1008 Virus

Virus info

Virus alias:	Suomi, Oulu
File size:	1008 bytes
Virus type:	Resident .COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

1260

Virus info

Virus alias:	-
File size:	1253 bytes
Virus type:	Resident .COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

1260

Virus info

Virus alias:	V2P1
File size:	1260 bytes
Virus type:	COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

Heavily encrypted virus which infects at an extremely fast rate.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

12-Ticks (Trojan horse)

Virus info

Virus alias:	-
File size:	-
Virus type:	-
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

405

Virus info

Virus alias:	-
File size:	405 bytes
Virus type:	Overwriting, non-resident .COM destroyer
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

4096

Virus info

Virus alias:	100 Years, IDF, Stealth, Frodo, Century
File size:	4096 bytes
Virus type:	Resident .COM and .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

8 Tunes

Virus info

Virus alias:	-
File size:	1971 bytes
Virus type:	Resident .COM and .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

903

Virus info

Virus alias:	-
File size:	903 bytes
Virus type:	Resident .COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

AIDS Information Introductory Disk 2.0 (Trojan horse)

Virus info

Virus alias: -
File size: -
Virus type: -
Infected operating systems: -
Damage: -
Discovered on: -
From VDF version: -

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Akuku

Virus info

Virus alias:	Hybrid
File size:	1306 bytes
Virus type:	Resident .COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Alabama

Virus info

Virus alias:	-
File size:	1560 bytes
Virus type:	Resident .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Amilia

Virus info

Virus alias:	-
File size:	1164 bytes
Virus type:	Memory-resident file virus
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Amoeba

Virus info

Virus alias:	Khetapunk, 1392, Maltese
File size:	1392 bytes
Virus type:	Memory-resident .COM and .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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"

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Angelina (boot record virus)

Virus info

Virus alias:	Stoned-Angelina
File size:	-
Virus type:	-
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Anthrax

Virus info

Virus alias:	-
File size:	1048 bytes
Virus type:	Resident .EXE and .COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

AntiExe (boot record virus)

Virus info

Virus alias:	D3, NewBug
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

April

Virus info

Virus alias:	Suriv
File size:	Approx. 900 bytes or more
Virus type:	Resident .COM and .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Azusa (boot record virus)

Virus info

Virus alias:	-
File size:	-
Virus type:	-
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Barrotes

Virus info

Virus alias:	-
File size:	1310 bytes
Virus type:	Resident .EXE and .COM infector
Infected operating systems:	-
Damage:	Destroys the master boot record on 4 January!
Discovered on:	-
From VDF version:	-

General information

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".

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Basic

Virus info

Virus alias:	-
File size:	5120, 5128, 5135 bytes
Virus type:	Non-resident .COM and .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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"

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

BDS/Arg

Virus info

Virus alias: Backdoor.VNC-based, BackDoor-ARG
File size:
Virus type:
Infected operating systems:
Damage:
Discovered on :
From VDF version:

General information

The Trojan secures VNC applications, after it names itself EXPLORER.EXE. It performs the installation of the file INST.EXE, which is used by the VNC application. The Trojan listens on TCP Port 5800 waiting for further commands.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

BDS/Ciadoor

Virus info

Virus alias:	Backdoor.Ciadoor, Backdoor.Ciadoor.12
File size:	117.977 Bytes
Virus type:	Worm
Infected operating systems:	
Damage:	Sent by email, TCP Ports
Discovered on:	14.05.2004
From VDF version:	6.25.00.75

General information

When activated, BDS/Ciadoor copies itself in %WinDIR%CSRSS.EXE. The file name can be different

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

BDS/Deloder

Virus info

Virus alias:	Backdoor.Tsunami.c, IRC-Pitchfork, Backdoor.Dvldr
File size:	29.336 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Connection through TCP Port 6667 Please get info from General Description if you consider necessary.
Discovered on:	01.01.2003
From VDF version:	6.23.00.00

General information

It is an IRC Trojan. When activated, it creates the following files:

%Font%

undll32.exe (29,336 Bytes)

%Systemdirectory%cygwin1.dll (944,968 Bytes)

and makes a Registry Entry, to be automatically activated on Systemstart.

The Trojan contacts IRC ports and listens for further commands. It creates the hidden file rundll32.exe in fonts directory and opens TCP Port 6667.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

BDS/Small.D

Virus info

Virus alias:	Backdoor.Dumador.c, PWS-Narod, IRC Trojan
File size:	9.216 Bytes
Virus type:	Worm
Infected operating systems:	
Damage:	Steals information from the computer
Discovered on:	01.01.2004
From VDF version:	6.23.00.00

General information

This password stealer Trojan tries to collect information on the local computer and to send it to its author by email

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

BDS/SubSeven.15

Virus info

Virus alias:	Backdoor.SubSeven, Sub7, Sub-7
File size:	variable
Virus type:	Worm
Infected operating systems:	
Damage:	Backdoor component
Discovered on:	22.08.2000
From VDF version:	6.20.00.00

General information

SubSeven is a Backdoor program (as for example NetBus, Back Orifice etc.), which allows a third party to have access to a system

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

BDS/SubSeven.16

Virus info

Virus alias:	SubSeven, Sub7, Sub-7
File size:	variable
Virus type:	Worm
Infected operating systems:	-
Damage:	Backdoor component
Discovered on:	22.08.2000
From VDF version:	6.20.00.00

General information

SubSeven is a Backdoor program (as for example NetBus, Back Orifice etc.), which allows a third party to have access to a system

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

BDS/SubSeven.17

Virus info

Virus alias:	SubSeven, Sub7, Sub-7
File size:	variable
Virus type:	Worm
Infected operating systems:	-
Damage:	Backdoor component
Discovered on:	22.08.2000
From VDF version:	6.20.00.00

General information

SubSeven is a Backdoor program (as for example NetBus, Back Orifice etc.), which allows a third party to have access to a system

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

BDS/SubSeven.18

Virus info

Virus alias:	SubSeven, Sub7, Sub-7
File size:	variable
Virus type:	Worm
Infected operating systems:	
Damage:	Backdoor component
Discovered on:	22.08.2000
From VDF version:	6.20.00.00

General information

SubSeven is a Backdoor program (as for example NetBus, Back Orifice etc.), which allows a third party to have access to a system

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

BDS/SubSeven.19

Virus info

Virus alias:	SubSeven, Sub7, Sub-7
File size:	variable
Virus type:	Worm
Infected operating systems:	
Damage:	Backdoor component
Discovered on:	22.08.2000
From VDF version:	6.20.00.00

General information

SubSeven is a Backdoor program (as for example NetBus, Back Orifice etc.), which allows a third party to have access to a system

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

BDS/SubSeven.1xx

Virus info

Virus alias:	SubSeven, Sub7, Sub-7
File size:	variable
Virus type:	Worm
Infected operating systems:	-
Damage:	Backdoor component
Discovered on:	22.08.2000
From VDF version:	6.20.00.00

General information

SubSeven is a Backdoor program (as for example NetBus, Back Orifice etc.), which allows a third party to have access to a system

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

BDS/SubSeven.213

Virus info

Virus alias:	Zeckentod, SubSeven, Sub7, Sub-7
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	-
Discovered on:	22.02.2001
From VDF version:	6.23.00.00

General information

When the system is infected with this version of SubSeven, a file with a random name appears in Windows directory.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

BDS/SubSeven.2xx

Virus info

Virus alias:	SubSeven, Sub7, Sub-7
File size:	variable
Virus type:	Worm
Infected operating systems:	-
Damage:	Backdoor component
Discovered on:	22.08.2000
From VDF version:	6.20.00.00

General information

SubSeven is a Backdoor program (as for example NetBus, Back Orifice etc.), which allows a third party to have access to a system.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Bestwish

Virus info

Virus alias:	-
File size:	970 bytes
Virus type:	Resident .COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Black Jack

Virus info

Virus alias:	Cascade, 1701, 1704, Falling Letters, Falling Leaves, Autumn Leaves
File size:	Usually 1701 bytes or 1704 bytes
Virus type:	Resident .COM infector (also .EXE version)
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Brain Boot (boot record virus)

Virus info

Virus alias:	Pakistani
File size:	-
Virus type:	-
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Breasts (boot record virus)

Virus info

Virus alias:	-
File size:	-
Virus type:	-
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

BSD/Ciadoor

Virus info

Virus alias:	Backdoor.Ciadoor, Backdoor.Ciadoor.12
File size:	4,099 Bytes
Virus type:	Trojan
Infected operating systems:	-
Damage:	-
Discovered on:	14.05.2004
From VDF version:	14.05.2004

General information

When activated, BSD/Ciadoor copies itself in %WinDIR%\CSRSS.EXE. The file name can vary. .

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Burger Virus

Virus info

Virus alias:	909090, CIA
File size:	560, 736, 1280 bytes
Virus type:	Overwriting, non-resident '.COM' infector (also '.EXE' version)
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Cascade

Virus info

Virus alias:	Black Jack, 1701, 1704, Falling Letters, Falling Leaves, Autumn Leaves
File size:	Usually 1701 bytes or 1704 bytes
Virus type:	Resident .COM infector (also .EXE version)
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Casper

Virus info

Virus alias:	-
File size:	1200 bytes
Virus type:	Non memory-resident .COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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:.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Christmas

Virus info

Virus alias:	Syslock
File size:	2764 bytes
Virus type:	Non-resident .COM and .EXE infector.
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

CMOS-One (boot record virus)

Virus info

Virus alias:	Often mistakenly identified as ExeBug (A)
File size:	-
Virus type:	-
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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!

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Contents

Each new virus is a challenge. How does it spread? What does it do? Does it manipulate the system? Does it generate new files? How is the potential damage and danger to be assessed?

Our experts find out the correct answers to these questions in the course of their analysis on isolated laboratory computers in our own virus research centre. A description of the viruses with specific instructions for removing the viruses are published.

In this help file you will find a current virus specification. More information with additional specific elimination pointers for malware and unwanted programs can be found in our website under virus info.

Crazy Eddie
CSFR 1000
Datacrime
dBase
Devils Dance
Diamond
Disk Killer (boot record virus)
Eddie
Faust
Fiche
Fish
Flash
Flip
Form (boot record virus)
Friday
FSP Killer
Fu Manchu
Ghost
Hafenstraße
Hallöchen
HONNECKER Trojan (Trojan horse)
Icelandic
Israel
Itavir
Jack Ripper (boot record virus)
Jerusalem
Joshi (boot record virus)
JS/Mimail.B
Junkie
Kennedy
Keypress
Kiev (boot record virus)
Kit/VBSWormGen.150
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
O97M/Cybernet.A
Ohio (boot record virus)
Omega
One Half
Oropax
Parity (boot record virus)
PDF/Peach

Perfume
Ping Pong (boot record virus)
Plastique
RedX
Sampo (boot record virus)
Silly Willy
Solano
Stimulation
Stoned (boot record virus)
SubSeven (TR.Sub7)
Sunday Virus
Sylvia
Tai Pan
Taiwan
Tenbytes
Tequila
TR.Worm.Navidad
TR/DoS.Boxed.a
TR/Dvldr
TR/IWorm.Fix2001
TR/Proxy.Bobax.b
TR/Proxy.Bobax.c
TR/Proxy.Ranky.AE
TR/Worm.QAZ
TR/Worm.RC5.WinInit
Traceback
Tremor
Tumen 0.5
Typo COM
V163
Vacsina
VBS/Caroline.B
VBS/Elva
VBS/Fireburn
VBS/Guorm
VBS/HappyTime
VBS/HomePage.1
VBS/Lee-ATX
VBS/LiveStages.A
VBS/LoveLetter
VBS/LoveLetter.BD
VBS/LoveLetter.CM
VBS/Netlog.Worm
VBS/NeueTarife
VBS/Redlof.A
VBS/SST.A
VBS/Staple.A
VBS/Vierika
VGen
Victor
Vienna
Vriest
W32/Aliz
W32/Apost.A
W32/Beast
W32/Elkern.B

W32/Elkern.C
W32/ExploreZip
W32/FBound.C
W32/Fono98
W32/Funlove.4099
W32/Hai.A
W32/Hantaner
W32/Jeefo
W32/Klez
W32/Klez.A
W32/Kriz
W32/Lovesong.998
W32/Magistr.B1
W32/Naked
W32/Navidad.B
W32/Nimda
W32/Nimda (W32/Nimda.eml)
W32/Nimda.eml
W32/Parite
W32/Parite.tmp
W32/Partie.B
W32/Perrum
W32/PrettyPark
W32/ProLin@mm
W32/Vote (Variations .a, .b & .
W32/Xorala
W32/Yaha.E
W32/YAWsetup
W64/Rugrat.3344
W95/Begemont.B
W95/CIH
W95/CIH.A
W95/CIH-1049
W95/Dupator.1503
W95/Fono
W95/Hybris
W95/Hybris.Gen.1
W95/Hybris.Gen.2
W95/Hybris.Gen.3
W95/Hybris.PI.003
W95/Kriz.4050
W95/MTX
W95/MTX.dr
W95/Spaces.1445.B
W95/Weird.10240.a
W97M/Resume.A
Whale
Wiener
Win95/Lorez
WinWord.Concept
WitCode
Worm./Bagle.F
Worm./Bagle.H
Worm/AceBot
Worm/Anacon
Worm/Anset.b

Worm/Aphex
Worm/Aphex.1
Worm/Aphex.2
Worm/Aphex.3
Worm/Avril.A
Worm/Avril.A.2
Worm/Avril.B
Worm/Avron.A.INI
Worm/Avron.C.INI
Worm/Badtrans
Worm/Badtrans.B
Worm/Bagle.A
Worm/Bagle.AA
Worm/Bagle.ab
Worm/Bagle.AC
Worm/Bagle.AD
Worm/Bagle.AF
Worm/Bagle.AI
Worm/Bagle.B
Worm/Bagle.C
Worm/Bagle.F
Worm/Bagle.H
Worm/Bagle.J
Worm/Bagle.M
Worm/Bagle.N
Worm/Bagle.R
Worm/Bagle.U
Worm/Bagle.V
Worm/Bagle.X
Worm/Banuris.P2P
Worm/Banuris.P2P.1
Worm/Bibrog.C
Worm/Bizex
Worm/Blackmal
Worm/BleBla
Worm/BleBla.3
Worm/Bobax
Worm/Bride.A
Worm/Bride.C
Worm/Brit.B
Worm/Brit.F
Worm/Bugbear
Worm/BugBear.1
Worm/BugBear.2
Worm/Bugbear.B
Worm/BugBear.B.dll
Worm/Calil
Worm/Cervivec
Worm/Chet
Worm/Choke.1
Worm/Choke.2
Worm/CodeRed
Worm/Colevo
Worm/Cuervo
Worm/Cult.B
Worm/Cydog.C

Worm/Dabber
Worm/Datom.1
Worm/Datom.2
Worm/Datom.3
Worm/DeadHat.A
Worm/Deborm.Q.1
Worm/Deborm.Q.3
Worm/Deborm.R.1
Worm/Deborm.R.2
Worm/Deborm.R.3
Worm/Deloder
Worm/Desos
Worm/Doomjuice
Worm/Dumaru.A
Worm/Dumaru.AC
Worm/Dumaru.B1
Worm/Dumaru.B3
Worm/Dumaru.C.3
Worm/Dumaru.K
Worm/Dumaru.K.DLL
Worm/Dumaru.Y
Worm/ExploreZip.E
Worm/Fizzu.A
Worm/Fizzu.A.2.E
Worm/Fizzu.A.2.F
Worm/Frethem
Worm/Frethem.001
Worm/Frethem.010
Worm/Frethem.014
Worm/Frethem.J
Worm/Frethem.l
Worm/FriendGreet
Worm/Ganda
Worm/Gibe
Worm/Gibe.B
Worm/Gibe.C
Worm/Gibe.C.1
Worm/Gnutella.MG
Worm/Gokar.1
Worm/Goner
Worm/Happy
Worm/Happy.A
Worm/Hawawi.A
Worm/Hawawi.G.Drp
Worm/Holar.C
Worm/Holar.C.1
Worm/Hybris.B
Worm/Hybris.PI.11
Worm/Inmota.1
Worm/Inmota.DLL
Worm/Isratz.1
Worm/Isratz.2
Worm/KakWorm.D
Worm/Kazaa
Worm/Klez.E
Worm/Korgo.M

Worm/Korgo.N
Worm/Korgo.Q
Worm/Lee.SP
Worm/Lee.SP3
Worm/Lentin.2
Worm/Lentin.A
Worm/Lentin.E
Worm/Loiten
Worm/Lovegate
Worm/Lovegate.G.1
Worm/Lovegate.G.2
Worm/Lovegate.J
Worm/Lovegate.J123
Worm/Lovegate.K
Worm/Lovelorn.2
Worm/Lovelorn.3
Worm/Lovelorn.4
Worm/Lovgate.A.1
Worm/Lovgate.A.2
Worm/Lovgate.A.3
Worm/Lovgate.B
Worm/LovGate.F
Worm/LovGate.F.2
Worm/LovGate.I
Worm/Lovgate.J
Worm/Lovgate.L.2
Worm/Lovgate.T
Worm/LovLorn.8
Worm/Lovsan.A
Worm/Lovsan.B
Worm/Lovsan.C
Worm/Lovsan.E
Worm/Lovsan.G1
Worm/Magold.A
Worm/Magold.E
Worm/Magold.E.1
Worm/Magold.E.3
Worm/Maldal.C
Worm/Maldal.E
Worm/Maldal.I
Worm/Mapson
Worm/Matcher
Worm/Matra
Worm/Melare
Worm/Mimail.A
Worm/MiMail.A1
Worm/Mimail.C
Worm/Mimail.C2
Worm/Mimail.E
Worm/Mimail.F
Worm/Mimail.G2
Worm/Mimail.H2
Worm/Mimail.I
Worm/Mimail.I1
Worm/MiMail.J2
Worm/Mimail.L

Worm/Mimail.M1
Worm/Mimail.q
Worm/Mofeir.B.1
Worm/Mofeir.B.2
Worm/Mumu.B.4
Worm/Myba.A
Worm/MyDoom
Worm/MyDoom.B
Worm/MyDoom.F
Worm/Mydoom.G
Worm/MyDoom.m
Worm/Mylife.M
Worm/Myparty
Worm/Nachi.A.1
Worm/Naco.D
Worm/Navidad
Worm/Nedal
Worm/Netsky.AA
Worm/Netsky.AB
Worm/Netsky.AC
Worm/NetSky.B
Worm/NetSky.C
Worm/NetSky.D
Worm/NetSky.E
Worm/Netsky.J
Worm/Netsky.K
Worm/Netsky.O
Worm/Netsky.P
Worm/Netsky.Q
Worm/Netsky.X
Worm/Netsky.Y
Worm/Netsky.Z
Worm/NiceHello
Worm/OpaSoft
Worm/Opasoft.AA
Worm/OpaSoft.BC
Worm/OpaSoft.D
Worm/Opasoft.E
Worm/OpaSoft.F
Worm/OpaSoft.G
Worm/OpaSoft.J
Worm/Opasoft.P
Worm/Opasoft.Q
Worm/Opasoft.R
Worm/Outsider
Worm/P2P.Surnova
Worm/Padobot.A
Worm/Padobot.B
Worm/Padobot.C
Worm/Padobot.D
Worm/Padobot.E
Worm/Padobot.F
Worm/Paukor
Worm/Pikachu
Worm/Purol.P2P.B
Worm/Randex.D

Worm/Roron.50
Worm/Roron.Gen
Worm/Sasser
Worm/Sasser.A
Worm/Sasser.B
Worm/Sasser.C
Worm/Sasser.D
Worm/Sasser.E
Worm/Sasser.F
Worm/Scold.A
Worm/Snapper.A
Worm/Sober
Worm/Sober.B
Worm/Sober.C
Worm/Sober.C1
Worm/Sober.D
Worm/Sober.E
Worm/Sober.G
Worm/Sober.H
Worm/Sobig.B
Worm/Sobig.C
Worm/Sobig.D
Worm/Sobig.E
Worm/Sobig.F
Worm/Sonic
Worm/Sorbig.A
Worm/Stator
Worm/Surnova.D
Worm/Symbi.Cabir.A
Worm/Tanked.A
Worm/Tettona
Worm/Torvil.B
Worm/W32.Sircam
Worm/Wallon
Worm/Warpigs.A1
Worm/Yaha.E
Worm/Yaha.J2
Worm/Yaha.L
Worm/Yaha.M
Worm/Yaha.P
Worm/Yaha.Q
Worm/Yaha.T
Worm/Zafi.B
WScr/Kak.Worm
Yankee Doodle
Zero Bug

Cookie

Virus info

Virus alias:	Syslock
File size:	2232 bytes
Virus type:	Non-resident .COM and .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Crazy Eddie

Virus info

Virus alias:	-
File size:	2727 bytes
Virus type:	Resident .COM and .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

CSFR 1000

Virus info

Virus alias:	-
File size:	1000 bytes
Virus type:	Resident .COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Datacrime

Virus info

Virus alias:	Columbus Day
File size:	1168, 1514, 2280 bytes
Virus type:	Non-resident .COM infector (also .EXE in some variants)
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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 ... ?!?)

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

dBase

Virus info

Virus alias:	-
File size:	1864 bytes
Virus type:	Resident .COM and overlay infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Devils Dance

Virus info

Virus alias:	-
File size:	941 bytes
Virus type:	.COM Infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Diamond

Virus info

Virus alias:	V1024
File size:	1024 bytes
Virus type:	Memory-resident .COM and .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Disk Killer (boot record virus)

Virus info

Virus alias:	Ogre
File size:	-
Virus type:	-
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Eddie

Virus info

Virus alias:	Dark Avenger
File size:	1800 (+16) bytes
Virus type:	Resident .COM and .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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'

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Faust

Virus info

Virus alias:	Spyer
File size:	1181 bytes
Virus type:	Resident .COM and .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Fiche

Virus info

Virus alias:	FEXE
File size:	897 bytes
Virus type:	Memory-resident .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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".

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Fish

Virus info

Virus alias:	-
File size:	3584 bytes
Virus type:	Resident .COM and .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Flash

Virus info

Virus alias:	-
File size:	688 bytes
Virus type:	Resident COM and EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Flip

Virus info

Virus alias:	Omicron
File size:	-
Virus type:	-
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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).

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Form (boot record virus)

Virus info

Virus alias: -
File size: -
Virus type: -
Infected operating systems: -
Damage: -
Discovered on: -
From VDF version: -

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Friday

Virus info

Virus alias:	South African, Miami, Munich
File size:	416, 540 bytes
Virus type:	Non-resident .COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

FSP Killer

Virus info

Virus alias:	-
File size:	789 bytes
Virus type:	Resident .COM and .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Fu Manchu

Virus info

Virus alias:	-
File size:	2080 bytes
Virus type:	Resident .COM and .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Ghost

Virus info

Virus alias:	Ghost Ball, Ghostballs
File size:	2351 bytes
Virus type:	Non-resident .COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Hafenstraße

Virus info

Virus alias:	-
File size:	809 bytes
Virus type:	Non memory-resident EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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

Hafenstraße

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Hallöchen

Virus info

Virus alias:	Halloechen, Hello
File size:	2011 bytes
Virus type:	Resident .COM and .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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
```

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Icelandic

Virus info

Virus alias:	Disk Eating, One In Ten, Disk Crunching, Saratoga 2
File size:	542, 656 bytes
Virus type:	Resident .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Israel

Virus info

Virus alias:	Jerusalem, PLO, Friday 13th
File size:	1803, 1808, 1813 bytes
Virus type:	Resident .COM and .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Itavir

Virus info

Virus alias:	-
File size:	3880 bytes
Virus type:	Resident .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Jack Ripper (boot record virus)

Virus info

Virus alias:	Jack The Ripper
File size:	-
Virus type:	-
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Jerusalem

Virus info

Virus alias:	Israel, PLO, Friday 13th
File size:	1803, 1808, 1813 bytes
Virus type:	Resident .COM and .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Joshi (boot record virus)

Virus info

Virus alias:	-
File size:	-
Virus type:	-
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

JS/Mimail.B

Virus info

Virus alias:	Exploit.CodeBaseExec (AVP), XMLid.Exploit (NAV), TrojanDropper.JS.Mimail.b, Exploit-CodeBase, Trojan.Sefex
File size:	variable
Virus type:	Worm
Infected operating systems:	
Damage:	variable
Discovered on:	01.01.2003
From VDF version:	6.23.00.00

General information

JS/Mimail.B uses an Internet Explorer security hole. It spreads exclusively through HTML files.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Junkie

Virus info

Virus alias:	-
File size:	3880 bytes
Virus type:	Resident .COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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".

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Kennedy

Virus info

Virus alias:	-
File size:	333 bytes
Virus type:	Non memory-resident COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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

\command.com
The Dead Kennedys

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Keypress

Virus info

Virus alias:	-
File size:	1232, 1472 bytes
Virus type:	Resident .COM and .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Kiev (boot record virus)

Virus info

Virus alias:	-
File size:	-
Virus type:	-
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Kit/VBSWormGen.150

Virus info

Virus alias:	VBS.AnnaKournikova.jpg VBS/OnTheFly
File size:	variable
Virus type:	Worm
Infected operating systems:	-
Damage:	Generates Internet worms (VB Script)
Discovered on:	16.02.2001
From VDF version:	6.23.00.00

General information

VBS Worm-Generator 1.5 easily generates Internet worms. Using its options, it choses the damage routines.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Lehigh

Virus info

Virus alias:	-
File size:	1280 bytes
Virus type:	Overwriting, resident COMMAND.COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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
```

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Liberty

Virus info

Virus alias:	-
File size:	2858 bytes
Virus type:	Memory-resident COM and EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Lisbon

Virus info

Virus alias:	-
File size:	648 bytes
Virus type:	Non memory-resident COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Macho

Virus info

Virus alias:	Syslock
File size:	3551 bytes
Virus type:	Non-resident .COM and .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Michelangelo (boot record virus)

Virus info

Virus alias: -
File size: -
Virus type: -
Infected operating systems: -
Damage: -
Discovered on: -
From VDF version: -

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

MIX

Virus info

Virus alias:	-
File size:	632, 1618, 1636 bytes
Virus type:	Resident .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Mummy

Virus info

Virus alias:	Platinum
File size:	1399-1414 bytes
Virus type:	Memory-resident .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Murphy

Virus info

Virus alias:	-
File size:	1614 bytes
Virus type:	Memory-resident COM and EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Music Bug (boot record virus)

Virus info

Virus alias:	-
File size:	-
Virus type:	-
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

MVF

Virus info

Virus alias:	Mad Virus Factory
File size:	1903 bytes
Virus type:	Resident .COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Natas

Virus info

Virus alias:	Satan
File size:	4744 bytes, memory 6144 bytes, 9 records HD/FD
Virus type:	Resident, stealth-type, polymorphic, multipartite
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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
```

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Neuroquila

Virus info

Virus alias:	<HAVOC>, Neuro.Havoc, Wedding
File size:	EXE programs: 4644-4675 bytes, hard disks & floppies: 9 records
Virus type:	Resident retrovirus, stealth-type, polymorphic, multipartite
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Neuroquila.N8FALL.A

Virus info

Virus alias:	Neuroquila, Art & Strategy, Nightfall
File size:	EXE programs: 4554-4585 bytes, memory: 4688 bytes
Virus type:	Resident retrovirus, stealth-type, polymorphic
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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

Virus info

Virus alias:	Neuroquila, Art & Strategy, Nightfall
File size:	EXE programs: 5801-5832 bytes, memory: 6048 bytes
Virus type:	Resident retrovirus, stealth-type, polymorphic
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Neuroquila.N8FALL.Companion

Virus info

Virus alias:	Neuroquila-Companion
File size:	COM programs: 527 bytes, memory: 672 bytes
Virus type:	Resident companion virus, semi-stealth type, fast infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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-
```

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

No Bock

Virus info

Virus alias:	-
File size:	440 bytes
Virus type:	Non-resident .COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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'.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

O97M/Cybernet.A

Virus info

Virus alias:	W97M/Cybernet@mm
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email, to the first 50 addresses found in Outlook
Discovered on:	30.05.2000
From VDF version:	6.20.00.00

General information

It infects the file "Normal.dot", which is delivered every time a Word document is opened. Then it creates the file "CyberNet.xls" in Excel start directory

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Ohio (boot record virus)

Virus info

Virus alias:	Den Zuk, Venzuelan
File size:	-
Virus type:	-
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Omega

Virus info

Virus alias:	-
File size:	440 bytes
Virus type:	.COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

One Half

Virus info

Virus alias:	FreeLove, Slovak Bomber
File size:	3544, 3577 bytes, memory 4096 bytes, 8 records HD/FD
Virus type:	Resident, stealth-type, polymorphic, multipartite
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Oropax

Virus info

Virus alias:	Music, Musician
File size:	2756 to 2806 bytes
Virus type:	Direct, resident .COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Parity (boot record virus)

Virus info

Virus alias:	Parity Check
File size:	-
Virus type:	-
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

PDF/Peach

Virus info

Virus alias:	VBS/PeachyPDF@MM
File size:	variable
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email to the first 100 addresses found in Outlook
Discovered on:	09.08.2001
From VDF version:	6.23.00.00

General information

The virus needs Adobe Acrobat to be installed, to spread on your system.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Perfume

Virus info

Virus alias:	4711, G
File size:	765 bytes
Virus type:	Resident .COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Ping Pong (boot record virus)

Virus info

Virus alias:	Bouncing Ball, Italian, Big Italian
File size:	-
Virus type:	-
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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:'.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Plastique

Virus info

Virus alias:	-
File size:	3004, 4096 bytes
Virus type:	Resident .COM and .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

RedX

Virus info

Virus alias:	Ambulance, Ambulance Car, Emergency
File size:	796 bytes
Virus type:	Non-resident .COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Sampo (boot record virus)

Virus info

Virus alias:	Wllop, Turbo
File size:	-
Virus type:	-
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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
```

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Silly Willy

Virus info

Virus alias:	-
File size:	COM files: approx. 2261 to 2314 bytes; .EXE files: 803 bytes are overwritten
Virus type:	Non memory-resident file virus
Infected operating systems:	-
Damage:	-
Discovered on:	1991
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Solano

Virus info

Virus alias:	-
File size:	2000 bytes
Virus type:	memory-resident COM and EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Stimulation

Virus info

Virus alias:	-
File size:	-
Virus type:	Extending file virus.
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Stoned (boot record virus)

Virus info

Virus alias:	New Zealand, Donald Duck
File size:	-
Virus type:	-
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

SubSeven (TR.Sub7)

Virus info

Virus alias:	-
File size:	varied
Virus type:	Trojan
Infected operating systems:	-
Damage:	-
Discovered on:	22.08.2000
From VDF version:	-

General information

SubSeven is a backdoor program (such as NetBus, Back Orifice etc), which gives a hacker access to a system.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Sunday Virus

Virus info

Virus alias:	-
File size:	1631 bytes
Virus type:	Resident .COM and .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Sylvia

Virus info

Virus alias:	Holland Girl
File size:	1332 bytes
Virus type:	Non memory-resident COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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...

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Tai Pan

Virus info

Virus alias:	Whisper
File size:	438 bytes
Virus type:	Resident .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Taiwan

Virus info

Virus alias:	-
File size:	708, 743 bytes
Virus type:	Non-resident .COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Tenbytes

Virus info

Virus alias:	V-Alert
File size:	1554 bytes
Virus type:	Resident .COM and .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Tequila

Virus info

Virus alias:	-
File size:	2468
Virus type:	Resident EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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!"

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

TR.Worm.Navidad

Virus info

Virus alias:	W32/Navidad@M
File size:	32,768 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	-
Discovered on:	10.01.2001
From VDF version:	-

General information

The Internet worm TR.Worm.Navidad is sent as email attachment from a contaminated computer. The attachment is named NAVIDAD.EXE

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

TR/DoS.Boxed.a

Virus info

Virus alias:	DDos.Win32.Boxed.d
File size:	26,694 Bytes
Virus type:	Trojan
Infected operating systems:	-
Damage:	-
Discovered on:	15.06.2004
From VDF version:	6.25.00.101

General information

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

TR/Dvldr

Virus info

Virus alias:	Backdoor.VNC-based, BackDoor-ARG.dr, Backdoor.Dvldr
File size:	212.992 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Is a Trojan, which enables unauthorized access to systems.
Discovered on:	01.01.2003
From VDF version:	6.xx.xx

General information

The Trojan secures VNC applications, after it names itself EXPLORER.EXE. It performs the installation of the file INST.EXE, which is used by the VNC application

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

TR/IWorm.Fix2001

Virus info

Virus alias:	I-Worm.Fix2001, W32/Fix, W95/Backdoor.Fix2001, W95.Fix2001
File size:	12,288 Bytes
Virus type:	Worm
Infected operating systems:	
Damage:	Sent by email.
Discovered on:	01.01.2003
From VDF version:	6.xx.xx.xx

General information

When activated, the worm installs itself on the local computer's Windows system directory under the same name as it was activated with.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

TR/Proxy.Bobax.b

Virus info

Virus alias:	W32.Bobax.B, TrojanProxy.Win32.Bobax.b, W32/Bobax.worm.b
File size:	21, 504 Bytes
Virus type:	Trojan
Infected operating systems:	
Damage:	Uses LSASS security hole, spreads by email.
Discovered on:	17.05.2004
From VDF version:	6.25.00.75

General information

When activated, the Trojan Proxy.Bobax.b makes a Mutex "04:12:20:%random number%". So it verifies if there is active any other of its own tasks on the system.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

TR/Proxy.Bobax.c

Virus info

Virus alias:	W32.Bobax.C, W32/Bobax.worm.c, TrojanProxy.Win32.Bobax.c
File size:	22,528 Bytes
Virus type:	Trojan
Infected operating systems:	-
Damage:	Uses LSASS security hole, spreads by email and listens on TCP Ports.
Discovered on:	18.05.2004
From VDF version:	6.25.00.79

General information

When activated, the worm Proxy.Bobax.c makes a mutex "06:08:07:%random number%". So it verifies if there is active any other of its own tasks on the system. It copies itself in %System%\%random characters %.exe and tries to make these two registry entries

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

TR/Proxy.Ranky.AE

Virus info

Virus alias:	Proxy-FBSR, Backdoor.Ranky.G
File size:	n/a
Virus type:	Worm
Infected operating systems:	-
Damage:	-
Discovered on:	21.06.2004
From VDF version:	6.25.00.101

General information

If activated, TR/Proxy.Ranky.AE opens a randomly chosen port, for enabling access of attackers commands.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

TR/Worm.QAZ

Virus info

Virus alias:	W32/QAZ.worm
File size:	120.320 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Backdoor function
Discovered on:	11.12.2000
From VDF version:	6.23.00.00

General information

Worm 'QAZ' is an executable .exe file and spreads over Windows 32-bit systems

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

TR/Worm.RC5.WinInit

Virus info

Virus alias:	Dnet.Dropper, W32/MsInit.worm.a [McAfee], Worm.Bymer.a [Kaspersky], TROJ_MSINIT.A [Trend], WORM_BYMER.A [Trend], W32/Bymer-A [Sophos], Win32.Bymer.A [Computer Associates], W32.HLLW.Bymer
File size:	variable
Virus type:	Worm
Infected operating systems:	
Damage:	Spreads on Intranet / Internet over shared drives
Discovered on:	01.01.2003
From VDF version:	6.xx.xx.xx

General information

There are two current versions of the worm: the first version comes as Wininit.exe file, the second one as Msinit.exe. They both have the same functionality, their routine being slightly different.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Traceback

Virus info

Virus alias:	-
File size:	2930, 3066 bytes
Virus type:	Resident .COM and .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Tremor

Virus info

Virus alias:	-
File size:	4000 bytes
Virus type:	Resident virus, stealth type, fast infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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
INT21H
MOV    AX,0F1E9H
INT21H
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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Tumen 0.5

Virus info

Virus alias:	-
File size:	1663 bytes
Virus type:	Memory-resident file virus
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Typo COM

Virus info

Virus alias:	Fumble
File size:	712, 867 bytes
Virus type:	Resident .COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

V163

Virus info

Virus alias:	-
File size:	163 bytes
Virus type:	Memory-resident COM and EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Vacsina

Virus info

Virus alias:	-
File size:	1339, 2764 (+ 132) bytes
Virus type:	Resident .COM, .EXE, .SYS and .BIN infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

VBS/Caroline.B

Virus info

Virus alias:	VBS/Australia.jpeg.vbs
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	16.02.2001
From VDF version:	6.23.00.00

General information

When activated, the worm copies itself in C:\%WINDir%\%SYSTEMDir% and makes a RUN entry in the registry

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

VBS/Elva

Virus info

Virus alias:	I-Worm.Elva
File size:	7.174 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	25.08.2000
From VDF version:	6.23.00.00

General information

The virus creates the file FS.VBE in C:\%WINDIR%\ and then copies it in C:\%WINDIR%\%SYSTEMDIR%\FS.VBS

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

VBS/Fireburn

Virus info

Virus alias:	VBS/Fireburn@MM
File size:	5.132 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email
Discovered on:	30.05.2000
From VDF version:	6.20.00.00

General information

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

VBS/Guorm

Virus info

Virus alias:	VBS/Gorum.a
File size:	-
Virus type:	Worm
Infected operating systems:	
Damage:	Sent by email.
Discovered on:	31.05.2000
From VDF version:	6.20.00.00

General information

The VB script multiplies itself as winuser.dll and user32.dll.vbs in Windows system directory.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

VBS/HappyTime

Virus info

Virus alias:	VBS/Haptime@MM
File size:	variable
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	06.06.2001
From VDF version:	6.23.00.00

General information

HappyTime is a VBS worm, with two damage routines: it deletes all .DLL and.EXE files in Windows directory and sends its wormcode via Outlook or Outlook Express.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

VBS/HomePage.1

Virus info

Virus alias:	VBS/SST.gen@MM
File size:	variable
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	15.05.2001
From VDF version:	6.23.00.00

General information

When the attachment is opened, the worm spreads and deletes all emails having the subject 'Homepage', from "Inbox" and "Deleted Items".

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

VBS/Lee-ATX

Virus info

Virus alias:	VBS/Anthrax
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email
Discovered on:	22.10.2001
From VDF version:	6.23.00.00

General information

VBS/Lee-ATX sends itself to all email addresses found in Outlook Address Book.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

VBS/LiveStages.A

Virus info

Virus alias:	VBS.Stages.A
File size:	39.936 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email to 100 Outlook addresses.
Discovered on:	20.06.2000
From VDF version:	6.01.00.14

General information

The virus file extension will not be shown in Windows.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

VBS/LoveLetter

Virus info

Virus alias:	VBScript Virus
File size:	variable
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	05.05.2000
From VDF version:	6.20.00.00

General information

According to Windows- and Email system settings, the file extension ".vbs" can be shown or hidden.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

VBS/LoveLetter.BD

Virus info

Virus alias:	-
File size:	12.607 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	18.08.2000
From VDF version:	6.20.00.00

General information

The virus makes a registry entry for skipping

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

VBS/LoveLetter.CM

Virus info

Virus alias:	VBS.LoveLetter.C
File size:	17.245 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	01.06.2001
From VDF version:	6.23.00.00

General information

If the file JENNIFERLOPEZ_NAKED.JPG.vbs is opened, the worm copies itself in c:\windows.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

VBS/Netlog.Worm

Virus info

Virus alias:	Network.vbs
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over shared directories.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

VBS/Netlog is written in Visual Basic Scrip

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

VBS/NeueTarife

Virus info

Virus alias:	VBS/VBSWG.K@MM
File size:	VBS/VBSWG.K@MM
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	16.02.2001
From VDF version:	6.23.00.00

General information

The version "Neue Tarif.txt.vbs" creates in C:\MIRC a file named SCRIPT.INI and then copies itself as C:\%WINDIR%\Neue Tarife.txt.vbs.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

VBS/Redlof.A

Virus info

Virus alias:	VBS/Redlof, VBS/Redlof@M
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	-

General information

VBS/Redlof.A starts directly from an infected message, using an Internet Explorer security hole, known as Microsoft VM ActiveX Control security hole.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

VBS/SST.A

Virus info

Virus alias:	-
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email
Discovered on:	13.02.2001
From VDF version:	6.23.00.00

General information

The worm sends itself by email, to addresses found in Outlook.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

VBS/Staple.A

Virus info

Virus alias:	VBS/Staple.a@MM
File size:	12.992 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email to the first 50 Outlook addresses.
Discovered on:	21.03.2001
From VDF version:	6.23.00.00

General information

VBS/Staple.A is a VBS (Visual Basic Script)worm and sends itself using Microsoft Outlook to the first 50 addresses found in Outlook Address Book.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

VBS/Vierika

Virus info

Virus alias:	VBS/Vierika@MM
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	14.03.2001
From VDF version:	6.23.00.00

General information

VBS/Vierika is an Internet worm, programmed in Visual Basic Script. The worm code was directly implemented in the HTML document Vindex2.html and is available on a GeoCities website, to start when the site is launched, automatically.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

VGen

Virus info

Virus alias:	-
File size:	-
Virus type:	-
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Victor

Virus info

Virus alias:	-
File size:	2442 to 2458 bytes
Virus type:	Memory-resident COM and EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Vienna

Virus info

Virus alias:	DOS-62, Blue Danube, Wiener, P, Unesco, Austrian
File size:	648 bytes
Virus type:	Non-resident .COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Vriest

Virus info

Virus alias:	-
File size:	1280 bytes
Virus type:	Resident .COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

W32/Aliz

Virus info

Virus alias:	I-Worm.Aliz, W32/Aliz@MM, W95/Aliz.A,W32.Aliz.Worm
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

W32/Aliz is an SMTP mass mailer worm, written in assembly and packed. The worm copies itself only on Win9X operating systems. It can not make copies on NT platforms. It takes from Windows Address Book the addresses it sends emails to.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/Apost.A

Virus info

Virus alias:	Worm/Readme
File size:	24.576 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	06.09.2001
From VDF version:	6.23.00.00

General information

W32/Apost is an Internet worm, programmed in Visual Basic 6. If the worm is activated, a window appears indicating a false WinZip error message. When the user clicks on "Aceptar" button, the worm sends itself by email, using Microsoft Outlook Address Book. After sending emails, another window appears.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/Beast

Virus info

Virus alias:	W95/Beast, W95/Beast.41472.A, Macro.Word97.Beast
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Copies itself in Office documents and it can open and close the CD-Rom drive.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

The virus creates a file in System or System32 directory. It chooses a random name and uses it, but with .exe extension, to be activated. For example: it uses Shell.dll and names its copy Shell.exe. This happens when an infected document is opened and the inserted virus is activated.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/Elkern.B

Virus info

Virus alias:	Win32.Elkern.b, W32/Elkern.cav, W95/Elkern.B, W32.ElKern (dr)
File size:	3587 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	W32/Elkern.B tries to infect different files. It attacks over networks..
Discovered on:	30.11.1999
From VDF version:	-

General information

W32/Elkern.B is a virus which creates files over shared and mapped drives. It also tries to infect all executable files from \%WinDIR%\%SystemDIR%. If the worm is activated on Windows 9x system and there are write-protected mapped networks, the computer crashes shortly. Some infected files do not modify their size.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/Elkern.C

Virus info

Virus alias:	Win32.Elkern.c [AVP], W32/Elkern.C [Sophos], Win32/WQK.C [CA], PE_ELKERN.D [Trend], W32/Elkern.cav.c [McAfee], W32.ElKern.4926
File size:	4,926 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	-

General information

The virus infects randomly chosen PE files. It scans the drives, starting with a certain letter, until it reaches Z. It can also infect files from shared network sources.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/ExploreZip

Virus info

Virus alias:	Worm.Explore.Zip, Zipped Files, Troj.Explore.Zip
File size:	210.432 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads using Outlook, Exchange or NetScape Mail
Discovered on:	11.06.1999
From VDF version:	6.20.00.00

General information

When the infected attachment is opened, an error message appears on the screen.

The virus is already active and "at work". It copies itself as "Explore.exe" or "setup.exe" in System directory: %windir%\%SystemDir% (usually c:\windows\system) on Windows 9x, or %windir%\%SystemDir% (usually c:\winnt\system32) on Windows NT.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/FBound.C

Virus info

Virus alias:	-
File size:	12.288 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	11.03.2002
From VDF version:	6.23.00.00

General information

The worm's size is 12.228 Bytes and it has no further damage routine. It does not create any files or registry entries and it is inactive, when the infected system restarts.

It only creates a file in C:\%WINDIR%\TEMP\, used for spreding.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/Fono98

Virus info

Virus alias:	Win95.Fono.15327, W95/Fono.mp, Fono.17152.A, W95.Fono (vxd)
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over IRC ports.
Discovered on:	30.11.1999
From VDF version:	-

General information

The worm uses mIRC to spread over IRC port on Internet.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/Funlove.4099

Virus info

Virus alias:	Win32_FLC, Win32.FLC, FLCSS
File size:	4,099 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	-
Discovered on:	12.11.1999
From VDF version:	-

General information

W32/Funlove.4099 is a hard-disk memory resident Win32 virus. It is not encoded or multi-level. The virus infects .exe files on the local drives and network drives. When an infected file is run, the virus makes the file FLCSS.EXE in Windows system. It only writes its code there and runs the generated file.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/Hai.A

Virus info

Virus alias:	Worm.Hai, W32/Hai.Worm, W95/Hai.A, W32.HLLW.Hai
File size:	69,635 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over shared directories.
Discovered on:	30.11.1999
From VDF version:	-

General information

W32/Hai.A spreads over networks, looking for a computer with NetBIOS protocol installed and full access for all users to \Windows directory. The worm drops a new thread in computers with open access to directories.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/Hantaner

Virus info

Virus alias:	W32/HLLP.Hantaner [McAfee], Win32.HLLP.Hantaner [KAV], PE_HANTANER.A [Trend], Win32.HLLP.Handy [CA], W32/Hantaner-A [Sophos]
File size:	24,064 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over KaZaA
Discovered on:	30.11.1999
From VDF version:	-

General information

The worm spreads over KaZaA, infecting .exe files. Other KaZaA users may infect their own systems, by downloading infected files.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/Jeefo

Virus info

Virus alias:	W32/Jeefo [McAfee], PE_JEEFO.A [Trend]
File size:	36,352 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	W32/Jeefo tries to infect PE files.
Discovered on:	30.11.1999
From VDF version:	-

General information

When an W32/Jeefo infected file is opened, the file SVCHOST.EXE (36,352 Bytes) in %WinDIR% is created.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/Klez

Virus info

Virus alias:	W32/Klez.gen@MM
File size:	57,345 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	-
Discovered on:	26.10.2001
From VDF version:	-

General information

The virus W32/Klez is sent as .EXE file, spreads over Windows32-bit systems and infects .EXE files. To make sure that the resident virus remains on the memory, W32/Klez will also infect the KERNEL32.DLL.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/Klez.A

Virus info

Virus alias:	Win32.Elkern.a, W32/Elkern.cav, W95/Elkern.A, W32.ElKern.gen
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over local networks.
Discovered on:	30.11.1999
From VDF version:	-

General information

When an infected file is opened on Win98/ME system, the worm copies the file in \%WINDIR%\ %SYSTEMDIR% directory, as WQK.EXE hidden file. This file has variable size and content.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/Kriz

Virus info

Virus alias:	W32/Kriz@MM
File size:	variable
Virus type:	Worm
Infected operating systems:	-
Damage:	It is sent as .EXE file, spreads on Windows 32-bit systems and infects .EXE files. It also changes the area of the Windows commands .
Discovered on:	22.12.2000
From VDF version:	6.23.00.00

General information

W32.Kriz is sent as .EXE file, spreads itself on Windows 32-bit systems and infects .EXE files. It also changes the area of Windows commands. The worm also infects KERNEL32.DLL, to become a memory resident virus.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/Lovesong.998

Virus info

Virus alias:	Win95.LoveSong.998, W95/Lovesong, W95.Lovesong.998
File size:	998 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Infects all files it can access.
Discovered on:	30.11.1999
From VDF version:	-

General information

When an infected file is opened, the virus is loaded in memory and infects all files it can access. The virus code is placed in .reloc part of the 32-bit executable. If this part of the file is not big enough, the virus eventually corrupts the file. The access technique is based on the one used by W95/CIH.A.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/Magistr.B1

Virus info

Virus alias:	Worm.Magistr.b [Kaspersky], W32.Magistr.B@mm, W32/Magistr.b@MM [McAfee], W32/Magistr.32768@mm [Frisk], PE_Magistr.B [Trend], W32/Magistr-B [Sophos], Win32.Magistr.29188 [Computer Associates]
File size:	39,921 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	-

General information

The difference between the original and this version of the worm is: a different kind of damage routine. The virus overwrites the file WIN.Com in Windows directory and the file NTLDR on C: level with a program, which deletes important drive data on start. If the computer is infected over network, the worm inserts iteslf in WIN.INI and SYSTEM.INI. The virus searches for GIF files and sends GIF pictures from the infected computer, just as it can send clean DOC files. The worm destroys *.NTZ files if it can detect them. It tries to terminate ZoneAlarm firewall, if installed.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/Naked

Virus info

Virus alias:	-
File size:	73.728 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	07.03.2001
From VDF version:	6.23.00.00

General information

If the attachment NAKEDWIFE.EXE is opened, a false Macromedia Flash Player program opens. On the same time, the virus sends itself to all addresses in MS Outlook.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/Navidad.B

Virus info

Virus alias:	Navidad.E, I-Worm.Navidad.b, W32/Navidad, W95/Navidad.16896
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	-

General information

The worm uses MAPI to send emails and works with Microsoft Outlook. It searches all inbox messages and answers to all messages which have an attachment. The answer email has the same subject and body as the received email. Attachment: Emanuel.exe.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/Nimda

Virus info

Virus alias:	W32/Nimda.gen@MM
File size:	57,344 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	-
Discovered on:	18.09.2001
From VDF version:	-

General information

W32/Nimda is an Internet virus that can send itself by email, as a mass mailer. It can be activated on all Microsoft Windows 9x/Me and NT/2000 Platforms. Nimda sends itself as email attachment. These attachments are named README.EXE, the extension being usually unlisted.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/Nimda (W32/Nimda.eml)

Virus info

Virus alias:	W32/Nimda.gen@MM
File size:	57.344 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	W32/Nimda is an Internet worm, which can send itself in email attachment, as a mass mailer .
Discovered on:	18.09.2001
From VDF version:	6.23.00.00

General information

If README.EXE is automatically opened, or double-clicked, the worm copies itself in Windows temp directory. It creates a file with a variable name of type MEvariable.TMP.EXE. This file is opened and then deleted by system start under Windows 9x/ME. Then, the worm copies itself in Windows and System directories.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/Nimda.eml

Virus info

Virus alias:	W32/Nimda.A@mm, W32/Nimda@mm, I-Worm.Nimda, Readme, Readme.exe
File size:	57,344 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email, Backdoor component.
Discovered on:	30.11.1999
From VDF version:	-

General information

The worm serches all '.htm' and '.html' files in existing Internet directory for email addresses. It scans the user's Inbox and collects senders' addresses. After finishing the address list, it uses its own SMTP engine to send the infected messages.

Attachment: README.EXE

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/Parite

Virus info

Virus alias:	Win32.Parite.a [KAV], W32/Pate.a [McAfee], Win32.Pinfi.A [CA], PE_PARITE.A [Trend], W32/Parite-A [Sophos], Win32/Parite.A [RAV], W32.Pinfi
File size:	~177,917 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over shared network resources.
Discovered on:	30.11.1999
From VDF version:	-

General information

W32/Parite spreads over shared network resources.
If a file infected with W32/Parite is opened, it registers: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersi on\Explorer PINF

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/Parite.tmp

Virus info

Virus alias:	Win32.Parite.a [KAV], W32/Pate.a [McAfee], Win32.Pinfi.A [CA], PE_PARITE.A [Trend], W32/Parite-A [Sophos], Win32/Parite.A [RAV], W32.Pinfi
File size:	~177,917 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over shared network resources.
Discovered on:	30.11.1999
From VDF version:	-

General information

W32/Parite.tmp spreads over shared network resources.
f a file infected with W32/Parite is opened, it registers: HKEY_CURRENT_USER\Software\Microsoft\ Windows\CurrentVersi on\Explorer PINF

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/Partie.B

Virus info

Virus alias:	PE_PARITE.A (Trend), W32.Pinfi (Symantec), W32/Parite-B (Sophos), W32/Parite.B (F-Prot), W32/Parite.B (Panda), W32/Pate.a, W32/Pate.b.dll, W32/Pate.b.tmp, Win32.Parite.b (AVP), Win32.Pinfi.A (CA)
File size:	177 kB
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over shared network resources.
Discovered on:	30.11.1999
From VDF version:	-

General information

W32/Partie.B attaches PE EXE and SCR files in Windows directory and in its subdirectories. It does not keep its original size.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/Perrum

Virus info

Virus alias:	-
File size:	11.780 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over .JPG files.
Discovered on:	14.06.2002
From VDF version:	6.23.00.00

General information

W32/Perrum is a Windows virus, which infects .JPG files. It is programmed in Visual Basic and packed with UPX.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/PrettyPark

Virus info

Virus alias:	Trojan Horse, W32.PrettyPark, Trojan.PSW.CHV, CHV, W32/Pretty.worm.unp, I-Worm.PrettyPark [Kaspersky], W32/Pretty.gen@MM [McAfee], W32/Pretty [Sophos], WORM_PRETTYPARK [Trend]
File size:	37,376 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	-

General information

When activated, W32/PrettyPark starts Windows 3D Pipes screen saver.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/ProLin@mm

Virus info

Virus alias:	-
File size:	36.864 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	05.12.2000
From VDF version:	6.23.00.00

General information

The Internet worm tries to send itself over Outlook to all addresses in the Address Book. The email's structure:

Subject: A great Shockwave flash movie

Body: Check out this new flash movie that I downloaded just now ... It's Great Bye Attachment: CREATIVE.EXE

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/Vote (Variations .a, .b & .

Virus info

Virus alias:	-
File size:	55,808 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	24.09.2001
From VDF version:	6.23.00.00

General information

W32.Vote is a mass mailer, written in Visual Basic. It spreads using Microsoft Outlook, sending itself to all addresses found in the Address Book.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/Xorala

Virus info

Virus alias:	-
File size:	2048 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	W32/Xorala infects selected files.
Discovered on:	30.11.1999
From VDF version:	-

General information

When W32/Xorala is activated, it infects active Win32 files in C:/%WinDir% and C:/%SystemDIR% directories. The virus infects the files by adding a string named "XOR" at the end of the final sector of the host.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/Yaha.E

Virus info

Virus alias:	I-Worm.Lentin.f
File size:	29.839 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	19.06.2002
From VDF version:	6.23.00.00

General information

Worm/Yaha.E is a mass mailer, which sends itself by email to addresses collected from the local * .HT* files, Windows Address Book , MSN Messenger, ICQ and Yahoo Messenger. The attachment of the email has the extension .BAT, .PIF or .SCR.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W32/YAWsetup

Virus info

Virus alias:	-
File size:	437.760 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	26.02.2002
From VDF version:	6.23.00.00

General information

The worm searches the hard drive for files of type *.htm, *.php, *.cgi, *.pl, *.shtm and gathers email addresses from them. Then, the worm sends itself to all collected addresses and to the addresses found in Microsoft Outlook. The worm is disguised as a newsletter from www.trojaner-info.de.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W64/Rugrat.3344

Virus info

Virus alias:	W64/Rugrat, W64.Rugrat.3344
File size:	3,344 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Infects WIN PE 64-bit files.
Discovered on:	26.05.2004
From VDF version:	6.25.00.81

General information

W64/Rugrat.3344 is a file infector, attacking only 64-bit Windows platforms. It is the first infector that infects 64-bit Windows executable files.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W95/Begemont.B

Virus info

Virus alias:	Magistr
File size:	30 KB
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	20.03.2001
From VDF version:	6.23.00.00

General information

W95/Begemont.B spreads over Internet, by sending infected emails on Outlook Express, Netscape Messanger or Internet Mail and News. For doing this, the worm reads all settings of the email Clients directly from the registry.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W95/CIH

Virus info

Virus alias:	PE_CIH, CIH, Tschernobyl, Spacefiller
File size:	varied
Virus type:	Worm
Infected operating systems:	-
Damage:	-
Discovered on:	10.08.1998
From VDF version:	-

General information

W95/CIH runs only on Windows 95/98. It only infects 32bit program files (Windows EXEs, PE files). When an infection file is first opened on an uninfected computer system, it enters the PageAllocate memory and there it places a copy of its infectious code. Then it copies the rest of its program parts. Probably because of a mistake in the program, the virus uses 8KB, when 4KB would have been enough.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W95/CIH.A

Virus info

Virus alias:	Chernobyl, PE_CIH, Win95.CIH, Win32.CIH, W95/CIH.1003, CIH.Spacefiller
File size:	up to 1 KB
Virus type:	Worm
Infected operating systems:	-
Damage:	Deletes files and provokes posible damage to CMOS
Discovered on:	30.11.1999
From VDF version:	-

General information

W95/CIH.A is a 32-bit Window95/98/ME virus which infects executable files. It works on Windows 95/98 or ME, but not on Windows NT or 2000. Among others, the virus also infects antivirus programs. The virus does not function on DOS, Windows 3.1 or Macintosh computers.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W95/CIH-1049

Virus info

Virus alias:	Bloodhound.W32.EP, W32/Elkern.C, Win95.CIH.1049, W95/CIH
File size:	1049 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Deletes files and provokes possible damage to CMOS
Discovered on:	30.11.1999
From VDF version:	-

General information

W95/CIH-1049 is a 32-bit Window95/98/ME virus which infects executable files. It works on Windows 95/98 or ME, but not on Windows NT or 2000. Among others, the virus also infects antivirus programs. The virus does not function on DOS, Windows 3.1 or Macintosh computers.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W95/Dupator.1503

Virus info

Virus alias:	W32/Dupator [McAfee], Win95.Dupator.1503 [KAV], PE_DUPATOR.1503 [Trend], Mid/W95/Dupator [Sophos]
File size:	1,503 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Hangs on Windows PE files.
Discovered on:	30.11.1999
From VDF version:	-

General information

When an infected file is opened, the virus copies the file Kernel32.dll from \Windows directory to \System directory; it inserts its code into the file Kernel32.dll in Windows directory and includes the executable command GetFileAttributesA in its code.

When the computer is restarted, the virus uses the infected Kernel32.dll file, to infect Windows PE files.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W95/Fono

Virus info

Virus alias:	Win95.Fono.15327, W32.Opaserv.Worm
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads through IRC ports.
Discovered on:	30.11.1999
From VDF version:	-

General information

The worm uses mIRC to spread through IRC ports over the Internet.
When W95/Fono is activated on Windows 95/98 computers, it creates the file C:\WINDOWS\SYSTEM\FONO98.VXD with hidden properties. It modifies files from C:\WIN95INCA.COM.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W95/Hybris

Virus info

Virus alias:	-
File size:	25.088 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	01.12.2000
From VDF version:	6.23.00.00

General information

If Windows uses WSOCK32.DLL and the worm can not change it, it makes a copy of the file, modifies the copy and using WININIT.INI, it will cause the replacement of the original with the altered file by the next system start.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W95/Hybris.Gen.1

Virus info

Virus alias:	dwarf4you.exe, Hybris, I-Worm.Hybris , I-Worm.Hybris.b, Snowhite and the Seven Dwarfs, TROJ_HYBRIS.A, W32/Hybris.dll@M , W32/Hybris.plugin@M, W95.Hybris.Gen.dr, W95/Hybris.worm, Win98.Vecna.23040
File size:	25,088 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over Newsgroups.
Discovered on:	30.11.1999
From VDF version:	-

General information

When first activated, W95/Hybris.Gen.1 tries to infect WSOCK32.DLL in %WinDIR%/%SystemDIR%.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W95/Hybris.Gen.2

Virus info

Virus alias:	dwarf4you.exe, Hybris, I-Worm.Hybris , I-Worm.Hybris.b, Snowhite and the Seven Dwarfs, TROJ_HYBRIS.A, W32/Hybris.dll@M , W32/Hybris.plugin@M, W95.Hybris.Gen.dr, W95/Hybris.worm, Win98.Vecna.23040
File size:	25,088 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over newsgroups.
Discovered on:	30.11.1999
From VDF version:	-

General information

When first activated, W95/Hybris.Gen.2 tries to infect WSOCK32.DLL in %WinDIR%/%SystemDIR%.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W95/Hybris.Gen.3

Virus info

Virus alias:	dwarf4you.exe, Hybris, I-Worm.Hybris , I-Worm.Hybris.b, Snowhite and the Seven Dwarfs, TROJ_HYBRIS.A, W32/Hybris.dll@M , W32/Hybris.plugin@M, W95.Hybris.Gen.dr, W95/Hybris.worm, Win98.Vecna.23040
File size:	25,088 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over newsgroups.
Discovered on:	30.11.1999
From VDF version:	-

General information

When first activated, W95/Hybris.Gen.3 tries to infect WSOCK32.DLL in %WinDIR%/%SystemDIR%.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W95/Hybris.PI.003

Virus info

Virus alias:	W32/Hybris.dll@MM, W95/Hybris.worm.B, W95.Hybris.gen
File size:	25,088 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over Newsgroups.
Discovered on:	30.11.1999
From VDF version:	-

General information

When first activated, W95/Hybris.PI.003 tries to infect WSOCK32.DLL in %WinDIR%/%SystemDIR%.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W95/Kriz.4050

Virus info

Virus alias:	Win32_Kriz, Win32.Kriz, W32.Kriz, W95/Kriz.4050
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	W95/Kriz.4050 infects various .exe files. These execute different actions when system restarts.
Discovered on:	30.11.1999
From VDF version:	-

General information

For infecting KERNELL32.DLL, the virus saves this file as KRIZED.TT6 and then changes it. By the next system start, the file KERNEL32.DLL is replaced with KRIZED.TT6, thanks to an entry made in WININIT.INI
The virus has an additional damage routine in its code: on December, 25th, the CMOS memory crashes, all files of the drive are overwritten and it tries to crash Flash BIOS.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W95/MTX

Virus info

Virus alias:	Iworm_MTX, I-Worm.MTX, Matrix
File size:	18.483 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email, Backdoor component.
Discovered on:	09.11.2000
From VDF version:	6.23.00.00

General information

MTX has three components: virus, email worm and backdoor.
The virus is first decoded and then executed. Then, the virus decompresses its components and installs them in Windows directory.
The worm uses the file WSOCK32.DLL in Windows directory, adding parts of its code at the end of the file and a send command. Thus, the worm controls all emails sent from the infected system. The worm detects when an email is composed an tries to attach a second email. This one contains no subject and body.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W95/MTX.dr

Virus info

Virus alias:	W95.Oisdbo, W95.MTX.dr, W95.MTX (.dll), W32/Apology-B [Sophos], I-Worm.MTX [Kaspersky], W95/MTX@M [McAfee], PE_Mtx.A [Trend], Win95.Mtx [Computer Associates], W95.MTX.dr
File size:	~9250 Bytes (variabel)
Virus type:	Worm
Infected operating systems:	-
Damage:	W95/MTX.dr searches for antivirus programs and terminates various files.
Discovered on:	30.11.1999
From VDF version:	-

General information

W95/MTX.dr has a worm and a virus component.
The worm component copies the file Wsock32.dll and renames it Wsock32.mtx.
The worm uses WININIT.INI to avoid deleting Wsock32.dll and renaming Wsock32.mtx in Wsock32.dll.
When this is done, the virus component comes in.
The Virus Component searches for antivirus programs. If it can find one, the virus decompresses the worm component, makes a copy in user's folder and executes it. The name of this file is Ie_pack.exe.
After execution, Ie_pack.exe is renamed as Win32.dll. It searches for WinDir files in the current, Windows and Temp directories.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W95/Spaces.1445.B

Virus info

Virus alias:	W95.Spaces.1633, W95.Spaces.1245, W95.Spaces.1445, W95/Busm.1445, W95/Busm99.1445
File size:	1,633 oder 1,245 oder 1,445 By
Virus type:	Worm
Infected operating systems:	-
Damage:	-
Discovered on:	30.11.1999
From VDF version:	-

General information

The virus has two known versions, adding 1,633 or 1,245 Bytes at the end of PE files.

When the virus is activated, it makes an active copy of itself in memory, which calls VxDcallIFSMgr_Get_Version and passes by AX Register 0x2020. On return it is 0xDEAD, if the virus is active in memory. In this case, the virus checks the date, because its routine starts on the 1st of June every year and corrupts the AT harddisk.

If the virus is not in memory, it allocates the memory by itself and attaches the system file. In this way, it can infect all .exe file it can access.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W95/Weird.10240.a

Virus info

Virus alias:	Win32.Weird, W95.Weird
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	W95/Weird.10240.a creates various files.
Discovered on:	30.11.1999
From VDF version:	-

General information

W95/Weird.10240.a inserts a hidden process, opens an IP address and waits for instructions. This hidden process resembles other Client/ Server Trojans, as NetBus, Backdoor and BackOrifice.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

W97M/Resume.A

Virus info

Virus alias:	W97M.Melissa.BG
File size:	41.472 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	W97/Resume.A tries to delete all files on harddisk and network.
Discovered on:	28.05.2000
From VDF version:	6.01.00.09

General information

The worm is hiding in an MS Word Document. It sends itself to all addresses saved in Outlook Address Book.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Whale

Virus info

Virus alias:	Motherfish, Z the whale
File size:	9216 bytes
Virus type:	Resident .COM and .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Wiener

Virus info

Virus alias:	DOS-62, Blue Danube, Vienna, P, Unesco, Austrian
File size:	648 bytes
Virus type:	Non-resident .COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Win95/Lorez

Virus info

Virus alias:	Win95.Lorez.1766.a, W95/Lorez, W95/Lorez.1766, W95.LoRez
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Win95/Lorenz infects .exe files.
Discovered on:	30.11.1999
From VDF version:	-

General information

Win95/Lorez infects all .exe files it has access to. It modifies Kernel32.dll file and saves it in C:\%WinDIR%.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

WinWord.Concept

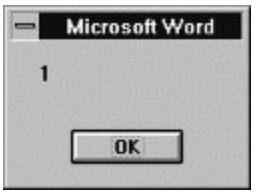
Virus info

Virus alias:	WW6Macro
File size:	-
Virus type:	Macro virus
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

WitCode

Virus info

Virus alias:	-
File size:	974 bytes
Virus type:	.EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Worm./Bagle.F

Virus info

Virus alias:	W32.Beagle.A@mm, Win32.Bagle.Gen@mm, i-Worm.Bagle.f
File size:	~24KB (PEX packed)
Virus type:	Worm
Infected operating systems:	-
Damage:	Sends itself by email * Open TCP port 2745 * Presence of the mentioned registry entries * Presence of the mentioned files * Increased email traffic
Discovered on:	29.02.2004
From VDF version:	6.24.00.27

General information

Worm/Bagle.F has a variable file size of ~24KB. The file is packed with PEX. The attachment of the email is in a ZIP format or it could also be an executable program type. It will copy itself into the %System% folder.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm./Bagle.H

Virus info

Virus alias:	W32.Beagle.H@mm, Win32.Bagle.Gen@mm, i Worm.Bagle.H
File size:	~21KB (Pex packed)
Virus type:	Worm
Infected operating systems:	-
Damage:	Sends itself as email * Open TCP port 2745 * Presence of the mentioned registry entries * Presence of the mentioned files * Increased email traffic
Discovered on:	01.03.2004
From VDF version:	6.24.00.32

General information

Worm/Bagle.H has a variable file size of ~24KB. The file is packed with PEX. The worm will copy itself in %System% folder.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/AceBot

Virus info

Virus alias:	Worm.Newbiero.54, W32.HLLW.Acebot,W32/AceBot.worm
File size:	variable, ~163,840 byte
Virus type:	Worm
Infected operating systems:	-
Damage:	Worm/AceBot allows hackers to attack the infected system and makes entries.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

Worm/AceBot is a typical Backdoor Trojan, allowing hackers to access infected PCs unnoticed. There are more known versions of Worm/AceBot. The size is ~163,840 bytes. When activated, the worm copies itself in \Windows\System with a random name.
The worm can spread over local networks through shared directories.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Anacon

Virus info

Virus alias:	W32.Naco.B@mm, Nocana.b
File size:	86,016 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Mass mailer, DoS attacker, backdoor The appearance of the files and registry entries written below.
Discovered on:	26.05.2003
From VDF version:	6.19.00.21

General information

Worm/Anacon has a file size of 86,016 bytes. It was programmed in Microsoft Visual Basic, therefore it needs its Runtime Libraries to activate its viral code. When activated, Worm/Anacon copies itself as "syspoly32.exe".

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Anset.b

Virus info

Virus alias:	W32/Anset@MM W32.Anset.Wourm
File size:	179.712 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Worm/Anset.b opens its attachment and makes a Registry entry.
Discovered on:	25.10.2001
From VDF version:	6.23.00.00

General information

Worm/Anset.b is a 179.712 Bytes file and is packed with UPX.

When the attachment ANTS3SET.EXE is activated, the worm copies an .EXE file in Windows directory with a random name.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Aphex

Virus info

Virus alias:	W32/Aplore.A
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over email, IRC or AIM.
Discovered on:	10.04.2002
From VDF version:	6.23.00.00

General information

When the attachment is opened, the worm is copied as Explorer.exe and psecure20x-cgi-install.vers.... in Windows directory and enters the following key in the registry:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVers ion\Run\Explorer=C:\%WinDIR%\ %SystemDIR%\Explorer.exe
It sends itself as email with Microsoft Outlook, using the Outlook Address Book.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Aphex.1

Virus info

Virus alias:	W32.Aphex@mm, Bloodhound.VBS.Worm, I-Worm.Aphex,
File size:	319,488 Bytes, variable.
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over Outlook Express, Mirc, Xirc, AIM, MSN, WebServer.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

The worm is a mass mailer, which spreads using its own webserver on port 8180.

When activated, the worm creates a VBScript in C:\%SystemDir%\Email.vbs.

This file is sent to all addresses found in Windows Address Book. Then the worm closes Outlook Express and deletes the file.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Aphex.2

Virus info

Virus alias:	I-Worm.Aplore, W32/Aplore@MM
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Worm/Aphex.2 makes a registry entry and copies itself.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated, the worm copies itself in System directory as "EXPLORER.EXE"

The worm sends itself to all email addresses it can find in the Address Book.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Aphex.3

Virus info

Virus alias:	I-Worm.Aphex, Psec. Aplore.A
File size:	319.488 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Worm/Aphex.3 makes a registry entry and prompts the user to download it.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When the worm is activated, it copies itself in Windows System directory as "explorer.exe".

The Visual Basic file "email.vbs" contains the damage routine and is attached to the virus email.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Avril.A

Virus info

Virus alias:	Worm/Naith.A
File size:	32,766 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	- On the 7th and 24th of the month a picture appears on the Windows desktop and the URL http://www.avril-lXXXXXe.de/ is run with the standard browser. - Terminates running processes, antivirus and firewalls applications, for example.
Discovered on:	01.07.2003
From VDF version:	-

General information

Worm/Avril.A (32,766 bytes) has its own SMTP engine. Therefore it does not need Outlook or any other email program, to send its emails.

Worm/Avril.A sends itself by email, using its SMTP engine and the IRC-program mIRC.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Avril.A.2

Virus info

Virus alias:	W32/Lirva.B, W32.Arvil.A, W32.Naith.A, Avril, Avron
File size:	34,815 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Worm/Avril.A.2 makes registry entries and tries to terminate various active processes.
Discovered on:	30.11.1999
From VDF version:	-

General information

Avril.A.2 brakes off some antivirus programs and security applications. It tries to find passwords in the system and to send them to an email address. It looks for email addresses in files. The email sent by the worm is in HTML format, packed with UPX.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Avril.B

Virus info

Virus alias:	Worm/Naith.B
File size:	34,815 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	On the 7th and 24th of the month a picture appears on the Windows desktop and the URL http://www.avril-IXXXXXe.de/ is run with the standard browser. Terminates running processes, antivirus and firewalls applications.
Discovered on:	07.01.2003
From VDF version:	-

General information

Worm/Avril.B (34,815 bytes) has its own SMTP engine. Therefore it does not need Outlook or any other email program, to send its emails.

Worm/Avril.B sends itself by email, using its SMTP engine. It spreads itself with the IRC-program mIRC, ICQ, file-sharing program KaZaA and mapped network drives.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Avron.A.INI

Virus info

Virus alias:	W32/Lirva.B, W32.Arvil, W32.Naith.B, Avril, Avron.B
File size:	34,815 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Avron sends itself over ICQ, Kazaa, mIRC and open net resources.
Discovered on:	30.11.1999
From VDF version:	-

General information

Worm/Avron.A.INI is an IRC Worm. Hundreds of versions are known.

The worm uses a mIRC script to send itself to all IRC users. However, there can be various spreading methods used by the worm's versions.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Avron.C.INI

Virus info

Virus alias:	I-Worm.Avron.b, MIRC/Generic, mIRC/Lirva.A, W32.Lirva@mm
File size:	34,815 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Avron sends itself over ICQ, Kazaa, mIRC and open net resources.
Discovered on:	30.11.1999
From VDF version:	-

General information

Worm/Avron.C.INI is an IRC Worm. It has hundreds of versions.

The worm uses a mIRC script to send itself to all IRC users. However, there can be various spreading methods used by the worm's versions.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Badtrans

Virus info

Virus alias:	W32/BadTrans@MM
File size:	13.312 Bytes Version A, 29.02
Virus type:	Worm
Infected operating systems:	-
Damage:	Worm/Badtrans makes registry entries and copies itself many times.
Discovered on:	26.04.2001
From VDF version:	6.23.00.00

General information

When the infected file is opened, the worm installs its components on the system. The worm copies itself as INETD.EXE in Windows directory. The Trojan component is copied in Windows as HKK32.EXE and executed. The Trojan moves to Windows System with the name KERN32.EXE and it installs HKSDLL.DLL in the same directory.

The worm opens all read or unread emails in Outlook or Outlook Express and sends them back with the original text and an infected attachment.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Badtrans.B

Virus info

Virus alias:	W32/BadTrans@MM
File size:	13,312 Bytes Version A, 29,02
Virus type:	Worm
Infected operating systems:	-
Damage:	Badtrans.B sends itself by email using MAPI (Messaging Application Program Interface).
Discovered on:	27.11.2001
From VDF version:	6.23.00.00

General information

When the attachment is opened, the worm copies itself in Windows System directory with the name KERNEL32.EXE and enters the following registry key: [HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce] Kernel32=\%WINDIR%\SYSTEM\KERNEL32.EXE

Then, the worm dropps the file KDLL.DLL in Windows directory, which activates a keyboard process protocol Trojan.

There is no text in the subject or body of the email sent by the worm.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Bagle.A

Virus info

Virus alias:	W32.Beagle.A@mm, I-Worm.Bagle, WORM_BAGLE.A
File size:	15,872 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	sends itself by email * When the worm is launched, calc.exe is started.
Discovered on:	18.01.2004
From VDF version:	6.23.00.34

General information

Worm/Bagle.A sends itself by email using its own smtp engine.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Bagle.AA

Virus info

Virus alias:	W32.Beagle.Z@mm
File size:	20,767 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email When activated, it shows a message box with the following text: "Can't find viewer associated with the file"
Discovered on:	28.04.2004
From VDF version:	6.25.00.38

General information

Worm/Bagle.AA sends itself by email.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Bagle.ab

Virus info

Virus alias:	WORM_BAGLE.AB, W32/Bagle.ab@mm
File size:	~67 kB
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email
Discovered on:	06.07.2004
From VDF version:	6.26.00.14

General information

Worm/Bagle.ab searches the system for email addresses.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Bagle.AC

Virus info

Virus alias:	I-Worm.Bagle.AC, TrojanProxy.Win32.Mitglieder.av, W32/Mitglieder.AV, W32/Bagle.AC
File size:	18,432 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email For further details, please refer to the Bagle.X description.
Discovered on:	13.05.2004
From VDF version:	6.25.00.60

General information

Sent by email
For further details, please refer to the Bagle.X description.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Bagle.AD

Virus info

Virus alias:	WORM_BAGLE.AD, W32/Bagle.ad@mm
File size:	~61 kBytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email
Discovered on:	06.07.2004
From VDF version:	6.26.00.14

General information

Worm/Bagle.ad searches the system for email addresses.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Bagle.AF

Virus info

Virus alias:	W32.Beagle.AB@mm, W32/Bagle.af@MM, WORM_BAGLE.AF
File size:	variable ~22 kBytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email; Opens TCP port 1080
Discovered on:	16.07.2004
From VDF version:	6.26.00.30

General information

Worm/Bagle.af searches the local system for email addresses

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Bagle.AI

Virus info

Virus alias:	I-Worm.Bagle.ai; W32/Bagle.ai@MM; W32/Bagle-AI; WORM_BAGLE.AH; Win32/Bagle.AH; Win32.Bagle.AJ@mm;
File size:	~21 kBytes (PEX v0.99 packed)
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email; Spreads through P2P directories; ends antivirus and firewall software.
Discovered on:	19.07.2004
From VDF version:	6.25.00.36

General information

Worm/Bagle.AI has a similar routine to the other versions of Bagle family.
Worm/Bagle.AI uses its own SMTP engine to spread by email. It searches for email addresses in files.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Bagle.B

Virus info

Virus alias:	W32.Alua@mm
File size:	11,264 bytes (UPX)
Virus type:	Worm
Infected operating systems:	-
Damage:	Sends emails using its own smtp engine * Increased email traffic.
Discovered on:	17.02.2004
From VDF version:	6.24.00.07

General information

Worm/Bagle.B sends itself by email with the help of its own smtp engine.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Bagle.C

Virus info

Virus alias:	W32.Beagle.C@mm; W32/Bagle.c@MM; W32/Bagle.C; I-Worm.Bagle.C
File size:	8,160 bytes or 15,872 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sends itself as email * Open TCP port 2745 * Presence of the mentioned registry entries * Presence of the mentioned files * Increased email traffic
Discovered on:	28.02.2004
From VDF version:	6.24.00.23

General information

Worm/Bagle.C has a file size of 15.872 bytes (UPX packed) or 28,160 bytes. The attachment of the email is a ZIP archive with a size of 15.994. It copies itself into the Windows folder.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Bagle.F

Virus info

Virus alias:	W32.Beagle.A@mm, Win32.Bagle.Gen@mm, I- Worm.Bagle.f
File size:	~24.000 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	29.02.2004
From VDF version:	6.24.00.27

General information

Worm/Bagle.F has a variable file size of ~24000 Bytes. The file is packed with PEX. The email attachment is a ZIP archive or even the executable program . If this is opened, the worm copies itself in Windows System with the name i1ru74n4.exe

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Bagle.H

Virus info

Virus alias:	W32.Beagle.H@mm, Win32.Bagle.Gen@mm, I- Worm.Bagle.H
File size:	~21.000 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	01.03.2004
From VDF version:	6.24.00.32

General information

Worm/Bagle.F has a variable file size of ~24000 Bytes. The file is packed with PEX. The email attachment is a ZIP archive or even an executable program . If this is opened, the worm copies itself in Windows System with the name i11r54n4.exe (~21.000 Bytes).

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Bagle.J

Virus info

Virus alias:	W32/Bagle.j@MM, W32.Beagle.J@mm, W32/Bagle-J, Bagle.J, W32/B
File size:	12,288 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sends itself by email * Open TCP port 2745 * Presence of the mentioned registry entries * Presence of the mentioned files * Increased email traffic
Discovered on:	02.03.2004
From VDF version:	6.24.00.35

General information

Worm/Bagle.J has a file size of 12.288 bytes. The worm will copy itself in %System% folder as: * IRUN4.EXE

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Bagle.M

Virus info

Virus alias:	W32/Bagle.n@MM, Bagle.N, Win32.Bagle.N
File size:	~ 21.000 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	13.03.2004
From VDF version:	6.24.00.56

General information

Worm/Bagle.M is a polymorph worm that uses its own SMTP engine to spread. Like the prior Bagle versions, it also has a backdoor component (TCP port 2556) and tries to copy and spread itself over shared networks.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Bagle.N

Virus info

Virus alias:	Win32.Bagle.N, Bagle.N, W32/Bagle.n@MM, W32/Bagle.N, W32/Bagle-N, PE_BAGLE.N
File size:	~21.000 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	10.03.2004
From VDF version:	6.24.00.56

General information

When activated, Bagle.N copies itself in %SystemDIR%\winupd.exe and makes a registry entry, for automatic start.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Bagle.R

Virus info

Virus alias:	W32/Bagle.r@MM, PE_BAGLE.R, W32/Bagle-R, Win32.Bagle.R, I-Worm.Bagle.q
File size:	25.600 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	12.03.2004
From VDF version:	6.24.00.56

General information

When activated, Worm/Bagle.R checks if the system date is 2006 or later. If this is the case, the worm deletes the a registry entry.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Bagle.U

Virus info

Virus alias:	W32.Beagle.U@mm, I-Worm.Bagle, WORM_BAGLE.U
File size:	8.208 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sends itself by email * the "Heart" game is launched.
Discovered on:	26.03.2004
From VDF version:	6.23.00.71

General information

Worm/Bagle.U sends itself by email.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Bagle.V

Virus info

Virus alias:	W32.Beagle.V
File size:	8,208 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email
Discovered on:	28.03.2004
From VDF version:	6.23.00.71

General information

When run, the worm copies itself in %SystemDIR%\syinfo.exe and makes the a registry entry, to be activated by the next system start.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Bagle.X

Virus info

Virus alias:	I-Worm.Bagle.z, WORM_BAGLE.Z, WORM_BAGLE.AB, W32/Bagle.ab@MM, Win32.Bagle.X
File size:	variable
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	28.04.2004
From VDF version:	6.25.00.60

General information

When activated, Bagle.X displays an error window.

It uses 7 mutexes, to ensure that only one version of the worm is active on the system.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Banuris.P2P

Virus info

Virus alias:	WORM_WINUR.A [Trend], W32/Winur.worm.a [McAfee], Worm.P2P.Winur [KAV]
File size:	61,440 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over shared KaZaA and WinMX programs.
Discovered on:	30.11.1999
From VDF version:	-

General information

Worm/Banuris.P2P tries to spread over shared KaZaA and WinMX programs.
When activated, Worm/Banuris.P2P copies itself in two files

C:\klez_removal.exe

A:\Important - read this.doc %62 spaces% .exe

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Banuris.P2P.1

Virus info

Virus alias:	WORM_WINUR.A [Trend], W32/Winur.worm.a [McAfee], Worm.P2P.Winur [KAV]
File size:	61,440 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over shared KaZaA and WinMX programs.
Discovered on:	30.11.1999
From VDF version:	-

General information

Worm/Banuris.P2P.1 tries to spread over shared KaZaA and WinMX programs.
When activated, Worm/Banuris.P2P.1 is copied in two files:

C:\klez_removal.exe

A:\Important - read this.doc %62 spaces% .exe

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Bibrog.C

Virus info

Virus alias:	W32/Bibrog@MM, W32/Bibrog.C@mm
File size:	235,520, 192,512
Virus type:	Worm
Infected operating systems:	-
Damage:	Worm/Bibrog.C is a massmailer and sends itself using Microsoft Outlook to all available addresses.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When active, the worm opens a program looking like a shooting game. It will possibly change the Windows background.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Bizex

Virus info

Virus alias:	Worm.Win32.Bizex, W32/Bizex.worm
File size:	86,538 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Keylogger, sends itself via ICQ * none provided
Discovered on:	25.02.2004
From VDF version:	6.24.00.17

General information

Worm/Bizex spreads over the ICQ instant messenger program, by sending a message containg a link to all users from contact list.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Blackmal

Virus info

Virus alias:	W32/MyWife.a@MM [McAfee], I-Worm.Nyxem [Kaspersky], W32/Nyxem-A [Sophos], WORM_BLUEWORM.A [Trend], W32.Blackaml@mm
File size:	about 75KB
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over email and shared networks.
Discovered on:	30.11.1999
From VDF version:	-

General information

Worm/Blackmal sends itself by email with the help of its own smtp engine.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/BleBla

Virus info

Virus alias:	W32/BleBla.a@MM
File size:	29.184 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	12.12.2000
From VDF version:	6.23.00.00

General information

'BleBla' virus (also known as Romeo&Juliet) spreads over the Internet and sends itself by email with two attachments. It proves to be really dangerous, as it becomes active and infects the system right after opening or previewing the email.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/BleBla.3

Virus info

Virus alias:	I-Worm.Blebla.b [KAV], W32/BleBla.b@MM [McAfee], WORM_BLEBLA.B [Trend], W32/Verona-B [Sophos], Win32.Verona.B [CA]
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email, spreads on servers.
Discovered on:	30.11.1999
From VDF version:	-

General information

When activated, the worm is copied as SYSRNJ.EXE in C:\\Windows\ directory and creates or modifies the following registry entry:

HKEY_CLASSES_ROOT\rnjfile\DefaultIcon= %1\shell\open\command = sysrnj.exe "%1" %*

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Bobax

Virus info

Virus alias:	W32/Bobax.worm.a, TrojanProxy.Win32.Bobax.a
File size:	20.480 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Uses the LSASS security hole, sent by email.
Discovered on:	19.05.2004
From VDF version:	6.25.00.60

General information

When activated, Worm/Bobax copies itself in %System%\%random name%.exe and makes registry entries, for automatic start.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Bride.A

Virus info

Virus alias:	I-Worm.Bradex, PE_BRID.A, W32/Brid.A@MM
File size:	114.687 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	04.11.2002
From VDF version:	6.23.00.00

General information

Worm/Bride.A spreads by email and works with another known virus. If the email is received on a system using Microsoft Outlook, it can occur that, by other versions, the virus is self-activated using a security hole in Microsoft Outlook (IFRAME).

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Bride.C

Virus info

Virus alias:	I-Worm.Bradex, Win32/Winevar.worm
File size:	91.000 Bytes and more.
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads by email.
Discovered on:	23.11.2002
From VDF version:	6.23.00.00

General information

As the worm's prior versions, Worm/Bride.C spreads by email and contains another packed virus. It infects PE executable files using W32/Funlove virus and deletes almost all files from the harddisk.

It can be self-activated on Microsoft Outlook systems, using a security hole (IFRAME). Thus, the worm can be automatically activated on Outlook preview.

Worm/Bride.C is even more dangerous than the prior versions.

In a short time, the worm begins to delete files from the harddisk. Windows operating system can not be loaded, on the next system start, at the latest.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Brit.B

Virus info

Virus alias:	-
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	26.03.2002
From VDF version:	6.23.00.00

General information

When "CAIFANES.CHM" is opened, a window is displayed, while Brit.B creates hh.dat in C:\%WinDIR%\Application Data\Microsoft\HTML Help\ and sends itself with Outlook. The file hh.dat contains important virus information, as for example the path where the attachment was opened.
It is a massmailer which sends itself with Microsoft Outlook, using the Outlook Address Book.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Brit.F

Virus info

Virus alias:	Chick.F, I-Worm.Brit.g
File size:	12.155 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads by email.
Discovered on:	13.06.2002
From VDF version:	6.23.00.00

General information

The worm copies itself in C:\Windows\Koreajapan.chm
Brit.F is an Internet worm, which spreads over Microsoft Outlook and mIRC program, using "Script.ini".

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Bugbear

Virus info

Virus alias:	I-Worm.Tanatos
File size:	50,688 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	It terminates running processes or applications of some antivirus software or firewalls. Opens port 36794 enabling the access to infected computers.
Discovered on:	30.09.2002
From VDF version:	-

General information

t is a worm, which spreads itself by sending emails. It can also spread over local Intranet, through mapped network drives. The worm's size is 50,588 bytes and it is packed with UPX.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/BugBear.1

‚Virus info

Virus alias:	I-Worm.Tanatos.a, W32/BugBearQMM, W95/BugBear.A@mm, W32.BugBear@mm
File size:	50,688 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads by email and over shared networks, Keylogger function.
Discovered on:	30.11.1999
From VDF version:	-

General information

When activated, the worm copies itself as .exe file in the Windows system directory.

The worm sends itself to all email addresses it can find on the local system. It uses words and file names collected from the system, to name its emails.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/BugBear.2

Virus info

Virus alias:	I-Worm.Tanatos.a, PWS-Hooker.dll, PWS. Hooker.Trojaner
File size:	29,020 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email, Keylogger function.
Discovered on:	30.11.1999
From VDF version:	-

General information

Worm/BugBear.2 inserts a keylogger function into the system directory, named KDLL.DLL. This Trojan tries to collect personal information and to send it to the author by email.

The worm searches for email addresses in all files of type "*.asp" and "*.ht*". It replies to the unread emails in Outlook. It also sends itself to all email addresses found on the system. The worm activates itself without the email to be opened.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Bugbear.B

Virus info

Virus alias:	Win32/BugBear.B.Worm, W32/Kijmo.A-mm
File size:	72,192 bytes (UPX packed)
Virus type:	Worm
Infected operating systems:	-
Damage:	An unknown .EXE file appears in the Autostart directory.
Discovered on:	05.06.2003
From VDF version:	6.19.00.xx

General information

When activated, Worm/Bugbear.B makes two .DAT files with different names in Windows directory.

Worm/Bugbear.B has a backdoor component that is listening on TCP port 1080. This way the attacker is able to run programs, terminate some processes and transfer system information.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/BugBear.B.dll

Virus info

Virus alias:	I-Worm.Tanatos.a, W32/BugBear.b.dll, PWS.Hooker.Trojanner
File size:	72,192 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads by email and over shared networks, Keylogger function.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

The worm copies itself with random names in startup directory.

The worm tries to copy itself as .exe file on a network computer. It listens on TCP port 1080 for access on a system.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Calil

Virus info

Virus alias:	W32/Lilac
File size:	12.208 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Worm/Calil spreads by email.
Discovered on:	08.07.2002
From VDF version:	6.23.00.00

General information

Worm/Calil is an 12208 Bytes (30720Bytes unpacked)Internet worm, written in Visual Basic language.

When activated, the worm sends itself using Outlook to all email addresses in WAB.

t sends itself to all email addresses in WAB (Windows Address Book) using Outlook.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Cervivec

Virus info

Virus alias:	W32/Cervivec@mm
File size:	228.872 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	26.03.2002
From VDF version:	6.23.00.00

General information

If the attachment is opened, the worm is installed in Windows system directory as "ntkrnl.exe" and enters a autorun registry key.

Worm/Cervivec is a massmailer with an 228.872 Bytes .EXE file. It sends itself by email using ICQ contacts list. Its emails are expressed in various languages.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Chet

Virus info

Virus alias:	Anniv911.exe; 11september.exe
File size:	26.628 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	10.09.2002
From VDF version:	6.23.00.00

General information

Worm/Chet is a massmailer. But due to a programming error, its email sending routine can not work on most of the Windows systems.

The worm tries to send itself using Outlook and the Windows Address Book (WAB).

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Choke.1

Virus info

Virus alias:	I-Worm.Choke.a, W32/Choke, W95/Worm.Choke, W32.Choke.Worm
File size:	40,960 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads using MSN Messenger.
Discovered on:	30.11.1999
From VDF version:	-

General information

When activated, it remains memory resident and creates files.

The worm spreads as ShootPresidentBUSH.exe, to all MSN Messenger users that chat with the infected user.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Choke.2

Virus info

Virus alias:	I-Worm.Choke.a, W32/Choke, W95/Worm.Choke, W32.Choke.Worm
File size:	40,960 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads using MSN Messenger
Discovered on:	30.11.1999
From VDF version:	-

General information

When activated, the worm is memory resident and creates files.

The worm spreads as ShootPresidentBUSH.exe, to all MSN Messenger users that are chatting with the infected user. The file contains the following message: President bush shooter is game that allows you to shoot Bush balzz hahaha

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/CodeRed

Virus info

Virus alias:	W32/CodeRed.a.worm
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	-
Discovered on:	25.07.2001
From VDF version:	-

General information

Worm/CodeRed uses a Microsoft IIS (Internet Information Server) security hole for its spreading. After the worm infects a server, it will look for other servers to invade.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Colevo

Virus info

Virus alias:	WORM_COLEVO.A [Trend], W32/Colevo@MM [McAfee], I-Worm.Colevo [KAV]
File size:	188,928 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	-

General information

It finds the MSN Messenger Contacts list and uses the email addresses to spread itself.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Cuervo

Virus info

Virus alias:	VBS/Cuerpo.A
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

Worm/Cuervo is programmed in Visual Basic. It creates a series of .HTML and .VBS files, it modifies registry entries and it replaces the Internet Explorer start site with its own HTML file.

Cuervo looks into Outlook Inbox for emails with attachments. If it finds such an email, the worm copies its code, in the system directory, into a file named after the attachment found, using the extension .VBS.

The worm searches for email addresses in all files with extension: .txt, .na2, .wab, .mbx, .dbx and .dat. It sends itself using Microsoft Outlook.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Cult.B

Virus info

Virus alias:	WORM_CULT.B, I-Worm.Cult.B
File size:	8,644 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	03.04.2003
From VDF version:	6.19.00.05

General information

The virus spreads over file-sharing networks and email.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Cydog.C

Virus info

Virus alias:	W32/Kickin@MM, W32Kickin.A@mm
File size:	109,056 bytes (UPX packed)
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	10.05.2003
From VDF version:	6.19.00.13

General information

When activated, Worm/Cydog.C copies itself in Windows with the filename CYBERWOLF.EXE which is set to "hidden" and "system file" rights.

The virus spreads over file-sharing networks, email and network drives.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Dabber

Virus info

Virus alias:	W32/Dabber-A, W32/Dabber.worm.a, WORM_DABBER.A, W32.Dabber.A
File size:	29,696 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Uses security hole LSASS
Discovered on:	14.05.2004
From VDF version:	6.25.00.60

General information

The worm scans over port 5554 for IP addresses of computers infected with Worm/Sasser. When an infected system is found, it spreads over FTP Server, a Worm/Sasser component. It will try to download components from an infected computer.

The worm opens a backdoor from an infected system. The process is done over port 9898. It gives the attacker the control over this system and enables him to collect informations on other systems.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Datom.1

Virus info

Virus alias:	W32/Datom-A [Sophos], Win32.Datom [CA], W32/Datom.worm [McAfee], Datom [F-Prot], Worm.Win32.Datom [KAV], WORM_DATOM.A [Trend], W32/Datom [Panda], Win32/Datom.worm [RAV]
File size:	58,368 Bytes (Msvxd.exe), 54,7
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over shared networks.
Discovered on:	30.11.1999
From VDF version:	-

General information

Worm/Datom. 1 has the following three files in %WinDIR%:

Msvxd.exe
Msvxd16.dll
Msvxd32.dll

Worm/Datom. 1 spreads over shared networks.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Datom.2

Virus info

Virus alias:	W32/Datom-A [Sophos], Win32.Datom [CA], W32/Datom.worm [McAfee], Datom [F-Prot], Worm.Win32.Datom [KAV], WORM_DATOM.A [Trend], W32/Datom [Panda], Win32/Datom.worm [RAV]
File size:	58,368 Bytes (Msvxd.exe), 54,7
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over shared networks.
Discovered on:	30.11.1999
From VDF version:	-

General information

Worm/Datom. 2 has the following three files in %WinDIR%:

Msvxd.exe
Msvxd16.dll
Msvxd32.dll

Worm/Datom. 2 spreads over shared networks.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Datom.3

Virus info

Virus alias:	W32/Datom-A [Sophos], Win32.Datom [CA], W32/Datom.worm [McAfee], Datom [F-Prot], Worm.Win32.Datom [KAV], WORM_DATOM.A [Trend], W32/Datom [Panda], Win32/Datom.worm [RAV]
File size:	784 Bytes (Msvxd16.dll), 81,40
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over shared networks.
Discovered on:	30.11.1999
From VDF version:	-

General information

Worm/Datom. 3 has the following three files in %WinDIR%:

Msvxd.exe
Msvxd16.dll
Msvxd32.dll

Worm/Datom. 3 spreads over shared networks.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/DeadHat.A

Virus info

Virus alias:	W32.HLLW.Deadhat, Vesser
File size:	55,808 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Backdoor function, spreading by Soulseek * A message box appears with the text "Error executing program!"
Discovered on:	09.02.2004
From VDF version:	6.23.00.61

General information

When the worm is active, a message box appears with the title "Corrupted File" and the text "Error executing program!".

Distribution:

* by P2P network program "Soulseek"

* by backdoor function of Worm/MyDoom

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Deborm.Q.1

Virus info

Virus alias:	W32/Deborm.worm [McAfee], Worm.Win32.Deborm.q [KAV], Worm.Win32.Deborm.r [KAV], TROJ_DROPPERFL.A [Trend], W32/Deborm-Q [Sophos], W32/Deborm-R [Sophos], Win32.Deborm.Q [CA], Win32.Deborm.R [Sophos], Win32.Deborm.S [Sophos]
File size:	variable.
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over shared networks.
Discovered on:	30.11.1999
From VDF version:	-

General information

When activated, the worm drops and executes Backdoor.Sdbot, Backdoor.Litmus (2), und Trojan.KillAV. If the opened system is Windows 95/98/Me, it registers as service process. It is not visible in Task list and it contiues to run after log out. In this case, the worm stops after system shut-down.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Deborm.Q.3

Virus info

Virus alias:	Backdoor.Litmus (AVP/KAV, AVG), Backdoor.Trojan (Symantec), BKDR_LITMUS (Trend), IRC Trojan (Symantec), security risk or a "backdoor" program (F-Prot), W32/Litmus (Norman, Eset, Vet)
File size:	variable (7kB-150kB)
Virus type:	Worm
Infected operating systems:	-
Damage:	Backdoor component.
Discovered on:	30.11.1999
From VDF version:	-

General information

This UPX-packed Trojan opens TCP/IP port 30005. Thus, an attacker can open, run and delete the local system user's file. Windows can also be affected.

This Trojan can connect to Internet Relay Chat sevrer and receives instructions through IRC port.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Deborm.R.1

Virus info

Virus alias:	W32/Deborm.worm, W32.HLLW.Nebiwo
File size:	variable
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over shared networks.
Discovered on:	30.11.1999
From VDF version:	-

General information

When activated, the worm drops and executes Backdoor.Sdbot, Backdoor.Litmus (2), und Trojan.KillAV. If the opened system is Windows 95/98/Me, it registers as service process. It is not visible in Task list and it contiues to run after log out. In this case, the worm stops after system shut-down.t

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Deborm.R.2

Virus info

Virus alias:	Trojan.PSW.Stealth [AVP], PWS-AC [McAfee], TROJ_PSW.STEAL [Trend], Troj/PWS-AC [Sophos]
File size:	variable
Virus type:	Worm
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

When activated, Worm/Deborm.R.2 looks for all system processes and terminates those processes that are related with antivirus programs.

They terminate software that may be needed for virus analysis. They also try to end antivirus programs installed on the computer.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Deborm.R.3

Virus info

Virus alias:	Backdoor.SdBot.gen (AVP), Backdoor/IRC.SdBot (RAV), Mindjail, W32.HLLW.Cult.C@mm (Symantec)
File size:	variable
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads by email and IRC.
Discovered on:	30.11.1999
From VDF version:	-

General information

When the attachment is opened, the local system is infected.

The worm is copied in Windows System directory (%SysDir%) as iexplorer.exe.

The Trojan connects to the IRC port to receive instructions for Denial of Service attacks or for downloading and executing programs.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Deloder

Virus info

Virus alias:	Worm/Deloder
File size:	745,984 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Unusually increased traffic on TCP port 445.
Discovered on:	09.03.2003
From VDF version:	6.18.00.xx

General information

Worm/Deloder (745,984 bytes) spreads itself over Windows networks by port 445. It tries to log as administrator of the remote system using a list of 85 passwords.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Desos

Virus info

Virus alias:	I-Worm.Desos.a, PE_MOE.A, W32/onamu@MM, W95/Onamu.A@mm, W95.Stoogy.6031
File size:	38,922 Bytes or 38,931 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	-

General information

Worm/Desos searches for email addresses in .ht* files and in Windows Address Book.
When the attachment is opened, the worm is copied in \Windir directory. For the file name, it uses 5 letters.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Doomjuice

Virus info

Virus alias:	W32.HLLW.Doomjuice, Mydoom.C
File size:	43,008 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	sends itself by email * the file 'sync-src-1.00.tbz' (28.569 Bytes) is created
Discovered on:	09.02.2004
From VDF version:	6.23.00.62

General information

Worm/Doomjuice, when activated, copies itself as INTRENAT.EXE in Windows System.

* Worm/Doomjuice infects the system using the backdoor routine of Worm/MyDoom.A or Worm/MyDoom.B

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Dumaru.A

Virus info

Virus alias:	I-Worm.Dumaru, W32/Dumaru@MM, W32/Dumaro.A, W32/Dumaru-A
File size:	~9 kbytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads itself by email Increased email traffic.
Discovered on:	19.08.2003
From VDF version:	6.21.00.21

General information

Worm/Dumaru.A sends itself by email.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Dumaru.AC

Virus info

Virus alias:	W32.Dumaru.AH@mm, W32/Mimail.u@MM
File size:	40,960 bytes, 28,020 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sends itself by email, backdoor functions, keylogger functions * When executed, Internet Explorer will be launched with a picture displayed.
Discovered on:	11.02.2004
From VDF version:	6.23.00.65

General information

If Worm/Dumaru.AV is executed, it will create the file NLOAD.EXE in the root of disk drive C: and execute it. The file NLOAD.EXE has a size of 28.020 bytes and is packed with FSG.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Dumaru.B1

Virus info

Virus alias:	I-Worm.Dumaru.b, W32/Dumaru, W95/Dumaru.J@mm, W32.Dumaru.M@mm
File size:	~ 33 KB
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	-

General information

It collects email adresses from files of type: .htm, .wab, .html, .dbx, .tbb and .abd. It uses its own SMTP engine to spread by email.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Dumaru.B3

Virus info

Virus alias:	Backdoor.Dumador.e, PWS-Narod, IRC Trojan
File size:	~ 33 KB
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	-

General information

It collects email adresses from files of type: .htm, .wab, .html, .dbx, .tbb and .abd. It uses its own SMTP engine to spread by email.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Dumaru.C.3

Virus info

Virus alias:	I-Worm.Dumaru.c, Pws-Narod, IRC Trojan
File size:	9216 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Worm/Dumaru.C.3 makes registry entries and tries to send information about the infected computer to its author.
Discovered on:	30.11.1999
From VDF version:	-

General information

This password stealer Trojan tries to send information about the infected computer to its author by email.

It creates dllreg.exe and sysdrv.exe in %WinDIR%. The worm copies itself in %Systemdir% as load32.exe and vxdmgr32.exe.

This Trojan also terminates some antivirus and firewall programs, using the file sysdrv.exe in %WinDIR%.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Dumaru.K

Virus info

Virus alias:	I-Worm.Dumaru.c, PWS-Narod, IRC Trojan
File size:	34,304 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	-

General information

It collects email adresses from files of type: .htm, .wab, .html, .dbx, .tbb and .abd. It uses its own SMTP engine to spread by email.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Dumaru.K.DLL

Virus info

Virus alias:	TrojanSpy.Win32.SilentLog.a, W32/Dumaru.dll, Keylogger.Trojan
File size:	34,304 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	-

General information

t collects email adresses from files of type: .htm, .wab, .html, .dbx, .tbb and .abd. It uses its own SMTP engine to spread by email.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Dumaru.Y

Virus info

Virus alias:	W32/Dumaru.y@mm, WORM_DUMARU.Y
File size:	17 kbytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads itself by email, backdoor routine * increased email traffic
Discovered on:	25.01.2004
From VDF version:	6.23.00.33

General information

Worm/Dumaru.Y is a mass-mailer that carries a backdoor key logger. It uses its own SMTP engine for email spreading.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/ExploreZip.E

Virus info

Virus alias:	Zipped_Files
File size:	91,048 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	It makes all .DOC, .XLS, .CPP, .C and .H of 0 bytes size.
Discovered on:	01.08.2003
From VDF version:	-

General information

If you receive an email with the text: "Hi [recipient's name]! I received your Email and I shall send you a reply ASAP. Till then, take a look at the attached zipped docs. Bye", then this is the virus.

This virus, like Melissa, uses the email settings of the windows system. It spreads through Outlook, Exchange or NetScape Mail. It reduces the files - even over the network - to 0 bytes! W32/ExploreZip spreads over email on Windows 9x and Windows NT computer systems. As email program, any MAPI email client is used.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Fizzu.A

Virus info

Virus alias:	W32/Fizzer@mm, W32/Fizzer.gen@MM
File size:	220,160 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Unexpected traffic on port 6667 (IRC) or on port 5190 (AIM).
Discovered on:	12.05.2003
From VDF version:	6.19.00.13

General information

The virus spreads over KaZaA and email as executables .exe.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Fizzu.A.2.E

Virus info

Virus alias:	I-Worm.Fizzer, W32/Fizzer.dll, W95/Fizzer.Keylogger, W32.HLLW.Fizzer
File size:	241,664 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email, Backdoor component, Keylogger.
Discovered on:	30.11.1999
From VDF version:	-

General information

The worm collects email addresses from Windows Address Book, cookie files, Internet temporary files and from personal folders.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Fizzu.A.2.F

Virus info

Virus alias:	I-Worm.Fizzer, W32/Fizzer.dll, W95/Fizzer.Keylogger, W32.HLLW.Fizzer
File size:	241,664 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email, Backdoor component, Keylogger.
Discovered on:	30.11.1999
From VDF version:	-

General information

The worm collects email addresses from Windows Address Book, cookie files, Internet temporary files and from personal folders.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Frethem

Virus info

Virus alias:	W32/Frethem
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads by email.
Discovered on:	13.06.2002
From VDF version:	6.19.00.00

General information

Worm/Frethem has its own SMTP engine and does not need an email program as Outlook, to send itself.

The worm file is ‘Decrypt-password.exe’. The second attachment ‘password.txt’ is empty and has no payload.

Worm/Frethem copies itself in Autostart folder from Windows Startmenu. so it will be activated by every system start.

Worm/Frethem is an Internet worm that spreads by email. It collects email addresses from Windows Address Book and .dbx files.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Frethem.001

Virus info

Virus alias:	I-Worm.Frethem.k [AVP], W32/Frethem.k@MM [McAfee], WORM_FRETHEM.J [Trend], W32/Frethem-Fam [Sophos], W32.Frethem.I@mm
File size:	47,616 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email, Backdoor component.
Discovered on:	30.11.1999
From VDF version:	-

General information

The worm searches for email addresses in Windows Address Book and files of type: .dbx .wab .mbx .eml .mdb

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Frethem.010

Virus info

Virus alias:	W32.Frethem.K@mm, I-Worm.Frethem.I [KAV], W32/Frethem.I@MM [McAfee], WORM_FRETHEM.K [Trend], W32/Frethem-Fam [Sophos], Win32.Frethem.K [CA], W32/Frethem.K [Panda], W32/Frethem.L [F-Prot]
File size:	48,640 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	-

General information

The worm searches for email addresses in Windows Address Book and files of type: .dbx .wab .mbx .eml .mdb

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Frethem.014

Virus info

Virus alias:	W32.Frethem.E@mm, I-Worm.Frethem.e, W32/Frethem, W32.Frethem.F@mm
File size:	35,840 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	-

General information

When activated, the worm gets information about the SMTP server, email addresses and SMTP server name from some registry entries.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Frethem.J

Virus info

Virus alias:	-
File size:	47.616 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads by email.
Discovered on:	16.07.2002
From VDF version:	6.23.00.00

General information

Worm/Frethem.J is a PE and UPX packed file of 47.616 Bytes. It spreads using its own SMTP engine.

When the attachment Decrypt-password.exe is opened, the worm is copied in Windows directory as Taskbar.exe and enters a registry key.

Worm/Frethem.J uses its own SMTP engine to spread to all email addresses it can find in Windows Address Book or in files

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Frethem.I

Virus info

Virus alias:	-
File size:	48.640 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads by email.
Discovered on:	15.07.2002
From VDF version:	6.23.00.00

General information

Worm/Frethem.I is a 48.640 Bytes file, packed with PE and UPX.

When the attachment Decrypt-password.exe is opened, the worm is copied in Windows directory as Taskbar.exe and enters a registry key.

Worm/Frethem.I sends itself by email, using its own SMTP engine. It finds email addresses in Windows Address Book or in files.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/FriendGreet

Virus info

Virus alias:	WORM_FRIENDGRT.A
File size:	1.142.044 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads by email.
Discovered on:	24.10.2002
From VDF version:	6.23.00.00

General information

Worm/FriendGreet is not really a 'normal' a virus or worm. It sends itself to all contacts in Microsoft Outlook. Before sending emails, the user has to agree the End User License Agreements (EULA). When such an email is received, and the link it contains is accessed, the standard browser is opened (eg Internet Explorer). While accessing this website, a Security Warning window is displayed and the worm is installed.

By pressing 'YES', the file "Friend Greetings.msi" or "Friend%20Greetins.msi" is downloaded. If there is no MSI Installations Software on the computer, it will be downloaded, too. When "Friend Greetings.msi" is installed, the End User License Agreements (EULA) window is displayed, which explains that the "Permissioned Media Inc." program can send itself to all contacts in Microsoft Outlook.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Ganda

Virus info

Virus alias:	W32/Ganda@MM , Win32.Ganda.A
File size:	45,056 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	- it ends running processes, such as antivirus or firewall applications; - the file SCANDISK.EXE (45,056 bytes) in %WinDir%; - an identical 45,056 bytes file with a random name (8 characters +.EXE) in %WinDir%; - the following registry entries: HKEY_LOCAL_MACHINE\SOFTWARE\SS\Sent HKEY_LOCAL_MACHINE\SOFTWARE\SS\Sent2
Discovered on:	17.03.2003
From VDF version:	6.18.00.16

General information

The email sent by Worm/Ganda can have English or Swedish components.

Worm/Ganda infects the windows .EXE files on the local drive with its 567 bytes code. But these files can not infect further other files and will be functional afterwards.

The worm has its own SMTP engine and sends itself to all email addresses found on the infected computer.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Gibe

Virus info

Virus alias:	W32/Gibe@mm, WORM_GIBE.A, W32/Gibe-A, I-Worm.Gibe
File size:	122,880 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When opening the Visual Basic file Q216309.exe, which contains parts of other viruses.

Worm/Gibe uses Microsoft Outlook and its own SMTP engine. This worm sends itself by email disguised as Microsoft Internet Security Update.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Gibe.B

Virus info

Virus alias:	Win32.Gibe.B@mm, WORM_GIBE.B
File size:	155,648 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	- The files and registry entries mentioned below. - Disguised as Microsoft Internet Update (see Technical Details).
Discovered on:	26.02.2003
From VDF version:	-

General information

The worm has its own SMTP engine and sends itself to all email addresses it finds on the infected computer. It also spreads over P2P network KaZaA and network drives from the infected computer.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Gibe.C

Virus info

Virus alias:	W32/Swen@mm
File size:	106.469 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	The worm can be attached in an email. It also spreads over KaZaA and IRC. Tries to switch off antivirus programs.
Discovered on:	18.09.2003
From VDF version:	6.21.00.47

General information

Worm/Gibe.C is a massmailer, which spreads using its own SMTP engine. It tries to spread over networks as KaZaA and IRC and to switch off antivirus and firewall programs.

The worm can be attached to an email. The subject, body and sender can vary. Some emails claim to be Microsoft Internet Explorer Patches or 'Delivery Failure' messages.

The worm uses a Microsoft Outlook or Outlook Express security hole, to activate itself when the message is opened or previwed.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Gibe.C.1

Virus info

Virus alias:	Swen [F-Secure], W32/Swen@mm [McAfee], W32/Gibe-F [Sophos], I-Worm.Swen [KAV], Win32 Swen.A [CA], WORM_SWEN.A [Trend], Worm.Automat.AHB [Previous Symantec Detection]
File size:	106,496 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads by email, KaZaA, IRC, mapped drives and Newsgroups.
Discovered on:	30.11.1999
From VDF version:	-

General information

When activated, Worm/Gibe.C.1 checks if it has already been installed on the computer. If this is the case, the installation process ends and a message is displayed.

The worm spreads by email, KaZaA, IRC, mapped drives and Newsgroups.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Gnutella.MG

Virus info

Virus alias:	P2P/Mandragore
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Worm/Gnutella.MG spreads through Gnutella networks.
Discovered on:	27.02.2001
From VDF version:	6.23.00.00

General information

This worm attacks only users of Gnutella related programs. So, the worm is dangeorus for Gnutella networks only.

When activated, the worm is copied in Autostart folder of every user, as GSPOT.EXE system hidden file. The next time Windows is started, the worm is executed and becomes a background memory resident process.

On Windows 9x, the worm registers in tasklist as hidden process. The worm contacts Gnutella network. The infected computer answers as 'server' enquiry to files and so it can be easily overloaded with many enquiries.

The worm creates a single file, containing the womrm code, available for download. The name of the file is randomly chosen.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Gokar.1

Virus info

Virus alias:	I-Worm.Gokar [Kaspersky], W32/Gokar-A [Sophos], W32/Gokar@MM [McAfee], WORM_GOKAR.A [Trend], Win32.Gokar [Computer Associates]
File size:	14,336 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	-

General information

The worm is copied in \Windows directory as Karen.exe.

The worm adds the email user name at the end of the email text and sends it to all addresses in Outlook.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Goner

Virus info

Virus alias:	W32/Goner@MM
File size:	38.912 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads using ICQ Instant Messanger
Discovered on:	05.12.2001
From VDF version:	6.23.00.00

General information

Worm/Goner copies itself as GONE.SCR in Windows system directory (usually C:\WINDOWS\SYSTEM\) and makes a autostart registry entry.

Worm/Goner spreads through ICQ, using standard ICQ components. It sends a request for file transfer to a connected user. If this allows the transfer, the worm is sent.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Happy

Virus info

Virus alias:	Happy99, I-Worm.Happy, W32/Ska.dll, W32/Ska.dll@m, W32/Ska@M
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	-

General information

When activated, Worm/Happy displays the message "Happy New Year 1999!!" and fireworks on the screen.

It can spread through email attachments or using its own SMTP engine for sending emails.

The email sent by the worm has the attachment:Happy99.EXE.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Happy.A

Virus info

Virus alias:	Happy99, I-Worm.Happy, W32/Ska.dll, W32/Ska.dll@m
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	-

General information

When activated, Worm/Happy.A displays the message "Happy New Year 1999!!" and fireworks on the screen.

It can spread through email attachments or using its own SMTP engine for sending emails.

The email sent by the worm has the attachment:Happy99.EXE.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Hawawi.A

Virus info

Virus alias:	I-Worm.Hawawi.a, W32/Holar, W95/Holar.D, W32.Hawawi.Worm
File size:	54,784 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreading by email, MSN Messenger and shared networks.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When the attachment is opened, the worm is copied in Windows system directory and makes a registry autostart entry.

The worm is spreading by email, MSN Messenger and shared networks.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Hawawi.G.Drp

Virus info

Virus alias:	I-Worm/Hawawi.e, W32/Holar, W32,Hawawi.Worm
File size:	58,009 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads by email and shared networks.
Discovered on:	30.11.1999
From VDF version:	-

General information

The worm collects email addresses from computer files. The collected data is saved, for example, with the following registry entries: HKEY_CURRENT_CONFIG\System "Emails1" = harvested address HKEY_CURRENT_CONFIG\System "Emails2" = next harvested addressetc etc

The worm uses its own SMTP engine for sending emails.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Holar.C

Virus info

Virus alias:	W32/SfxDeth.A-mm, W32/Lagel.A
File size:	54,514 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email, spread over local networks - Screen dialogues appear (see technical details). - Outgoing emails, as described below.
Discovered on:	04.12.2002
From VDF version:	-

General information

Worm/Holar.C is an Internet worm, which sends itself by email, using its own SMTP engine. The email addresses are collected from the local .HTM and .HTML files.

It sends itself by email as executable .EXE files, using its own SMTP engine, to the email addresses found on the infected computer.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Holar.C.1

Virus info

Virus alias:	W32.Holar.C@mm, W32/Holar.c@MM [McAfee], W32/Lagel.A [Panda], Win32.Holar.C [CA], WORM_HOLAR.C [Trend], I-Worm.Galil [KAV]
File size:	54,514 Bytes, 80,626 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	-

General information

The worm saves the email addresses of the current users in the file C:\%systemdir%\Mmails.dll. It uses its own SMTP engine or Microsoft Outlook, for sending itself to all addresses found on the computer. There can be more worm copies attached to the email.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Hybris.B

Virus info

Virus alias:	W95.Hybris.Plugin, W32/Hybris@MM [McAfee], I-Worm.Hybris.dropper [Kaspersky], WORM_HYBRIS.DR1 [Trend], Win32.Hybris.dr [Computer Associates]
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Worm/Hybris.B contains Plug-In infected PE files.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

It concerns Plug-In infected PE files. Only PE files with long enough code section are infected.

The virus infection contains packs of the original code and overwrites it, if it is in the same place.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Hybris.PI.11

Virus info

Virus alias:	W32/Hybris.dll@MM, W95/Hybris.worm.B, W95.Hybris.gen
File size:	25,088 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads through newsgroups.
Discovered on:	30.11.1999
From VDF version:	-

General information

When activated, W95/Hybris.PI.11 tries to infect WSOCK32.DLL in %Windir%/%Systemdir%. If it can not infect the file directly, because it is already in use, the worm creates an infected copy of WSOCK32.DLL. The file name has 8 characters and no extension.

It registers the new WSOCK32.DLL file in WININIT.INI, for autostart.

The modified WSOCK32.DLL file monitors the Internet activity and tries to email an .exe or .scr worm copy.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Inmota.1

Virus info

Virus alias:	I-Worm.Inmota, W32.Inmota.Worm
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	-

General information

When activated, Worm/Inmota.DLL copies itself as

default.html<222 blank spaces>.pif in %Systemdir% and %Windir% directories.

The worm counts the addresses in Microsoft Outlook or in Outlook Express and replies them with the attachment:

Default.html<222 blank spaces>.pif.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Inmota.DLL

Virus info

Virus alias:	I-Worm.Ínmota, W32.Inmota.Worm
File size:	variable
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	-

General information

When activated, Worm/Inmota.DLL copies itself as

default.html<222 blank spaces>.pif in %Systemdir% and %Windir% directories.

The worm counts the addresses in Microsoft Outlook or in Outlook Express and replies them with the attachment:

Default.html<222 blank spaces>.pif.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Isratz.1

Virus info

Virus alias:	W32.Akosw@mm, Win32.Israz.A [CA], W32/Israz.worm [McAfee], Worm_Israz.A [Trend], W32/Israz-A [Sophos], I-Worm.Israz [KAV]
File size:	147,456 Bytes, 16,384 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	-

General information

The worm sends itself to all email addresses found in Windows Address Book.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Isratz.2

Virus info

Virus alias:	W32.Akosw@mm, Win32.Israz.A [CA], W32/Israz.worm [McAfee], Worm_Israz.A [Trend], W32/Israz-A [Sophos], I-Worm.Israz [KAV]
File size:	147,456 Bytes, 16,384 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
30.11.1999	30.11.1999
From VDF version:	6.23.00.00

General information

The worm sends itself to all email addresses it can find in Windows Address Book.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/KakWorm.D

Virus info

Virus alias:	Tam, I-Worm.Kakworm.d, Out
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

Worm/KakWorm.D is related to JS/Kak. It uses the same security hole to infect the system. There is a free Microsoft Update patch available at:

http://www.microsoft.com/security/Bulletins/ms99-032.asp

The worm overwrites the Outlook Express 5.0 settings with its own, to send the virus with every outgoing email.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Kazaa

Virus info

Virus alias:	-
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over Peer-to-Peer network KaZaA.
Discovered on:	23.05.2002
From VDF version:	6.23.00.00

General information

Worm/Kazaa is a worm that spreads over Peer-to-Peer network KaZaA. This network is used for transferring programs, games, movies etc.

When an infected file is opened, a dialog window is displayed.

he directory C:\Windows\Temp\Sys32\ is registered as shared folder by P2P KaZaA software, so that the KaZaA user will unintentionally download the worm.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Klez.E

Virus info

Virus alias:	W32/Klez.G, W32/Klez.H@mm
File size:	~80 kbytes
Virus type:	Worm
Infected operating systems:	-
Damage:	-
Discovered on:	19.04.2002
From VDF version:	-

General information

This new version of Worm/Klez copies itself as WINKxxx.EXE ("xxx" = random character combination) in Windows and places a key in the registry.

Worm/Klez.E sends a HTML-mail with a 64base encoded copy of itself. By the email reception, the worm is activated, although it is not opened, but previewed. It is sent to e-mail clients (from Microsoft Outlook, for example).

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Korgo.M

Virus info

Virus alias:	W32.Korgo.M
File size:	11,391 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	-
Discovered on:	22.06.2004
From VDF version:	6.25.00.108

General information

When activated, Worm/Korgo.M deletes Ftpupd.exe file. It uses some Mutexes, to be sure that there is only one active version of itself.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Korgo.N

Virus info

Virus alias:	W32.Korgo.N
File size:	9,344 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	-
Discovered on:	23.06.2004
From VDF version:	6.25.00.109

General information

When activated, Worm/Korgo.N deletes Ftpupd.exe file. It uses uterm18 Mutex, to be sure that there is only one active version of itself.

Worm/Korgo.N opens TCP ports 113, 5111 and another random port, between 256 and 8191, for spreading itself.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Korgo.Q

Virus info

Virus alias:	W32.Korgo.Q
File size:	9,534 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	-
Discovered on:	26.06.2004
From VDF version:	6.26.00.07

General information

When activated, Worm/Korgo.Q deletes Ftpupd.exe file. It uses uterm19 Mutex, to be sure that there is only one active version of itself.

Worm/Korgo.Q opens a random TCP port 113 between 256 and 8191, for spreading itself on other computers.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Lee.SP

Virus info

Virus alias:	-
File size:	2.195 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	07.06.2002
From VDF version:	6.23.00.00

General information

When the attachment is opened, the worm is copied as ShakiraPics.jpg.vbs in Windows directory and overwrites all .vbs files with its own code.

The worm copies itself in \Recycled\-folder on a local drive and sends itself over Microsoft Outlook. It can also spread by IRC, using the file Script.ini.

Worm/Lee.SP spreads by email, using the Outlook Address Book.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Lee.SP3

Virus info

Virus alias:	I-Worm.Lee-based, VBS/VBSWG.gen@MM,VBS/VBSWG.AQ
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Searches for certain files to infect them. Spreads by email and mIRC.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

On June, 7th, 2002, the spreading of Wurm Worm/Lee.SP3 is increased. It is also known as Shakira, based on Visual Basic Script and containing a VBSWG virus.

The virus spreads over mIRC and by email, using Outlook.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Lentin.2

Virus info

Virus alias:	-
File size:	23,320 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated, Worm/Lentin.2 copies the Address Book into C:\%WinDIR%\%variable%.dll, where the varaible file name has 5 random letters. For example: ABCDEABCDE.dll or CEGIKCEGIK.dll.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Lentin.A

Virus info

Virus alias:	W32/Valscr.A-mm, W32/Yaha.eml, I-Worm.Lentin.a, W32/Yaha@MM, W95/Lentin.A@mm, W32.Yaha.F@mm
File size:	20,992 Bytes (UPX packed)
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

Worm/Lentin.A it infects the local computer right after activated.

The worm searches for email addresses in the Internet files of the current user. It writes some of the addresses into %WINDIR%\SCREEND.DLL.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Lentin.E

Virus info

Virus alias:	W32.Yaha.D@mm, I-Worm.Lentin.e [AVP], W32/Yaha.e@MM [McAfee], W32/Yaha-D [Sophos], WORM_YAHA.D [Trend], Win32.Yaha.D [CA]
File size:	25,619 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	-

General information

The email addresses collected by the worm are saved into \%Windows%\%variable%%variable%.dll, where the variable file name has 6 random numbers. For example, if the random number is 123456, the file name is \%Windows%\123456123456.dll.

The worm sends itself to all email addresses it can find.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Loiten

Virus info

Virus alias:	Iraq_oil, Datrix, W32.Lioten, W32/Lioten, I-Worm.Lioten
File size:	16,896 Bytes [UPX], 40,960 Byt
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over shared archives.
Discovered on:	30.11.1999
From VDF version:	-

General information

Loiten does not spread by email. It looks on Internet for Windows 2000 or XP computers, which have shared archives and are not protected by firewalls. When such a computer is found, the worm is copied as .exe file (usually named iraq_oil.exe) and executed. It tries to find the users of a computer over IP. It uses the following words for passwords:

admin root 111 123 1234 123456 654321 1 !@#$ asdf asdfgh !@#$% !@#$%^ !@#$%^& !@#$%^&* server

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Lovegate

Virus info

Virus alias:	Supnot, I-Worm.Supnot
File size:	84,992 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	A backdoor component is installed and opens the port 10168 on the infected computer.
Discovered on:	24.02.2003
From VDF version:	-

General information

Worm/Lovegate (84,882 bytes) is a mass mailer packed with ASPack. It spreads both by email and over network drives and has a backdoor component. If the worm finds a shared network drive, it copies itself on this.

The worm has its own SMTP engine and sends itself to all email addresses it finds on the infected computer. It also spreads over network drives from the infected computer.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Lovegate.G.1

Virus info

Virus alias:	WORM_LOVGATE.F [Trend], WORM_LOVGATE.G [Trend], W32/Lovgate.f@M [McAfee], W32/Lovgate.g@M [McAfee], W32/Lovgate-E [Sophos], I-Worm.LovGate.f [KAV], Win32/Lovgate.F.Worm [CA]
File size:	107,008 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	-

General information

When activated, the worm is copied in %SystemDIR%.

It collects email addresses from all HTML files and replies all messages in Microsoft Outlook Inbox.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Lovegate.G.2

Virus info

Virus alias:	WORM_LOVGATE.F [Trend], WORM_LOVGATE.G [Trend], W32/Lovgate.f@M [McAfee], W32/Lovgate.g@M [McAfee], W32/Lovgate-E [Sophos], I-Worm.LovGate.f [KAV], Win32/Lovgate.F.Worm [CA]
File size:	107,008 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	-

General information

When activated, the worm is copied in %SystemDIR%.

It collects email addresses from all HTML files and replies all messages in Microsoft Outlook Inbox.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Lovegate.J

Virus info

Virus alias:	I-Worm.LovGate.j, W32/Lovgate, W95/Lovgate.J@mm, W32.HLLW.Lovgat
File size:	127.488 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads by email and over shared network resources; Backdoor component.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

The worm replies to all unread messages from Microsoft Outlook or Outlook Express Inbox.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Lovegate.J123

Virus info

Virus alias:	W32/Lovgate.j@MM / PE_LOVGATE.J / Supnot
File size:	127.488 Bytes (ASPack)
Virus type:	Worm
Infected operating systems:	-
Damage:	-
Discovered on:	13.05.2003
From VDF version:	6.19.00.15

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Lovegate.K

Virus info

Virus alias:	I-Worm.LovGate.h, W32/Lovgate,W95/Lovgate.K@mm
File size:	127.488 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads by email, and shared network resources. Backdoor component.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

The worm replies to all unread messages from Microsoft Outlook or Outlook Express Inbox.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Lovelorn.2

Virus info

Virus alias:	W32/Lovelorn@MM [McAfee], WORM_LOVELORN.A [Trend], Win32.Lovelorn.A [CA], I-Worm.Lovelorn [KAV], W32/Cailont-A [Sophos], W32.Nolor@mm
File size:	101,888 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email, using its own SMTP engine .
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

Lovelorn searches drives C: D: and E:. It tries to collect email addresses from files.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Lovelorn.3

Virus info

Virus alias:	W32/Lovelorn@MM [McAfee], WORM_LOVELORN.A [Trend], Win32.Lovelorn.A [CA], I-Worm.Lovelorn [KAV], W32/Cailont-A [Sophos], W32.Nolor@mm
File size:	101,888 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email, using its own SMTP engine .
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

Lovelorn searches drives C: D: and E:. It tries to collect email addresses from files.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Lovelorn.4

Virus info

Virus alias:	W32/Lovelorn@MM [McAfee], WORM_LOVELORN.A [Trend], Win32.Lovelorn.A [CA], I-Worm.Lovelorn [KAV], W32/Cailont-A [Sophos], W32.Nolor@mm
File size:	101,888 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email, using its own SMTP Engine .
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

Lovelorn searches drives C: D: and E:. It tries to collect email addresses from files.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Lovgate.A.1

Virus info

Virus alias:	I-Worm.Supnot.a, Supnot.A
File size:	84,992 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email. Backdoor Component.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

Apart from its massmailer function, this worm can spread through Windows components and it steals passwords.

The worm uses its own SMTP engine and sends itself to all email addresses it can find on the infected computer.

The backdoor component of Worm/Lovegate saves keylogging information and passwords.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Lovgate.A.2

Virus info

Virus alias:	I-Worm.Supnot.a, Supnot.A
File size:	84,992 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email. Backdoor Component.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

The most important difference between version B and version A is the absence of the reply to Inbox messages.

Without this function, the spreading relies on collecting email addresses from networks and *.ht* files.

Apart from the massmailer function, this worm can spread through Windows components and steal passwords. It is packed with ASP.

The worm has its own SMTP engine and sends itself to all email addresses it can find on the infected computer. It also spreads over the network drives of the infected system.

The backdoor component of Worm/Lovegate saves keylogging information and passwords.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Lovgate.A.3

Virus info

Virus alias:	I-Worm.Supnot.a, Supnot.A
File size:	84,992 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email., Backdoor component.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

The most important difference between version B and version A is the absence of the reply to Inbox messages.

Without this function, the spreading relies on collecting email addresses from networks and *.ht* files.

Apart from the massmailer function, this worm can spread through Windows components and steal passwords. It is packed with ASP.

The worm has its own SMTP engine and sends itself to all email addresses it can find on the infected computer. It also spreads over the network drives of the infected system.

The backdoor component of Worm/Lovegate saves keylogging information and passwords.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Lovgate.B

Virus info

Virus alias:	Win32/Lovgate.A@mm [RAV], W32/Lovgate.a@M [McAfee], I-Worm.Supnot.b [KAV]
File size:	77,312 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email. Backdoor component.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

Apart from the massmailer function, this worm can spread through Windows components and steal passwords. It is packed with ASP and copies itself.

The worm has its own SMTP engine and sends itself to all email addresses it can find on the infected computer. It also spreads over the network drives of the infected system.

The backdoor component of Worm/Lovegate saves keylogging information and passwords.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/LovGate.F

Virus info

Virus alias:	W32.HLLW.Lovgate.F@mm, I-Worm.LovGate.f, W32/Lovegate, W95/Lovgate.J@mm, W32.HLLW.Lovgate
File size:	172,842 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email. Backdoor components.
Discovered on:	30.11.1999
From VDF version:	-

General information

This is an improved version of the version B of the worm. It contains a longer password list, for attempting to access shared resources.

The worm has its own SMTP engine and sends itself to all email addresses it can find on the infected computer. It also spreads over the network drives of the infected system.

The backdoor component of Worm/Lovegate saves keylogging information and passwords.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/LovGate.F.2

Virus info

Virus alias:	W32.HLLW.Lovgate.F@mm, I-Worm.LovGate.f, W32/Lovegate, W95/Lovgate.J@mm, W32.HLLW.Lovgate
File size:	172,842 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email. Backdoor component.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

It contains a longer password list, for attempting to access shared resources.

The worm has its own SMTP engine and sends itself to all email addresses it can find on the infected computer. It also spreads over the network drives of the infected system.

The backdoor component of Worm/Lovegate saves keylogging information and passwords.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/LovGate.I

Virus info

Virus alias:	I-Worm.LovGate.i, W32/Lovgate, W95/Lovgate.L@mm
File size:	variable
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads by email and shared netresources. Backdoor component.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

The worm replies to unread messages in Microsoft Outlook or in Outlook Express Inbox.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Lovgate.J

Virus info

Virus alias:	W32/Lovgate.j@MM, PE_LOVGATE.J, Supnot
File size:	127,488 kbytes (ASPack)
Virus type:	Worm
Infected operating systems:	-
Damage:	Opens the port 10168 on the infected system
Discovered on:	-
From VDF version:	-

General information

When activated, Worm/Lovgate.J copies itself in Windows (in Microsoft Windows 9x Systems \Windows\System\ and in Microsoft Windows NT Systems in Windows\System32\ or in Winnt\System32\).

The virus spreads via email and shared network drives and copies itself in Outlook Inbox.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Lovgate.L.2

Virus info

Virus alias:	I-Worm.Lovgate.i [KAV]
File size:	163,587 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

It infects all .exe files on the local drives and shared network directories.

The worm tries to terminate processes of various programs, including antivirus software.

The worm tries to reply to inbox emails. It also searches for email addresses in HTML files.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Lovgate.T

Virus info

Virus alias:	I-Worm.LovGate.t [Kaspersky], W32/Lovgate.s@MM [McAfee]
File size:	98,304 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads by email and shared networks. Backdoor component.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated, Worm/Lovgate.T is copied as read-only, hidden, system files.

The worm replies to emails from Microsoft Outlook Mailbox.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/LovLorn.8

Virus info

Virus alias:	W32/Lovelorn@MM [McAfee], WORM_LOVELORN.A [Trend], Win32.Lovelorn.A [CA], I-Worm.Lovelorn [KAV], W32/Cailont-A [Sophos], W32.Nolor@mm
File size:	101,888 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads by email, using its own SMTP engine.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

It tries to collect email addresses from files.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Lovsan.A

Virus info

Virus alias:	W32/Lovsan.worm, WORM_MSBLAST.A
File size:	6,176 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	DDOS attack A file named MSBLAST.EXE appears in Windows System32 directory.
Discovered on:	11.08.2003
From VDF version:	6.21.0.10

General information

The UPX packed worm tries to make a connection using the port 135. It scans for vulnerable addresses and if it finds one, it sends special commands to the TFTP program (Trivial File Transfer Protocol).

This program starts the download of the worm program and runs it. The worm copies itself in Windows System32 directory (generally C:\Windows\System32\ or C:\WINNT\System32\) in the file named MSBLAST.EXE.

In order to be run by the next system start, the worm makes a registry entry.

The worm uses the security hole of RPC DCOM for getting full control over the Windows system. The spreading is done over network and Internet.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Lovsan.B

Virus info

Virus alias:	W32/Blaster-C, Win32.Poza.B
File size:	5,360 kbytes
Virus type:	Worm
Infected operating systems:	-
Damage:	DDOS attack A file named TEEKIDS.EXE appears in Windows System32 directory.
Discovered on:	13.08.2003
From VDF version:	6.21.0.14

General information

The worm tries to make a connection using the port 135. It scans the network and if it finds a vulnerable system, it sends special commands to the TFTP program (Trivial File Transfer Protocol).

This program starts the download of the worm program and runs it. In most of the cases Worm/Lovsan.B comes with the help of a dropper. This dropper named Index.exe (32,045 bytes) makes the files TEEKIDS.EXE (5,360 bytes) and ROOT32.EXE (19,798 bytes) in the Windows system 32 directory (C:\Windows\System32\ or C:\WINNT\System32\).

In order to be run by the next system start, the worm makes a registry entry.

The worm uses the security hole of RPC DCOM for getting full control over the Windows system. The spreading is done over network and Internet.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Lovsan.C

Virus info

Virus alias:	W32/Blaster-C, Win32.Poza.C
File size:	7,200 kbytes
Virus type:	Worm
Infected operating systems:	-
Damage:	DDOS attack A file named PENIS32.EXE appears in Windows System32 directory.
Discovered on:	13.08.2003
From VDF version:	6.21.0.14

General information

The worm tries to make a connection using the port 135. It scans for IP addresses and if it finds a vulnerable system, it sends special commands to the TFTP program (Trivial File Transfer Protocol).

This program starts the download of the worm program and runs it. It enters the file PENIS32.EXE (7,200 bytes) in the Windows system32 directory (C:\Windows\System32\ or C:\WINNT\System32\).

In order to be run by the next system start, the worm makes a registry entry.

The worm uses the RPC DCOM security hole for getting full control over the Windows system. The spreading is done over network and Internet.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Lovsan.E

Virus info

Virus alias:	Worm.Win32.Lovesan, W32/Msblast.E, W32/Blaster-E, W32/Blaste
File size:	6,176 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	DDOS attack A file named mslaugh.exe appears in Windows System32 directory
Discovered on:	29.08.2003
From VDF version:	6.21.0.31

General information

The worm, packed with UPX, tries to connect to 135 port. It scans for vulnerable systems, and sends special commands to the TFTP program (Trivial File Tranfere Protocol). This program starts the download of the worm and runs it.

The worm uses a security hole in RPC DCOM and gets full control over Windows system. The spreading is done by network and Internet.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Lovsan.G1

Virus info

Virus alias:	W32/Lovsan.worm.f, W32/Blaster-F, WORM_MSBLAST.G
File size:	11,808 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Worm/Lovsan.G1 uses DCOM RPC on TCP Port 135 . It attacks only Windows2000/XP.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated, Worm/Lovsan.G1 performs the following actions:

1. checks if there is an infected computer and if the worm is active;

2. makes the following autostart registry entry: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVers ion\Run "www.hidro.4t.com"="enbiei.exe"

3. generates an IP address and tries to infect it;

4. sends data through port 135, using DCOM RPC. There are two possiblities:

for attacking Windows XP (for 80% of the cases) or Windows 2000.

5. using Cmd.exe it starts a "Remote Shell Process", which monitors the TCP port 4444. This allows an attacker to control the infected system.

6. monitoring UCP port 69. If the worm detects a reply of the computer, connected using DCOM RPC, it sends the file Enbiei.exe and tries to run it.

7. if the current date is between 16th and 31st of January to August or September to December, the worm tries to run a DoS on tuiasi.ro. Still, this only succeeds if:

- The virus is active on Windows XP
- The virus is active on Windows 2000
- The virus is active on Windows 2000, that was restarted after infection and the user has administrator access.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Magold.A

Virus info

Virus alias:	W32/Auric@MM [McAfee], W32/Magold-A [Sophos], WORM_MAGOLD.A [Trend], Win32.Auric.A [CA], I-Worm.Magold [KAV], W32.HLLW.Magold
File size:	240,640 bytes(packed), 622,592
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads by email, P2P networks and IRC Chat .
Discovered on:	30.11.1999
From VDF version:	6.23.00.00.

General information

Magold.A copies itself as %WinDIR%\raVe.exe. It tries to describe a site.

The virus sends itself to all email addresses it can find in Windows Outlook and in files of type: .html, .htm or .hta. It can use a false sender's address.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Magold.E

Virus info

Virus alias:	Maya Gold, Auric
File size:	238,592 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	mass mailer Windows applications take longer to load.
Discovered on:	23.06.2003
From VDF version:	6.20.00.15

General information

Worm/Magold.E has a 238,592 bytes file size, is packed with UPX.

Distribution:

- Email
- P2P (Peer-to-Peer) networks

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Magold.E.1

Virus info

Virus alias:	WORM_AURIC.E [Trend], I-Worm.Magold.e [KAV], W32/Magold-D [Sophos]
File size:	238,592 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

Worm/Magold.E.1 tries to terminate various programs, including antivirus software.

The worm uses its own SMTP engine to send itself by email to all addresses found in Windows Address Book and in files that begin or end in "ht."

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Magold.E.3

Virus info

Virus alias:	VBS/Pica.worm.gen[McAfee], I-Worm.Kagra.b[AVP], VBS/Kagra@mm[Frisk], I-Worm.Magold.a, W32.HLLW.Magold
File size:	2,557 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

First, the worm tries to copy itself into the last subfolder of the drive C:, beginning with "Win". Usually, it is C:\Windows or C:\Winnt. It copies itself as

Run32dll.vbs and Clickme.vbs.

The worm uses MAPI for replying to all emails it can find in Microsoft Outlook.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Maldal.C

Virus info

Virus alias:	Keyluc, Zacker, Zaker, Christmas.exe
File size:	37.376 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over Microsoft Outlook.
Discovered on:	21.12.2001
From VDF version:	6.23.00.00

General information

After performing its email routine, Maldal.C copies itself in Windows directory as Christmas.exe and enters the registry.

Maldal.C replaces the Internet Explorer start site with an URL of the Internet Provider Geocities.com.

Maldal.C spreads through the email attachment CHRISTMAS.EXE. When this file is opened, the worm is sent using Outlook to all email addresses it can find in Windows Address Book.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Maldal.E

Virus info

Virus alias:	I-Worm.Maldal.d [KAV], I-Worm.Maldal.e [KAV], I-Worm.Maldal.f [KAV], W32/Maldal.d@MM [McAfee], W32/Maldal.e@MM [McAfee], W32/Maldal.f@MM [McAfee], W32/Maldal.g@MM [McAfee], WORM_MALDAL.D [Trend], WORM_MALDAL.E [Trend], WORM_MALDAL.F [Trend], WORM_MALDAL.G
File size:	27 KByte
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated, the worm is copied as C:\WinDIR\SystemDIR\Win.exe.

It makes an autostart registry entry.

It deletes all antivirus programs it can find.

Finally, it deletes some files, including those with extensions:

.ini .php .exe .com .mpeg .dat .zip .txt .exe .xls .doc .jpg

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Maldal.I

Virus info

Virus alias:	W32/Maldal.i@MM
File size:	23.552 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	20.02.2002
From VDF version:	6.23.00.00

General information

When the worm is activated, a window is displayed:

"Sorry! You are not registered.

Please contact us..."

It immediately copies itself in Windows and in Windows System directory as ZaCker.pif.

Maldal.I sends itself by email using Microsoft Outlook.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Mapson

Virus info

Virus alias:	W32/Mapson@MM [McAfee], W32/Mapson-A [Sophos], WORM_MAPSON.A [Trend], Win32.Mapson.A [CA], I-Worm.Mapson [KAV]
File size:	180,736 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

Worm/Mapson copies itself in the system directory.

It tries to send itself to all email addresses it can find in MSN Contacts List.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Matcher

Virus info

Virus alias:	W32.Matcher.Worm
File size:	29 Kbytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	26.04.2001
From VDF version:	6.23.00.00

General information

In order for the virus to be activated, the file MSVBV60.DLL must be installed on the computer.

The email worm Matcher is an .EXE file, programmed in Visual Basic 6.0.

It spreads using the Address Book, over Microsoft Outlook and Outlook Express.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Matra

Virus info

Virus alias:	VBS_DAIRA.A, VBS/Daira@MM, VBS.Daira@mm, VBS/SSIWG2.A.Worm, VBS.SSIWG2 worm
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads by email, using Microsoft Outlook and it can infect Microsoft Word 2000 documents.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated, the worm is copied as "MATSUDARIA_V" on drive C:(hidden).

Another copy is made in System directory, as "W32BACKUP.DLL.VBS" (also hidden).

Worm/Matra spreads over Microsoft Outlook.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Melare

Virus info

Virus alias:	W32/Melare@MM [McAfee], I-Worm.Melare, W32.Ahlem.A@mm
File size:	6,144 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

Worm/Mapson copies itself as %Windir%\Csrss.exe and it makes an autostart registry entry.

It sends itself to all contacts in Windows Address Book.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Mimail.A

Virus info

Virus alias:	I-Worm.Mimail.e [Kaspersky], W32/Mimail-E [Sophos], WORM_MIMAIL.E [Trend], Win32.Mimail.E [Computer Associates], W32/Mimail.e@mm [McAfee], Mimail.E [F-Secure]
File size:	10.912 bytes (.zip), 10,784 by
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

Worm/Mimail.A copies itself as %WinDIR%\cnfrm.exe and makes a registry entry.

The worm spreads by email, using its own SMTP engine.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/MiMail.A1

Virus info

Virus alias:	WORM_MIMAIL.A [Trend], W32/Mimail@MM [McAfee], Win32.Mimail.A [CA], W32/Mimail-A [Sophos], I-Worm.Mimail [Kaspersky]
File size:	~ 16 KBytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

It copies itself as: %WinDIR%\Videodrv.exe and makes an autostart registry entry.

It collects email addresses from files, excluding the following types: .bmp .jpg .gif .exe .dll .avi .mpg .mp3 .vxd .ocx .psd .tif .zip .rar .pdf .cab .wav .com

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Mimail.C

Virus info

Virus alias:	W32.Mimail.C@mm, W32/Mimail.c@mm, WORM_MIMAIL.C, W32/Mimail-
File size:	12,832 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	sends itslef by email System instability.
Discovered on:	31.10.2003
From VDF version:	6.22.00.23

General information

When activated, it creates files in Windows. Email spreading, using its own SMTP engine

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Mimail.C2

Virus info

Virus alias:	W32/Mimail.c@mm [McAfee], WORM_MIMAIL.C [Trend], W32/Mimail-C [Sophos], I-Worm.Mimail.c [Kaspersky], Win32.Mimail.C [Computer Associates]
File size:	12,832 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

Worm/Mimail.C2 copies itself as %WinDIR%\Netwatch.exe and makes a registry entry.

The worm uses its own SMTP engine for email spreading.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Mimail.E

Virus info

Virus alias:	W32.Mimail.D@mm, W32/Mimail@mm, WORM_MIMAIL.E
File size:	10,784 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	sends itself by email System instability
Discovered on:	01.11.2003
From VDF version:	6.22.00.25

General information

When activated, it creates files in Windows and a registry entry.

Email spreading, using its own SMTP engine.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Mimail.F

Virus info

Virus alias:	I-Worm.Mimail.f [Kaspersky], W32/Mimail.f@MM [McAfee], WORM_MIMAIL.G [Trend], Win32.Mimail.E [Computer Associates], W32/Mimail-E [Sophos], Mimail.F [F-Secure], W32.Mimail.D@mm
File size:	10.912 Bytes (.zip), 10,784 By
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated, Worm/Mimail.F copies itself as %WinDIR%\cnfrm.exe and makes a registry entry.

The worm uses its own SMTP engine for email spreading.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Mimail.G2

Virus info

Virus alias:	WORM_MIMAIL.F [Trend], Win32.Mimail.G [Computer Associates], Mimail.G [F-Secure], W32/Mimail-F [Sophos], I-Worm.Mimail.g, W32.Mimail.E@mm
File size:	10.912 Bytes (.zip), 10,784 By
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated, Worm/Mimail.G2 copies itself as %WinDIR%\sysload32.exe and makes a registry entry.

The worm uses its own SMTP engine for email spreading.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Mimail.H2

Virus info

Virus alias:	I-Worm.Mimail.h [Kaspersky], W32/Mimail-H [Sophos], W32/Mimail.h@MM [McAfee], WORM_MIMAIL.H [Trend], Mimail.H [F-Secure], W32.Mimail.G@mm
File size:	10.912 Bytes (.zip), 10,784 By
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated, Worm/Mimail.H2 copies itself as %WinDIR%\cnfrm33.exe and makes a registry entry.

The worm uses its own SMTP engine for email spreading.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Mimail.I

Virus info

Virus alias:	W32.Paylap@mm, W32/Mimail-I
File size:	12,832 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	sends itself by email * the following files appear in Windows folder: EL388.TMP, SVCHOST32.EXE
Discovered on:	14.11.2003
From VDF version:	6.22.00.38

General information

Worm/Mimail.I sends itself by email using its own SMTP engine.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Mimail.I1

Virus info

Virus alias:	W32.Paylap@mm, W32.Mimail.H@mm, W32/Mimail-I [Sophos], WORM_MIMAIL.I [Trend], Win32.Mimail.I [Computer Associates], W32/Mimail.i@MM [McAfee], I-Worm.Mimail.i [Kaspersky]
File size:	12,832 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated, Worm/Mimail.I1 copies itself as

%WinDIR%\svchost32.exe

%WinDIR%\ee98af.tmp

and makes a registry entry.

The worm uses its own SMTP engine for email spreading.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/MiMail.J2

Virus info

Virus alias:	W32/Mimail.j@MM [McAfee], WORM_MIMAIL.J [Trend], Win32.Mimail.J [Computer Associates], W32/Mimail-J [Sophos], I-Worm.Mimail.j [Kaspersky]
File size:	13,856 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated, Worm/MiMail.J2 copies itself as

C:\%WinDIR%\svchost32.exe

C:\%WinDIR%\ee98af.tmp,

and makes a autostart registry entry.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Mimail.L

Virus info

Virus alias:	W32.Mimail.Gen, W32/Mimail.I@MM
File size:	11,296 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	sends itself by email * increased email traffic
Discovered on:	02.12.2003
From VDF version:	6.22.00.54

General information

When the worm is active, it copies itself in the following directories:

* C:\%Windows%\svchost.exe

* C:\%Windows%\XU39REU.TMP

and creates the file X8WUI12S.TMP in Windows directory.

It makes a registry entry, so that it will be automatically run at the next system start.

Sends itself by email, using its own SMTP engine

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Mimail.M1

Virus info

Virus alias:	W32.Mimail.Gen, W32/Mimail.gen@MM [McAfee], W32.Mimail.M@mm, W32/Mimail
File size:	10,784 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated, Worm/Mimail.M1 copies itself as %WinDIR%\netmon.exe and makes a registry entry.

The worm collects email addresses from all files, excluding the following types:

com wav cab pdf rar zip tif psd ocx vxd mp3 mpg avi dll exe gif jpg bmp. These addresses are saved in the file %WinDIR%\xjwu2.tmp.

The worm uses its own SMTP engine for email spreading.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Mimail.q

Virus info

Virus alias:	W32/Mimail.q@MM, WORM_MIMAIL.Q
File size:	32.758 Bytes, 50.720 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads itself by email, backdoor routine * increased email traffic
Discovered on:	26.01.2004
From VDF version:	6.23.00.45

General information

When the worm is active, it shows a dialog box, with the message: "ERROR: Bad CRC32". In this time, it creates the following files:

* \%WinDIR%\Sys32.exe

* \%WinDIR%\Outlook.exe

It registers itself as a service process and makes a registry entry.

The worm sends itself by email.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Mofeir.B.1

Virus info

Virus alias:	Worm.Win32.Mofeir.b, W32/MoFei.worm.dll, W95/Mofeir.B, W32.Fomot.Worm
File size:	20480 (dll) Bytes, 20992 (dll)
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over shared networks.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated on Windows 98/ME, Worm/Mofeir.B.1 creates the following files in C:\%WinDIR%\ %SystemDIR%:

NAVPW32.EXE (11,776 bytes)

SCARDSVR32.EXE

It makes an autostart registry entry.

When the worm detects a connected computer, it tries to log on to ADMIN$ and IPC$. For doing this, it uses various passwords, which differ from one version to another. When access succeeded, the worm copies itself on the connected computer.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Mofeir.B.2

Virus info

Virus alias:	W32/MoFei.worm [McAfee], WORM_MOFEI.A [Trend], WORM_MOFEI.B [Trend], W32/Mofei-A [Sophos], Backdoor.Mofeir.101 [KAV], Worm.Win32.Mofeir.b [KAV], Win32.Mofei.A [CA], Win32.Mofei.B [CA], W32.Femot.Worm
File size:	variable.
Virus type:	Worm
Infected operating systems:	-
Damage:	Backdoor component.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated, Worm/Mofeir.B.2 copies itself as %WinDIR%\SystemDIR\Scardsvr32.exe

and creates the file

%WinDIR%\Systemdir\Mofei.cfg. This file works as a Backdoor component.

The worm makes an autostart registry entry.

The worm tries to connect to other computers, as current user or as administrator and copies itself on other systems.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Mumu.B.4

Virus info

Virus alias:	IRC.Mimic (NAV), IRC/Mimic, mIRC.Mimic (Panda)
File size:	variable
Virus type:	Worm
Infected operating systems:	-
Damage:	Backdoor Trojan
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

The infected computers can be used for a Denial of Service attack on other systems. These attacks can destroy the aimed systems or disconnect them from the Internet.

This Trojan is usually sent as backdoor. It is attached to the user visiting the website. Thus, the hacker can invade the infected computer and start a Denial of Service attack.

Worm/Mumu.B.4 can perform this attacks in various ways. For example, it can create texts that are sent through IRC with high speed and big font size.

This worm is usually associated with a backdoor Trojan. When the program starts, this is also installed.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Myba.A

Virus info

Virus alias:	W32/Myba@mm
File size:	77,824 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	02.03.2001
From VDF version:	6.23.00.00

General information

When the attachment MYBABYPIC.EXE is opened, an obscene picture is displayed, while the worm is copied in Windows system directory.

Worm/Myba.A sends itself by email, using Microsoft Outlook Address Book.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/MyDoom

Virus info

Virus alias:	W32/Novarg@mm, Shimgapi
File size:	22,528 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads itself by email and P2P network KaZaA, starts a DoS attack, backdoor routine * Windows Notepad.exe is opened, with binary trash * The data Shimgapi.dll can be seen in Windows system.
Discovered on:	26.01.2004
From VDF version:	6.23.0.47

General information

When the worm is active, it creates the following files:

* \%WinDIR%\%SystemDIR%\Shimgapi.dll
* \%WinDIR%\%SystemDIR%\Taskmon.exe
* \%WinDIR%\%Temp%\Message.

Distribution

* Sends itself by email, using its own SMTP engine;
* Spreads over P2P network KaZaA, by shared directories.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/MyDoom.B

Virus info

Virus alias:	W32/Novarg.B@mm
File size:	29,184 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads itself by email and P2P network KaZaA, starts a DoS attack, backdoor routine * ctfmon.dll can be found in Windows system.
Discovered on:	28.01.2004
From VDF version:	6.23.00.51

General information

When the worm is active, it creates the following files:

* \%WinDIR%\%SystemDIR%\ctfmon.dll (6.144 Bytes)
* \%WinDIR%\%SystemDIR%\Exlplorer.exe

Distribution

* Sends itself by email, using its own SMTP engine;
* Spreads over P2P network KaZaA, by shared directories.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/MyDoom.F

Virus info

Virus alias:	I-Worm.Mydoom.F, W32/Mydoom.f@MM, W32/Mydoom.F.worm, W32/MyD
File size:	34.568 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreading over email and mapped network drives, performs a DOS attack, starts a backdoor routine * A fake error message appears, with the message: "file is corrupted"
Discovered on:	20.02.2004
From VDF version:	6.24.00.12

General information

It copies itself as a "zip" archive into different folders on the local drives. Zip archives have sizes of 34,688 bytes and also have random file names.

Distribution

* Sends itself via email using its own smtp engine
* Spreading over mapped network drives

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Mydoom.G

Virus info

Virus alias:	W32/Mydoom.g@MM, W32.Mydoom.G@mm
File size:	29,696 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sends itself by email * Open TCP port 1080 * Presence of the mentioned registry entries * Presence of the mentioned files * Increased email traffic * Notepad is opened with "data garbage"
Discovered on:	02.03.2004
From VDF version:	6.24.00.35

General information

Worm/Mydoom.G has a file size of 29.696 bytes. The file is packed with UPX. In the unpacked version of Worm/MyDoom.G, one can find the following text strings: "to netsky's creator(s) imho, skynet is a decentralized peer-to-peer neural network. we have seen P2P in Slapper in Sinit only. they maybe called skynets, but not your shitty app."

Sends itself via email using its own smtp engine

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/MyDoom.m

Virus info

Virus alias:	W32/Mydoom.o@MM, I-Worm.Mydoom.R
File size:	28,832 Bytes (variable)
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	26.07.2004
From VDF version:	6.26.00.44

General information

Worm/MyDoom.m (28,832 Bytes)is packed with UPX. When activated, it creates files.

Worm/MyDoom has its own SMTP engine. The email sent by the worm can vary.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Mylife.M

Virus info

Virus alias:	W32/Mylife.M-mm, W32.Mylife.N@mm, Win32/Juli.A
File size:	8,192 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	mass mailer
Discovered on:	07.04.2003
From VDF version:	6.20.00.31

General information

In order to be run by the next system start, the worm makes a registry entry.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Myparty

Virus info

Virus alias:	W32/Myparty.a@MM
File size:	A: 29.696 Bytes; B: 28.160 Byt
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email, Backdoor component.
Discovered on:	20.01.2002
From VDF version:	6.23.00.00

General information

Version A:

Worm/Myparty (29.696 Bytes) spreads by email, using its own SMTP engine. It installs a backdoor in the Autostart directory of the infected folder, named MSSTASK.EXE.
When the attachment is opened, Worm/Myparty is copied as REGCTRL.EXE in C:\RECEYCLED\ or C:\RECEYCLER\.

It searches for email addresses in Windows Address Book and in *.DBX files. It sends itself to these addresses, using its own SMTP engine. So, the worm does not need any email program for spreading.

Then, the worm checks if the Russian keyboard feature is active. If not, the worm installs a backdoor in the Start Menu's Autostart directory (\Windows\Startmenu\Programs\Autostart\ for Win9x and \Documents and Settings\%user%\ Startmenu\Programs\Autostart\ for Windows NT/XP) as MSSTASK.EXE (6.144 Bytes).

This will be automatically opened when Windows starts and run by a CGI script, from a website with the IP address 209.252.250.270.

Version B: the difference consists in the file size: 28.160 Bytes.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Nachi.A.1

Virus info

Virus alias:	W32/Welchia.worm10240, W32/Nachi.worm, WORM_MSBLAST.D,Lovsan.D, W32/Nachi-A, Win32.Nachi.A, Worm.Win32.Welchia, W32.Welchia.Worm
File size:	10,240 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	-
Discovered on:	18.08.2003
From VDF version:	6.23.00.00

General information

When opened, Nachi.A.1 copies itself as C:\%SystemDIR%\Wins\Dllhost.exe. It makes a copy of C:\%Systemdir%\Dllcache\Tftpd.exe, named C:\%System%\Wins\svchost.exe.

It makes a registry subkey.

It starts the TFTP Server on the attacked computer and downloads Dllhost.exe and Svchost.exe on it. When the update is downloaded and run, the worm restarts the computer, to install the correction routine.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Naco.D

Virus info

Virus alias:	I-Worm.Win32.Naco.D
File size:	45,568 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Email and Internet spreading Active applications of firewall and antivirus software are terminated.
Discovered on:	12.06.2003
From VDF version:	6.19.00.08

General information

Worm/Naco.D copies itself in these directories:

- C:\%Windows%\Start Menu\Programs\StartUp\<%Name%>.exe
- C:\%Windows%\%System%\csrss32.exe

and makes the C:\bgii.exe file.

It infects certain .exe files in the Windows directory and makes registry entries.

Distribution

- Email sending
- Local networks
- P2P networks

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Navidad

Virus info

Virus alias:	W32/Navidad@MM
File size:	32.768 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Internet worm. Spreads by email, as attachment named Navidad.exe.
Discovered on:	10.01.2001
From VDF version:	6.23.00.00

General information

Because of a programming error, after the worm is activated, no .exe aplication can be performed.

When NAVIDAD.EXE is opened, a false Error window is displayed.

In this time, the worm creates the file WINSVRC.VXD in %WINDIR%\%SystemDIR%\ and changes the standard registry entries with .exe files:

[HKEY_CLASSES_ROOT\exefile\shell\open\command]C:\WINDOWS\ SYSTEM\winsvrc.exe "%1" %*"
Thus, the worm should be activated every time an .exe file is opened but, because of a programming error, no .exe application can be opened.

Then, an autostart registry entry is made (but the same error occurs)

If you use a MAPI email Client (using MAPI32.DLL), the Internet worm infects the unread emails, by attaching the file NAVIDAD.EXE and sends back all the emails to their senders.

Attachment: NAVIDAD.EXE

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Nedal

Virus info

Virus alias:	I-Worm.Melhack; OsamaLaden.vbs
File size:	122.664 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	12.09.2002
From VDF version:	6.23.00.00

General information

Worm/Nedal is an Internet Worm, spread by email.

When the email is opened, the virus code is activated using ActiveX. Some computer systems show a Windows message to ask if ActiveX should be run. If the user answers YES, the worm is activated. Worm/Nedal creates the file OsamaLaden.vbs and copies it.

The email has no attachment. The virus code is inserted as HTML text, used for showing the message.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Netsky.AA

Virus info

Virus alias:	WORM_NETSKY.AA, W32/Netsky.aa@MM, Win32.Netsky.AA, W32/Netsky-AA, W32.Netsky.X@mm, W32.Netsky.Y@mm,
File size:	17.408 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	27.04.2004
From VDF version:	6.25.00.60

General information

When activated, Netsky.AA copies itself as %WinDIR%\Winlogon.scr and makes an autostart registry entry.

The worm uses its own SMTP engine to send itself to xdfggra@yahoo.com and to email-addresses it can find.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Netsky.AB

Virus info

Virus alias:	W32/Netsky-AB, W32/Netsky.ab@MM, WORM_NETSKY.AB, Win32.Netsky.AB, I-Worm.Netsky.ac,
File size:	17.920 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	27.04.2004
From VDF version:	6.25.00.60

General information

When activated, Netsky.AB copies itself as %WinDIR%\csrss.exe and makes an autostart registry entry.

The worm uses its own SMTP engine to send itself to email-addresses it can find.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Netsky.AC

Virus info

Virus alias:	WORM_NETSKY.AC, W32/Netsky-AC, Win32.Netsky.AC
File size:	18,432 Bytes/ 36,864 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email
Discovered on:	03.05.2004
From VDF version:	6.25.00.60

General information

The worm has 2 components: .CPL file and .EXE file. When the .CPL file is run, the worm is copied in %WinDIR%\comp.cpl, the .exe file is copied in %WinDIR%\wserver.exe and run. After starting WSERVER.EXE, the worm checks for another active task. It copies itself in %WinDIR%\wserver.exe and makes a registry entry, to be run by the next system start.

It spreads by email, using its own SMTP engine.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/NetSky.B

Virus info

Virus alias:	Moodown.B
File size:	22,016 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sends itself as email * When launched, a fake message with the following text will be generated: "The file could not be opened!"
Discovered on:	18.02.2004
From VDF version:	6.24.00.09

General information

Worm/NetSky.B has a size of 22.016 bytes and is packed with UPX. If it's executed, the worm copies itself into the Windows folder using the file name SERVICES.EXE. Subsequently, the worm creates a entry in registry.

Distribution

* Sends itself as email
* Copies itself in shared folders

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/NetSky.C

Virus info

Virus alias:	W32/Netsky.c@MM, i-Worm.Moodown.c
File size:	25,352 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sends itself as email * If the local system time is between 6:00 AM and 9:00 AM on February 26, 2004, the computer speaker will continuously beep.
Discovered on:	25.02.2004
From VDF version:	6.24.00.19

General information

Worm/NetSky.C is a massmailer, with a size of 25.352 bytes. It uses its own smtp engine to send the emails.Thus the worm is not dependent on the email client. The worm will scan files for email addresses, and will send itself to them, using a spoofed sender address.

Sends itself via email using its own smtp engine

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/NetSky.D

Virus info

Virus alias:	W32/Netsky.D@MM, i-Worm.Moodown.d
File size:	17,424 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sends itself by email * Increased email traffic
Discovered on:	01.03.2004
From VDF version:	6.24.00.29

General information

Worm/NetSky.D is a mass-mailer, with a size of 17.424 bytes.It uses its own smtp engine to send the emails. Thus the worm is not dependent on the email client. It scans files on all local drives for email addresses, to which it will send itself after that.

Sends itself via email using its own smtp engine

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/NetSky.E

Virus info

Virus alias:	W32/Netsky.E@MM, i-Worm.Moodown.e
File size:	24,840 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sends itself by email * Increased email traffic
Discovered on:	01.03.2004
From VDF version:	6.24.00.31

General information

Worm/NetSky.E is a mass-mailer, with a size of 24.840 bytes. It uses its own smtp engine to send the emails. Thus the worm is not dependent on the email client. It scans files on all local drives for email addresses, to which it will send itself after that.

Sends itself via email using its own smtp engine.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Netsky.J

Virus info

Virus alias:	W32.Netsky.J@mm, NetSky.J, W32/Netsky-K, Win32.Netsky.K, WO
File size:	27,648 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sends itself by email * Increased email traffic
Discovered on:	08.03.2004
From VDF version:	6.24.00.44

General information

Worm/Netsky.J has a file size of 27.648 bytes. It copies itself as:

* %windir%\avpguard.exe

It will add a registry entry.

Sends itself via email using its own smtp engine.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Netsky.K

Virus info

Virus alias:	W32.Netsky.K@mm, W32/Netsky-J, Win32.Netsky.J, W32/Netsky.j
File size:	22,016 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sends itself by email * Increased email traffic
Discovered on:	08.03.2004
From VDF version:	6.24.00.44

General information

Worm/Netsky.K has a file size of 22.016 bytes. It copies itself as:

* %windir%\winlogon.exe

It will add a registry entry.

Sends itself via email using its own smtp engine

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Netsky.O

Virus info

Virus alias:	W32.Netsky.O@mm, W32/Netsky-O,
File size:	16.384 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	18.03.2004
From VDF version:	6.24.00.60

General information

Worm/Netsky.O (16.384 Bytes) is packed with the newest version of UPX. When activated, it is copied as:

C:\%WinDir%\AVBgle.exe
C:\%WinDir%\base64.tmp (22.456 bytes / Base64 archive)

It makes a registry entry and deletes enties, if present.

The email sent by the worm can look differently. It uses a list for Subject, Body and Attachment.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Netsky.P

Virus info

Virus alias:	W32.Netsky.Q@mm, W32/Netsky.p@MM, Win32.Netsky.P, NetSky.P, W32/Netsky.P.worm, W32/Netsky-P, WORM_NETSKY.P
File size:	29,568 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email
Discovered on:	22.03.2004
From VDF version:	6.23.00.00

General information

When Worm/Netsky.P is run, it makes a Mutex _-oO]xX|-S-k-y-N-e-t-|Xx[Oo-_" , to verify that no active task of itself is on the system. It copies itself as %WinDIR%\FVProtect.exe and makes the file %WinDIR %\userconfig9x.dll.

It deletes the values of registry entries.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Netsky.Q

Virus info

Virus alias:	W32.Netsky.Q
File size:	28,008 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated, Worm/Netsky.Q is copied in %WinDIR%\SysMonXP.exe (28,008 Bytes) and it creates the file %WinDIR%\Firewalllogger.txt (23,040 bytes).

It downloads the .dll file Firewalllogger.txt and runs it.

The worm uses a mutex named "_-oOaxX|-+S+-+k+-+y+-+N+-+e+-+t+-|XxKOo-_", that only allows a single version of the worm on the infected system.

The worm searches for email addresses in files.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Netsky.X

Virus info

Virus alias:	Win32.Netsky.X, W32/NetSky.X@mm, W32/Netsky.X.worm, W32/Netsky-Y, WORM_NETSKY.X
File size:	26,112 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads by email, using its own SMTP engine.
Discovered on:	20.04.2004
From VDF version:	6.25.00.60

General information

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVersion\ Run\"FirewallSvr"="%WinDIR%\Firewa llSvr.exe"

It uses a process named "____--->>>>U<<<<--____", which allows only one version of the worm on the infected system.

It creates a MIME encoded copy of itself: %WinDIR%\fuck_you_bagle.txt.

It communicates with the attacker on TCP port 82 for sending executable files. The worm is automaticaly started, after downloading.

The worm uses its own SMTP engine to send itself to hukanmikloiuo@yahoo.com and to all email addresses it can find. It checks the domain of the email address and uses the detected language for the subject, body and attachment.

For example, if the address is someone@hostname.it, the email message is sent in Italian.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Netsky.Y

Virus info

Virus alias:	W32.Netsky.Y@mm, W32/Netsky-Y
File size:	18,944 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email, DoS attacks Increased email traffic.
Discovered on:	20.04.2004
From VDF version:	6.25.00.21

General information

Worm/Netsky.Y (18,944 bytes) creates the following files:

* %WinDir%\FirewallSvr.exe
* %WinDir%\Fuck_You_Bagle.txt (MIME file)

and makes a registry entry.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Netsky.Z

Virus info

Virus alias:	W32/Netsky.z@MM
File size:	22.016 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads by email, using its own SMTP engine.
Discovered on:	21.04.2004
From VDF version:	6.25.00.60

General information

When activated, the worm is copied as %WinDIR%\Jammer2nd.exe.

It creates a .zip file, containing the worm: %WinDIR%\PK_ZIP_ALG.LOG.

It also creates 8 MIME encoded .zip files, that contain the worm:

%WinDIR%\PK_ZIP_ALG.LOG

It makes an autostart registry entry.

It uses its own SMTP engine to send itself by email to jamainlbbbsdef@yahoo.com and to all emails it can find.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/NiceHello

Virus info

Virus alias:	W32/NiceHello@mm
File size:	99,328 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Worm/NiceHello sends itself by email, using its own SMTP engine. It copies itself in Windows system folder as "Sys64dvr.exe" (99,328 bytes) and makes a run entry in the registry. The files and registry entries mentioned below.
Discovered on:	12.03.2003
From VDF version:	6.18.00.xx

General information

Worm/NiceHello sends itself by email, using its own SMTP engine. This enables it to send emails without depending on other email programs, such as Outlook. The addresses are collected from the Contact List of Microsoft Messenger.

The worm has its own SMTP engine and sends itself to all email addresses found on the infected computer.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/OpaSoft

Virus info

Virus alias:	W32/OpaServ.Worm
File size:	28,672 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	- the files and registry entries mentioned below. - Increased traffic on port 139 (UDP).
Discovered on:	30.09.2002
From VDF version:	-

General information

When activated, the worm copies itself as ScrSvr.exe in Windows system and makes a registry entry.

Worm/OpaSoft looks for mapped network drives and copies itself as "ScrSvr.exe" wherever it has writing rights.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Opasoft.AA

Virus info

Virus alias:	W32/Opaserv.worm [McAfee], W32/Opaserv-A [Sophos], Win32.Opaserv [CA], WORM_OPASOFT.A [Trend], Worm.Win32.Opasoft [AVP], W32.Opaserv.Worm
File size:	28,672 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreading over unprotected net resources.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated, Worm/Opasoft.AA checks for 'ScrSvrOld' in the registry.

Next, the worm checks if the file %windir%\ScrSvr.exe was run. If not, the worm copies itself in this file and makes a registry entry.

It tries to spread over unprotected net resources.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/OpaSoft.BC

Virus info

Virus alias:	W32.Opaserv.Worm, WORM_OPASERV.E [Trend], W32/Opaserv-C [Sophos], Win32.Opaserv.E [CA], W32/Opaserv.worm [McAfee]
File size:	24,064 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over unprotected network resources.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated, Worm/OpaSoft.BC checks for 'BrasilOld' in the registry.

Next, the worm checks if the file C:\Windows\Brasil.exe or C:\Windows\Brasil.pif was activated. If not, it copies itself in this file and makes a registry entry.

After controlling the registry and the place of its activity, the worm ensures that it has only one version in system memory, using a Mutex named Brasil31415.

It tires to spread over unprotected network resources.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/OpaSoft.D

Virus info

Virus alias:	W32.Opaserv.Worm, WORM_OPASERV.G [Trend], W32/Opaserv-F [Sophos], Win32.Opaserv.G [CA], W32/Opaserv.worm [McAfee]
File size:	12,800 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreading over unprotected network resources.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated on a Windows 95/98/Me computer, Worm/OpaSoft.D checks for 'Cuzao!Old' in the registry.

If present, the related file is deleted. If not, the worm checks for 'cronos' in the registry

If not present, the worm makes a registry entry.

Then, it checks if the file C:\WINDOWS\marco!.scr has been activated. If not, it copies itself in this file and makes a registry entry.

The worm uses a security vulnerability of Microsoft Windows 95/98/Me. It sends single password characters to the network resource for accessing other Windows 95/98/Me files, without knowing the password.

It tries to spread over unprotected network resources.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Opasoft.E

Virus info

Virus alias:	W32.Opaserv.Worm, WORM_OPASERV.E [Trend], W32/Opaserv-C [Sophos], Win32.Opaserv.E [CA], W32/Opaserv.worm [McAfee]
File size:	24,064 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreading over unprotected network resources.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated on Windows 95/98/Me Computers, Worm/Opasoft.E checks for 'BrasilOld' in the registry.

After controlling the registry and the place of its activity, the worm ensures that it has only one version in system memory, using a Mutex named Brasil31415.

The worm uses a security vulnerability of Microsoft Windows 95/98/Me. It sends single password characters to the network resource for accessing other Windows 95/98/Me files, without knowing the password.

t looks like the worm is able to update itself, reading files from a website.

It also tries to download a file named Puta!!.exe.

It tries to spread over unprotected net resources.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/OpaSoft.F

Virus info

Virus alias:	Win32.Opaserv.H [CA], WORM_OPASERV.H [Trend], W32/Opaserv-G [Sophos], W32/Opaserv.worm.k [McAfee]
File size:	21,504 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over unprotected network resources.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated on Windows 95/98/Me computers, Worm/OpaSoft.F checks for 'GustavVED' in the registry.

After controlling the registry and the place of its activity, the worm ensures that it has only one version in system memory, using a Mutex named GustavoDist.

It looks like the worm is able to update itself, reading files from a website.

It also tries to download a file named Tavinh.scr.

It tries to spread over unprotected network resources.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/OpaSoft.G

Virus info

Virus alias:	Trojan.Win32.OpaKill.a, W32/Opaserv.worm, W95/Opaserv.worm.F, W32.Opaserv.K.W
File size:	28,672 Bytes or 32,256 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreading over unprotected network resources.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated on Windows 95/98/Me computers, Worm/Opasoft.G checks for 'ALEVIROld' in the registry.

After controlling the registry and the place of its activity, the worm ensures that it has only one version in system memory, using a Mutex named ALEVIR.

It looks like the worm is able to update itself, reading files from a website.

It also tries to download a file named ALEVIR.exe.

It tries to spread over unprotected network resources.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/OpaSoft.J

Virus info

Virus alias:	Worm.Win32.Opasoft.h, W32/Opaserv.worm, W95/Opaserv.worm.P, W32.Opaserv.J.W
File size:	18,432 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over unprotected network resources, Backdoor function.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated, Worm/OpaSoft.J checks for 'Srv32Old' in the registry.

After controlling the registry and the place of its activity, the worm ensures that it has only one version in system memory, using a Mutex named Srv3231415.

It looks like the worm is able to update itself, reading files from a website.

It also tries to download a file named Sccss.

Worm/OpaSoft.J also has backdoor functions, that allow the attacker access to a computer. Thus, the worm opens a random TCP and UDP port for contacting the attacker.

Spreads over unprotected network resources.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Opasoft.P

Virus info

Virus alias:	W32/Opaserv.worm.ac [McAfee], Worm.Win32.Opasoft.p [KAV], Win32/Opaserv.AA.worm [GeCAD]
File size:	24,064 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over unprotected network resources.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated, Worm/Opasoft.P checks for 'SpeedBoss' in the registry.

After controlling the registry and the place of its activity, the worm ensures that it has only one version in system memory, using a Mutex named SpeedyDoS2!.

It looks like the worm is able to update itself, reading files from a website.

It tries to spread over unprotected network resources.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Opasoft.Q

Virus info

Virus alias:	Worm.Win32.Opasoft.p, W32/Opaserv.worm, W32.Opaserv.AD.
File size:	18,432 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over unprotected network resources.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated on Windows 95/98/Me computers, Worm/Opasoft.Q checks for 'SRV32Old' in the registry.

After controlling the registry and the place of its activity, the worm ensures that it has only one version in system memory, using a Mutex named SVR32.

It looks like the worm is able to update itself, reading files from a website.

It also tries to download a file named SVR32.exe.

It tries to spread over unprotected network resources.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Opasoft.R

Virus info

Virus alias:	W32.Opaserv.AD.Worm, Worm.Win32.Opasoft.q
File size:	18,691 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over unprotected network resources.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated on Windows 95/98/Me computers, Worm/Opasoft.R creates and checks a Mutex named 4wsDosFDPS!. Thus, a single version of the worm will be active on the system.

The worm uses a security vulnerability of Microsoft Windows 95/98/Me. It sends single password characters to the network resource for accessing other Windows 95/98/Me files, without knowing the password.

It tries to spread over unprotected network resources.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Outsider

Virus info

Virus alias:	I-Worm.Tanger (AVP), W32.HLLW.Tang@mm (NAV), W32/Gant@MM, W32/Gant.gen@MM
File size:	21, 504 Bytes (UPX)
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads by email and shared networks.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

Worm/Outsider creates multiple copies in Windows directory.

It also creates worm copies in C:\%WINDIR%\%SYSTEMDIR%

The worm also modifies the registry

The worm tries to spread by email, IRC and over P2P shared networks. It collects email addresses from Windows Address Book.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/P2P.Surnova

Virus info

Virus alias:	I-Worm.Supova (VirusBuster), W32.Supova.Worm (Symantec), W32/Supova.worm!p2p, Win32.HLLW.Supernova (DrWeb), Win32.Kitty (Esafe), Worm.P2P.Surnova (AVP), WORM_SURNOVA (Trend)
File size:	40,960 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads through KaZaA and MSN Messenger
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When Worm/P2P.Surnova is activated, an error message appears, named "CHEESE-BURGER.exe".

Then, the worm copies itself in C:\%WinDIR%\Media

A worm copy is saved in WINDOWS directory.

The worm makes an autostart registry entry.

Worm/P2P.Surnova spreads through KaZaA and MSN Messenger. It tries to determine the KaZaA user to download the worm, using a software title.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Padobot.A

Virus info

Virus alias:	W32.Korgo.A, Worm.Win32.Padobot.b, Exploit-Lsass.gen
File size:	34,880 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Uses "LSASS Windows" security hole
Discovered on:	22.05.2004
From VDF version:	6.25.00.70

General information

When activated, Padobot.A deletes the file go.exe from the folder it was run on. The worm makes "r10", "u2" and "uterm5" mutexes, to verify if one of its tasks is active on the system.

If there is the file "WinUpdate", but not in the same folder as the worm, then it copies itself.

The worm starts an attack over Port 445 using the LSASS Windows security hole. If it succeeds, the contacted computer tries to connect to the host PC and downloads the worm. Then it generates an endless loop, which hides that the computer has been overtaken.

Worm/Padobot.A listens on TCP ports 113, 3067 and 2041. If it can connect to another system over one of these ports, it sends itself there. Worm/Padobot.A spreads using LSASS security hole, as Worm/Sasser did.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Padobot.B

Virus info

Virus alias:	Worm.W32.Padobot, W32.Korgo.B
File size:	10.240 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Uses "LSASS Windows" security hole.
Discovered on:	24.05.2004
From VDF version:	6.25.00.75

General information

When activated, Padobot.B deletes the file go.exe from the directory it was opened on.

The worm uses the mutexes "r10", "u2" and "uterm5", that only allow one active version of the worm on the system.

The worm also tries to connect to IRC servers on TCP port 6667.

The worm starts an attack on TCP port 445, using the LSASS Windows security hole. If connection succeeds, the contacted PC tries to reach the host PC and to download the worm. Then, an endless loop starts, preventing the computer to shut down.

Padobot.A listens on TCP ports: 113, 3067 and 2041. If it can connect through one of these ports, it sends itself to other computers.

Worm/Padobot.B spreads through TCP ports, using LSASS security hole, as Worm/Sasser does.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Padobot.C

Virus info

Virus alias:	W32.Korgo.B, W32.Korgo.C
File size:	10.240 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Uses "LSASS Windows" security hole.
Discovered on:	25.05.2004
From VDF version:	6.25.00.75

General information

When activated, Padobot.C deletes the file ftpupd.exe from the directory it was opened on.

The worm uses the mutexes "r10", "u7", "u6" and "uterm7", that only allow one active version of the worm on the system.

The worm starts an attack on TCP port 445, using the LSASS Windows security hole. If connection suceeds, the contacted PC tries to reach the host PC and to download the worm.

Worm/Padobot.C, as Worm/Sasser, spreads using LSASS security hole, by contacting various TCP ports. It listens on TCP ports 113 and 3067. If connection succeeds, the worm sends itself through.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Padobot.D

Virus info

Virus alias:	W32.Korgo.D, Worm.Win32.Padobot.Gen
File size:	9,728 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	-
Discovered on:	30.05.2004
From VDF version:	6.25.00.83

General information

When activated, Padobot.D deletes the file ftpupd.exe from the current folder. It uses Mutexes u6, u7, u8 and uterm8, for ensuring that there are none of its active tasks on the system.

Worm/Padobot.D starts an attack over TCP port 445, using LSASS Windows security hole. If this succeeds, the worm tries to contact the host PC of other clean computers, for downloading its components.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Padobot.E

Virus info

Virus alias:	W32.Korgo.E
File size:	10.752 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Uses "LSASS Windows" security hole.
Discovered on:	31.05.2004
From VDF version:	6.25.00.83

General information

When activated, Padobot.E deletes the file ftpupd.exe from the directory it was opened on.

The worm uses the mutexes "u9", "u7", "u6" and "uterm_9", that only allow one active version of the worm on the system.

The worm starts an attack on TCP port 445, using the LSASS Windows security hole. If connection suceeds, the contacted PC tries to reach the host PC and to download the worm.

Worm/Padobot.E spreads through TCP ports.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Padobot.F

Virus info

Virus alias:	W32.Korgo.F, Worm.Win32.Padobot.e, W32/Korgo.worm.g, WORM_KORGO.F
File size:	10,752 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Uses LSASS security hole (MS04-011 Microsoft Security Bulletin)
Discovered on:	01.06.2004
From VDF version:	6.25.00.83

General information

When activated, Padobot.F deletes the file ftpupd.exe from the folder it was run on.

If it finds the registry entry for "Disk Defragmenter", the worm randomly generates a file and copies it in Windows System.

Worm/Padobot.F listens on TCP ports: 113, 3067 and other similar ports. If it succeeds to connect to a port, it tries to upload its viral file. The worm also tries to contact IRC servers on TCP Port 6667.

The worm starts an attack on TCP Port 445, using the LSASS Windows security hole. When succeeded, the contacted PC tries to connect to the Host-PC and to download the virus file.

As Worm/Sasser before it, Worm/Padobot.F spreads using LSASS security hole. More information is to be found on MS04-011 Microsoft Security Bulletin.

The worm connects to other systems using TCP Port 445. When connected, the worm file is downloaded from the infected system and activated.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Paukor

Virus info

Virus alias:	-
File size:	416.256 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	27.11.2001
From VDF version:	6.23.00.00

General information

When the attachment is opened, W32.Paukor creates two files in Windows directory: Systray.exe and Msp.dll.

Then, other two files are created in Windows: Images_zipped.exe and Msd.vbs.

Images_zipped.exe is the attachment to be sent with Microsoft Outlook.

Msd.vbs runs the email sending routine with Outlook, using the address book.

A message window is displayed, with an "OK" button to be pressed:

"This WinZip archive seems to be incomplete. Please download again the file,or contact the vendor for an other copy"

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Pikachu

Virus info

Virus alias:	WIN32/Pikachu.32768
File size:	32.768 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Deletes all files from Windows System directory.
Discovered on:	20.09.2000
From VDF version:	6.23.00.00

General information

A harmless Pokemon-Icon tries to determine the user to open the file. When opened, the virus displays an image, with a message.

n this time, the virus overwrites Autoexec.bat:

@ECHO OFF

del C:\WINDOWS*.*

del C:\WINDOWS\SYSTEM*.*

Its commands will delete all Windows and Windows System directory content on the next system start. This means a total data loss. A new installation of the operating system will be needed.

The Internet worm Pikachu (alias Pokey) spreads via MS Outlook to all Contacts in the Address Book. It is not a VBS worm, but a normal application (.exe).

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Purol.P2P.B

Virus info

Virus alias:	-
File size:	38,225 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over shared network resources.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated, Worm/Purol.P2P.B tries to delete files from directories.

It spreads over shared network resources.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Randex.D

Virus info

Virus alias:	W32/Slanper.worm [McAfee], W32/Slanper-A [Sophos], Worm.Win32.Randex.d [KAV]
File size:	32,256 Bytes, 13,824 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over shared networks.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated, Worm/Randex tries to connect to other computers, using random IP addresses. The worm tries to contact every computer user, using a list of passwords.

It makes an autostart registry entry.

Worm/Randex.D tries to copy itsel into administrative archives with weak passwords.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Roron.50

Virus info

Virus alias:	I-Worm.Roron.50.a, W32/oror, W32.HLLW.Oror@m
File size:	106,496 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreading by email and shared networks.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated, Worm/Roron.50 displays a false WinZip error message.

It copies itself as C:\%WinDIR%\Rundll16.exe and makes an autostart registry entry.

The worm is sent to all email addresses found in Inbox.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Roron.Gen

Virus info

Virus alias:	I-Worm.Roron.12 [AVP], W32/Oror, W95/Roro.P@mm, W32.HLLW.Oror.B
File size:	131,072 Bytes, 139,264 Bytes,
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated, Worm/Roron.40.B.2 displays a false error message.

It copies itself with random names into Windows directory. Then, it makes an autostart registry entry.

The worm sends itself by email to all addresses found in the Inbox. The email is randomly composed.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Sasser

Virus info

Virus alias:	W32/Sasser.worm.a, WORM_SASSER.A
File size:	15.872 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Uses LSASS security hole.
Discovered on:	30.04.2004
From VDF version:	6.25.00.30

General information

A mutex (Jobaka3l) ensures that there is no other active task of the worm on the system.

The worm is copied as %WinDIR%\avserve.exe and it makes an autostart registry entry.

It uses AbortSystemShutdown API, for hiding computer shut-down or restart.

The Lsass.exe process is ended after the worm has used Windows LSASS security hole. Windows displays a message and shuts the system down in a minute.

The worm creates the file C:\win.log, which contains the IP addresses of the computers it tried to infect and the number of infected systems.

It starts an FTP server on TCP port 5554 and so it spreads on other systems.

It collects IP addresses from the infected systems and generates new ones, similar to those collected.

Through TCP port 445, the worm contacts other systems, on which the LSASS security hole has not been patched. If the connection succeeds, a shell code is sent to the other system, for opening the TCP port 9996. If the shell code is used for reaching back to the infected computer, it switches on TCP port 5554 and the other 'clean' system gets a worm copy. This copy is named using 4 or 5 numbers, followed by _up.exe. For example: 74354_up.exe.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Vorlage

Virus info

Virus alias:	Sasser
File size:	15,872 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Uses the LSASS vulnerability In drive C: the file WIN.LOG can be seen.
Discovered on:	01.05.2004
From VDF version:	6.25.00.42

General information

Worm/Sasser.A spreads itself using the Microsoft LSASS (Local Security Authority Subsystem Service) security hole. See:

http://www.microsoft.com/technet/security/bulletin/MS04-0 11.mspx

The worm can install itself on the Windows XP or Windows 2000 system if the above patch was not applied. It searches for more vulnerabile computers over port TCP 445/ TCP 9996. It uses a FTP Script to send files over port 5554. Worm/Sasser.A copies itself in Windows as AVSERVE.EXE and makes a registry entry, to be activated by the next system start.

The file C:\WIN.LOG contain the number of the infected hosts, together with the IP address of the host most recently attempted to be compromised.

The worm creates more copies of itself in Windows, named

<%5 random numbers%>_up.exe.

Distributes by using Microsoft LSASS vulnerability.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Sasser.B

Virus info

Virus alias:	WORM_SASSER.B, W32/Sasser.worm.b, Worm.Win32.Sasser.b, W32/S
File size:	15,872 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Uses LSASS security hole (Microsoft Security Bulletin MS04-011)
Discovered on:	01.05.2004
From VDF version:	6.25.00.60

General information

It starts a FTP server over TCP Port 5554. This server is used for spreading the worm to other systems. It collects IP addresses from the infected systems and generates new IP addresses, similar to the ones it gathered.

It contacts on TCP Port 445 other systems, which did not have the LSASS security hole fixed. When connected to another computer, it sends to it a Shell Code to open the TCP Port 9996. After that, it will use TCP Port 5554 to send a copy of the worm to the clean computer. This copy has a name of 4 or 5 numbers, followed by _up.exe. For example: 74354_up.exe.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Sasser.C

Virus info

Virus alias:	W32/Sasser-C, Worm.Win32.Sasser.c, W32/Sasser.worm.c, WORM_S
File size:	15,872 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Uses LSASS security hole (Microsoft Security Bulletin MS04-011)
Discovered on:	02.05.2004
From VDF version:	6.25.00.60

General information

It starts an FTP server over TCP Port 5554. This server is used for spreading the worm to other systems. It collects IP addresses from the infected systems and generates new IP addresses, similar to the ones it gathered.

It contacts on TCP Port 445 other systems, which did not have the LSASS security hole fixed. When connected, it sends to it a Shell Code to open the TCP Port 9996. After that, it will use TCP Port 5554 to send a copy of the worm to the clean computer. This copy has a name of 4 or 5 numbers, followed by _up.exe. For example: 74354_up.exe.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Sasser.D

Virus info

Virus alias:	W32/Sasser-D, WORM_SASSER.D, W32/Sasser.worm.d, Win32.Sasser
File size:	16,384 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Uses LSASS security hole (Microsoft Security Bulletin MS04-011)
Discovered on:	03.05.2004
From VDF version:	6.25.00.60

General information

It starts a FTP server over TCP Port 5554. This server is used for spreading the worm to other systems. It collects IP addresses from the infected systems and generates new IP addresses, similar to the ones it gathered.

It contacts on TCP Port 445 other systems, which did not close the LSASS security hole. When connected, it sends to it a Shell Code to open the TCP Port 9996. After that, it will use TCP Port 5554 to send a copy of the worm to the clean computer. This copy has a name of 4 or 5 numbers, followed by _up.exe. For example: 74354_up.exe.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Sasser.E

Virus info

Virus alias:	-
File size:	15,872 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Uses LSASS security hole (Microsoft Security Bulletin MS04-011)
Discovered on:	09.05.2004
From VDF version:	6.25.00.60

General information

It starts an FTP server over TCP Port 5554. This server is used for spreading the worm to other systems. It collects IP addresses from the infected systems and generates new IP addresses, similar to the ones it gathered.

It contacts on TCP Port 445 other systems, which did not have the LSASS security hole fixed. When connected, it sends to it a Shell Code to open the TCP Port 9996. After that, it will use TCP Port 5554 to send a copy of the worm to the clean computer. This copy has a name of 4 or 5 numbers, followed by _up.exe. For example: 74354_up.exe.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Sasser.F

Virus info

Virus alias:	-
File size:	74,752 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Uses LSASS security hole (Microsoft Security Bulletin MS04-011)
Discovered on:	10.05.2004
From VDF version:	6.25.00.60

General information

It starts an FTP server over TCP Port 5554. This server is used for spreading the worm to other systems. It collects IP addresses from the infected systems and generates new IP addresses, similar to the ones it gathered.

It contacts on TCP Port 445 other systems, which did not have the LSASS security hole fixed. When connected, it sends to it a Shell Code to open the TCP Port 9996. After that, it will use TCP Port 5554 to send a copy of the worm to the clean computer. This copy has a name of 4 or 5 characters, followed by _up.exe.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Scold.A

Virus info

Virus alias:	W32/Scold@MM, Win32.Scold.A, W32.Scold@mm
File size:	28,160 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	sends itself by email * increased email traffic
Discovered on:	11.12.2003
From VDF version:	6.22.00.06

General information

When activated, the worm copies itself in the following directories:

* C:\%Windows%\warm.scr
* C:\%Windows%\pf17.scr

It creates a registry entry, so that it will be run at the next system start.

Then it sends itself to all contacts found in Microsoft Outlook Address Book.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Snapper.A

Virus info

Virus alias:	W32.Snapper.A@mm, I-Worm.Snapper [Kaspersky], W32/Snapper@MM [McAfee], Snapper [F-Secure]
File size:	9kB
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

Worm/Snapper.A contains a .dll file, which may be found as:

%WinDIR%\ieload.dll
%SystemDIR%\ieload.dll

The worm is activated every time Internet Explorer starts.

Regularly, a website is opened on TCP port 80.

By opening the html file of the email, a file named Banner.htm is downloaded. This is an empty website, which contains a link to the worm. This site uses the Internet Explorer Object Tag vulnerability (described in Microsoft Security Bulletin MS03-032) and downloads a malicious html file named Htmlhelp.cgi. This file contains a worm copy and a VBSkript, which installs the worm as %WinDIR%\ieload.dll.

The worm uses its own SMTP engine for sending itself to email addresses from Windows Address Book.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Sober

Virus info

Virus alias:	I-Worm.Sober, W32/Sober.A, Win32/Sober.A, W32/Sober@MM, W32.
File size:	~63,488 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Overwrites files When activating the worm, a false "Error" dialog box appears.
Discovered on:	24.10.2003
From VDF version:	6.22.00.15

General information

The worm Sober was developed in Visual Basic 6.0 (German version) and packed with UPX. The UPX header was changed, so the unpacking with traditional methods would be more difficult.

At the first start the worm infects all the executables in "My Shared Folder" where it generally occupies the first position. The worm performs as so called "overwriter" and causes permanent damage to these executables. The purpose of this procedure is the intentional spreading, over file sharing networks, of the data which the worm regularly places in the exchanged files. If the host file is smaller than the worm, then the file will be completely overwritten.

Finally, a false dialog box appears.

The worm generally starts in two instances, which means it runs simultaneously twice in the system. So, if one of the processes is terminated, the other establishes its absence and another procedure is initiated to substitute the finished one. Thus, the user has no chance of terminating the both processes at the same time, using Task Manager.

If one attempts to remove the Auto Start entry of the active worm, it immediately writes itself back into the registry. This behavior is obtained with a Visual Basic Timer Object, which periodically checks the registry for this Autorun entry.

Email spreading, using its own SMTP engine and over Kazaa via "My Shared Folder".

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Sober.B

Virus info

Virus alias:	I-Worm.Sober.b
File size:	54,784 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sends itself by email When activating the worm, a false dialog box appears informing about an error: "Header is missing".
Discovered on:	18.12.2003
From VDF version:	6.23.00.13

General information

The worm Sober.B was developed in Visual Basic 6 and packed with UPX, thus hiding the viral code. The size of the attachment in a Worm/Sober.B email can be different. The worm chooses random characters for the end of the file and so the size of the files can vary between 54 and 60 kbytes.

When the attachment is open, a window appears with the message "Header is missing". In background, the worm Sober.B copies itself.

The file "mscolmon.ocx" contains the email addresses found by the malware. Using its own STMP engine the worm Sober.B sends itself to these addresses.

Worm/Sober.B infects the files in "My Shared Folder" and so it can spread using filesharing programs (P2P) as Kazaa or Emule.

The worm starts in two instances, so it is running in two places simultaneously in the system. If one of the processes is terminated, the other will establish its absence. The file spooler.exe, inserted by the worm, will restart the deactivated process. The names of the both processes are randomly generated and are not identical to the viral .EXE files. The user has no chance of terminating the both processes at the same time, using Task Manager.

If one attempts to remove the Auto Start entry of the active worm, it immediately writes itself back into the registry. This behavior is obtained with a Visual Basic Timer Object, which periodically checks the registry for this Autorun entry.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Sober.C

Virus info

Virus alias:	I-Worm.Sober.C, W32.Sober.C@mm, Win32.Sober.C@mm
File size:	Variable, ~72 kbytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Overwrites files When activating the worm, a dialog box appears informing about a Runtime Error
Discovered on:	20.12.2003
From VDF version:	6.23.00.17

General information

The worm Sober.C, like its precedent, was developed in Visual Basic 6.0 (German version) and packed in UPX. Later the UPX header was changed, so that the unpacking with traditional methods would be more difficult.
At the first start the worm infects all the executables in "My Shared Folder" where it generally occupies the first position. The worm performs as so called "overwriter" and causes permanent damage to these executables. The purpose of this procedure is the intentional spreading, over file sharing networks, of the data which the worm regularly places in the exchanged files. If the host file is smaller than the worm, then the file will be completely overwritten.
Worm/Sober.C makes three copies of itself in Windows system, two of them having different (random) names, like a file named "SYSHOSTX.EXE".
Then, a message box appears, with the following message: "%FILENAME% has caused an unknown error. Stop: 00000010x08"
The worm generally starts in two instances, which means it runs simultaneously twice in the system. So, if one of the processes is terminated, the other detects its absence and another procedure is initiated to substitute the finished one. Thus, the user has no chance of terminating both processes at the same time, using Task Manager.
Beyond that the worm blocks the normal read access for its files. For this, it uses the "exclusive rights" mode, so that these files could not be open in normal read rights. This is similar to the Windows procedure used for protecting paging files. If one attempts to remove the Auto Start entry of the active worm, it immediately writes itself back into the registry. This behavior is obtained with a Visual Basic Timer Object, which periodically checks the registry for this Autorun entry.
Email spreading, using its own SMTP engine and over P2P file sharing programs, like "Kazaa" or "Edonkey".

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Sober.C1

Virus info

Virus alias:	W32/Sober-C [Sophos], Win32.Sober.C [Computer Associates], W32/Sober.c@MM [McAfee], WORM_SOBER.C [Trend], I-Worm.Sober.c [Kaspersky], W32/Sober, W95/Sober.C@mm, W32.Sober.C@mm
File size:	(min) 74,346 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	-

General information

When activated, Worm/Sober.C1 is copied in %SystemDIR% with two random file names.

It searches in files for email addresses and saves them in C:\%SystemDIR%\Savesyss.dll

It enters autostart registry entries.

When first activated, the worm displays the following error message:

Title: Microsoft

Text: "first" has caused an unknown error. Stop: 00000010*08

Worm/Sober.C1 uses its own SMTP engine for email spreading.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Sober.D

Virus info

Virus alias:	I-Worm.Sober.D, W32.Sober.D@mm, Win32.Sober.D@mm
File size:	33,792 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sends itself by email When the worm is launched, a message window will be generated, having the string "%Filename%" in the titlebar, where %Filename% is the name of the infected file.
Discovered on:	08.03.2004
From VDF version:	6.24.00.43

General information

The worm Sober.D was also developed like its predecessors in Visual Basic 6.0 (German version) and packed with UPX. Again the UPX headers were later altered, in order to make unpacking more difficult with conventional means.

The worm copies itself with a random name in %System%. This file name is randomlly built up from two strings.

Sends itself via email using its own smtp engine.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Sober.E

Virus info

Virus alias:	W32.Sober.E
File size:	30,720 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	-

General information

When activated, Worm/Sober.E copies itself as %Systemdir%\%random filename%.exe

It makes an autostart registry entry.

The worm starts Microsoft PaintBrush or displays a message:

"Graphic Modul not found".

If the date is past March, 24th, 2004, the worm downloads the file %Windir%\ndhaqqth.exe from one of the following websites, through TCP port 80:

home.arcor.de
people.freenet.de

It searches for email addresses on all local drives. The collected email addresses are saved in %Systemdir%\WinRun32.dll. Then the worm is sent to these addresses.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Sober.G

Virus info

Virus alias:	I-Worm.Sober.g, WORM_SOBER.G, W32/Sober.g@MM
File size:	49,661 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Overwrites files
Discovered on:	-
From VDF version:	-

General information

When activated, Worm/Sober.G opens a "File not found" window, with the message "Special-UnZip Data-Module is missing Open with Notepad?". When "yes" button is pressed, the worm creates the file "converted_%filename%.txt", where %filename% is the worm's name. In this file it writes random characters and numbers and opens it with Notepad.

Then the worm is installed in the system and copied in Windows System directory under a random name and having an .exe extension

The worm sends e-mail messages in English and German, having an attachment. The attached file is an executable or a ZIP archive.

Send itself by email, using its own SMTP engine.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Sober.H

Virus info

Virus alias:	W32.Sober.H@mm, Troj/Sober-H, Trojan.Ascetic.A
File size:	59,747 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	-
Discovered on:	11.06.2004
From VDF version:	6.25.00.92

General information

When activated, Worm/Sober.H drops the following files in Windows system:

* bcegfds.lll
* zhcarxxi.vvx
* cvqaikxt.apk
* Odin-Anon.Ger
* mswn32sock.dats
* llsapwin32.dats

Then it copies itself in the system folder, under a random name. The name of this file is randomly composed.

Distribution

* Sent by SPAM emails
* Downloaded by WIN PE files

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Sobig.B

Virus info

Virus alias:	Win32/Palyh.A@mm, W32.HLLW.Mankx@mm
File size:	49,000 bytes- 54,000 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sends itself by email, registry entries The file msccn.exe appears in the Windows folder.
Discovered on:	19.05.2003
From VDF version:	6.19.00.18

General information

When started, it copies itself in Windows directory as "msccn.exe" and makes registry entries.

The worm looks for files with extension .TXT, .EML, .HTM* .DBX and for the Windows Address Book (WAB). Here it can find email addresses and sends itself to them using the default SMTP engine.

The worm gathers all the addresses it found in one file: "hnks.ini". Worm/Sobig.B looks for shared networks. When it finds a computer on which it has writing rights, it searches for the following paths and copies itself there:

* \Windows\All Users\Start Menu\Programs\StartUp\
* \Documents and Settings\All Users\Start Menu\Programs\Startup\

Sobig.B is an Internet worm, which sends itself by email and spreads over shared Windows networks.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Sobig.C

Virus info

Virus alias:	-
File size:	59 kbytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Email and network spreading The file mscvb32.exe appears in the Windows folder.
Discovered on:	01.06.2003
From VDF version:	6.19.00.xx

General information

Worm/Sobig.C is ca. 59 kbytes, packed with UPX. When started, it copies itself in Windows directory as mscvb32.exe and makes the files msddr.dll and msddr.dat. In msddr.dat file it gathers the email addresses it found in the local files of type .HTML, .HTM, .TXT, .EML and .WAB. These email addresses are saved encoded.

Distribution

- Email sending

- Networks

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Sobig.D

Virus info

Virus alias:	W32.Sobig.D@mm
File size:	59 kbytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Email and Internet spreading The ~59 kbytes file "CFTRB32.EXE" appears in the Windows directory.
Discovered on:	18.06.2003
From VDF version:	6.20.00.13

General information

Worm/Sobig.D is ca. 59 kbytes, packed with UPX. When started, it copies itself in Windows directory as cftrb32.exe and makes the file rssp32.dat. In this file it gathers the email addresses it found in the local files of type .HTML, .HTM, .TXT, .EML and .WAB. These email addresses are saved encoded.

If the worm can find the following paths in the local network, it copies itself there:

* \Documents and Settings\All Users\Start Menu\Programs\Startup
* \Windows\All Users\Start Menu\Programs\StartUp

Distribution

- Email sending

- Local networks

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Sobig.E

Virus info

Virus alias:	W32/Sobig.E@mm, Win32.HLLW.Reteras
File size:	86,528 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Email and network spreading The file WINSSK32.EXE in the Windows directory.
Discovered on:	25.06.2003
From VDF version:	6.20.00.18

General information

Worm/Sobig.E is about 86,528 kbytes, packed with ASPACK and TELock. The characters forming the virus file are encoded using a complex algorithm.

When started, it copies itself in Windows directory as WINSSK32.EXE and makes registry entries.

The worm makes the MSRRF.DAT file in Windows. Worm/Sobig.E spreads itself by email. Thus it sends messages with different subjects, a certain body text and various attachments.

Distribution

- Email sending

- Networks

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Sobig.F

Virus info

Virus alias:	W32/Sobig.f@MM, WORM_SOBIG.F, W32.Sobig.F@mm
File size:	~ 70 - 75 Kbytes
Virus type:	Worm
Infected operating systems:	-
Damage:	sends itself by email * The file %windir%\winppr32.exe * Unexpected intensive NTP traffic
Discovered on:	19.08.2003
From VDF version:	6.21.00.20

General information

Worm/Sobig.F is about 70-75 kbytes, packed with Telock and written in Visual C. It tries to escape identification by long variation. When started, it copies itself in Windows directory under the filename

* winppr32.exe
and makes the following file:
* winstt32.dat

The worm makes registry entries.

From then on, the worm files can be loaded on Internet and for example self update or run new files. By this function it can also mail important and security data (passwords) from an infected computer on Internet. The infected computer can be used as a spam relay too. For the data transfer, the worm uses NTP protocol.

Worm/Sobig.F opens ports 995 to 999 on the local system and waits for instructions, for example downloads and opening Trojans.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Sonic

Virus info

Virus alias:	W32/Sonic.worm
File size:	25.088 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	09.11.2000
From VDF version:	6.23.00.00

General information

When the .exe file is opened, the virus is saved on memory and remains active in the background.

To be active after system restart, the worm copies itself in C:\%WinDIR%\%SystemDIR%\ and registers:

HKLM\Software\Microsoft\Windows\CurrentVersion\RunGDI =% WinSystem%\GDI32.EXE

To hide its own activity, the virus displays a false error message:

"C:\LOVERS.EXE is not a valid Win32 application."

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Sorbig.A

Virus info

Virus alias:	Win32.Sorbig.A@mm
File size:	65,536 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	* The files and registry entries mentioned below. * A backdoor component downloaded from Internet.
Discovered on:	09.01.2003
From VDF version:	-

General information

Worm/Sorbig.A (65,536 bytes) is searching the *.txt, *.eml, *.html, *.html, *.dbx, and *.wab files for email addresses and sends itself to these.

Worm/Sorbig.A copies itself in all Autostart directories in all mapped network drives it can find. Then a registry entry is made, so that the worm will be activated by the next system start.

Sends itself by email as executable .PIF. Worm/Sorbig.A can be activated directly from the Outlook Preview, without opening the attachment. For this it uses an existing security hole of Microsoft Outlook.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Stator

Virus info

Virus alias:	I-Worm.Stator.a [AVP], W32/Stator@MM [McAfee], Win32/Stator.Worm [CA], WORM_STATOR.A [Trend], W32/Stator-A [Sophos]
File size:	62,464 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

The worm tries to contact an SMTP server in Russia and then it sends itself from there. The email contains:

Attachment: Photo1.jpg.pif

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Surnova.D

Virus info

Virus alias:	W32.Supova.B.worm (Symantec), W32/Supova.E (Panda), Win32.Kitty.d (ESafe), Win32.Supova.D.pac (VET), Worm.P2P.Surnova.d (AVP)
File size:	14,336 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads over KaZaA and MSN Messenger
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated, Worm/Surnova.D displays an error message, named 'CHEESE-BURGER.exe':

"Application attempted to read memory at 0xFFFFFFFFh

Terminating application"

Then, the worm copies itself in C:\%WinDIR%\Media directory.

A worm copy is also made in Windows directory, named BigMac.exe.

It makes a autostart registry entry.

Worm/Surnova.D spreads over KaZaA and MSN Messanger. The worm is disguised under software names, for tempting KaZaA users to download it.

For spreading over MSN Messenger, it uses the Contacts list.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Symbi.Cabir.A

Virus info

Virus alias:	EPOC.Cabir
File size:	~
Virus type:	Worm
Infected operating systems:	-
Damage:	-
Discovered on:	15.06.2004
From VDF version:	6.25.00.96

General information

Worm/Symbi.Cabir.A is the first known mobile phone worm. However, it can not spread, without the user confirming the receipt. The worm can spread on 60-series Nokia Smartphones, operating on "Symbian" system. It sends itself as installation file (.SIS) to all near equipment and tries to copy itself in "APPS" folder.

Finally, the worm tries to send itself to all mobiles in the area, which have their Bluetooth reception activated. Anyway, the user must confirm the receipt. The worm is presently classified as Proof-of-Concept and is not a subject of serious spreading.

Distribution

The worm searches the area for mobile phones that have receive-activated Bluetooth and tries to send itself to them. If the receipt is confirmed, the worm runs and starts the bellow mentioned routines.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Tanked.A

Virus info

Virus alias:	Worm.P2P.Tanked.a
File size:	250,500 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	The files and registry entries mentioned below.
Discovered on:	20.03.2003
From VDF version:	6.18.00.19

General information

When activated, Worm/Tanked.A copies itself as \%WinDir%\%SystemDir%\net_32.exe (250.500 Bytes, hidden)

and then it makes more copies of itself with different .EXE file names and sizes in \%WinDir%\Cache32\:

The virus code has a 250,500 bytes size. For camouflage, the worm "fills" the end of the shared files with the required number of blanks. In this way, the worm can have any file size, for exp 1,471,500 bytes.This brings the advantage that no specific size could be attributed to the worm.

Worm/Tanked.A makes the following registry entry, in order for its files to be able to download over P2P program KaZaA and to infect other systems:

[HKEY_CURRENT_USER\Software\Kazaa\LocalContent]

"Dir1"="012345:C:\\WINDOWS\\Cache32"

As a precaution, the user should scan for viruses all downloaded files and applications.

Distribution

P2P file sharing programs as KaZaA, Morpheus, Edonkey2000

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Tettona

Virus info

Virus alias:	-
File size:	34.761 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreads by email.
Discovered on:	14.06.2002
From VDF version:	6.23.00.00

General information

Tettona spreads by email using its own SMTP routine. It also has a backdoor routine.

When the infected attachment is opened, the worm copies itself in Windows directory, as DLLMGR32.EXE and enters the following autorun registry key:

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVer sion\Run] "DllManager"="C:\ %WinDIR%\dllmgr32.exe"

Worm/Tettona displays a false message:

"VBRUN49.DLL not found!

Unable to execute."

For email spreading, Worm/Tettona uses its own SMTP routine. It sends itself to all email addresses it can find in WAB (Microsoft Windows Adressbuch).

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Torvil.B

Virus info

Virus alias:	I-Worm.Torvil.b, W32/Torvil@MM, W95/Swen.A@mm, W32.Swen.A@mm
File size:	-
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

When activated, Worm/Torvil.B copies itself as:

%WinDIR%\Spoolxx.exe
%WinDIR%\SMSSxx.exe
%WinDIR%\svchost.exe

It makes registry entries.

The worm collects email contacts from files with the following extensions:

INBOX
HTML
MBOX

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/W32.Sircam

Virus info

Virus alias:	W32/SirCam@MM
File size:	137,216 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	-
Discovered on:	18.07.2001
From VDF version:	-

General information

SirCam is a worm and a Win32 virus and its size is ca. 150 kbytes. When activated, it creates the following files:

* C:\Recyled\SirC32.exe
* C:\Recyled\LoveJoy_.com
* C:\Windows\System\Scam32.exe
* C:\Windows\Temp\LoveJoy_.com

The file SirC32.exe is inserted in the registry shell, to ensure that every time an .EXE file is opened, the worm will be activated. For this, it makes registry entries.

Scam32.exe file is inserted as "driver" in the registry, so that the worm will be activated by every system start.

If the files Scam32.exe or SirC32.exe were provided with the extension .DOC.COM, then the worm would delete all the saved files on the C: drive.

If a network is infected by SirCam, the worm can reach the mapped drives on other workstations (Windows 9x/NT). If it can have writing rights on any of these drives, the worm looks for files or folders.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Wallon

Virus info

Virus alias:	WORM_WALLON.A, Win32.Wallon, W32/Wallon.worm.a, I-Worm.Wallo
File size:	36,352 Bytes, 150,528 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Uses security hole LSASS
Discovered on:	11.05.2004
From VDF version:	6.25.00.60

General information

Worm/Wallon is an email with a link. The email uses an Internet Explorer security hole. This is described in Microsoft Security Bulletin MS04-004. When the link is accessed, Internet Explorer starts and downloads the file "wmplayer.exe" in Windows Media Player. The worm overwrites the exe file of Media Player. Every time the user attempts to open WMP, this generates a copy of the worm.

When the file wmplayer.exe is opened, the makes registry entries.

These will generate 5 buttons on the Internet Explorer Toolbar. Each of them is linked to http://www.google.com.super-fast-search.apsua.com.

The worm uses its own SMTP engine to send itself to the collected email addresses.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Warpigs.A1

Virus info

Virus alias:	Worm.Win32.Warpigs.a, W95/Warpigs.B, W32.HLLW.Warpig
File size:	63,520 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Spreading over shared networks.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

Worm/Warpigs.A1 copies itself as C:\%System%\Discworld.exe. It creates the file C:\%System%\Pgonwe.exe. It uses this file for sending worm copies to computers with weak administrator passwords.

Then, the worm tries to terminate processes.

It makes autorun registry entries.

It connects to a special mIRC sevrer, for receiving instructions.

It tries to spread over shared networks.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Yaha.E

Virus info

Virus alias:	I-Worm.Lentin.f
File size:	29,839 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Terminates running processes, like antivirus software and firewall applications.
Discovered on:	19.06.2002
From VDF version:	-

General information

Worm/Yaha.E is a mass mailer, which sends itself by email to addresses collected from the local * .HT* files, Windows Address Book , MSN Messenger, ICQ and Yahoo Messenger. The attachment of the email has the extension .BAT, .PIF or .SCR.

The subject, body and attachment can have different appearance.

It sends itself by email, as executable .pif .bat .scr files.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Yaha.J2

Virus info

Virus alias:	W32/Yaha.j [McAfee], W32/Yaha-j [Sophos], I-Worm.Lentin.h, W32/Yaha, W32.Yaha.J@mm
File size:	25,746 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

The worm displays a false message:

"Application innitilisation error".

It copies itself into the following hidden files:

C:\%SystemDIR%\Msnmsg32.exe
C:\%SystemDIR%\Nav32.exe
C:\%SystemDIR%\WinReg.exe

It makes autostart registry entries.

It tries to terminate all antivirus and firewall processes.

The worm collects email addresses from the following files:

Windows Address Book
MSN Messenger Contacts
Yahoo pager Contacts
ICQ Contacts

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Yaha.L

Virus info

Virus alias:	I-Worm.Lentin.j, W32/Yaha, W95/Lentin.M@mm, W32.Yaha.L@mm
File size:	34,304 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

Worm/Yaha.L copies itself as the following hidden files:

C:\%SystemDIR%\WinServices.exe.
C:\%SystemDIR%\Nav32_loader.exe
C:\%SystemDIR%\Tcpsvs32.exe

It makes autostart registry entries.

It tries to terminate all antivirus and firewall processes.

It copies itself into C:\%WinDIR%\%SystemDIR%:

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Yaha.M

Virus info

Virus alias:	W32/Yaha.K, I-Worm.Lentin.i
File size:	34,304 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email, spread over local networks Terminates running processes, like antivirus software and Firewall applications.
Discovered on:	24.12.2002
From VDF version:	-

General information

Worm/Yaha.M is an Internet worm, which sends itself by email, using its own SMTP engine. The email addresses are collected from the local .HTM and .HTML files, Windows Address Book and contacts lists of MSN Messenger, .NET Messenger and Yahoo Pager.

The worm copies itself in the Windows system as three files: WinServices.exe, Nav32_loader.exe and Tcpsvs32.exe. Then it makes registry entries.

It sends itself by email, using its own SMTP engine, to the email addresses found on the infected computer.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Yaha.P

Virus info

Virus alias:	W32/Lentin.M, W32/Yaha.P@mm
File size:	45,568 bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email, spread over local networks - terminates running processes, like antivirus software and firewall applications.
Discovered on:	-
From VDF version:	-

General information

The new version of Worm/Yaha.P (45,568 bytes) is packed with UPX. When activated, the worm copies itself as MSTASK32.EXE in Windows system and makes registry entries, in order to be run by the next system start.

Worm/Yaha.P sends itself by mail using its own SMTP engine. This enables it to use the email addresses, without the need for email programs, as Outlook. The worm searches for addreses in Windows Address Book, in files of type *.HT* and in Yahoo, MSN, NET Messenger and ICQ folders.

The email sent by Worm/Yaha.P has certain characteristics, because the Sender's Name, Subject, Body and Attachment are composed out of a list of words and phrases.

It spreads itself over email and computer networks.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Yaha.Q

Virus info

Virus alias:	I-Worm.Lentin.o (AVP), W32/Yaha-R (Sophos), WORM_YAHA.Q (Trend)
File size:	44,544 Bytes UPX gepackt
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

orm/Yaha.Q copies itself in Windows System directory as: EXELOADER.EXE and WINTASK32.EXE. It makes autostart registry entries.

It tries to terminate all antivirus processes.

Worm/Yaha.Q copies itself into shared networks. It also spreads by email, to addresses it can find in Windows Address Book, MSN Messenger, .NET Messenger, Yahoo pager, *.HT* files.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Yaha.T

Virus info

Virus alias:	I-Worm.Lentis.gen [KAV], W32/Yaha.t@MM [McAfee], W32/Yaha-T [Sophos], I-Worm.Lentin.t, W32/Yaha, W32.Yaha.T@mm
File size:	51,424 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	30.11.1999
From VDF version:	6.23.00.00

General information

he worm copies itself as the following hidden files:

C:\%SystemDIR%\WINTSK32.EXE
C:\%SystemDIR%\EXELDR32.EXE

It makes autostart registry entries.

It copies itself in C:\%Windir%\%Systemdir%

It tries to terminate all antivirus processes.

The worm looks for email addresses in: Windows Address Book, MSN Messenger, .NET Messenger, Yahoo pager, *.ht* files. It uses its own SMTP engine to spread.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Worm/Zafi.B

Virus info

Virus alias:	W32/Zafi.b@MM, PE_ZAFI.B, W32.Erkez.B@mm
File size:	12,800 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	-
Discovered on:	10.06.2004
From VDF version:	6.25.00.91

General information

When activated, Worm/Zafi.B uses "_Hazafibb," mutex, which enables its activity for merely one time in system's memory. The worm copies itself in Windows system, choosing a random 8 character file name:

* %SystemDir%\%random_name%.exe
* %SystemDir%\%random_name%.dll

Likewise, a .DLL named in this way will be provided. Worm/Zafi.B makes the registry entries.

One entry ensures that the worm will be activated by the next system start.

The worm searches for all folders containing "Share" or "Upload" string in their names and drops copies of itself there.

Then, the worm uses Internet Explorer and opens a Website to check for an active Internet connection.

Distribution

* DoS attacks on various websites.
* Sent by email, using its own SMTP engine.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

WScr/Kak.Worm

Virus info

Virus alias:	JS/Kak@M, Worm/KakWorm
File size:	0 Bytes
Virus type:	Worm
Infected operating systems:	-
Damage:	Sent by email.
Discovered on:	08.06.2000
From VDF version:	6.20.00.00

General information

Worm KAK only attacks English and French Windows 95/98 systems. It uses Microsoft Internet Explorer 5 to spread the infection, and Microsoft Outlook Express 5, as email Client. This means that the virus can be attached to every HTML email as Java Script.

It creates the file "KAK.HTA" in Windows autostart directory. It will be activated by the next system start. A window named "Driver Memory Error" will shortly display a message: "S3 driver memory alloc failed". In this time, the virus copies itself in Windows system directory with a new file name. This name is composed out of the first 8 letters of the last directory in the folder:

C:\%WinDIR%%\Application Data\Identities.

The worm is copied as "KAK.HTM" in Windows directory and modified, so that it can relaunch its attack.

After completing its action, the worm modifies AUTOEXEC.BAT, so that the next time the system is restarted, the created files are deleted from autostart directory.

It changes the Microsoft Outlook Express 5 registry settings, so that the file "%Windows%\KAK.HTM" is attached as signature to every composed email

If you already use a signature, it will no longer be used.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area

Yankee Doodle

Virus info

Virus alias:	TPxx
File size:	1881+16 bytes
Virus type:	Resident .COM and .EXE infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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.

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.

Zero Bug

Virus info

Virus alias:	Palette, ZBug
File size:	1536 bytes
Virus type:	Resident .COM infector
Infected operating systems:	-
Damage:	-
Discovered on:	-
From VDF version:	-

General information

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

You can find closer information regarding Malware and unwanted programs on our website in the virus information area.