it has infected by adding 100 to the hundred digit of the year figure in the relevant directory entries. This sleight of hand enables it to return the original file length in the directory output. It also fools CRC programs, since although a file may be physically infected, the virus always returns the original file at the DOS level when the file is opened, thus neatly concealing any modifications from other programs. Once infected, a computer will simply stop working between 22.9. and 31.12. of the year in question. The following message should in fact appear on the screen when a boot record is infected:

FRODO LIVES

The 4096 manipulates the FAT of a hard disk, so that the file system is generally turned completely upside down (as will become clear when you use the CHKDSK command). The virus can also infect data files.

8 Tunes

Type: Resident .COM and .EXE infector
Length: 1971 bytes

This causes a medley of eight German folk songs to be played after approx. 30 minutes. In some versions, an interval of three months may elapse between infection and the playing of the first tune.

903

Length: 903 bytes
Type: Resident .COM infector

The 903 virus, so called because of its length, installs itself by conventional means in the lower DOS memory and infects all files in the current directory. The virus contains a code designed to destroy the first 6 records on the hard disk. If and when this code is executed is the subject of current investigation. If several memory-resident programs are installed, the system is likely to crash as the virus uses an area from 384 Kbytes upwards for its own purposes - an area which might be occupied by other programs.

The 903 uses an interrupt routine to check whether ALT-CTRL-DEL has been pressed, and remains active in the memory even after a warm restart.

AIDS Information Introductory Disk 2.0 (Trojan horse)

On Monday, 11 December 1990, several thousand disks were mailed to some 7,000 subscribers of the English magazine PC Business World in the UK, and to an unknown number of other participants of an Aids conference of October 1988. The program was supposed to provide information on the risk to the individual from Aids, but was unable to be used without an installation program. The installation program contained a Trojan horse.

During the installation routine, this installation program generates several new files and hidden directories on the hard disk whose names consist of a combination of the ASCII character 255, which is normally represented as a blank character, and the 'normal' blank character, ASCII code 32. Beginning with the main directory of the hard disk, the installation program creates five other directory levels with variations of these character combinations.

These subdirectories are used by the installation program to store various files which are necessary for the subsequent sequence of a counter loop. The AUTOEXEC.BAT file is modified in the main directory in such a way that the 'normal' AUTOEXEC.BAT is called under the name AUTO.BAT once AUTOEXEC.BAT file has been processed. This new AUTOXEC.BAT contains an inconspicuous line with the following (shortened) text:

```
REM  PLEASE USE THE auto.bat FILE INSTEAD OF autoexec.bat
```

The two blank characters after the REM are not normally noticeable. However, the first blank is the ASCII character 255, and the operating system does not interpret these four characters as a normal REM in batch files, but as a program call. What has in fact happened is that the installation program has installed a file called REM .EXE in one of these subdirectories, which is now called and begins to increment a counter in another subdirectory.

The damage routine begins after approx. 90 restarts, whereupon the hard disk is encrypted. During this time, a message appears on the screen asking the user not to switch off the computer. Afterwards, the user is requested to renew his software licence. The hard disk contains only one 'visible' file: CYBORG.DOC.

The encrypting process is effected by changing the filename extensions. The extensions of all filenames are compared with an internal table. If a particular filename extension appears in the table, that extension is replaced by the second table entry available for this entry in the first table. The letters of the filename itself are encrypted character by character. Then all directories are marked READ-ONLY and HIDDEN, which means that they no longer appear under "dir". The directory names themselves, both system files in the main directory and COMMAND.COM file are not encrypted.

Akuku

Alias: Hybrid
Type: Resident .COM infector
Length: 1306 bytes
Similarities: Vienna

Every Friday 13th from 1992 onwards, this virus copies a Trojan horse to the boot record of the current drive, sets the number of drives to 1 and the storage capacity to 256 KB whenever an infected program is called. The following message then appears:

Wirus v. 1.0 (c) Hybrid Soft Specjalne podziekowania dla Andrzeja Kadlofa i Marriuze Deca za artykuly w Komtuterze 11/88.

This is followed by partial formatting of the relevant drive.

Alabama

Type: Resident .EXE infector
Length: 1560 bytes

This virus eludes the operating system in order to become resident about 30 KB below the upper DOS limit, but does not reduce the maximum size of DOS, which can lead to unexpected problems. It also latches onto the keyboard interrupt and 'monitors' the keyboard with various IN and OUT commands while waiting for the reset combination <Ctrl-Alt-Del>. If the system is reset by <Ctrl-Alt-Del>, the virus still remains in the memory by booting the computer itself.

Once the virus has been active in the system for about an hour, the following message appears in a flashing window:

> SOFTWARE COPIES PROHIBITED BY INTERNATIONAL LAW.....
> Box 1055 Tuscambia ALABAMA USA.

The special feature of this virus is its infection routine, however. It does not infect the currently active program unless it happens to be the last uninfected program in this directory. Instead of infecting a file, it simply swaps its FAT entries now and then with those of the program you are about to run without renaming it. In this way, you may start the HDFORMAT format unintentionally by entering XCOPY. As a rule, however, this exchanging of FAT entries only takes place every Friday.

Amilia

Type: Memory-resident file virus
Length: 1164 bytes
Similarities: Murphy

Infects all COM and EXE files which are executed or opened, provided they are larger than 1614 bytes. COM files have to be smaller than 64000 bytes. If an infected EXE program is called on a Sunday, the following text appears:

```
Amilia I Virii - [Nuke]
Released Dec91 Montreal
(C) Nuke Development Software Inc
```

after which the program is terminated.

Amoeba

Alias: Khetapunk, 1392, Maltese
Type: Memory-resident .COM and .EXE infector
Length: 1392 bytes

This virus only infects files with a minimum length of 512 bytes and a maximum length of 60 KB. It does not have any damaging functions but merely simulates errors which can lead to side effects. The virus contains the following encrypted text:

> SMA KHETAPUNK - NOUVEL Band A.M.O.E.B.A by Primesoft Inc"

Angelina (boot record virus)

Alias: Stoned-Angelina
Similarities: Parity

The Angelina virus is a resident boot record infector (BRI) which is able to hide on the infected medium (in other words a stealth virus). Like all pure BRIs, it enters the system when you boot from contaminated data media. During the infection process, the virus copies the clean original boot record to a rarely used area of the main directory of the relevant medium and redirects all read accesses from the boot record to this copy. It installs itself in the upper part of the conventional memory area and reduces the storage available for DOS by 1 KB.

Angelina has a brief installation routine for anchoring itself in the memory. This routine begins by decrementing the storage capacity by the required number of kilobytes, and then uses this value to calculate the segment into which it copies itself. Afterwards, the text "Greetings for ANGELINA !!!/by Garfield/Zielona Gora" is decrypted in the data area of the virus, and the interrupt vector 13h is saved and redirected to the Int 13h handler of the virus. Angelina (or to be more exact, the infected Int 13h) is now installed, and the bootstrap loader (interrupt 19h) can be rerun.

The Int 13h handler only intercepts attempts to read the boot record: all other records can be read or written normally. The boot record is read into the memory designated by the application, and the Angelina virus checks whether this record has already been infected. If so, Angelina reads the copy of the clean boot record into the buffer of the application and then returns to the latter. If the boot record is not infected, Angelina calculates the position in which to write the record it has just read. This position is calculated from the disk parameters and thus depends on the storage capacity of the medium. The virus then attempts to write the clean boot record in this position. The write error occurring here is hidden on write-protected disks, and the application proceeds unaware of the activities of the virus. Once the boot record has been successfully saved, the areas of the disk parameter table and partition record are copied to the virus segment and written in the boot record together with the Angelina code. Finally, the initially saved processor registers are reset to their original values, and Int 13h only returns the saved, clean record to the application which called the boot record. The Angelina virus is described as a variant of the Stoned virus, although it bears a much closer resemblance to the Parity virus.

Anthrax

Length: 1048 bytes
Type: Resident .EXE and .COM infector

Anthrax infects hard disks by copying its code at the end of the start partition of the first hard disk. If data were stored here, they are subsequently destroyed. When an infected program is started, the virus enters the master boot record, but does not remain resident in the memory at this point. It does not become resident in the memory until you boot from the hard disk, whereupon it infects every program which is started without checking whether or not it is already infected. As a result, COMMAND.COM grows with every call until it is ultimately too big for the operating system to load and execute, so that the system can no longer be booted. Interestingly enough, another virus (V2100) checks the upper end of the hard disk for the Anthrax code and copies it back into the master boot record. If you wish to carry out manual repairs, e.g. using the Norton Utilities - this area must be overwritten following the restoration of the boot record.

AntiExe (boot record virus)

Alias: D3, NewBug

The AntiEXE virus, also known as NewBug or D3, only affects boot records. It reduces the available main storage in the 640 KB area and searches for certain anti-virus programs.

This virus is a resident stealth boot record virus. If a computer system is booted from an infected disk, the virus will infect the system. During the infection of a hard disk, it copies the clean master boot record to an unused area (head 0, cylinder 0, sector 13) and redirects all further attempts to read the master boot record to this copy.

If a disk is infected, a copy of the clean boot record is stored in the last record of the root directory, thus overwriting any existing entries. Data losses are therefore inevitable, though relatively rare.

The installation routine of the AntiEXE virus detects the entry address of interrupt 13h. Then the virus reduces the available lower main memory area (0-640 KB) by one kilobyte and corrects the reported conventional main memory accordingly. The virus then copies itself into the memory thus "allocated". The detected address of interrupt vector 13h is transferred to interrupt vector D3h. Both interrupt vectors still "point" to the same program code at this stage; later on, the virus only uses interrupt D3h to deactivate resident virus guards and blockers instead of interrupt 13h.

If the system is booted from an infected disk, the virus becomes resident and checks whether the master boot record of the first hard disk has already been infected. If not, the original master boot record is copied elsewhere "for future use". Then the current master boot record is modified and the original boot record of the disk is reloaded for the next booting procedure.

When the virus is active, the boot record is not infected every time a clean disk is accessed. Equipped with the usual stealth properties, the virus always returns the original record whenever the boot record is accessed in the case of floppy disks, or the master boot record in the case of hard disks, i.e. the virus simply redirects the access attempts.

When an attempt is made to access a particular record, and bits 0 and 1 of the tick counter (increment register for counting the number of ticks since midnight) are set, the virus checks whether the read record corresponds to the start record of a particular EXE program and then modifies this record so that it can no longer be executed.

April

Alias: Suriv
Type: Resident .COM and .EXE infector
Length: Approx. 900 bytes or more

The April virus operates in two different ways. On the first of April, the relatively harmless part is activated and sends the system into a loop from which it cannot escape, while deleting files at the same time. The second part is rather more spectacular. Once the virus has become resident, it infects each new program, including both '.COM' and '.EXE' files, and, after 53 minutes, the infected computer system stops working altogether. The following message then appears on the screen:

> 'APRIL 1ST HA HA HA - YOU HAVE A VIRUS'.

Some variations also display a shorter text whenever a file is infected:

> 'YOU HAVE A VIRUS'

This virus differs from standard viruses in terms of its method of infecting .EXE files. It wedges itself between the last relocation entry in the relocation table and the code. This displaces the code of the program itself, which means that all relocation entries in the relocation table have to be recalculated.

Azusa (boot record virus)

The Azusa virus attempts to lodge itself in the master boot record of the hard disk and in the boot record of floppy disks. Every time the floppy disk is accessed, it checks to make sure the inserted disk is not already infected. In other words, the disk can be infected simply by entering DIR A: when the virus is active.

Barrotes

Type: Resident .EXE and .COM infector
Length: 1310 bytes
Symptoms: Destroys the master boot record on 4 January!

This virus, which appears to originate from Spain, infects programs and program modules (overlays in separate files) when the user attempts to run them. It also immediately infects the COMMAND.COM file in the main directory of drive C:. It does not infect programs whose overlays are located within the EXE file of the main program. The virus checks whether it is already resident in the memory via the command INT 21h/AH=Eeh. If so, the code AH=FEh is returned. On 5 January, the virus overwrites the master boot record of the first hard disk in the system with parts of the interrupt table, then bars appear on the (colour) screen in constantly changing colours and the following text is displayed:

Virus¯BARROTES¯pos¯OSoften

The virus contains the texts: "c:\command.com" and, at the end of infected files, "I7SO".

Basic

Type: Non-resident .COM and .EXE infector
Length: 5120, 5128, 5135 bytes

The first form of the Basic Virus started spreading after 6 July 1989. This virus was probably written in Turbo Basic using assembler components. As a rule, it infects one file in the current subdirectory with every call, then it attempts to infect another file on drive C:. The error messages of the operating system are not intercepted by the virus. There is a risk of destroying data files or data/programs due to the cross-linking of files.

In the version existent since 1 April 1992, loaded programs are aborted and the following message appears on the screen:

```
Access denied
```

The loaded program file still exists nevertheless. The Basic-I virus can be identified by the following text strings in the virus code:

```
"BASRUN"
"BRUN"
"IBMBIO.COM"
"IBMDOS.COM"
"COMMAND.COM"
"Access denied"
```

The Basic-II Virus has new destruction routines which render hard disks unusable and destroy the contents of CMOS. The Basic-II virus can be identified by the following text strings:

```
"BRUN"
"BASRUN"
"COBRUN"
"NET$OS"
"LOGIN"
"USERLIB"
"AV"
...
"IBMBIO.COM"
"IBMDOS.COM"
"COMMAND.COM"
"Access denied"
```

These strings are located close to the end of the file. Please note that the virus now also searches specifically for 'AV' (the name under which the AntiVir program was formerly supplied). As you can see, it is a good idea to rename the AntiVir program. In another variation, the string "AV" was changed to "AVS", the name of a earlier utility.

Basic-III contains the following sequences:

```
"KEYB*.COM"
"KEYB*.EXE"
"BASRUN"
"BRUN"
"COBRUN"
"NET$OS"
```

"LOGIN"
"USERLIB"
"AV"
...
"IBMBIO.COM"
"IBMDOS.COM"
"COMMAND.COM"
"Access denied"

Bestwish

Type: Resident .COM infector
Length: 970 bytes

Infects Windows and OS/2 files as well as .EXE files, but merely enlarges them by 970 bytes without actually being able to activate the virus when a program is loaded. The AntiVir repair program can only detect these enlargements in GURU mode.

Black Jack

Alias: Cascade, 1701, 1704, Falling Letters, Falling Leaves, Autumn Leaves
Type: Resident .COM infector (also .EXE version)
Length: Usually 1701 bytes or 1704 bytes

Black Jack (a reference to the card game '17 and 04', which is also the length of the virus), is a so-called time bomb which is not activated until a certain trigger date (before this, the virus merely spreads from one file to another). It is impossible to give a more precise trigger date for Black Jack than 'the autumn of the year in question', as a large number of variants and derivatives now exists which may have their own trigger dates. Once activated, Black Jack disrupts the screen display, causing letters to 'fall' from the screen (hence the alias 'Autumn Virus' or 'Falling Letters/Falling Leaves'). These effects do not occur for a long time, however, so that the virus goes unsuspected by the user, who puts the faults down to a system error. Another peculiarity of Black Jack is the fact that there is one version which does not infect any original IBM systems (whereby computers with an IBM ROM-BIOS are also spared), while a new version also infects .EXE files. Infected files are enlarged by 1704 bytes (give or take a few bytes for the different variants). The virus itself is internally encrypted and begins by decrypting itself during the runtime. Like the Israel virus, it monitors the loading of programs and has the names of files to be infected delivered 'free'. Via sub-function 0FFh of INT 21h, the virus is able to check whether or not it is already present and active in the system.

Brain Boot (boot record virus)

Alias: Pakistani
Similarities: Ashar

One version of this virus attacks floppy disks only, while another also infects hard disks. The virus occupies between 3KB and 7KB of storage space depending on its size. Infected data media usually bear the volume label '(c) Brain'. Infected floppy disks have about 3KB of bad records, i.e. 6 x 512 bytes. One version is designed to destroy the FATs (FAT - File Allocation Tables) from 5 May 1992 onwards. The virus usually announces itself as follows:

> Welcome to the Dungeon
> (c) 1986 Brain & Amjads (pvt) Ltd
> VIRUS_SHOE RECORD V9.0
> Dedicated to the dynamic memories
> of millions of virus who are no longer with us
> today - Thanks GOODNES!!

The virus also slows down the disk access and generates so-called timeouts, which renders some disk drives unusable. It monitors INT 13h, via which all disk operations are performed. This makes it very difficult for anti-virus programs to read the original boot record, as the virus appears to return the original record. In this way, a floppy disk read for the first time on a contaminated hard disk is also infected incidentally.

Breasts (boot record virus)

Breasts is a very simple boot record virus which is not encrypted and does not have any camouflage properties. It occupies 16384 bytes of memory and "hijacks" the interrupt vector 13h for its own routine.

Breasts stores the original boot record of HD floppy disks on track 79. If this already contains data, these are overwritten (risk of data loss!). 2-D disks (e.g. 360K or 720K) only have 40 tracks and, since the virus does not check the disk format, the original boot record of these disks is lost. It is impossible to boot from an infected 2D disk, as the virus reboots itself constantly in an infinite loop.

The master boot record of hard disks is "filed" in a (normally) unused area and can thus be restored by AntiVir. The variant known to us has neither a damage routine nor an on-screen text display.

Burger Virus

Alias: 909090, CIA
Type: Overwriting, non-resident '.COM' infector (also '.EXE' version)
Length: 560, 736, 1280 bytes

The code of this virus is usually 909090h at the beginning of a file. When an infected file is loaded, the virus attempts to infect another .COM file. One version simply renames all '.EXE' files to '.COM' once it runs out of .COM files and the whole thing starts all over again. The first 560 bytes are then overwritten as a rule, however.

After classifying this virus as a Burger Virus in our programs, we received a written warning from the solicitors of the person named in the copyright (who, incidentally, partially contributed to his books). Our reply to this warning has gone unanswered for six months, however. Unfortunately, the computers of today do not yet have a sufficient grasp of the law to know that this virus isn't a virus at all, i.e. a virus which is not allowed to be called one. Despite the solicitors' claim that this is not a virus, this 'unvirus' still destroys files (thereby incidentally committing an offence under the penal code). The only logical conclusion the solicitors can draw, therefore, is that the computer commits a criminal offence by doing something with this program which, according to the solicitors, it is not allowed to do.

CMOS-One (boot record virus)

Alias: Often mistakenly identified as ExeBug (A)

This virus occupies 1024 bytes of memory and hijacks the interrupt 13h for its own purposes. It uses camouflage tactics in order to avoid detection.

Its damage routine deletes the CMOS entry in the first floppy disk drive, so that drive A: is no longer recognised as installed. When data are written on the floppy or hard disk, the virus checks whether the first record begins with the letter 'M'. If this and a further test prove positive, the virus copies one of two possible routines to the beginning of the record, thus overwriting its original contents. The EXE files modified in this way usually begin with the letters 'MZ'!

Once an EXE file has been thus manipulated, it is treated as a COM file by DOS, as the signature at the beginning of the file is no longer 'MZ'. If the affected file is larger than 65280 bytes, it can no longer be booted. If the file is smaller, however, the damage routine entered by the virus is executed.

One of the routines is comparatively harmless, as an error it contains causes the program to be terminated immediately. However, the second possible routine overwrites large parts of the first hard disk, beginning with cylinder 0. If this happens, the hard disk has to be reformatted, and unsaved data are lost!

CSFR 1000

Length: 1000 bytes
Type: Resident .COM infector

This virus infects all .COM files which are executed or copied. It installs itself in the upper memory area used by DOS, where the storage space occupied by the virus is flagged as unused. This means that the virus will be overwritten by larger programs or programs requiring the entire available memory. One of these programs is AntiVir, which will cause the system to crash immediately as soon as it is loaded.

Cascade

Alias: Black Jack, 1701, 1704, Falling Letters, Falling Leaves, Autumn Leaves
Type: Resident .COM infector (also .EXE version)
Length: Usually 1701 bytes or 1704 bytes

Cascade or Black Jack (a reference to the card game '17 and 4', which is also the length of the virus), is a so-called time bomb which is not activated until a certain trigger date (before this, the virus is merely spread from one file to another). It is impossible to give a more precise trigger date for Black Jack than 'the autumn of the year in question', as a large number of variants and derivatives now exists which may have their own trigger dates. Once activated, Black Jack disrupts the screen display, causing letters to 'fall' from the screen (hence the alias 'Autumn Virus' or 'Falling Letters/Falling Leaves'). These effects do not occur for a long time, however, so that the virus goes unsuspected by the user, who puts the faults down to a system error.

Another peculiarity of Black Jack is the fact that there is one version which does not infect any original IBM systems (whereby computers with an IBM ROM-BIOS are also spared), while a new version also infects .EXE files. Infected files are enlarged by 1704 bytes (give or take a few bytes for the different variants).

The virus itself is internally encrypted and begins by decoding itself during the run time. Like the Israel virus, it monitors the loading of programs and has the names of files to be infected delivered 'free'. Via sub-function 0FFh of the INT 21h, the virus is able to check whether or not it is already present and active in the system.

Casper

Type: Non memory-resident .COM infector
Length: 1200 bytes

This virus contains the following text in encrypted form:

> "Hi! I'm Casper the Virus; And On April The 1'st
> I'm Gonna Fuck Up Your Hard REAL BAD!
> In Fact It Might Just Be Impossible To Recover!
> How's That Grab Ya! <Grin>".

If an infected program is called on 1st April, the virus will format track 0 of the disk in drive A:.

Christmas

Alias: Syslock
Type: Non-resident .COM and .EXE infector.
Length: 2764 bytes
Similarities: Cookie, Macho

This virus, like its above named relatives, can be controlled by an environment variable called 'VIRUS'. If 'VIRUS=OFF' is set in the environment, the virus will not be activated. During the Advent period of the year in question, candles and the words 'Merry Christmas' are displayed on the screen to the tune of "O Christmas Tree". Only files in the current subdirectory are infected. The encrypting of the virus is variable.

Contens

Please do not regard the following as hard and fast rules, as any old programmer can always modify damage routines or on-screen displays. All viruses are subject to constant change and are then unleashed on the unsuspecting public as 'new' viruses by dubious characters.

Friday
FSP Killer
Fu Manchu

Ghost

Hafenstraße
Hallöchen
HONECKER Trojan (Trojan horse)

Icelandic
Israel
Itavir

Jack Ripper (boot record virus)
Jerusalem
Joshi (boot record virus)
Junkie

Kennedy
Keypress
Kiev (boot record virus)

Lehigh
Liberty
Lisbon

Macho
Michelangelo (boot record virus)
MIX
Mummy
Murphy
Music Bug (boot record virus)
MVF

Natas
Neuroquila
Neuroquila.N8FALL.A
Neuroquila.N8FALL.B
Neuroquila.N8FALL.Companion
No Bock

Ohio (boot record virus)
Omega
One Half
Oropax

Parity (boot record virus)
Perfume
Ping Pong (boot record virus)
Plastique

RedX

Sampo (boot record virus)
SillyWilly

Stimulation
Solano
Stoned (boot record virus)
Sunday Virus
Sylvia

Tai Pan
Taiwan
Tenbytes
Tequila
Traceback
Tremor
Tumen
Typo COM

V163
Vacsina
VGen
Victor
Vienna
Vriest

Whale
Wiener
WinWord.Concept
WitCode

Yankee Doodle

Zero Bug

Cookie

Alias: Syslock
Type: Non-resident .COM and .EXE infector
Length: 2232 bytes
Similarities: Christmas, Macho

This virus has existed since 1988 and is activated on 1st April of each year. The following message then appears on the screen:

'I want a COOKIE !'

This message is present in encrypted form in the virus. After this, the low-level hard disk is usually formatted. If the word 'COOKIE' is then typed in, the virus will 'burp':

'BURPS'

This virus can be controlled by an environment variable called 'VIRUS'. If 'VIRUS=OFF' is set in the environment, the virus will not be activated. This message is present in encrypted form in the virus. After this, the low-level hard disk is usually formatted. One variant remains completely inactive after 1st April, i.e. it no longer attempts to infect files, etc.

Crazy Eddie

Type: Resident .COM and .EXE infector
Length: 2727 bytes

Crashes on many computer systems, as it depends largely on the version of the operating system. Crazy Eddie infects COM and EXE files when executed, but also on entry of the DIR command. It overwrites the hard disk every Monday 28th, as well as on 28 June.

Datacrime

Alias: Columbus Day
Type: Non-resident .COM infector (also .EXE in some variants)
Length: 1168, 1514, 2280 bytes

This virus usually attaches itself to the end of a file. As a rule, it infects all .COM files whose seventh letter is not a 'D'. Once the virus is activated, the following message appears on the screen between the 12th October 31st December of each year:

> DATACRIME VIRUS
> RELEASED: 1 MARCH 1989

When Datacrime II infects an .EXE file, it overwrites the SS and SP values stored in the EXE header. If the infected file was smaller than 60 KB, no runtime problems should occur, while larger files may crash uncontrollably. AntiVir renames files which have been damaged in this way. (Or are you one of those intrepid types who rename the files back to *.EXE to see what happens next ... ?!?)

Devils Dance

Type: .COM Infector
Length: 941 bytes

This virus overwrites the first FAT after approximately 5000 keystrokes. After a warm restart by the <Ctrl-Alt-Del> method, the following message appears on the screen:

DID YOU EVER DANCE WITH THE DEVIL IN THE WEAK MOONLIGHT?
PRAY FOR YOUR DISKS!!
The Joker

Diamond

Alias: V1024
Type: Memory-resident .COM and .EXE infector
Length: 1024 bytes

This virus displays a diamond composed of four smaller diamonds on colour screens every hour on the hour. Shortly afterwards, the four small diamonds begin to move about and delete any character they collide with. Only files with a minimum length of 1024 bytes are infected by this virus, which also sets the seconds figure of the file generation time to 60 seconds.

Disk Killer (boot record virus)

Alias: Ogre

Disk Killer infects the boot record and loads itself into a allocated space of 3KB to 8KB below the upper limit of the main memory. Like the others of its species, it patches the boot record so that its routine is executed first. This routine is stored in three clusters on the data medium. During an infection, the virus attempts to flag the three occupied clusters in the FAT as 'bad records'. In some variants, this attempt fails, so that the problem of overwritten data is compounded by incorrect flagging of 'bad' records. Depending on the version of the virus, the hard disk is either formatted after about 48 hours or the data records of a hard disk are alternately encrypted with the values 0AAAAh and 05555h (for techies: geXORt). Before it does this, however, the virus issues another message:

> Disk Killer -- Version 1.00 by COMPUTER OGRE 04/01/89

This virus can generally be identified in the boot record by the code 03CCBh at offset 03Eh.

Eddie

Alias: Dark Avenger
Type: Resident .COM and .EXE infector
Length: 1800 (+16) bytes

Dark Avenger, alias Eddie, is a highly infectious virus which can be spread simply by reading a file: even a simple XCOPY or COPY command will do, both in the case of the original and target files. In the boot record, the virus carries a downward counter which is initialised to 16. After every 16th boot procedure, the virus overwrites a randomly selected record with the boot record of the relevant data medium.

Overwritten programs should always be deleted and renewed, as the original contents of the overwritten record cannot usually be recovered. The virus generally also infects files during closing. This means that even newly generated/complied programs will contain the virus on a contaminated computer. Earlier versions of this virus infected .COM files several times over, while more recent versions set the countdown to begin at 64. The virus overwrites the transient part of every COMMAND.COM file it infects. To create more space for application programs, the DOS developers divided the COMMAND.COM file into two parts - a resident part and a transient part. The resident part is always present and contains the error routines and the reloading element for the transient part. The area of the transient part may be used by applications for their own purposes. Dark Avenger also betrays itself in that COMMAND.COM has to be reloaded more frequently than usual. At the beginning of the virus, the following message may be found: 'Eddie lives ... somewhere in time' At the end of an infected file, you will usually find the following:
'This Program was written in the City of Sofia (C)1988-1989 Dark Avenger'

FSP Killer

Type: Resident .COM and .EXE infector
Length: 789 bytes

This virus appears to work specifically within the code segment of the last INT 21h vector to have been loaded. This virus is currently undergoing analysis, and, according to initial results, the virus seems to occupy 66.288 bytes in the resident state. The virus uses INT 21h, sub-function 0A1D5h to check whether or not it is already resident in the system, and expects the returned hex value 900Dh in the AX register. If the virus is resident, it will modify the attributes of two files by setting the hidden attribute of these files.

Faust

Alias: Spyer
Type: Resident .COM and .EXE infector
Length: 1181 bytes

Occupies approx. 1.7 KB of the main memory. Faust, alias Spyder, infects every new program which is loaded and subsequently causes the computer system to crash.

Fiche

Alias: FEXE
Type: Memory-resident .EXE infector
Length: 897 bytes

Infects files during opening and closing. One version of this virus overwrites the first six records of the first hard disk with the text:

"FEXE 1.0 vous a eu".

Fish

Type: Resident .COM and .EXE infector
Length: 3584 bytes
Similarities: Whale

Occupies between 4 KB and 8 KB in the main memory and infects all files as soon as they are opened. Entering CHKDSK /F while the virus is active leads to a loss of clusters.

Flash

Type: Resident COM and EXE infector
Length: 688 bytes

Flash becomes resident in the uppermost memory area and flags this area as unavailable in order to avoid being overwritten itself. When a program is run, the virus attaches itself to this file. Once a system is infected, the virus is activated after the year 1990. Every few minutes the screen flickers due to the manipulation of the video card register.

Flip

Alias: Omicron
Similarities: Tequila

Overwrites the load routine of the master boot record (partition record) with its own load routine. The actual master boot record is saved elsewhere on the hard disk.

Following further manipulations, the capacity of the 1st logical hard disk is reduced by 6 records (3 KB). In the memory, Flip lodges itself at the upper limit of DOS and infects programs and overlay files. Once a file is infected, the figure 62 appears in the seconds display of its generation time. If the first file to be loaded after booting is COMMAND.COM, this is modified so that the correct file size appears to be displayed in response to 'DIR'. As well as during the infection process, Flip is also activated between 1600 and 1700 h. In the case of EGA and VGA video adapters, the screen is temporarily mirrored in the horizontal direction (hence the name Flip).

Form (boot record virus)

This virus is a memory-resident boot record infector which occupies two kilobytes of main memory. It infects the boot records of both hard disks and floppy disks, where it occupies two records. In the case of floppy disks, the original boot record is displaced and stored in an area flagged as "bad". Interrupt vector 13h at offset 0346h and 09h at offset 035dh are modified.

The following text can be found in the boot record, but is not displayed on the screen:

The FORM-Virus sends greetings to everyone who's
reading this text. FORM doesn't destroy data!
Don't panic! Fuckings go to Corinne.

As a rule, "clicks" can be heard through the loudspeaker on the 18th of each month, which are generated by a keyboard handler installed on that day only. This can delay the acceptance of keyboard inputs. Apart from the programming errors, the virus does not have any obviously damaging function - all it does is overwrite the last two records, which can lead to "entanglements" of the unformat program during unformat operations.

Unlike "normal" boot record viruses, the Form virus does not infect the master boot record of hard disks, but the boot record. Once again, this virus can only enter the system by booting from an infected data medium, including an infected data disk.

If you boot from an infected disk, the virus reduces the available lower main memory area (0-640 KB) by two kilobytes and corrects the reported conventional main memory accordingly. The virus then copies itself into the memory area thus "occupied". This is only half the battle, however, as the currently loaded record only consists of 512 bytes, and the virus itself is bigger than this. The rest is therefore "post-loaded", then the entry addresses (segment address and offset address) are placed on the stack in this "occupied" memory area and the whole thing is started by Ret Far. The virus is now executed in this upper "occupied" memory area and is protected against overwriting by correcting the conventional main memory size.

Next, the clean, copied boot record is read from the contaminated data medium in its original position in the main memory during a start routine. Then the virus determines the partition parameters of a hard disk: this is done by reading the master boot record of drive 80h and scanning the partition table for the first partition flagged as active. The virus stores the physical position of the boot record of this partition and reads in the boot record. If it is not infected, it is written in the last record of the hard disk, thereby overwriting any existing data. The second record of the virus code is stored in the penultimate record, once again overwriting any existing data.

In the first record of the resident virus, the areas relevant to the BPB (BIOS Parameter Block) within the virus are adapted to the values of the boot record to be infected. This record is then written as a new boot record in the previously stored physical position of the original boot record. Once the hard disk has been infected and the interrupt vector 13h hijacked, the current date is checked to see if it is "18". If the date is correct, the keyboard interrupt is also hijacked. The original boot record of the floppy or hard disk is already in the right place in the main memory and transfers this program code to the virus for it to execute the rest of the boot procedure.

The virus's own interrupt 13h handler now concentrates solely on infecting floppy disks. It is only activated by attempts to read track 0 if it detects a clean boot record on reading in a boot record. If the disk is not infected, the virus calculates the start of the data area of the disk to be infected. In this area, it searches for the first unused cluster and flags two records in the FAT as defective. In the first record it writes the clean, original boot record, and in the second record the second part of its own code. Once the disk-related parts of the virus itself have been adapted, the boot record of the disk is infected.

Friday

Alias: South African, Miami, Munich
Type: Non-resident .COM infector
Length: 416, 540 bytes

As a rule, this virus infects all files not yet infected in the active directory, although some of its variants also infect '.COM' files present in the path of the system. Some variants only infect two additional files, however. On Friday 13th, one variant deletes every program called, while another variant displays the following message on the screen:

> We hope, we haven't inconvenienced you

Fu Manchu

Type: Resident .COM and .EXE infector
Length: 2080 bytes
Similarities: Israel

The virus uses the sub-function 0E1h of INT 21h to find out whether or not it is already resident in the system. If not, it attaches itself to the beginning of .COM files or the end of .EXE files. The checksum in the '.EXE header' of an infected file contains the hex value 1988H (similar to the Israel virus, from which Fu Manchu is derived). Towards the end of the actual virus part, the following text is usually found:

sAXrEMHOr
COMMAND.COM

The virus infects all executable programs and eludes the operating system in order to become resident by manipulating the MCBs directly. Depending on the version, the following message appears after a warm restart or after the 16th successful infection:

The world will hear from me again!!

The virus also monitors all keyboard inputs and responds to the names of certain politicians (Waldheim, Thatcher) with rather coarse comments.

Ghost

Alias: Ghost Ball, Ghostballs
Type: Non-resident .COM infector
Length: 2351 bytes

Infected files show the figure '62' in the seconds area of the directory entry and, in most cases, every 8th infected file is overwritten. The virus attempts to install a ping- pong like boot record virus which is, however, unable to reproduce. Once a boot record has been infected, a 'bouncing' ball appears on the screen. The following plain text can be found in the virus:

GhostBalls, Product of Iceland
CopyRight 1989, 4418 and 5F19

HONECKER Trojan (Trojan horse)

The Honecker Trojan, also known as DOSINFO Trojan, is not actually a real virus, but a Trojan horse. The Honecker Trojan spreads by modifying batch files in such a way as to ensure that it is called as often as possible. On certain dates, HONECKER then plays the national anthem of the GDR and some fancy graphics appear on the screen. Apart from that, however, HONECKER is not particularly harmful.

1.5. - Labour Day
17.6 - Uprising of 17 June
13.8. - Building of the wall
3.10. - German Unification Day
7.10. - Republic Day (National holiday of the GDR)
9.11. - Opening of borders
25.12 - Not really a socialist holiday!

Every time it is called, the host program DOSINFO.EXE copies itself into several directories which also contain batch files. These batch files in turn contain the DOSINFO call as their first call in order to guarantee that the program is actually started.

Once all DOSINFO.EXE files are deleted and all calls to these files removed from the batch files, the "virus" is also removed.

Hafenstraße

Type: Non memory-resident EXE infector
Length: 809 bytes

Every time an infected program is called, this virus creates an invisible file in the current directory which contains the word:

Hafenstraße

Hallöchen

Alias: Halloechen, Hello
Type: Resident .COM and .EXE infector
Length: 2011 bytes

This virus becomes resident through direct manipulation of the MCB chains in the computer system without making use of the operating system with its INT 21h. The operating system uses the MCBs (Memory Control Blocks) to manage individual memory areas from the pool, whose normal size is 640KB. When an infected file is called, this slows down the computer system. This virus only affects files in which the month and year in the file date differ from the current system date. The virus can be identified within a file from the following two character strings:

```
Hallöchen, here I'm
Acrivate Level I
```

Icelandic

Alias: Disk Eating, One In Ten, Disk Crunching, Saratoga 2
Type: Resident .EXE infector
Length: 542, 656 bytes
Similarities: MIX

The last four bytes of an infected file contain the hex combination

```
44 18 5F 19
```

from which the virus can be identified. The virus installs itself below the upper DOS limit and reduces the reported available storage space by 2KB. It infects every tenth program that is loaded, unless the INT 13h is being used by another program. As a rule, the virus flags vacant records as bad once it has infected a file, thus leading to a continual reduction of the available hard disk or floppy disk capacity.

Israel

Alias: Jerusalem, PLO, Friday 13th .
Type: Resident .COM and .EXE infector
Length: 1803, 1808, 1813 bytes

This is currently one of the most widespread viruses. It increases infected files by 1803 or 1813 bytes (although other figures are possible in the case of certain variants). It remains relatively inactive until every Friday 13th, when it either deletes files or formats the hard disk depending on the variant in question. The virus does not infect COMMAND.COM as a rule, but slows down the computer system about 30 minutes after infecting it.

The virus intercepts INT 21h, sub-function 04Bh, via which the operating system starts new programs, and so ensures that the filenames to be infected are delivered to it 'free'. '.COM' files are only infected once, while '.EXE' files are infected several times. It is these program errors which first betray the virus, as it often suddenly becomes impossible to load perfectly normal programs. This error has been eliminated in more recent versions.

The virus latches onto the system's internal clock via the timer interrupt. Many variants of the Israel virus create a 'black hole' on the left-hand side of the screen about half an hour after infecting the computer system. Partly for reasons for self-detection, Israel viruses define a new function in addition to INT 21h (usually function 0E0H), which the virus uses to check whether it is already resident. Nevertheless, AntiVir has to admit defeat in the case of some Israel infections, as it is sometimes no longer possible to repair an infected program due to a program error in the virus. Such errors cause the virus to change in the case of certain original program sizes from 'add' to 'overwrite' mode, often partially destroying itself in the process. This means that AntiVir may still be able to remove the virus, but can no longer restore overwritten areas for obvious reasons. The infected program can therefore no longer be run even before any repairs are attempted. In this case, AntiVir issues a corresponding message and offers to delete the infected immediately in order to prevent the virus from spreading any further (or the infected file from crashing uncontrollably!).
If the user is reluctant to delete this file or eliminate it in any other way, he may have to leave the virus in his computer system. Much worse, however, is the fact that this virus may no longer be complete due to its own errors, which means that it can write itself arbitrarily into other areas when the program is called. It is therefore better to delete the program after all and then reinstall it from the original disks.

The Israel virus can be easily identified, partly because many versions contain the string 'MsDos' and because it also sets the checksum in EXE files to the value 1984h.

Itavir

Type: Resident .EXE infector
Length: 3880 bytes

Infects Windows and OS/2 files as well as .EXE files, and overwrites the boot record after 24 hours of activity in the system.
Sometimes, however, this virus only enlarges files without being able to activate the virus when a program is loaded. The repair function of AntiVir can only detect such enlargements in /GURU mode.

Jack Ripper (boot record virus)

Alias: Jack The Ripper

Jack Ripper is a simple boot record virus, comparable with the Parity boot record virus. Depending on how it is encrypted, the virus is sometimes also identified in the memory as the Parity virus. Attempts to access the boot or master boot records directly when the virus is in operation expose the original, uncontaminated records.

The virus occupies 2048 bytes of memory and "hijacks" the interrupt vector 13h for its own routine. The available main memory is then reported to contain 2048 bytes less than before. In the case of a computer system equipped with 640KB of lower main memory, CHKDSK will therefore only show 653312 bytes of memory instead of 655360. What's more, it often proves impossible to start Windows in the 32-bit mode.

Jack Ripper saves the original boot record of floppy disks in the last record of the root directory. If this contains directory entries, these are overwritten, which may lead to data losses. The master boot record of hard disks is "stored" in a (normally) unused area and can therefore be restored by AntiVir.

Jack Ripper infects the master boot record of a hard disk if an infected floppy disk (including a data disk) is used to boot the system. After booting from an infected hard disk, non write-protected floppy disks are infected by read access alone - simply entering the "DIR" command is enough!

The name of the virus comes from encrypted text fragments in the body of the virus, and the message FUCK EM UP! points to the damage routine of the virus, which modifies the written data slowly and imperceptibly. From a possible range of 1 to 1024 write accesses to a data medium, the virus simply exchanges two consecutive double bytes in the record to be written. This leads to an insidious, gradual modification of data on the relevant data medium. For this reason, the entire stock of data should be checked for consistency whenever this virus occurs.

Jerusalem

Alias: Israel, PLO, Friday 13th
Type: Resident .COM and .EXE infector
Length: 1803, 1808, 1813 bytes
Similarities: Anarkia, Mendoza, Frere Jacques

Very well known virus which enlarges infected files by 1803 or 1813 bytes (though other figures are possible in other variants). It remains relatively inactive until every Friday 13th, when it either deletes files or formats the hard disk depending on the variant in question. The virus does not infect COMMAND.COM as a rule, but slows down the computer system about 30 minutes after infecting it.

The virus intercepts INT 21h, sub-function 04Bh, via which the operating system starts new programs, and so ensures that the filenames to be infected are delivered to it 'free'. '.COM' files are only infected once, while '.EXE' files are infected several times. It is these program errors which first betray the virus, as it often suddenly becomes impossible to load perfectly normal programs. This error has been eliminated in more recent versions.

The virus latches onto the system's internal clock via the timer interrupt. Many variants of the Israel virus create a 'black hole' on the left-hand side of the screen about half an hour after infecting the computer system. Partly for reasons for self-detection, Israel viruses define a new function in addition to INT 21h (usually function 0E0H), which the virus uses to check whether it is already resident.

The Israel virus can be easily identified by the user himself, partly because many versions contain the string 'MsDos' and because it also sets the checksum in EXE files to the value 1984h.

The user can easily detect the Jerusalem virus himself because it contains the string 'MsDos' in many versions and also sets the checksum in EXE files to the value 1984h.

Joshi (boot record virus)

This virus becomes resident when the system is booted and takes up about eight records on the hard disk in addition to the boot record on floppy disks and the master boot record on the hard disk. Joshi is a 'stealth' boot record virus which destroys data on 720 KB floppy disks. On 5th January of each year, the virus is activated and displays the following message on the screen:

Type "Happy Birthday Joshi!"

After entering the birthday greeting, the computer continues the boot routine. Like other boot record viruses, the Joshi virus can only infect a hard disk if the system is booted from a contaminated disk. From an infected hard disk, the virus simply formats itself a new track at the end of the disk (if it intends to infect a floppy), in which to store the original boot record and its own program code. The new boot record created by the virus in place of the old one contains all the messages, so that a virus goes unsuspected on superficial analysis. On a 360 KB disk, the virus is located on track 40 (counting from 0 to 39) in the first five records, and on a 1.2 MB disk it is located on track 80 (counting from 0 to 79), again in the first five records. In the case of 720 KB disks, data on track 41 are destroyed and the disk is rendered unusable.

When an infected computer system is booted, the virus checks whether it is already resident in the system, as it is able to survive a warm restart. If not, it reduces the available main memory by 6 KB, and loads itself into this memory. After checking to make sure the interrupt vectors it uses are also located in this area, the virus loads the original boot record in the memory location which this original boot record would have adopted during a normal boot procedure, and this record then assumes control.

Junkie

Type: Resident .COM infector
Length: 3880 bytes

The JUNKIE virus was spread at the end of May 1994 via various European mailboxes, in most cases through the file HV-PSPTC.ZIP. According to the description, the program is supposed to allow illegal copies of games to be installed on the hard disk, but the package only contained the program PSPATCH.COM, which was the JUNKIE virus.

JUNKIE originates from Sweden and is a multipartite virus, i.e. it infects both master boot records and COM files. When an infected program is started for the first time on an uncontaminated computer, the virus overwrites the master boot record of the hard disk (otherwise it does nothing). The next time the virus is called, JUNKIE becomes resident in the memory and infects all COM programs started from there.

Infected COM files are enlarged by 1035 bytes. Since the virus can only infect COM files, it destroys all programs which have a COM extension but are not real COM files (e.g. some EXE programs). The virus is doubly encrypted and contains the following text (also encrypted):

> Dr White - Sweden 1994
> Junkie Virus - Written in Malmo...M01D

The JUNKIE can also be identified from the fact that the available main memory is reduced, causing programs to generate error messages such as "Program too big to fit in memory".

Kennedy

Type: Non memory-resident COM infector
Length: 333 bytes

This virus modifies the FATs, resulting in lost clusters and cross-linked files. The virus contains the following text:

\command.com
The Dead Kennedys

Keypress

Type: Resident .COM and .EXE infector
Length: 1232, 1472 bytes

Approximately half an hour after infecting a computer system, this virus usually quadruples the length of keyboard inputs. .COM files are only infected if they are larger than 1232 bytes.

Kiev (boot record virus)

This virus occupies 1024 bytes of memory and hijacks interrupt 13h for its own routine. It does not have a camouflage function. If the system is booted from an infected floppy disk, the virus checks whether any installed hard disks are already infected and infects them accordingly if not.

The interrupt 13h routine is activated the first time a floppy disk drive is accessed, then no further action is taken. The virus checks and infects the inserted disk by saving the original boot record in another record and writing its code in the boot record.

If the system is booted from an infected hard disk, the virus decrements a counter in the master boot record. When this counter reaches the value 0, it encrypts part of the hard disk (the first 17 records of cylinders 0 to 4 and of all write/read heads). The counter is not initialised by the virus and usually has the value 0, so that this damage routine is triggered after the 256th boot routine. The virus requires an 80286 processor or higher.

Lehigh

Type: Overwriting, resident COMMAND.COM infector
Length: 1280 bytes

The Lehigh virus only infects the COMMAND.COM file, which it does by locating and latching on to the stack area of this file. This enables it to avoid enlarging the file. One variant of this virus attaches itself to an infected COMMAND.COM, however. In both versions, the following code is found at the end of the file:

```
A9 65
```

After four or ten infections, the virus generally destroys the boot record and the FAT. At the end of the virus, the name COMMAND.COM may appear:

```
command.com
```

Liberty

Type: Memory-resident COM and EXE infector
Length: 2858 bytes

The Liberty virus does not have any harmful functions, but merely contains the text:

-MYSTIK -COPYRIGHT (c) 1989 - 2000, by SsAsMsUsEsL

It does not affect files which are smaller than 1280 bytes.

Lisbon

Type: Non memory-resident COM infector
Length: 648 bytes
Similarities: Vienna

This virus contains the word "@AIDS" which appears in the last five bytes of an infected file. It does not affect files which are smaller than 10 bytes or bigger than 64 000 bytes. The virus overwrites the first five bytes of some files with the word "@AIDS" and so destroys them.

MIX

Type: Resident .EXE infector
Length: 632, 1618, 1636 bytes
Similarities: Icelandic

Infected files can be identified by the following string at the end of the file:

MIX1

If the value 77h is found at location 0:33Ch in the system storage, the virus is probably resident. In this case, all outputs to devices connected via serial or parallel ports are distorted, and the NUM lamp in more modern keyboards lights up continuously. The computer crashes when the system is booted after the 6th infection, and a 'ball' appears on the screen.

MVF

Alias: Mad Virus Factory
Type: Resident .COM infector
Length: 1903 bytes

The encrypted virus infects programs during execution. It also attacks the COMMAND.COM file, after which the computer system often crashes. More recent versions of the MVF virus also infect files as they are opened.

Macho

Alias: Syslock
Type: Non-resident .COM and .EXE infector
Length: 3551 bytes
Similarities: Cookie, Christmas

This encrypted virus is controlled via the computer system environment, and attempts to infect all executable programs. It is unable to do this, however, if 'SYSLOCK=@' is entered in the computer environment. Otherwise it will infect all program files. As a joke, it sometimes replaces all incidences of the word 'Microsoft' with 'Machosoft', while one particular variation creates a file called IBMIONET.SYS.

Michelangelo (boot record virus)

The Michelangelo virus lodges itself in the boot record of a floppy disk or the master boot record of a hard disk, where it substitutes its own code for the original (start) program code. In this way, the virus is able to take control before the operating system the next time you boot the computer, and is thus loaded into the main memory.

When a computer system is booted from a disk, the boot record of the disk is normally read first in order to load the operating system stored on the disk. If the disk is infected, however, the Michelangelo virus will be loaded instead of the usual boot program, and will anchor itself in the main memory.

The virus then allows the computer system to continue the boot routine, but monitors every attempt to access the floppy and hard disk. If the computer system is infected, Michelangelo will check every newly inserted disk and infect it if this has not already been done.

As long as you do not boot from an infected disk, the files can be easily transferred to a non-infected data medium via the command COPY or XCOPY. The infected disk should then be formatted to be on the safe side (using the parameter /U from DOS 5.0 onwards, as otherwise UNFORMAT information will contain the infected boot record). From DOS 5.0 onwards, the master boot record of an infected hard disk can be overwritten again with a clean copy via FDISK /MBR (undocumented parameter) without modifying the variable partition data itself. For users of earlier DOS versions, the only option (unless a low-level format is used) is to copy back the original master boot record from cylinder 0, head 0, sector 7 to cylinder 0, head 0, sector 1 with the aid of the Norton Utilities.

In order to infect a floppy disk, the Michelangelo virus copies the original boot record from the first record of the disk to the last sector of the root directory. As a result, files may be lost or, if new files are added, the disk rendered completely unusable. On hard disks, data losses may occur within DOS versions before 3.0 due to the storage of the master boot record. In this case, it is usually no longer possible to set up a RAM disk either.

The Michelangelo virus carries out its damage routine on 6 March of each year. It copies the contents of the memory from the address 5000:0000h via heads 0 to 4, cylinders Ø to 255 and sectors 1 to 8 of a hard disk. This usually renders the first 9 MB of the hard disk unusable and also does irreparable damage to the most important components, the FAT and root directory. The hard disk is then no longer bootable and has to be built up again from scratch including partitioning.

The Michelangelo virus reduces the available main memory by 2048 bytes. This means that CHKDSK will report only 653,312 free bytes instead of 655,360 on a computer system equipped with 640KB. This reduction of the memory may also be caused by variants of the Stoned virus, however, as well as by BIOS shadowing or a PS/2 bus mouse.

Infected disks may have an incomplete boot record, in which case not all messages will be fully legible. On hard disks, the master boot records will also have incomplete messages as well as less free space.

Mummy

Alias: Platinum
Type: Memory-resident .EXE infector
Length: 1399-1414 bytes
Similarities: Jerusalem

This virus installs itself as a TSR program and flags the memory used as belonging to DOS. EXE files are infected on execution and opening, i.e. a file can be infected simply by copying it. One version of the virus has an infection counter which is decremented with each successful infection. When the counter reaches zero, the virus overwrites the first 100 records on the hard disk.

Murphy

Type: Memory-resident COM and EXE infector
Length: 1614 bytes

This virus infects the above files on opening, provided they are more than 1614 bytes long. COM files which are bigger than 64,000 bytes are resistant to this virus. All infected files contain the following message:

Amilia I Virii (NuKE),99i; By Rock Steady/NuKE

In an EXE file is called on a Sunday, the following text appears:

Amilia I Virii-(NuKE) Released dec.91 Montreal (c) NuKE Development Softwarw Inc.

after which the program is aborted. A peculiarity of this virus is its habit of checking INT 13H constantly in order to avoid detection by virus guards.

Music Bug (boot record virus)

The Music Bug infects the boot records of both floppy and hard disks. If you boot from an infected disk, the virus plays a random series of notes through the loudspeaker. If HD disks are formatted on an infected AT, the virus changes the disk format to 360 KB, so that 1.2 MB disks are no longer recognised.

Natas

Alias: Satan
Type: Resident, stealth-type, polymorphic, multipartite
Length: 4744 bytes, memory 6144 bytes, 9 records HD/FD

Natas is a complex virus which infects the partition record of hard disks and the boot records of floppy disks as well as .COM and .EXE programs. It shows stealth characteristics in all areas and cannot be located anywhere except in the memory while the virus is active. The virus is polymorphic and, moreover, destructive. Natas takes the form of a little devil (Tip: try reading the name backwards...).

If an infected program is started, the virus decrypts itself and checks whether it is already resident. For this purpose, it uses the self-defined interrupt function INT 21h/30h, BX=F99Ah and expects the result AX/BX = 0. Before the virus becomes active, the last MCB is shorted by 5664 bytes and the upper limit of the DOS memory reduced by 6K. Natas then copies itself into this area and traces the original interrupt vectors 13h, 15h, 21h and 40h.

The tracer uses a special trick to find out whether the trace flag of the CPU has been set: it pretends that the trace flag is not set in order to circumvent virus blockers. Natas then occupies the interrupt vectors and infects the partition record of the hard disk.

During the installation routine, the virus checks at various points whether TBCLEAN or a debugger is active. In this case, it deactivates TBCLEAN or the debugger and formats all available hard disks. This method of detecting TBCLEAN only works with older versions which still use the single-step mode of the CPU, however.

The virus is now active, and since the transient part of COMMAND.COM has been overwritten, the command interpreter is infected directly by Natas during subsequent loading.

The infected partition and boot record only contains a small loader, which reduces the memory by 6K and subsequently loads the remaining part of the virus. These 9 records are located at the end of cylinder 0, head 0 on hard disks and within the last track of floppy disks. The virus only infects boot records whose first command is a SHORT or NEAR JMP. It then copies itself to the location pointed to by this jump command.

Natas behaves purely as a stealth virus in the record and file area. Attempts to read the partition or boot record are redirected to the stored originals. When an infected program is read, the length, date and contents of the original file are simulated. Virus scanners or checksum programs area which have not already detected the virus in the memory, will be unable to find Natas while the virus is active. Before an infected file can be modified, it is wiped completely clean, and CHKDSK does not generate any error messages like most file stealth viruses.

The virus deactivates its file stealth properties immediately if it detects that the active program is called ARJ, LHA or PKZIP. It also checks whether the name of the active program contains the word BACK or MODEM. This property is selected randomly on activation of the virus, however, and is not always evident.

The virus infects programs when they are started or closed, and resets NIT 13h and INT 40h to their original values in order to elude resident virus programs. This method leads to data losses if a cache with a write delay function, e.g. SmartDrv, is active. If the program to be infected is located on a disk, the virus checks whether the disk is write-protected by accessing the record directly. At the same time, INT 24h is deactivated in order to suppress error messages. Natas also checks the EXE signatures "MZ"/"ZM" and even infects programs which do not have the file extension ".EXE". EXE programs with internal overlays are not infected. The virus adds 100 years to the date of an infected file, though this normally remains invisible. During the infection process, the virus uses the System File Table to change the file access mode, for instance.

Natas uses a polymorphic engine which is capable of generating a large number of possible decoding routines. Scanning via scan strings is not possible, as the virus can identify itself via the file date. Besides the word "Natas", the words "BACK" and "MODEM" are also stored in the code in encrypted form.

The author of this virus (with the pseudonym "Priest") is also responsible for the "SatanBug" virus.

Natas-4988

The source code of Natas was published in the virus magazine 40Hex, which led to the appearance of a number of variants of this virus. The variant originating from Belgium is almost identical to the original, but with a few slight modifications, i.e. the length of the virus has been changed to 4988 bytes and the text in the virus to:

> Time has come to pay (c)1994 NEVER-1

Neuroquila

Alias: <HAVOC>, Neuro.Havoc, Wedding
Length: EXE programs: 4644-4675 bytes, hard disks & floppies: 9 records
Type: Resident retrovirus, stealth-type, polymorphic, multipartite

Neuroquila infects the partition of hard disks, boot records of 1.2 and 1.44MB floppy disks and .EXE programs. It can be activated by all three types of infection. If you boot from a contaminated partition or disk, the virus copies itself into the available memory after 7C00:0. Interrupts 13h and 21h are assigned in the normal way and the virus is thus activated. Jump instructions are inserted in the memory after 0:4E0 and 0:4F0, to which the interrupt vectors 21h and 13h are redirected by Neuroquila. The virus attempts to infect the hard disk partition at this point and subsequently loads the original partition or boot record, which is encoded and then booted.

The virus waits until interrupt 21h is occupied by DOS and then activates a further INT 21h routine which intercepts the boot routine of MSDOS.SYS. If DOS or XMS-UMA is available at this point, the virus will occupy its memory space, otherwise it extends the STACKS area. In both cases, the virus occupies 5344 bytes of memory. Once the virus code has been copied to the new storage area and both "hooks" at 0:4e0h and 0:4f0h have been corrected, the virus attempts to calculate the entry point to the DOS kernel of the HMA, where a jump to the virus code is inserted into the INT 21h entry (splicing). Interrupt lists and system information programs do not indicate any change in Int 21h. The final INT 21h routine checks the following DOS functions: 4Bh, 4Ch, 11h, 12h, 4Eh, 4Fh, 3Fh, 3Eh, 3Dh, 32h, 44h, 25h, 40h. During the booting process, the CONFIG.SYS file is checked and the following programs skipped: "VIRSTOP.EXE" (F-PROT) and DOSDATA.SYS (QEMM). A program called "QC*" is also deactivated, which is the H+BEDV anti-virus program "QCDRV".

If an infected program is loaded, the virus installs itself, if not already active (self-test: INT 13h, function F2h: Carryflag), in the available memory space after 7C00:0, possibly overwriting any memory-resident programs already active there. Interrupts 13h and 21h are run in single-step mode (tracer) and the original entry addresses in the DOS kernel or BIOS are determined. As in the boot procedure, the DOS kernel is patched, the INT 13h and INT 21h routines of the virus activated, the partition infected and finally the actual program loaded. During the tracing procedure, already active anti-virus programs are patched so that they are no longer able to stop the virus. Neuroquila uses the same method for checking function 25h of the Int 21h. Resident anti-virus programs attempting to install themselves area instantly deactivated by the virus in the memory. Neuroquila modifies "TBDRIVER", "TBDISK" (TBAV), "VSAFE/TSAFE" (CPAV, MSAV and TNT) and "-D". (KAMI) If the anti-virus program "NEMESIS" (1.10) is active, the computer stops functioning, or an exception is triggered.

Since the virus is active in the available memory space, the computer will crash whenever you try to load programs of any size. However, since the partition is infected immediately, the virus can activate itself normally the next time the system is restarted and the computer will not crash again.

The partition and boot record of the hard disk are encrypted and the partition after cylinder 0, head 0 and sector 7 copied. The infected partition sector only contains a small loader, which subsequently loads the rest of the virus from cylinder 0, head 0 and sector 8. The partition data are deleted and the actual virus code written in records 8 to 16. If you try to access the hard disk from a clean start disk, you will only obtain the error message "INVALID DRIVE C:".

Any attempt to remove the virus with "FDISK /MBR" from a boot record will lead to data losses, and will be ineffective if the virus is active. Neuroquila only infects partitions of the DOS-12BIT, DOS-16BIT and BIGDOS type. If the partition is immunised with "TBUTIL" (TBAV), this partition will always be modified before it is started so that the virus goes unnoticed. In the 32-bit access mode, Windows does not generate an error message as is normally the case with partition or boot record viruses.

Disks which are not write-protected are infected when you access the boot record, e.g. as soon as you enter "DIR A:". The virus formats 10 boots from track 81 onwards, into which it copies the original boot

record and its own program code. The contaminated boot record now once again only contains the small virus loader.

Once the virus is active, it checks the entire operating system. Read and write access to the contaminated partition, the encrypted boot record of the hard disk and boot records of floppy disks are detected and redirected to the stored originals, which are decrypted again by the virus in the memory. Attempts to read or write infected programs are also detected and filtered. Contaminated programs have the same file length and contents as before the infection. "CHKDSK" does not report file allocation errors as with other file stealth viruses. The virus uses its stealth functions to elude all scanners and checksum programs and can only be found outside the memory if the virus is deactivated in the memory. The virus does not use the file date (+100 years) or the file time (seconds over 59) as an infection flag. Although the virus extends files by a variable value, the correct, original file length is displayed when you enter DIR. If a directory contains a number of infected programs, the DIR display will be perceptibly slower unless a disk cache is active.

Neuroquila circumvents the self-test of "TBSCAN" and deactivates its antistealth mode when the file is accessed. The virus manipulates attempts to access the checksum files "SMARTCHK" or "CHKLIST" of CPAV or MSAV.

The virus infects EXE programs during loading. Programs are extended by 4644 to 4675 bytes, although the change is no longer visible when the virus is active. The file date and time remain unchanged, and write-protection attributes are circumvented. The virus does not generate any write-protect error messages in the event of an attempt to infect programs on write-protected disks. Programs are only infected if they are larger than 10000 bytes, do not contain any internal overlays (e.g. Windows programs) and have a file date which does not coincide with the current month and year. During the infection process, the virus occupies memory space after BE00:0 (text memory). The virus checks whether the display is in text mode and does not infect any programs when graphics are displayed (e.g. within Windows). If you try to debug or modify contaminated programs, these will be wiped clean by Neuroquila beforehand.

In infected programs, the virus is polymorphically encrypted. The Neuroquila engine takes up about 1300 bytes of the virus's length and generates a huge number of ciphers, whereby the selection of encryption methods and filler bytes is dependent to a large extent on the date and time. The deciphering routines (decryptors) are approx. 64 bytes long and use encryption techniques such as XOR, ADD, ADC, SUB, SBB, NEG, NOT, ROL and ROR. The Neuroquila engine is clearly not one of the well known engines such as MtE, TPE or SMEG. The virus code in the partition and in the boot records is not encrypted and can be found with scan strings provided the virus is not already active in the memory.

When the partition is infected, the current system date is stored in the virus. After three months, delay loops are activated which slow down the system increasingly with each access attempt, and when a certain value is reached, the following text is displayed:

<HAVOC> by Neurobasher'93/Germany

-GRIPPED-BY-FEAR-UNTIL-DEATH-US-DO-PART-

The program just interrupted can be continued by pressing any key. The active virus slows down the loading of programs, the DIR display and the accessing of floppy disks.

Neuroquila contains 80286 Opcodes, contains anti-heuristic structures and has certain similarities with the "Tremor" and "AlphaStrike" viruses, which also originate from the same author according to the internal text.

Neuroquila.N8FALL.A

Alias: Neuroquila, Art & Strategy, Nightfall
Length: EXE programs: 4554-4585 bytes, memory: 4688 bytes
Type: Resident retrovirus, stealth-type, polymorphic

N8FALL is clearly based on Neuroquila, although it does not have the ability to infected hard and floppy disks. The polymorphic engine resembles that of Neuroquila except for a few minor modifications. Instead, N8FALL also spreads when you close programs (fast infector) and infects COM programs in addition to EXE programs.

If an infected program is loaded, the virus first decrypts itself in the memory and checks memory location 0:4e0h in order to ascertain whether it is already active. If not, the virus proceeds to occupy DOS or XMS UMA, or, if this is not possible, memory below the 640K limit. 4688 bytes are occupied and flagged as a SYSTEM area. Like Neuroquila, this virus does not use the single-step mode (tracer) to detect the original INT 21h entry, but searches for the typical entry directly within the HMA and patches it so as to ensure that the virus is called. The address of INT 2Fh is ascertained by the same method, although the interrupt itself is not assigned. If the search for the DOS kernel was successful, the virus will infect the command interpreter, which is usually COMMAND.COM, via the "COMSPEC=" entry.

In the case of COM programs, the virus restores the first three bytes of the program, and in EXE programs the original MCB length (without the virus) before skipping to the actual program (MCB stealth)

Like <Neuroquila>, the virus checks a series of INT 21h functions: 4Bh, 4Ch, 11h, 12h, 4Eh, 4Fh, 42h, 3Fh, 3Eh, 3Dh, 32h, 44h, 25h, 40h, 48h, 4Ah, 45h and 46h, by means of which the virus can assume complete control of the file access procedure. Programs are infected during loading or closing, whereby intensive use is made of the SYSTEM FILE TABLE, e.g. in order to change the write access mode of the opened program. The virus only infects programs which either have the file extension "COM" or the program identifier "MZ" or "ZM". If an infected COM program containing an active virus is renamed, the copy will be clean. Similarly, the virus can only spread to programs containing at least 4000 bytes and, in the case of COM, no more than 60000 bytes. Also immune to infection are programs which have the current system date (month and year) as their file date or which are called "NE*.*" / "IB*.*", as are programs with internal overlays such as Windows programs, for example. During the infection procedure, the virus uses the text memory as a buffer. If the computer is in graphic mode (e.g. within Windows), none of the programs will be infected. N8FALL extends programs by 4554-4585 bytes, whereby the virus attaches itself in the usual way to the end of the file.

When the virus is active, it is impossible to detect any extensions or modifications to files. The virus is a stealth virus through and through, but, unlike many other stealth viruses, it does not use the file date for identification purposes, but the file length. CHKDSK does not report any errors, and DIR is slowed down unless a hard disk cache is available. Apart from in the memory, N8FALL can only be found in programs provided the virus is not active in the memory.

If a program is called via DEBUG, N8FALL wipes the file completely clean first. Once the damage routine is activated, the virus displays the following text after exiting the program:

```
Invisible and silent - circling overland :

        \\\ N 8 F A L L ///

   Rearranged by Neurobasher - Germany

-MY-WILL-TO-DESTROY-IS-YOUR-CHANCE-FOR-IMPROVEMENTS-!
```

Then the computer beeps until you press a key. The virus is activated 3 months after infecting COMMAND.COM. The virus then prints out the screen at random intervals and modifies INT 33h (mouse

support).

During installation and normal operation, the virus checks whether any anti-virus TSRs are installed. If NEMESIS (1.10) is resident, the virus will not be activated, while TBDRIVER and VSAFE/TSAFE are patched in the memory and rendered ineffective. If TBSCAN is loaded, the virus switches the scanner to compatibility mode and thus manages to escape detection.

If programs with the names "ME*.*", "MI*.*", "MF*.*", "CH*.*", "CO*.*", "SI*.*" or "SY*.*" (e.g. MEM, SYSINFO, CHKDSK) are loaded, the virus appears to release the memory it has occupied, and these programs then display the original amount of free storage space.

The virus is polymorphically encrypted, so that no scan strings can be entered. The engine resembles that of Neuroquila, but with slight modifications. N8FALL is encrypted at two levels, whereby only the outer level is polymorphic. The engine generates a variety of possible encryption methods, whereby the random generator makes intensive use of the system's time and date functions. The virus evidently stems from the same author as Tremor and Neuroquila.

Neuroquila.N8FALL.B

Alias: Neuroquila, Art & Strategy, Nightfall
Length: EXE programs: 5801-5832 bytes, memory: 6048 bytes
Type: Resident retrovirus, stealth-type, polymorphic

This virus is considerably larger than the original variant, but does not contain any major modifications to the actual virus code. The virus length is 5801 to 5832 bytes in infected programs, and takes up 6048 bytes of memory. Like N8FALL.A, the virus occupies the memory through direct MCB manipulation or allocates DOS or UMA memory.

The jump instruction to the actual virus code has been shifted in this case from 0:4E0h to 0:5E0h, but the method of activating the virus in the DOS kernel is the same.

The second level of the encryption process now contains anti-debugger tricks, but has not undergone any other modifications. The polymorphic encryption itself is also identical to that of N8FALL.A.

A new feature is the fact that the virus now only infects programs which are at least 5000 bytes long, and that it contains the text "C:\NCDTREE\NAVINOC.DAT" and another entirely independent virus, the "N8FALL.Companion". The path entry for the checksum file of Norton Antivirus is present in encrypted from, but - strangely enough - is not otherwise used. The interval before the trigger function has also been increased from three to six months and the encrypted text contained in the virus has been modified as follows:

'Any means necessary for survival'

* N8FALL/2XS *

'By the perception of illusion we experience reality'

Art & Strategy by Neurobasher 1994 - Germany

'I don't think that the real violence has even started yet'

This information leads us to conclude that this variant was programmed after the Neuroquila virus, from which large parts of the program code have been copied.

N8FALL.B does not generate any 'Print Screens' and does not manipulated interrupt 33h (mouse), but after six months of activity the second virus contained in the code, "N8FALL.Companion" is activated. If a contaminated program is loaded with a debugger, the virus will wipe the program clean before it is accessed and display the above text after terminating the debugger.

Neuroquila.N8FALL.Companion

Alias: Neuroquila-Companion
Length: COM programs: 527 bytes, memory: 672 bytes
Type: Resident companion virus, semi-stealth type, fast infector

This virus is activated by Neuroquila.N8FALL.B six months after the infection of COMMAND.COM.

N8FALL.Companion is memory-resident and occupies 672 bytes of conventional DOS memory by shortening the last MCB and flagging it as a system area. The virus uses the memory address 0:5D2h for self-identification, at which the number 5832h can be found when the virus is active.

INT 21h is assigned in the usual way by direct manipulation of the interrupt table. Antivirus guard programs would normally block this virus during installation, but since N8FALL.B is already active and has deactivated many of the known protection programs itself, N8FALL.Companion is usually able to activate itself without hindrance.

The virus infects programs when the DOS functions 'Start Programs' and 'Create File' are called, but only spreads to floppy disks during the generation of new programs. N8FALL.Companion checks whether the loaded or generated program contains EXE structures and then creates COM programs with the same name, in which the file attributes are set to READ-ONLY, HIDDEN and SYSTEM and the file date to 1-1-94, 11:55:00. These newly generated files contain the virus in non-encrypted form and are always 527 bytes long. In the case of programs with the filename "F-", the virus does not generate a file in order to avoid detection by F-PROT. When the virus is active, it hides the generated double files in directory displays by means of stealth routines, but does not generate any error messages when you enter CHKDSK. Apart from its nasty habit of infecting programs, this virus does not have any other harmful functions. The following text appears in the 527-byte files:

```
-A-VICTORY-THAT-WON`T-LAST-
```

No Bock

Type: Non-resident .COM infector
Length: 440 bytes

This virus contains this encrypted message:

No Bock today Error, System halted!

Incidentally, mankind has a firm in Göttingen to thank for this virus (we are unaware of the name of the programmer and the firm concerned). The firm claims to have created it in order to protect one of its programs against 'modifications of the copyright'. The program in question is now available without the 'free gift'.

Ohio (boot record virus)

Alias: Den Zuk, Venzuelan
Similarities: Brain Boot

Judging by the code, the author of this virus has stolen some components from the Brain virus and used them as a construction kit for his own virus, which is evidently the classical way of writing a new virus. Like the Brain virus, this virus is roughly 3KB to 7KB long and is 'brain-aware', which means that, if it comes across a Brain virus in the boot record, it will fetch the boot record already stored by the Brain virus and save it for itself. A floppy disk infected with Ohio or Denzuk can no longer be attacked by the Brain virus.

The virus can be identified by the following text string in the virus code:

Y.C.1.E.R.P

The dots in the first message are the characters with the hex code 0F9h. The virus writes itself into the boot record after saving the original boot record on track 40 and head 0 of a floppy disk. If necessary, the disk is formatted in a non-standard format at this point. In some variants of this virus, the letters DEN ZUK appear on the screen every time the computer is booted. Sometimes the disk in drive 'A:' is simply formatted in response to an internal counter.

Omega

Type: .COM infector
Length: 440 bytes

On Friday 13th, the Greek letter omega appears and the hard disk is destroyed.

One Half

Alias: FreeLove, Slovak Bomber
Type: Resident, stealth-type, polymorphic, multipartite
Length: 3544, 3577 bytes, memory 4096 bytes, 8 records HD/FD

One Half infects the partition of the hard disk as well as programs of the type .COM and .EXE. If an infected program is loaded, the virus decrypts itself in the memory and uses the self-defined INT 21h function AX=4B53h (result: AX=454Bh) to check whether it has already been activated in the memory. If not, the virus runs INT 13h in single-step mode in order to elude any active anti-virus programs with the original address. During the tracing procedure, the partition record of the hard disk is read and checked to see if it has already been infected (offset 25h=00d3h, offset 180h=072eh). If the partition is not yet infected, the virus determines the maximum number of records and cylinders on the hard disk and searches for its active partition, whereby only partitions of the type DOS 12 Bit, DOS 16 BIT and DOS 32 BIT are infected. A key is determined and written into the partition record together with the data of the hard disk. The rest of the virus (7 records) is located within the first cylinder of the hard disk. The virus now restores those parts of the loaded file which have been overwritten by its decrypting routine and the jump instruction to the virus code. If the infected program is of the EXE type and relocation entries were overwritten during the infection process, the virus subsequently loads the original entries and corrects the program in the memory. The virus does not become resident until it is loaded by a contaminated partition.

If you boot from an infected hard disk, the virus reduces the upper memory limit by 4K, assigns interrupts 13h and 1Ch and subsequently loads the remaining 7 records. One Half deciphers a further record each time the computer is booted and works its way from the end of the hard disk to half way through the available cylinders. When it reaches this record, One Half displays the following message with every restart:

```
Dis is one half. Press any key to continue
```

The key is variable and is stored within the infected partition record (offset 29h). When the virus is active, encrypted records are deciphered before they can be accessed by other programs. If the virus is removed, however, it is highly likely that data will be lost. It is then no longer possible to determine which value the virus has used for the encryption process and what stage it had reached.

As with most multipartite viruses, One Half waits until the INT 1Ch routine detects that DOS is being loaded and does not become fully active until interrupt 21h is also assigned.

When the virus is active, it can no longer be found in the partition and within the first cylinder of the hard disk. When the partition is read, the access attempt is redirected to the stored original record. When the area of the hard disk used by the virus is read, the read buffer is filled up with noughts.

The virus infects .COM and .EXE programs during loading, opening, renaming, closing and generation, but only if the relevant program is on a floppy disk or other removable medium, i.e. it does not normally affect programs on a hard disk. The virus checks the signature "MZ"/"ZM", and therefore also infects programs which do not have the file extension "EXE". One Half eludes all write-protect attributes of DOS and does not generate any error messages if the floppy disk containing the program to be infected is write-protected.

One Half extends programs by 3544 or 3577 bytes (depending on the variant concerned), whereby the file enlargement is not visible when you enter DIR and the infected programs are detected via the file date. CHKDSK does not generate any error messages. The virus circumvents anti-virus program warnings by making sure that it does not infect SCAN, CLEAN, FINDVIRU, GUARD, NOD, VSAFE and MSAV.

The virus attaches itself to the end of the program, but also modifies the original program approx. 1K before the virus code. This contains the code fragments of the deciphering routine in random order and at

random intervals, thus making it impossible to detect the virus without a special algorithm. This insertion of code fragments is reminiscent of the COMMANDER BOMBER virus, but is less complex.

The encryption routine is generated polymorphically, but basically only consists of XOR [Offset],factor1 / ADD factor1,factor2, whereby factor1 and factor2 are selected randomly.

The virus also contains the text "Did you leave the room ?", although it is not visible in programs due to the encryption.

The virus should not simply be removed from the partition with "FDISK /MBR" or other tools, as the areas encrypted by the virus will then be irrecoverably lost. Many anti-virus programs only remove the virus from the partition, but leave the encrypted area of the hard disk untouched. The safest method is to make a backup of all data on the hard disk if the virus is still active. You can then use FDISK /MBR and FORMAT on the hard disk and finally re-read all the data again.

Oropax

Alias: Music, Musician
Type: Direct, resident .COM infector
Length: 2756 to 2806 bytes

Roughly five minutes after the infection of a file, this virus plays up to six different pieces of music at seven-minute intervals. The 'Blue Danube' doesn't sound too bad. Infected files have a length divisible by 51. Close analysis is hindered by a self-modified code. This virus infects files not only during write access, but also during deletion.

Parity (boot record virus)

Alias: Parity Check

The Parity virus only affects boot records and reduces the available main memory in the 640 KB area by 1 KB. Unless a keyboard driver is loaded, the virus causes the computer system to crash every hour on the hour. The message "PARITY CHECK" appears on the screen in 40*25 mode, but without any further details of the address where this parity error apparently occurred. If you run a debugger, this may cause the system to crash, and the warm boot sequence (Strg)+(Alt)+(Entf) only pretends to carry out a warm restart.

The virus is a resident stealth-type boot record virus. If a computer system is booted from an infected floppy disk, the virus will infect the system. During the infection of the hard disk, it copies the clean master boot record to an unused area (head 0, cylinder 0, sector 14) and redirects all further attempts to read the master boot record to this copy.

During the infection of a floppy disk, a copy of the uninfected boot record is stored in the last record of the root directory. Any entries here will be lost, which means that data losses are inevitable, though relatively rare. The generated copies of the boot record are located at head 1, track 0, sector 3 on 360 KB and 720 KB disks, at head 1, track 0, sector 5 on 1.2 MB disks and at head 1, track 0, sector 14 on 1.44 MB disks.

The installation routine of the Parity virus determines the entry address of interrupts 09h and 13h and stores these together with the hour count of the current internal clock. Then the virus reduces the available main memory area (0-640 KB) and corrects the reported amount of conventional main memory. The virus then copies itself into the memory thus "allocated". The interrupt vectors 09h and 13h in the interrupt vector table are assigned the new addresses of both handlers, which are now located below the upper DOS limit. To conclude the installation routine, interrupt 19h is now called, thus causing the system to be rebooted. During this restart, either the boot record head 1, track 0, sector 0 of floppy disks or the master boot record head 0, cylinder 0, sector 1 of hard disks is supposed to be read (triggered by the BIOS) via interrupt 13h. However, the virus is present in this interrupt and redirects the read access to the clean record in each case. Once the program code of the original boot record or master boot record has been given control of the program, the computer system starts up with slightly less memory than usual. Since the operating system has no idea of the existence of an additional one kilobyte of memory, it is relatively unlikely that the virus will be overwritten.

When called, the virus's routine for handling interrupt 13h of the virus returns the function code AH=AAh to the caller immediately. First, it attempts to read a boot record and master boot record, which it checks for previous infection. If it is not infected, the read original record is written in a specific record for future use. For this purpose, the BPB (BIOS Parameter Block) is adapted within the virus to the values of the disk to be infected prior to writing. If a write-protected floppy or hard disk is to be written on, the error message from the relevant controller is rejected and the floppy or hard disk is not infected. The stored hour count is increased by one with each new infection. Before returning to the caller, all registers are always tidied up again to make it look as if the clean record had been read from the normal place.

By intercepting the keyboard interrupt, the virus not only detects the normal key actuations but also the key combination for a warm restart. With every normal key actuation, the virus compares the hour count of the current internal clock with the value obtained from the hour count of the system boot increased by the number of infected boot records. If both are identical, the screen is switched to the 40*25 mode and deleted, then the message "PARITY CHECK" is displayed and the process is stopped.

If the last key combination was (Strg)+(Alt)+(Entf) for a warm restart, the system will simply be restarted without deleting or resetting any interrupt vectors instead of a proper warm restart. Although this only causes the system files to be reloaded, it leaves the virus in the activated, resident state. This "simulated" warm restart is easily identified from the fact that the usual copyright information of the BIOS

manufacturer does not appear and the system starts booting immediately.

By installing a keyboard driver (KEYB, MFKEY), it is possible to deactivate the keyboard routine of the virus. In this case the virus can no longer stop the system, but still continues to infect clean data media.

Perfume

Alias: 4711, G
Type: Resident .COM infector
Length: 765 bytes

The Perfume virus is a distant relative of the Black Jack virus and operates in a similar way, installing itself in resident form. However, it is largely a 'joke virus' , which merely prevents every infected file after the 80th attempted infection from being loaded unless a password is entered (currently '4711'). It does not cause any destruction.

Ping Pong (boot record virus)

Alias: Bouncing Ball, Italian, Big Italian

This virus exists in both a floppy disk and a hard disk version. Unlike the Stoned virus, the Ping Pong virus carries out a series of error checks, e.g. to find out whether an infection is actually possible or worthwhile. When an infected floppy disk is booted, the original boot record of the hard disk is loaded into the memory unless the hard disk is already contaminated (identifier 01357h at offset 02FCh). Then the virus finds itself a vacant cluster (a cluster is normally an area consisting of four 512-byte records) on the hard disk and overwrites the boot record with the first part of itself. The second part ends up in the first vacant record of the cluster and the original boot record is stored in the second record of the cluster. The cluster is then flagged by the virus as bad in only one FAT. Earlier versions of the virus occupied about 2KB below the upper limit of the maximum available memory and were unable to run on 80286 and 80386 computers.

Sometimes the virus causes a bouncing ball or dot to appear every half hour or so. This can only be stopped by restarting the computer. Floppy disks can be infected from the hard disk simply be entering 'dir a:'.

Plastique

Type: Resident .COM and .EXE infector
Length: 3004, 4096 bytes
Similarities: Plastique Virus A, Plastique Virus B

Plastique Virus A:
After about 20 minutes music is played, individual tracks are formatted and hard disks become unbootable. Plastique infects both .EXE and .COM files, but not COMMAND.COM. It is not compatible with memory managers such as QEMM or 386MAX, however. Infected files are extended by an average of 3012 bytes, or by a maximum of 3020 (Plastique Virus B). And while we're on the subject of this variant:

Plastique Virus B:
Unlike the A-version, this one not only modifies the INT 21h, but also interrupts 13h, 9h and 8h. Why it needs interrupt Edh is not yet known. Infected files are increased by 4096 bytes, though this should not be confused with the 4096 virus.

RedX

Alias: Ambulance, Ambulance Car, Emergency
Type: Non-resident .COM infector
Length: 796 bytes

This virus is identified by an ambulance which travels across the screen from time to time. This ambulance with a flashing light on its roof is a simple model constructed from ASCII characters in the form of a block diagram. After infecting a file, the virus attempts to infect up to two other files, but not the first the '.COM' file in a directory.

Sampo (boot record virus)

Alias: Wllop, Turbo

This boot record virus infects the master boot record of a hard disk if you boot from an infected floppy disk. If you booted from an infected data medium, the virus will infect non write-protected disks with every read or write access, e.g. DIR A:

Once the virus is resident, any attempt to access an infected master boot record will cause the non-infected one to be returned. Sampo can survive a warm restart via (Strg)+(Alt)+(Entf).

If a write-protected disk is accessed, the virus returns a boot record apparently infected with the Telefonica virus. On 30 November, the virus displays the following message:

S A M P O
"Project X"
Copyright (c)1991 by the
SAMPO X-Team. All rights
reserved.
University Of The East
Manila

Silly Willy

Type: Non memory-resident file virus
First appearance: 1991 in Munich
Length: .COM files: approx. 2261 to 2314 bytes; .EXE files: 803 bytes are overwritten

Infected EXE programs display a face on the screen made up of ASCII characters, whereby the eyebrows and mouth keep changing from happy to sad. The following texts appear:

> The User of This Computer is Stupid!
> Please wait while I'm formatting your Harddisk.

Despite this message and the illumination of the drive lamp, the hard disk is NOT formatted. EXE files are only infected (destroyed) if the year of the system date is above 1989. Only .COM files are infectious.

Solano

Type: memory-resident COM and EXE infector
Length: 2000 bytes

12 minutes after the virus has installed itself in the memory, it begins to swap around the characters on the screen. This process is repeated every few minutes.

Stimulation

Type: Extending file virus.

This virus searches the current directory for .COM files. Each copy of the virus is encrypted differently. When the system clock reaches zero, the following text appears:

HA HA HA YOU HAVE A VIRUS FRODO LIVES!
Have you ever danced with the Devil in the pale moonlight?
DATA CRIME VIRUS RELEASED: 1 MARCH 1989 ALIVE:
Your system is infect by the STIMULATION virus. Have a nice day!

After this, the PC is blocked.

Stoned (boot record virus)

Alias: New Zealand, Donald Duck
Similarities: Stoned II, Angelina

Frequently encountered resident boot record virus. As with the Brain virus, the first versions of this virus were only able to infect 360 KB floppy disks, whereas the "improved" version can now also infect hard disks and HD floppies equally "well". Earlier versions had problems in this respect and would simply delete what it held to be unused records from the directory area.

The virus contains two text identifiers, one of which ("LEGALISE MARIJUANA!") is not displayed.

The virus usually generates the following message after every eighth boot:

Your computer is now stoned

or

Donald Duck is a lie

The virus occupies two kilobytes in the lower main memory (despite being only 400 bytes long itself) and one record on the hard disk (usually record 7 or 11). On a hard disk (with FDISK within DOS 3.0 or higher), this hardly matters, since this area of the first cylinder is not used by the operating system anyway. This only applies to hard disks which are partitioned with DOS 3.0 or higher, however. In the case of operating system versions below 3.0, this area is not usually vacant, but assigned to the FAT, and overwriting it will cause unforseeable damage. When a floppy disk is infected, a copy of the clean boot record is stored in the last record of the root directory, where any existing entries will be lost. Data losses are therefore inevitable, though relatively rare. In some versions, the hard disk is formatted if the current date reads 1-1-80 (which often occurs in the event of a battery failure).

The Stoned virus is one of the oldest boot record viruses, and has numerous variants and a very simple structure. If a computer system is booted from an infected disk, the virus infects the system. While infecting the hard disk, it copies the clean master boot record to an unused area (head 0, cylinder 0, sector 7) and redirects all subsequent attempts to read the master boot record to this copy.

Once the system has been booted from an infected data medium, the virus stores the interrupt 13h vector, reduces the available lower main memory area (0-640 KB) by two kilobytes and corrects the reported amount of conventional main memory. It then copies itself into the memory thus "allocated" and hijacks the interrupt 13h vector for its own routine. After this, the execution of the program is continued in the upper memory area and the resident installation process is completed.

After a reset, the original record is subsequently loaded in its normal place in the main memory. The virus now distinguishes whether booting took place from a hard or floppy disk.

If the system was booted from the hard disk, the hard disk is already infected and the virus can hand over control to the program code of the original record already loaded at the correct main memory location so that it can continue booting the system.

If the virus detects that the system was booted from a floppy disk, however, the system timer decides on a random basis whether or not to display the text "Your PC is now Stoned!". Then the master boot record of the first physical hard disk is read in and checked for previous infection. If it is already infected, the system will be stopped provided the above text was displayed.

If the master boot record is not infected, it is stored in record 7 for "special future use". After modifying the master boot record still stored in the memory, the virus writes the infected boot record back to the hard disk. After this infection process, the virus continues the normal boot procedure and hands over control of

the program to the original boot record of the floppy disk.

However, the virus is already resident and checks during every interrupt 13h access to establish whether the disk motor of drive A: is already running. As long as the disk drive motor is running, the virus will not check for infection. If the motor is not running, however, and has not yet reached the run-up stage, the virus will check whether any inserted disks have already been infected. If not, it will infect them accordingly, overwriting the FAT of more recent disk formats in the process.

Sunday Virus

Type: Resident .COM and .EXE infector
Length: 1631 bytes

This virus objects to people working on Sundays. It issues the following 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!
```

Part of this virus is derive from the Israel virus. Under certain circumstances, it may partially destroy the FATs. One variant of the Sunday virus is never activated, i.e. the message does not appear.

Sylvia

Alias: Holland Girl
Type: Non memory-resident COM infector
Length: 1332 bytes

This virus infects .COM files in the current directory and in the main directory of drive C:. The virus code contains the following text:

This program is infected by a HARMLESS Text Virus V2.1
Send a FUNNY postcard to : Sylvia
You might get an ANTIVIRUS program.....

This last suggestion of Sylvia's isn't such a bad idea...

Tai Pan

Alias: Whisper
Type: Resident .EXE infector
Length: 438 bytes
Similarities: Tai Pan-666, Tai Pan 434

Tai-Pan is a simple, resident file virus. When an infected program is loaded, the virus uses a self-defined INT 21h function AX=7BCEh (result: AX=7BCEh) to check whether it is already active in the memory. If so, it shortens the MCB chain by 528 or 752 bytes and copies itself into this area of the memory. In order to avoid being overwritten, the virus flags this memory area as SYSTEM-MCB. The virus assigns interrupt 21h without any special tricks and returns to the actual program booting procedure once activated.

The virus monitors the EXEC function of DOS and infects all programs which are smaller than 64833 bytes which have the EXE signature "MZ". The value of IP in the EXE header is used as an infection flag in order to prevent re-infection. Tai Pan attaches itself to the end of the file and extends it by 438 bytes. The virus retains the original file date during infection, but cannot circumvent the DOS file attributes READ-ONLY, SYSTEM or HIDDEN.

The new EXE header calculated by the virus has an invalid stack and may possibly cause the program to crash. Apart from this, the virus has no other damage routines.

The following text is found in every infected file:

```
[Whisper presenterar Tai-Pan]
```

Tai-Pan is very widespread in Germany, and was introduced together with Terminate 1.50, a CD of Power-Play magazine and other shareware archives.

Tai Pan-434

Tai Pan-434 is a slightly modified version of the original virus which enlarges programs by 434 bytes and contains the text:

```
CoSmO
```

It also controls the writing of data (via file handles). Screen displays are not longer legible when Tai Pan-434 is active.

Tai Pan-666

This variant is almost identical to the original Tai-Pan virus, except that the interrupt self-identification has been modified to AX=7BCFh and new virus length to 666 bytes. The text within the virus has also been changed to:

```
DOOM2. EXE
Illegal DOOM II signature
Your version of DOOM2.EXE matches the illegal RAZOR release of DOOM2
Say bye-bye HD
The programmer of DOOM II DEATH is in no
way affiliated with ID software.
ID software is in no way affiliated with DOOM II DEATH.
```

Fortunately, this text is merely a joke, and the virus does not contain any destructive routines. It does not even check whether the program in question is called "DOOM2. EXE".

This variant was introduced with a tool for the game DOOM II - DMNCHEAT.ZIP.

Taiwan

Type: Non-resident .COM infector
Length: 708, 743 bytes

On the 8th of every month, this virus overwrites 160 records starting with record 1 of hard disks 'C' and 'D', thereby destroying the FAT and the main directory among other things. If a .COM file is larger than the virus, the infected file is doubled in size. With every infection, the virus launches a further three infection attempts. The virus code is inserted at the beginning of the infected file.

Tenbytes

Alias: V-Alert
Type: Resident .COM and .EXE infector
Length: 1554 bytes

Following its activation between September and December, this virus overwrites the first ten bytes of every write-accessed file.

Tequila

Length: 2468
Type: Resident EXE infector
Similarities: Flip

Overwrites the load routine of the master boot record (partition record) with its own load routine, but not without saving the original elsewhere on the hard disk. By means of further manipulations, it then reduces the capacity of the 1st logical hard disk by 6 records (3 KB), into which it subsequently copies itself. In the memory, it lodges itself at the upper DOS limit, not when an infected program is loaded, but only after you have booted your computer from the hard disk. Programs and overlay files are infected during execution. Once a file is infected, the figure 62 appears in the seconds display of the file generation time. If a program attempts to determine the size of an infected file, Tequila subtracts its own size from it first. This takes place at a lower level than in the case of the Flip virus, which allows Tequila to fool other programs as well as COMMAND.COM.

WARNING:
Once Tequila is resident, i.e. active, CHKDSK detects file allocation errors which are not in fact real, as the virus uses stealth techniques to deceive the operating system with the wrong file length. If you enter CHKDSK /F here, you will chop up your files.

The virus contains the following text in encrypted form:

> 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 !"
> "$Execute: mov ax, FE03 / int 21. Key to go on!"

Traceback

Type: Resident .COM and .EXE infector
Length: 2930, 3066 bytes

This virus can be identified by the following 16-byte character string, which is found at the end of the virus code:

```
58 2B C6 03 C7 06 50 F3 A4 CB 90 E8 E2 03 8B
```

About half an hour after the infection of the system, the letters begin to fall from the screen as in the Black Jack virus. After a minute, the letters automatically return to their places. Depending on the variant or version of this virus, this interval can be shortened by pressing a key. Otherwise pressing a key sends the computer into an infinite loop.

Tremor

Length: 4000 bytes
Type: Resident virus, stealth type, fast infector

Enlarges the infected files by 4000 bytes and adds 100 years to the file date. Tremor uses the interrupts INT 21h, INT 15h, INT 9 and INT 24h.

Self-detection:

```
MOV   AH,2Ah
int   21h
MOV   AH,30h
INT   21H
MOV   AX,0F1E9H
INT   21H
CMP   AX,0CADEh
JE    already_resident
```

The virus is polymorphic and attempts to install itself in the Upper Memory Area during the installation routine using first the DOS function, then the XMS function. The Tremor virus is equipped with a tracing function for finding the entry point for INT 21h. The master PSP is modified so as to ensure that the current command interpreter hands over control to Tremor at the end of every program. It always infects COMMAND.COM first, causing the computer to seem very "sluggish".

CHKDSK displays the old figures for the main memory. If CLEAN, SCAN, MEM, CHKDSK, F-PROT, SYS, MIRROR, SI or ARJ are loaded, the virus will wipe these files clean on the hard disk (1) and track down any resident guard programs. VSAFE and TSAFE are simply deactivated.

Thanks to its stealth functions, the virus is able to hinder any attempt to detect infected files. The file system itself is not attacked. After a warm restart, the following text is displayed, having been stored in the virus in encrypted form:

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

After this, the computer system is rebooted.

Chronology of the Channel Videodat incident (Tremor), May 1994:

First, a few words on the transmission of data by satellite. Not all lines are required for broadcasting TV images, so that three lines are vacant per screen page and can be used for other tasks. The extra capacity of a video channel can be used transmitting texts or programs, for example. In order to receive these, each subscriber needs to install a converter between their TV set and PC (available from Wiegand Video Datensysteme GmbH in Wesseling, for example).

In this particular case, the company Videodat Medien GmbH in Wesseling had rented part of the channel capacity used by the TV broadcaster Pro 7. This channel can be received in Europe via satellite or cable. The editorial responsibility for the information and programs transmitted under the name "Channel Videodat" lies with Videodat Medien GmbH, Wesseling.

A company hit by the virus claimed that it had been infected by downloading a program from Channel Videodat. No clear proof of who was responsible for spreading the Tremor-infected files has so far been found, however. Videodat Medien GmbH was informed of this suspicion immediately. It argued that no infected programs had been transmitted, but described the techniques it used for tracking down viruses, a written inquiry having already been received from a subscriber.

At 14.04 h on 17 May, Channel Videodat transmitted version 104 of McAfee's SCAN, together with the program PKUNZIP.EXE required for unpacking the file SCANV104.ZIP before use. The PKUNZIP.EXE file was infected with Tremor, a virus which the transmitted version of SCAN is unable to detect. However, with the aid of a special program supplied by MicroBIT for identifying the Tremor virus, the infection was able to be detected on a PC (or rather main memory) which was guaranteed clean by cold-booting it from a clean disk) before the broadcast and disaster was thus averted. The infection of the PKUNZIP.EXE file was presumably reported immediately by observant subscribers. In any case, a clean version was transmitted via Channel Videodat at 16.00 h on the same day. Only subscribers who were still online at this time received the clean version with which the infected version had been overwritten. In addition, Channel Videodat subsequently transmitted several anti-virus programs and warnings.

Some virus victims claim that - as already mentioned - infected files had already been transmitted via Channel Videodat. This cannot now be proved, but the fact remains that the Tremor virus, which first appeared in January 1993, has since spread very rapidly and widely in Germany at least.

Tumen 0.5

Type: Memory-resident file virus
Length: 1663 bytes

An acoustic signal sounds when STRG+ALT is pressed together with any other key, then the colour palette appears on EGA or VGA screens. This happens again after each successful infection.

Typo COM

Alias: Fumble
Type: Resident .COM infector
Length: 712, 867 bytes

When a file is infected, the virus checks all files in the active directory and infects them if they are not already contaminated. Depending on the version in question, the virus either disrupts the print output to the parallel port or falsifies keyboard inputs. This is particularly annoying for speed typists. One variant of the virus only infects files on even days.

V163

Type: Memory-resident COM and EXE infector
Length: 163 bytes

This virus infects all files which do not begin with an "M" (4Dh). The value "M" (4Dh) is set by V 163 itself in the first byte of a file. The virus is unable to infect Read-Only files, however.

VGen

In the case of a VGen virus, AVWin will only find a virus signature, in which case it is highly likely that virulent code has been detected. To be on the safe side, please send in any files in which AVWin has detected a VGen virus to us.
Since AVWin can only locate the signature of VGen viruses, it is unfortunately unable to repair the affected files.

Vacsina

Type: Resident .COM, .EXE, .SYS and .BIN infector
Length: 1339, 2764 (+ 132) bytes
Similarities: Yankee Doodle

Vacsina is a virus with an automatic update function. If a recent version encounters an older version, the older version is deleted by the virus itself and replaced by the new one. The Vacsina virus usually emits a beep every time it infects a file.

The infection of .EXE files takes place in two stages, as the virus only appears to be able to infect .COM files 'properly'. When the virus is resident, the .EXE file to be infected is assigned a relocator the first time it is called. Equipped with this relocator, the file behaves outwardly like a .COM file as far as the virus is concerned, and can then be infected by it when it is called for the second time.

In the existing versions of Vascina, infected files do not have their original date and time restored, but are assigned the system date and time valid at the time of infection.

Another interesting feature is the identification of internal versions. In most cases, the last two bytes of an infected file represent the 'version number' of the virus. In the memory, the version number is located in segment 0 at offset 0C7h.

Victor

Type: Memory-resident COM and EXE infector
Length: 2442 to 2458 bytes

This virus destroys files in the currently active directory between the following times: 9.00-10.00, 11.00-12.00, 13.00-14.00 and 15.00-16.00 h. The virus code contains the following text:

Victor V1.0 The incredible high Performance Virus Enhanced versions available soon. This program was imported from USSR. Thanks to Ivan.

Vienna

Alias: DOS-62, Blue Danube, Wiener, P, Unesco, Austrian
Type: Non-resident .COM infector
Length: 648 bytes

The Vienna virus is a very primitive but nevertheless effective virus. It destroys files under certain conditions, namely whenever the last 3 bits of the system time have just been set to 0 during an attempted infection. In some versions, Vienna renders the infected file unusable in one in eight cases, whereby the newly infected file is completely 'demolished'.

A peculiarity of the Vienna virus is that it only infects or deletes files in the current path and subdirectory. If the user therefore sets 'PATH = C:\TEST' and work within this empty TEST directory, the virus cannot infect any more files; the trouble is, the user can no longer work efficiently in most cases either.

Since the Vienna virus destroys files now and again, you should be careful not to delete any data files by accident when removing these destroyed files with the AntiVir repair program in GURU mode. AntiVir cannot distinguish whether the first five bytes of a restart sequence (JMP FFFF:00F0) represent a valid - and intentional - restart program, or whether they are due to the destructive activities of a virus. This is something which you must decide for yourself. This is particularly difficult if the virus 'sometimes' writes five NOPs into the file instead of the jump instruction from above.

Vriest

Type: Resident .COM infector
Length: 1280 bytes

Extends files by 1280 bytes. On 3.5.1991, the following text appears on the screen:

> Something's coming up ...

This is followed by the sound of a siren, after which the screen is scrolled up and the following text is displayed:

> Vriest of g greats Vic ear Moeli~

The virus uses the operating system in order to become resident. It occupies 1584 bytes of memory and does not infect files in the usual way, e.g. during the loading of a .COM file, but spreads itself via the COPY routine, for instance.

Whale

Alias: Motherfish, Z the whale
Length: 9216 bytes
Type: Resident .COM and .EXE infector
Similarities: Fish

This is one of the biggest yet least harmful viruses in existence. An infection can be detected immediately, as the computer capacity is reduced so severely that it is no longer possible to work effectively and the screen displays take ages to build up. Infected programs generally crash straightaway. If detected immediately and then eliminated, this virus does not usually do any serious damage.

The command "CHKDSK /F" cannot be used when the virus is active in resident form, as it will only try to conceal its presence by means of stealth techniques, and this will cause damage to the files. Roughly four fifths of the virus code are debugger traps designed to hinder the disassembly of the code. The virus was probably written by two programmers, whereby one was responsible for the assembler side (the self-encrypting and encrypting/decrypting elements), and the other for the other routines, which were mainly written in high-level language. This virus has been assigned the attribute 'armoured', with the direct consequence of perceptible time delays which cost precious processor time. When the virus is active, only fragments of the program code exist in executable form, as these fragments have to be decrypted first and then re-encrypted after execution before a new fragment can be decrypted and re-encrypted.

Wiener

Alias: DOS-62, Blue Danube, Vienna, P, Unesco, Austrian
Type: Non-resident .COM infector
Length: 648 bytes

It destroys files under certain conditions, namely whenever the last 3 bits of the system time have just been set to 0 during an attempted infection. In some versions, Vienna renders the infected file unusable in one in eight cases, whereby the newly infected file is completely 'demolished'.

A peculiarity of the Vienna virus is that it only infects or deletes files in the current path and subdirectory. If the user therefore sets 'PATH = C:\TEST' and work within this empty TEST directory, the virus cannot infect any more files; the trouble is, the user can no longer work efficiently in most cases either.

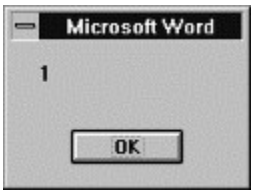
Since the Vienna virus destroys files now and again, you should be careful not to delete any data files by accident when removing these destroyed files with the AntiVir repair program in GURU mode. AntiVir cannot distinguish whether the first five bytes of a restart sequence (JMP FFFF:00F0) represent a valid - and intentional - restart program, or whether they are due to the destructive activities of a virus. This is something which you must decide for yourself. This is particularly difficult if the virus 'sometimes' writes five NOPs into the file instead of the jump instruction from above.

WinWord.Concept

Alias: WW6Macro
Type: Macro virus

This "virus" is purely a macro virus which modifies document (DOC) files. WinWord.Concept uses the well documented macro language WinBasic of the application program Word for Windows. The "virus" does not contain any direct processor instructions itself, but consists entirely of macros.

As soon as you open a document file containing one of these macros, the macro AutoOpen is executed. This means that the "virus" has already gained control, as a macro from the template assigned to the active document has the highest priority - and the document itself is the template! The virus then modifies the global template file, which is usually NORMAL.DOT. A message box subsequently appears displaying the number:



Strictly speaking, the opened document file is not really a document (DOC) file, but a template (DOT) file. The virus modifies the default macro "SaveFileAs", so that documents are now saved in format 1, i.e. as document templates, which means that you will have difficulty saving in selected directories. Each file saved via "File / Save As..." in turn contains the macros from WinWord.Concept.

If a document saved in this way, or rather this template, is opened on an intact Word for Windows System, the AutoOpen macro will also be executed again and the new macros will be assigned to the global template file. Since WinWord.Concept is based on the macro language WordBasic, it can also run on the various operating systems (Windows 3.1, Windows for Workgroups, Windows 95, Windows NT, Mac OS) for which Word is equipped with this macro language (Word for Windows 6.0, Word for Windows 7.0, etc.).

WinWord.Concept can be identified quite easily from the following three macros:

AAAZAO
AAAZFS
Payload

The macro AutoOpen may also have been added to these in the meantime. If the macro AutoOpen already existed before, its contents will be changed. In addition to the macro names, the following text strings are also detectable in the documents:

see if we´re already installed
iWW6IInstance
That´s enough to prove my point

The following entry has now been added to the file WINWORD6.INI:

WW6= 1

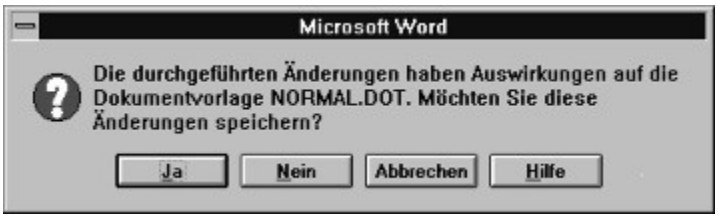
WinWord.Concept can be removed from all documents by manual deletion of the macros in question. If you are not sure whether a document or the existing global template have already been modified by this "virus", you should call the program with "disabled" macros. This can be done either via the command lines or by starting WinWord via Shift+click on the icon, in which case no macros will be executed. In

Word for Windows 6.0, you should not double-click the name of the document or simply click OK in order to select a document, but open the document via Shift+OK: that way WinWord 6.0 will open the document without macros.

It is also generally possible to set the existing NORMAL.DOT to READONLY, although this attribute then has to be removed manually before every change. Another possibility is to suppress all automatic macro functions, e.g. by using the following macro as an AutoExec:

```
Sub MAIN
AutoMacroSuppress 1
MsgBox "Supressing automatic macros", "AutoMacro Suppression", -1
"AutoMacro Suppression", -1
End Sub
```

Such a macro can also be added to the global template under a different name and then deliberately called when you start Word for Windows (winword /M<name>). By using the parameter /A, you can also instruct WinWord to start without document templates and add-ins.



WitCode

Type: .EXE infector
Length: 974 bytes

The virus appropriates roughly 1.5 KB of memory, into which it then copies itself. The MCB of this PSP is then modified so that it looks like part of the active command interpreter. When you exit a program, various messages will now appear depending on the system clock reading. On 24 December, for example, you will see Christmas greetings, while the following message appears every Sunday:

You really shouldn't work on Sundays...

Depending on the type of installed processor, the virus will complain that your computer is too slow:

Gee, I wanna sleep now!

or congratulate you if you have a fast computer:

You got a fine machine!

Depending on the system clock, WitCode modifies the boot record on Mondays and on every Friday 13th so that subsequent restarts become stuck in an infinite loop in the boot record.

Yankee Doodle

Alias: TPxx
Type: Resident .COM and .EXE infector
Length: 1881+16 bytes
Similarities: Vacsina

Depending on the relevant variant, this virus the tune "Yankee Doodle" via the integrated loudspeakers. This may happen either at 17:00 h or after the successful infection of a file. During installation, the virus eludes the operating system by directly modifying the MCBs and then infects every new program that is loaded. Since this virus derives from the Vacsina virus, it has also inherited the ability to update itself with new versions. One version of the virus kills the Ping Pong virus if it is present on your hard disk.

Zero Bug

Alias: Palette, ZBug
Type: Resident .COM infector
Length: 1536 bytes

With this virus, file enlargements are not displayed in the directory. Once a file is infected, the virus writes the figure '62' in the seconds display of the file date to identify it as infected. Once the COMMAND.COM has also been infected on the hard disk, letters on the screen are usually 'eaten up' by the 'Smiley', (ASCII code 01) after a certain time, while large .COM files are 'demolished' by the virus. The virus can be identified from the following character strings in an infected file:

ZE
COMPSEC=C:
C:\COMMAND.COM

dBase

Type: Resident .COM and overlay infector
Length: 1864 bytes

Once this virus becomes resident, it modifies data from dBase-compatible databases. It then stores the names of the databases whose contents it has modified in the invisible file BUGS.DAT. When data are written in a .DBF file, adjacent bytes are exchanged; when the data are read, this 'encryption' process is reversed again. This process continues fairly harmlessly for two months, when the virus decides to overwrite the FATs and the root directory. The name of the file is stored in character form in the virus itself: 'c:\bugs.dat'. The virus uses INT 21h, sub-function 0FB0Ah to check whether or not is already resident.