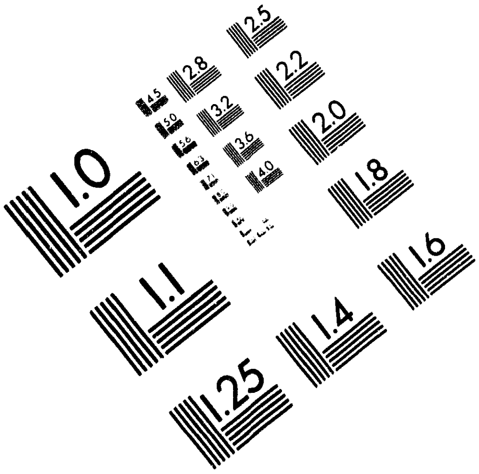
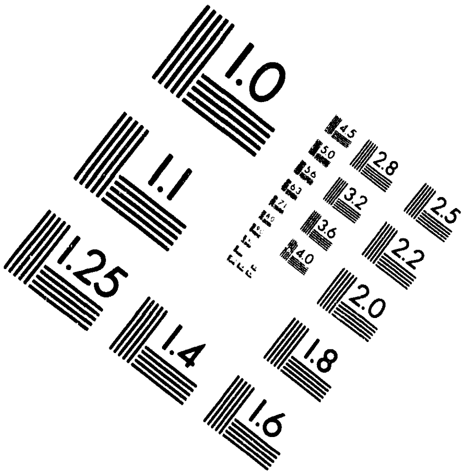


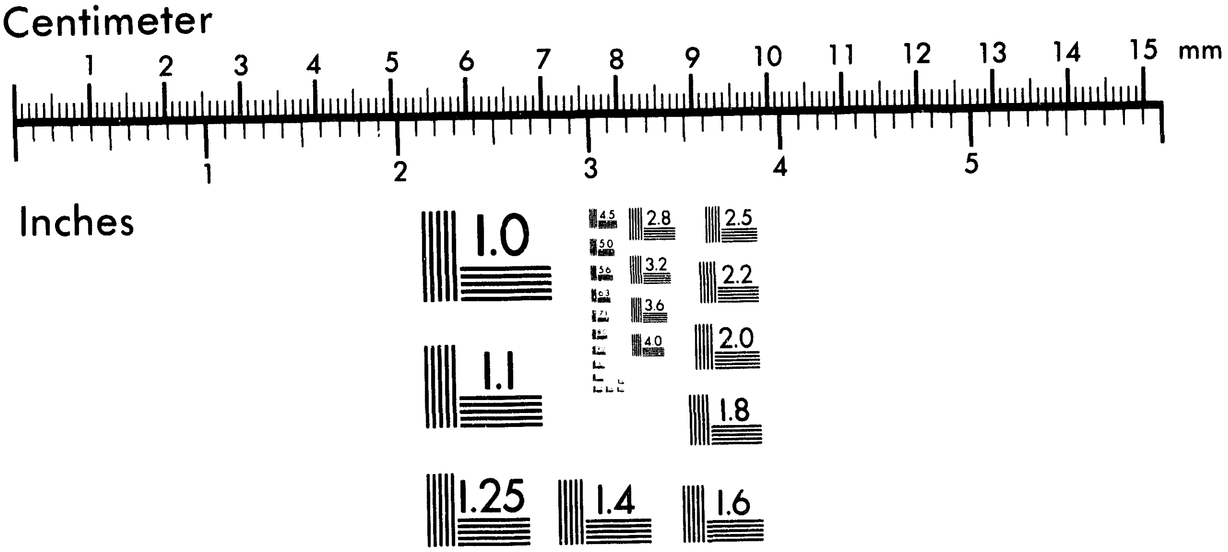
AIIM

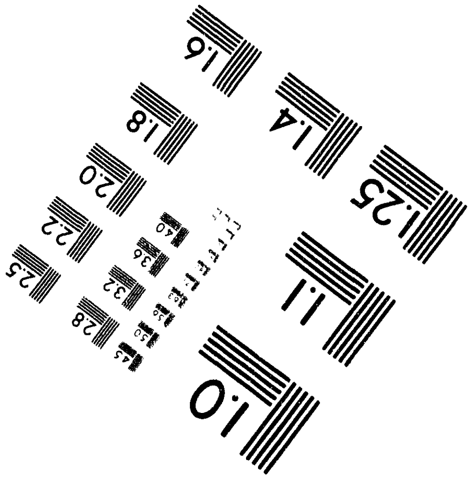
Association for Information and Image Management

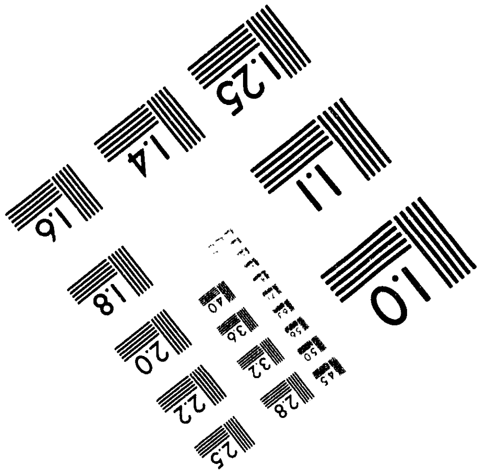
1100 Wayne Avenue, Suite 1100
Silver Spring, Maryland 20910

301/587-8202









MANUFACTURED TO AIIM STANDARDS
BY APPLIED IMAGE, INC.

1 of 2

UCRL-MA-115896

Department of Energy
CIAC
Computer Incident Advisory Capability

Computer Virus Information Update
CIAC-2301

William J. Orvis

January 15, 1994

Lawrence Livermore National Laboratory

DISCLAIMER

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

Work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-ENG-48

Table of Contents

The CIAC Computer Virus Information Update

Introduction

Purpose of this document

While CIAC periodically issues bulletins about specific computer viruses, these bulletins do not cover all the computer viruses that affect desktop computers. The purpose of this document is to identify most of the known viruses for the MS-DOS and Macintosh platforms and give an overview of the effects of each virus. We also include information on some Windows, Atari, and Amiga viruses. This document is revised periodically as new virus information becomes available. This document replaces all earlier versions of the CIAC Computer Virus Information Update. The date on the front cover indicates date on which the information in this document was extracted from CIAC's Virus database.

What's in this document

The CIAC computer virus database contains information about small computer viruses and trojan horses. There are eleven tables in this document. The first five tables contain computer virus information for the Macintosh, PC-DOS/MS-DOS, Windows, Amiga, and Atari computers. The sixth table is a list of known viruses for which we do not yet have any information in the main tables.

Because there are so many PC-DOS/MS-DOS virus names and aliases, the seventh table is a cross-reference of PC-DOS/MS-DOS virus names and aliases. To locate a PC virus by name, find the name in the first column of the cross-reference table. The name given in the second column is the virus name we have used in the PC-DOS/MS-DOS computer virus table. All the virus tables are sorted in alphabetical order by the virus name.

The last four tables contain expanded definitions for descriptions used in the virus description tables.

Information sources

Please keep in mind that these tables are made with the most recent information that we have, but they are not all based on first-hand experience. We depend on many sources of information, some of which include:

- Bill Kenny, Digital Dispatch Inc.
- Joe Wells, Symantec
- Gene Spafford, Purdue University
- Dr. Klaus Brunnstein and Simone Fischer-Huebner, Virus Test Center, Faculty for Informatics, University of Hamburg
- John Norstad, Academic Computing and Network Services, Northwestern University
- Joe Hirst, British Computer Virus Research Center
- McAfee Associates
- CERT, the Computer Emergency Response Team at the Software Engineering Institute, Carnegie-Mellon University
- VIRUS-L, the virus news service moderated by Ken Van Wyk

Some of the information is hearsay in nature, but is included because we felt it was reliable. We believe that reliable hearsay information is better than nothing when dealing with a computer virus.

The Virus Tables

The computer viruses in the first five tables in this document are described in the format shown below. In most cases, short phrases are used to describe the type, features, and other characteristics of the virus. The last four tables in this document expand on the phrases used in the virus tables.

<table>
<tr><td><b>Name:</b> The name of the virus used in this report. Note that virus names are not unique, and that the same virus may be known by more than one name. The virus descriptions are sorted alphabetically by the first name in this field.</td><td colspan="3"></td></tr>
<tr><td><b>Aliases:</b> This field gives the different names by which the virus is known, including different names for the same virus, and the names of any nearly identical variants (clones).</td><td colspan="3"><b>Type:</b> The virus is classified here according to where it hides or how it attacks a system.</td></tr>
<tr><td colspan="2"><b>Disk Location:</b> This field describes where the virus hides on a disk, which is generally the vehicle by which it is transferred to another machine. For Trojans, the name of the Trojan program is also listed here.</td><td colspan="2"><b>Features:</b> This field describes where the virus hides in memory and how it infects new disks. Included here are any special features, such as encryption and stealth capabilities.</td></tr>
<tr><td colspan="2"><b>Damage:</b> This field describes the intentional and unintentional damage done by the virus.</td><td><b>Size:</b> This field describes any changes that a virus makes to other programs and data on disk, especially increases in file length. Not all viruses increase the length of an infected file.</td><td><b>See Also:</b> This field points to related virus descriptions that may contain more information.</td></tr>
<tr><td colspan="4"><b>Notes:</b> This field contains descriptive information, information on how to detect and eradicate a virus, and any information that does not fit in the categories above.</td></tr>
</table>

Anti-Virus Software Availability

Availability

There are numerous commercial and shareware anti-virus packages available for both Macintosh and MS-DOS computers. If you have Internet access, the public domain and shareware packages are available on many of the anonymous FTP file servers. Several of these products are available on the CIAC anonymous FTP server and via telephone on the CIAC BBS (see "Additional Information and Assistance" below).

MS-DOS computers

For MS-DOS based computers, the Department of Energy has purchased a site-license for DDI's Data Physician Plus! package. This is available at no charge to all DOE personnel and their contractors for official use at DOE and contractor sites. Contact your operations office for details on how to obtain a copy for your use.

Updates

Please keep in mind that anti-virus software must be periodically updated to be effective against new computer viruses. Also, if you use a shareware package, do not forget to compensate the author. The cost is minimal for the functionality you receive.

Additional Information and Assistance

From CIAC

DOE sites and contractors may obtain additional information or assistance from CIAC:

• Phone:	(510) 422-8193
• FAX:	(510) 423-8002
• Internet:	ciac@llnl.gov

Other government agencies should contact their respective response teams.

From Felicia and irbis

Anti-virus documents and software are available via telephone/modem from the CIAC BBS (Felicia) and via the Internet from irbis.llnl.gov.

- Access **Felicia** at 1200 or 2400 baud at (510) 423-4753 or at 9600 baud at (510) 423-3331 (8 bit, no parity, 1 stop bit). High speed ISDN access can be obtained at the Lawrence Livermore National Laboratory and the Lawrence Berkeley National Laboratory using 423-9885.
- Access to **Irbis** is via the Internet (IP address 128.115.19.60) using anonymous FTP. Log in with FTP, use "anonymous" as the user name and your E-mail address as the password.

For emergencies

For emergencies only, call 1-800-SKYPAGE and enter PIN number 855-0070 or 855-0074.

Macintosh Computer Virus Table

Name: Aliens 4		
Aliases: Aliens 4	**Type:** Vaporware Virus; not real.	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: NOT A VIRUS! August 17, 1992 the DISA office published a Defense Data Network Security Bulletin about this non-virus. Quote: "It's fast, It mutates, It likes to travel, Every time you think you've eradicated it, it pops up somewhere else." They gave no way to identify it, and suggested you reformat your macintosh. No Mac anti-virus people were contacted before sending this alert out. On August 23, the alert was cancelled with a epilogue note. All this was sent out on the Internet, so it is fairly far-reaching.		

Name: ANTI		
Aliases: ANTI, ANTI-ANGE, ANTI A, ANTI B	**Type:** Patched CODE resource.	
Disk Location: Application programs and Finder.	**Features:**	
Damage: Interferes with a running application.	**Size:**	**See Also:**
Notes: Attacks only application files, and causes some problems with infected applications. VirusDetective search string: Resource Start & Pos -1100 & WData 000FA146#90F#80703 ; For finding ANTI A & B SAM def: Name=ANTI, Resource type=CODE, Resource ID=1, Resource Size=any, Search String=000A317CFFFF000CA033303C0997A146, String Offset=any		

Macintosh Computer Viruses

Name: CDEF

Aliases: CDEF | **Type:** Bogus resource. CDEF

Disk Location: The Desktop file | **Features:**

Damage: No damage, only replicates. | **Size:** CDEF ID#1 in Desktop File | **See Also:** WDEF

Notes: It only infects the invisible "Desktop" files used by the Finder. Infection can occur as soon as a disk is inserted into a computer. An application does not have to be run to cause an infection. It does not infect applications, document files, or other system files. The virus does not intentionally try to do any damage, but still causes problems with running applications.

Like WDEF, does not infect System 7 (virus-l, v4-223)
VirusDetective search string: Creator=ERIK & Executables ; For finding executables in the Desktop
Find CDEF ID=1 in the Desktop file.
SAM def: Name=CDEF, Resource type=CDEF, Resource ID=1, Resource Size=510, Search String=45463F3C0001487A0046A9AB, String Offset=420 Rebuild the Desktop - Hold down Command and Option while inserting the disk.

Name: CODE 252

Aliases: CODE 252 | **Type:** Bogus CODE resource.

Disk Location: System program.Application programs and Finder. | **Features:**

Damage: Corrupts a program or overlay files. | **Size:** | **See Also:**

Notes: This virus triggers if an infected application is run or system booted between JUNE6 and DECEMBER 31. Between Jan 1 and June 6 the virus simply replicates.
Under System 7, the System file can be seriously damaged by this virus as it spreads. This damage may cause a system to not boot, crash, or other unusual behavior.
The virus does not spread to other applications under MultiFinder on System 6.x systems, and does not spread at all under System 7, HOWEVER, it will run if a pre-infected application is executed. When triggered, a message appears in a dialog box that says all disks are being erased, but NO ERASURE TAKES PLACE. Disinfectant 2.8, Gatekeeper 1.2.6 (but earlier versions can find virus, just not by name), Rival 1.1.9v,
SAM 3.0.8, Virex INIT 3.8, Virus Detective 5.0.4, also after June 6, if you see the message Disinfectant 2.8, Gatekeeper 1.2.6, Rival 1.1.9v, SAM 3.0.8, Virex INIT 3.8, Virus Detective 5.0.4
The message displayed is:

```
You have a virus.
Ha Ha Ha Ha Ha Ha Ha
Now erasing all disks...
Ha Ha Ha Ha Ha Ha Ha
P.S. Have a nice day.
Ha Ha Ha Ha Ha Ha Ha
(Click to continue...)
```

USERS SHOULD NOT POWER DOWN THE SYSTEM IF THEY SEE THIS MESSAGE. Powering down the system can corrupt the disk, leading to possible serious damage.

Name: CODE-1		
Aliases: CODE-1, CODE 1	**Type:** Bogus CODE resource.	
Disk Location: Application programs and Finder.System program.	**Features:**	
Damage: Corrupts a program or overlay files.Renames Hard disk	**Size:** CODE	**See Also:**
Notes: Virus: CODE-1 Damage: Alters applications and system file; may rename hard disk; may crash system or damage some files. See below. Spread: possibly limited, but has potential to spread quickly Systems affected: All Apple Macintosh computers, under Systems 6 & 7. Several sites have reported instances of a new Macintosh virus on their systems. This virus spreads to application programs and the system file. Its only explicit action, other than spreading, is to rename the hard disk to "Trent Saburo" if the system is restarted on October 31 of any year. However, the virus changes several internal code pointers that may be set by various extensions and updates. This may lead to system failures, failures of applications to run correctly, and other problems. Under some conditions the virus may cause the system to crash. The virus detected by some virus protection programs on some Macintosh machines (but no anti-virus program released prior to this date specifically recognizes this virus). This behavior depends on the nature of the hardware and software configuration of the infected machine.		

Name: CPro 1.41.sea		
Aliases: CPro 1.41.sea, CompacterPro, log jingle	**Type:** Trojan.	
Disk Location: CPro 1.41.sea program	**Features:**	
Damage: Attempts to format the disk.	**Size:**	**See Also:**
Notes: CPro 1.41.sea appears to be a self extracting archive containing a new version of Compactor Pro. When run, it reformats any disk in floppy drive 1, and attempts (unsuccessfully) to format the boot disk. The program contains a 312 byte snd resource named "log jingle" containing a sound clip from the Ren and Stimpy cartoon series. Formats floppy disk in drive 1 File named CPro 1.41.sea Contains:312 byte snd resource named "log jingle" All current utilities		

Name: Dukakis		
Aliases: Dukakis	**Type:** Program.	
Disk Location: Hypercard stack.NEWAPP.STK stack	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.Interferes with a running application.	**Size:**	**See Also:**
Notes: Written in HyperTalk on a HyperCard stack called "NEWAPP.STK". Adds itself to Home Card and other stacks. Flashes a message saying, "Dukakis for President in 88, Peace on Earth, and have a nice day." This virus can be eliminated by using the Hypertalk editor and removing the well commented virus code.		

Macintosh Computer Viruses

Name: FontFinder Trojan		
Aliases: FontFinder Trojan	**Type:** Trojan.	
Disk Location: FontFinder program	**Features:**	
Damage: Corrupts a program or overlay files.Corrupts a data file.Attempts to erase all mounted disks.	**Size:**	**See Also:**
Notes: Trojan found in the Public Domain program called 'FontFinder'. Before Feb. 10, 1990, the application simply displays a list of the fonts and point sizes in the System file. After that date, it immediately destroys the directories of all available physically unlocked hard and floppy disks, including the one it resides on. VirusDetective search string: Filetype=APPL & Resource Start & WData 4E76#84EBA#E30#76702 ; For finding Mosaic/FontFinder Trojans		

Name: HC		
Aliases: HC, HyperCard virus	**Type:** Program; activates when run.	
Disk Location: HyperCard Stacks	**Features:** Direct acting.	
Damage:	**Size:**	**See Also:**
Notes: Sam 3.o search def: Virus Name: HC Virus File Type: STAK Search String pop-up menu: ASCII Search String text field: if char 1 to 2 of LookAtDate <11 The string in the Search String text field above is an ASCII string. Blank area between words are spaces. The string IS case sensitive. As a guard against incorrect entry, SAM 3.0 has a "Check field" in the Definitions dialog boxes. If all of the above information is entered correctly, then your check field should be A0BD.		

Name: Hermes Optimizer 1.1		
Aliases: Hermes Optimizer 1.1	**Type:** Trojan.	
Disk Location: Hermes Optimizer 1.1 program	**Features:**	
Damage: Deletes or moves files.Renames files.	**Size:**	**See Also:**
Notes: The Hermes Optimizer 1.1 Stack is supposed to decrease the level of fragmentation in a HermesShared file. It is actually a Trojan Horse program that renames all files on your hard disk, moves them and then deletes them. You can recover the files with most standard utiltiies, but must go through each one, one at a time to figure out what it is and where it belongs. No files left on your disk. You find a stack with the name Hermes Optimizer 1.1 Don't run the Hermes Optimizer 1.1 stack, dump it in the trash. Recover any lost files with standard file utilities like those supplied with Norton Utilities or Central Point's MacTools. Check each file individually to see what it's name is and where it belongs.		

Name: INIT 1984

Aliases: INIT 1984, INIT1984 — **Type:** Bogus INIT.

Disk Location: INIT program. — **Features:**

Damage: Deletes files.Modifies names & attribs of files and folders — **Size:** INIT # 1984 added to system folder. — **See Also:**

Notes: Infects system extensions of type "INIT" (startup documents). Does NOT infect the System file, desktop files, control panel files, applications, or document files. As INIT files are shared less frequently than are applications, and also due to the way the virus was written, this virus does not spread very rapidly.
There have been very few confirmed sightings of this virus as of 3/17/92. (incl one in Netherlands and 1 in NYState). Virus works on both System 6 and System 7. Damage only occurs when system is BOOTED on Friday the 13th, after 1991. On old Mac's with 64K ROMs, it will crash.
Gatekeeper and SAM Intercept, in advanced and custom mode were able to detect this virus's spread. on any Friday the 13th in any year 1991 and above, will trigger. Damage includes changing names and attributes of folders&files to random strings, and deletion of less than two percent of files

Name: INIT-17

Aliases: INIT-17, INIT17 — **Type:** Bogus INIT.

Disk Location: Application programs and Finder.System program. — **Features:**

Damage: Corrupts a program or overlay files. — **Size:** INIT #17 added to files. — **See Also:**

Notes: The virus is to display an alert message in a window entitled "From the depths of Cyberspace" the first time an
infected machine is rebooted after 6:06:06 pm, 31 Oct 1993.
Lots of bugs in this virus cause earlier Macs to crash.

Name: INIT-M

Aliases: INIT-M — **Type:** Bogus CODE resource.

Disk Location: Applications and the Finder — **Features:**

Damage: Corrupts a program or overlay files.Corrupts a data file.Deletes or moves files. — **Size:** CODE — **See Also:**

Notes: INIT-M rapidly spreads only under System 7; it does not spread or activate on System 6 systems.
The virus activates on any system running on Friday the 13th, files and folders will be renamed to random strings, creation and modification dates, and file creator and type information will be changed, files will be deleted.
Recovery from this damage will be very difficult or impossible.
The file "FSV Prefs" will be found in the Preferences file. Delete infected files

Name: INIT29

Aliases: INIT29

Type: Bogus INIT.

Disk Location: Application programs and Finder.Document file.INIT program.

Features:

Damage: Corrupts a program or overlay files.Interferes with a running application.Corrupts a data file.

Size: INIT ID#29

See Also:

Notes: It infects any file with resources, including documents. It damages files with legitimate INIT#29 resources. If you see the following alert whenever you insert a locked floppy, it is a good indication that your system is infected by INIT 29.

The disk "xxxxx" needs minor repairs. Do you want to repair it?

Also, printing problems and unexplained crashes

If you find an INIT ID=29 on an application or the System file, you may have this virus.

There are two Virus Detective search strings, one for the Finder and Applications, and one for nonapplications:

Resource Start & Size<800 & WData 41FA#92E#797 ; For finding INIT29 in Appl's/Finder

Filetype≠APPL & Resource INIT & Size<800 & WData 41FA#92E#797 ; For finding INIT29 in non-Appl's

Removing the INIT repairs the files.

Name: MBDF A

Aliases: MBDF A

Type: Bogus resource. MBDF

Disk Location: Applications and the FinderTETRICYCLE TrojanTetris-rotating Trojan

Features:

Damage: Corrupts a program or overlay files.

Size: Modifies CODE #0, adds 630 bytes to infected files

See Also: MBDF, MBDF-B

Notes: March 4, 1992: Correction: it DOES spread on ALL types of macintoshes if the operating system is System 7. It will not spread on a MacPlus or SE if that system is using System 6.x

Virus has to rewrite System file to infect it, can take up to 3 mins, if interrupted (think it hung) will destroy system and would have to reload all of it. Does NOT affect data files. Does not do malicious damage.

2 Cornell students have been accused of releasing it on Feb 14, 1992 to archive sites.

The file TETRICYCLE (also named "Tetris-rotating) is a trojan which installs the virus, the first anti-viral updates did not locate this virus. See also below for more details. SAM's old version knows something was up (when it was installed with all options on) , but it would give an alert and not allow the option to push the DENY button Disinfectant 2.6, Gatekeeper 1.2.4, Virex 3.6, SAM 3.0, VirusDetective 5.0.2, Rival 1.1.10

Claris applications will note code change, old ver. SAM running full tilt will also detect. Anti-viral products mentioned above

Name: MBDF-B		
Aliases: MBDF-B, MBDF B	**Type:** Bogus resource. MBDF	
Disk Location: Application programs and Finder.	**Features:**	
Damage: Corrupts a program or overlay files.	**Size:** Modifies CODE #0, adds 630 bytes to infected files	**See Also:** MBDF-A

Notes: Virus: MBDF-B
Damage: minimal, but see below
Spread: probably limited
Systems affected: Apple Macintosh computers. The virus spreads on all types of Macs except MacPlus systems and (perhaps) SE systems; it may be present on MacPlus and SE systems and not spread, however.

A new variant of the MBDF-A virus has recently been discovered. It seems that a person or persons unknown has modified the original MBDF-A virus slightly and released it. Like the original, this virus does not intentionally cause damage, but it may spread widely.

The virus does not necessarily exhibit any symptoms on infected systems. Some abnormal behavior has been reported in machines infected with MBDF-A, involving system crashes and malfunctions in various programs, which may possibly be traced to the virus. Some specific symptoms include:
* Infected Claris applications will indicate that they have been altered
* The "BeHierarchic" shareware program ceases to work correctly.
* Some programs will crash if something in the menu bar is selected with the mouse.

The MBDF-B virus should behave similarly and will spread under both System 6 and System 7.

Name: MDEF		
Aliases: MDEF, MDEF A, Garfield, MDEF B, Top Cat, MDEF C	**Type:** Bogus resource. MBDF	
Disk Location: System program.Application programs and Finder.Desktop file.Document file.	**Features:**	
Damage: Interferes with a running application.	**Size:** MDEF ID#0	**See Also:**

Notes: MDEF infects applications, the System file, other system files, and Finder Desktop files. The System file is infected as soon as an infected application is run. Other applications become infected as soon as they are run on an infected system. MDEF's only purpose is to spread itself, and does not intentionally attempt to do any damage, yet it can be harmful. Odd menu behavior. VirusDetective search string: Resource MDEF & ID=0 & WData 4D44#A6616#64546#6A9AB ; For finding MDEF A & MDEF B
SAM def: Name=Garfield, Resource type=MDEF, Resource ID=0, Resource Size=314, Search String=2F3C434F44454267A9A0, String Offset=42
SAM def: Name=GARFIELD-2, Resource type=MDEF, Resource ID=0, Resource Size=532, Search String=2F3C4D4445464267487A, String Offset=304
SAM def: Name=MDEF C, Resource type=MDEF, Resource ID=0, Resource Size=556, Search String=4D4445464267487A005EA9AB, String Offset=448

Name: merryxmas		
Aliases: merryxmas, Merry Xmas	**Type:** Program.	
Disk Location: Hypercard stack.	**Features:** Direct acting.	
Damage: No damage, only replicates.Can cause Hypercard to quit	**Size:** 0 to 1 file allocation block	**See Also:**

Notes: Analysis of the Macintosh Merry Xmas virus 11/3/93
W. J. Orvis

Type: Program virus in a Hypercard script
Infection: Infects all open, unlockable stacks by copying itself to the end of the stack script.
Damage: None intentional
Size: 0 to 1 allocation block since it adds to the end of the stack script, and the stack script is increased by an allocation block whenever the script extends passed the end of the current block.

Disinfection: Open hypercard, switch to the last card in the home stack and set it to scripting. Open the infected stack select Objects Stack Info and click Script. Find the virus at the end of the script and delete it. To make it so SAM won't detect it, type enough characters to overwrite the script, save it, then delete the typed characters and save it again. Check the stack script on your home stack to see if it was infected while you were disinfecting the infected stack.

When the virus is active, the disk is continually accessed by an 'on idle' procedure, even though it is not infecting the stack. If the stack is from Hypercard version 1, the virus can not infect it because it can not be unprotected. If the stack is converted to version 2, the virus can unprotect and infect it.

SAM with the 4/27/93 virus definitions will see this virus. If the virus has simply been deleted, the virus key will still be in the stack beyond the EOF for the stack script causing SAM to detect the virus in a disinfected stack. The virus inserts itself by counting off a number of lines from the bottom of the stack, so adding lines to the virus will mess it up.

Name: Mosaic Trojan		
Aliases: Mosaic Trojan	**Type:** Trojan.	
Disk Location: Mosaic program	**Features:**	
Damage: Corrupts a program or overlay files.Corrupts a data file.Attempts to erase all mounted disks.	**Size:**	**See Also:**

Notes: Imbedded in a program called 'Mosaic', when launched, it immediately destroys the directories of all available physically unlocked hard and floppy disks, including the one it resides on. The attacked disks are renamed 'Gotcha!'. VirusDetective search string: Filetype=APPL & Resource Start & WData 4E76#84EBA#E30#76702 ; For finding Mosaic/FontFinder Trojans

Macintosh Computer Viruses

Name: nVIR

Aliases: nVIR, nVIR A, nVIR B, AIDS, Hpat, MEV#, FLU, Jude, J-nVIR

Type: Patched CODE resource.

Disk Location: Application programs and Finder.System program.

Features:

Damage: Corrupts a program or overlay files.Interferes with a running application.

Size: nVIR In system ID #0,1,4,5,6,7; In application ID#1,2,3,6,7CODE In applciation ID#256INIT In system ID#32Hpat, MEV#,AIDS,FLU Varations of nVIR resource name in other mutations

See Also:

Notes: It infects the System file and applications. nVIR begins spreading to other applications immediately. Whenever a new application is run, it is infected. Symptoms include unexplained crashes and problems printing.
Works on Atari ST's in MAC emualtion mode. Unexplained system crashes, problems printing.
There are two Virus Detective search strings, one for applications and one for the System file:
"Resource Start & Size<800 & WData 2F3A#F00#C80#B00 ; For finding nVIR, etc. in Appl's/Finder"
"Filetype=ZSYS & Resource INIT & Size<800 & WData 2F3A#F00#C80#B00 ; For finding nVIR, etc. (System)"

Name: Peace

Aliases: Peace, MacMag virus, Drew, Brandow, Aldus

Type: Bogus INIT.

Disk Location: Hypercard stack.System program.

Features:

Damage: Corrupts a program or overlay files.Interferes with a running application.

Size: INIT ID#6 on System

See Also:

Notes: First virus on the Macintosh. Displays "Peace on Earth" message on March 2, 1988 and removes itself the next day. Distributed via a HyperCard stack. Its presence causes problems with some programs.
Rumored that a writer for the current show "Star Trek: The Next Generation" wrote it and was being accused in court and being sued: this info came out in late 1992
Unexplained program crashes.
"Peace on Earth" message on March 2, 1988 INIT number ?? found on system file.
VirusDetective search string: "Resource INIT & Size<2000 & WData 494E#37A#86700 ; For finding Peace"
SAM search string: "" Remove the INIT from the System File.

Macintosh Computer Viruses

Name: Scores		
Aliases: Scores, NASA	**Type:** Patched CODE resource.	
Disk Location: Application program.System program.	**Features:**	
Damage: Corrupts a program or overlay files.Interferes with a running application.	**Size:** INIT ID#6, 10, and 15 on the System, Notepad, Desktop, and Scrapbook filesatpl ID#128 on systemDATA ID#400 on the SystemCODE ID# n+1 on applications, n is the first unused CODE resource ID.	**See Also:**
Notes: Infects applications and the system, and attempts to destroy files with creator types: VULT, and ERIC. Causes problems with other programs, including unexplained crashes and pronting errors. Changes the icons of the NotePad and Scrapbook files to the blank document icon. Check the icons for the Note Pad and Scrapbook files. They should look like little Macintoshes. If they both look like blank sheets of paper with turned-down corners, your software may have been infected by Scores There are two Virus Detective search strings, one for the Finder and Applications, and one for the System file: Resource Start & Size<8000 & WData FD38#FBA#5A3 ; For finding Scores in Appl's/Finder Filetype≠APPL & Resource INIT & Size<1100 & WData FD38#FBA#5A3 ; For finding Scores in System, etc.		

Name: Sexy Ladies Trojan		
Aliases: Sexy Ladies Trojan	**Type:** Trojan.	
Disk Location: Sexy Ladies application	**Features:**	
Damage: Attempts to erase all mounted disks.	**Size:**	**See Also:**
Notes: Not a virus, but a Trojan Horse. Given away at 1988 San Fransisco MacWorld Expo, erased whatever hard disk or floppy disk it was on when it was lanched. An application named Sexy Ladies that erases the disk that contains it. Presence of the Application Sexy Ladies Delete the application		

Name: Steroid Trojan		
Aliases: Steroid Trojan	**Type:** Trojan.	
Disk Location: Steroid INIT programINIT program.	**Features:**	
Damage: Attempts to erase all mounted disks.	**Size:** Steroid INIT inserted in the System Folder.	**See Also:**
Notes: The steroid INIT is claimed to speed up QuickDraw on Macintoshes with 9 inch screens. The INIT has code that checks for dates after June 30, 1989, and is active every year thereafter from July through December. When it is activated, it attempts to erase all mounted drives. All mounted drives are erased. You may be able to save them with a disk editor like SUM or MacTools. Find the Steroid INIT in the System file VirusDetective search string: Resource INIT & Size<1200 & WData FE680C6E#E4EBA#F60 ; For finding Steroid Trojan SAM def: Name=Steroid Trojan, Resource type=INIT, Resource ID=148, Resource Size=1080, Search String=ADE9343C000A4EFAFFF24A78, String Offset=96 Remove the Steroid INIT from the System file.		

Macintosh Computer Viruses

Name: T4		
Aliases: T4, T4-A, T4 B, GoMoku, T4-C	**Type:** Program; activates when run.	
Disk Location: Applications and the FinderGoMoku versions 2.0 and 2.1	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.Damages system file	**Size:**	**See Also:**
Notes: The T4 virus was discovered in the game GoMoku versions 2.0 (T4-A) and 2.1 (T4-B). The name of the person in the game is not the virus author. The virus infects applications and the Finder, and attempts to alter the system file. Infected applications can not be fixed. The altered system file may not boot, or may not load INITS. The virus masquerades as Disinfectant to try to bypass protection software such as GateKeeper. Once installed, the virus does not seem to do any overt damage. INITs don't load. Alerts that disinfectant is changing a file when Disinfectant is not running indicates the virus is present. System Won't boot. Use a virus checking program Replace applications and reinstall the System and Finder. The applications, System, and Finder can not be repaired.		

Name: Virus Info Trojan		
Aliases: Virus Info Trojan	**Type:** Trojan.	
Disk Location: Virus Info Program	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: This application has not been sighted outside of the Edmonton, Province of Alberta, Canada area where it was discovered. When activated, destroys the directory structure VirusDetective search string: Filetype=APPL & dataFork & Size < 10000 & WData A003#24E94 ; For finding Virus Info Trojan		

Name: WDEF		
Aliases: WDEF, WDEF-A, WDEF-B	**Type:** Bogus resource.	WDEF
Disk Location: Desktop file.	**Features:**	
Damage:	**Size:** WDEF ID = 0 in Desktip file	**See Also:** CDEF
Notes: WDEF only infects the invisible "Desktop" files used by the Finder. It can spread as soon as a disk is inserted into a machine. An application need not be run to cause infection. Does not infect System 7 and above versions of the operating system due to changes in the O/S VirusDetective search string: Creator=ERIK & Executables ; For finding executables in the Desktop Find WDEF ID=0 in the Desktop file. Rebuild the Desktop - Hold down Command and Option while inserting the disk.		

Macintosh Computer Viruses

Name: ZUC		
Aliases: ZUC, ZUC 1, ZUC 2	**Type:** Patched CODE resource.	
Disk Location: Application programs and Finder.	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: It infects only applications files. Before March 2, 1990 or less than two weeks after an application becomes infected, it only spreads from application to application. After that time, approximately 90 seconds after an infected application is run, the cursor begins to behave unusually whenever the mouse button is held down. The cursor moves diagonally across the screen, changing direction and bouncing like a billiard ball whenever it reaches any of the four sides of the screen. The cursor stops moving when the mouse button is released. Wild shifts in cursor position. Changes in the background pattern VirusDetective search string: Filetype=APPL & Resource CODE & ID=1 & WData A746*A038#31E*A033; For finding ZUC.Virus 1&2 SAM def: Name=ZUC A, Resource type=CODE, Resource ID=1, Resource Size=any, Search String=4E56FF74A03641FA04D25290, String Offset=any SAM def: Name=ZUC B, Resource type=CODE, Resource ID=1, Resource Size=any, Search String=7002A2604E752014A0552240, String Offset=any		

MS-DOS/PC-DOS Computer Virus Table

Name: 10 past 3		
Aliases: 10 past 3	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 748	**See Also:**
Notes:		

Name: 1024PrScr		
Aliases: 1024PrScr, 1024, PrSc, PrScr	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.	**Size:** 1024	**See Also:**
Notes: This virus will occasionally produce a "Print Screen" effect.		

Name: 109 Virus		
Aliases: 109 Virus	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: 1st discovered January 1992, this virus is a non-resident, direct action .COM file infector. It contains no text or payload and is a simple, yet effective replicater When an infected program is executed, it infects all .COM files in the current directory that meet the following conidions, adding 109 bytes. a. the file must be a .com file, filesize between 2 bytes and 64 kb. b. if the 1st bytre is BEh, assume that the file is already infected and do next file c. the file must have normal attributes, so if it is hidden or read-only, virus won't infect No error handling is done, the file time and date stamps will be changed upon infection It may damage a program larger than 65427 bytes, for the end of the infected program will be lost. hex string: BE 00 01 56 8C C8 80 C4 10 8E C0 33 FF		

Name: 12-TRICKS Trojan		
Aliases: 12-TRICKS Trojan, Twelve Tricks Trojan, Tricks	**Type:** Trojan.	
Disk Location: CORETEST.COM, , Hard disk boot sectors.	**Features:**	
Damage: Corrupts the file linkages or the FAT., Attempts to format the disk., Interferes with a running application., Corrupts boot sector	**Size:**	**See Also:**
Notes: Contained in "CORETEST.COM", a file that tests the speed of a hard disk. It installs itself in the boot sector of the hard disk. Every time the computer boots, one entry in the FAT will be changed. With a probability of 1/4096, the hard disk will be formatted (Track 0, Head 1, Sector 1, 1 Sector) followed by the message: "SOFTLoK+ V3.0 SOFTGUARD SYSTEMS,INC, 2840 St.Thomas Expwy,suite 201, Santa Clara,CA 95051 (408)970-9420". The following printed on the screen: "SOFTLoK+ V3.0 SOFTGUARD SYSTEMS,INC,2840 St.Thomas Expwy,suite 201, Santa Clara,CA 95051 (408)970-9420" Damaged FATs and directories. All sorts of strange changes to typed or printed characters. Strange things happening when keys are typed. Text within the program CORETEST.COM, readable with HexDump-utilities:"MEMORY$" Text within the boot sector of the hard disk:"SOFTLoK+ V3.0 SOFTGUARD SYSTEMS,INC,2840 St.Thomas Expwy,suite 201, Santa Clara,CA 95051 (408)970-9420"		

Name: 1226		
Aliases: 1226, 1226D, 1226M, V1226, V1226D, V1226DM, (Phoenix related)	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes:		

Name: 1260		
Aliases: 1260, V2P1, Variable, Chameleon, Camouflage, Stealth	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Encrypted, Direct acting., Polymorphic	
Damage: Corrupts a program or overlay files., Interferes with a running application.	**Size:** 1260, Polymorphic: each infection different	**See Also:** Vienna
Notes: This appears to be related to the Vienna virus. The virus infects any COM file in the current directory. Uses variable encryption techniques The seconds field of the timestamp of any infected program will be 62 seconds.		

MS-DOS/PC-DOS Computer Viruses

Name: 1701		
Aliases: 1701, Cascade, Cascade B, Autumn, Herbst	**Type:** Program., Memory resident.	
Disk Location: COM application.	**Features:** Encrypted, Direct acting.	
Damage: Interferes with a running application., Corrupts a program or overlay files. .	**Size:** 1701	**See Also:**
Notes: A variation of the 1704 (Autumn) virus. Spreads between COM files. Occasionally causes odd screen behavior (the characters on the screen fall into a heap at the bottom of the screen!). One rare variant can destroy data on hard disks.		

Name: 1704-Format		
Aliases: 1704-Format, Cascade Format	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.	**Features:** Encrypted, Stealth, Direct acting.	
Damage: Interferes with a running application., Corrupts a program or overlay files., Attempts to format the disk.	**Size:** 1704	**See Also:**
Notes: Spreads between COM files. Occasionally causes odd screen behavior (the characters on the screen fall into a heap at the bottom of the screen!). One rare variant can destroy data on hard disks.		

Name: 2387		
Aliases: 2387	**Type:** Boot sector.	
Disk Location: COM application., EXE application., Floppy disk boot sectors., Hard disk boot sectors.	**Features:** Memory resident; TSR., Polymorphic	
Damage: Corrupts a program or overlay files., Corrupts boot sector	**Size:** Polymorphic: each infection different	**See Also:**
Notes: Polymorphic multi-partite fast infector Trigger: some time after it has been loaded in memory, it displays a rough fractal image using text mode and pseudo-graphic characters (it's hard to get this picture to come up) To spread, it infects the MBSector. When you boot from an infected HD, it infects EXE files as you execute them. PC's without a hard disk are immune.		

Name: 3X3SHR		
Aliases: 3X3SHR	**Type:** Trojan.	
Disk Location: 3X3SHR.???	**Features:**	
Damage: Erases the Hard Disk.	**Size:** 78848 bytes 3X3SHR file	**See Also:**
Notes: *TROJAN* Time Bomb type trojan wipes the Hard Drive clean.		

MS-DOS/PC-DOS Computer Viruses

Name: 405		
Aliases: 405	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** Overwrites first 405 bytes of a .COM file.	**See Also:**
Notes: The virus spreads itself by overwriting the first 405 bytes of a .COM file. One file is infected each time an infected file is executed.		

Name: 4096		
Aliases: 4096, Century, Century Virus, 100 Years Virus, Frodo, IDF, Stealth	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application., EXE application., Program overlay files., COMMAND.COM	**Features:** Encrypted, Direct acting.	
Damage: Interferes with a running application., Corrupts a program or overlay files., Corrupts a data file., Corrupts the file linkages or the FAT.	**Size:** 4096 bytes increase in length, but hidden from the DIR cmd.	**See Also:**
Notes: It infects both .COM or .EXE applications. It is nearly impossible to detcct once it has been installed since it actively hides itself from the scanning packages. Whenever an application such as a scanner accesses an infected file, the virus disinfects it on the fly. DIR will also not show the change in length. virus-l, v5-063: tries to place a new boot sector over the orig. on Sept 21 but the code to do this is garbled, so the computer will hang. v6-084: Frodo can infect certain types of non-executable files Almost none. The computer will hang at a Get Dos Version call when the date is after 9/22 and before 1/1 of next year. virus-l, v5-063: report that this virus will Activate on Sept 21. Compare file lengths with DIR and a Disk editor like Norton utilities. If they differ by 4096 you have the virus. If the date of the file is 20XX (XX being the last 2 digits of the original date) then the file has probably been infected by the 4096 virus Copying a file to a file with a non-executable extension results in a disinfected file because the virus removes itself when the file is copyed by COMMAND.COM. A Do-it-yourself way: Infect system by running an infected file, ARC/ZIP/LHARC/ZOO all infected .COM and .EXE files, boot from uninfected floppy, and UNARC/UNZIP/LHARC E etc. all files. Pay special attention to disinfection of COMMAND.COM.		

Name: 4870 Overwriting		
Aliases: 4870 Overwriting	**Type:** Program.	
Disk Location: EXE application.	**Features:** Direct acting.	
Damage:	**Size:** 4870	**See Also:**
Notes: This virus infects programs by overwriting, and thus destroying them.		

Name: 512		
Aliases: 512, 512-A, 512-B, 512-C, 512-D	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage:	**Size:**	**See Also:**
Notes: The virus hides in the first 512 bytes of free space in the last cluster of a .COM file. When RAM-Resident, it hides in the disk buffer space for code in order not to take-up memory. Files do not appear to change in length, because the virus removes itself on the fly when the file is accessed by another program. virus-l, v4-131 says that a variant of the 512 and Doom-II virus can put executable code into video memory. "666" at offset 509. A Do-it-yourself way: Infect system by running an infected file, ARC/ZIP/LHARC/ZOO all infected COM and EXE files, boot from uninfected floppy, and UNARC/UNZIP/LHARC E etc. all files. Pay special attention to disinfection of COMMAND.COM.		

Name: 66a		
Aliases: 66a	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Direct acting.	
Damage:	**Size:** 512	**See Also:**
Notes:		

Name: 99%		
Aliases: 99%, 99 percent	**Type:** Program.	
Disk Location: EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files., Corrupts a data file.	**Size:** 821	**See Also:**
Notes: This virus may overwrite files with a small Trojan that displays a message which starts with the line "Het 99%-virus heeft toegeslagen."		

Name: Ada		
Aliases: Ada	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 2600	**See Also:**
Notes: Ada is a resident .COM file infector found in Argentina. The virus may interfere with the operation of the PC-cillin anti-virus program.		

Name: Adolf		
Aliases: Adolf	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 475	**See Also:**
Notes: Adolf is a resident, .COM file infector that contains the string Adolf Hitler.		

MS-DOS/PC-DOS Computer Viruses

Name: Advent		
Aliases: Advent, 2761	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application., EXE application., COMMAND.COM.	**Features:** Encrypted, Direct acting.	
Damage: Interferes with a running application.	**Size:** 2761-2776 Bytes are appended on a paragraph boundary	**See Also:**
Notes: Spreads between .COM and .EXE files. Beginning on every "Advent"(the 4th Sunday before Christmas until Christmas eve), the virus displays after every "Advent Sunday" one more lit candle in a wreath of four, together with the string "Merry Christmas" and plays the melody of the German Christmas song "Oh Tannenbaum". By Christmas all four candles are lit. This happens until the end of December, whenever an infected file is run. If the environment variable "VIRUS=OFF" is set, the virus will not infect.		

Name: AIDS		
Aliases: AIDS, Hahaha, Taunt, VGA2CGA	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** Overlays application, no increase	**See Also:**
Notes: It infects .COM files.		

Name: AIDS II		
Aliases: AIDS II, AIDS	**Type:** Trojan.	
Disk Location: AIDS Information Introductory Diskette	**Features:**	
Damage: Encrypts the file directory.	**Size:** Adds File REM#.EXE 146188 bytes (hidden file), Adds File AIDS.EXE 172562 bytes	**See Also:**
Notes: On Monday, 11th December 1989, several thousand diskettes named "AIDS Information Introductory Diskette Version 2.0" were mailed out containing a program that purported to give you information about AIDS. These diskettes actually contained a trojan that will encrypt the file names on your hard disk after booting your computer about 90 times. If you have installed this program, you should copy any important data files (no executables) and reformat your hard disk. All your file names are encrypted and the disk is full. In the root directory, files named: AIDS.EXE, AUTO.BAT, AUTOEXEC.BAK Two hidden subdirectories called # and ###### The # subdirectory contains a readonly, hidden file called REM#.EXE. The ###### subdirectory contains a hidden subdirectory called ###### The ###### subdirectory contains a hidden subdirectory called ###### The ###### subdirectory also contains a subdirectory called ERRORIN.THE, and five files named ____.__, _._, ___._, _._ and _.__ (where _ is the underline character, is the space character, and # is Ascii 255). The minimum required to disable the virus is to remove the AUTOEXEC.BAT file that runs the program REM#.EXE and to remove all the hidden directories. This will not insure removal of the virus. It would be better backup any needed data files (no applications) and to do a low level format of the hard disk. If the virus has already been activated, you can recover the encrypted file names using the table below in the summary, and then reformat the disk.		

Name: AIDS II		
Aliases: AIDS II, AIDS-II	**Type:** Companion program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage:	**Size:** 8064, Adds File	**See Also:**
Notes: AIDS II is a companion virus. When activated, it creates .COM files with the same name as .EXE files. DOS will always execute the .COM file first, which is the virus. The virus then executes the .EXE file when it is finished.		

Name: Aircop		
Aliases: Aircop	**Type:** Boot sector.	
Disk Location: Hard disk boot sectors., Floppy disk boot sectors.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sector	**Size:**	**See Also:**
Notes: from a report in virus-l, v4-220: Causes FPROT 2.01 to hang, while FPROT 1.15 sometimes says its cured (but it never is) CLEAN 7.9v84 says "Virus cannot be safely removed from boot sector" DOS/SYS says "Not able to SYS to .3L File System" The virus may display Red State, Germ Offensive AIRCOP when booting with an infected disk.		

Name: Akuku		
Aliases: Akuku, Metal Thunder, Copmpl	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Direct acting.	
Damage:	**Size:** 889, 892, 1111 - Copmpl variant	**See Also:**
Notes: Contains the string A kuku, "Nastepny komornik !! " The Copmpl variant contains the string. "Sorry, I'm copmpletly dead"		

Name: Alabama		
Aliases: Alabama, Alabama-B	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: EXE application.	**Features:** Encrypted, Direct acting.	
Damage: Corrupts the file linkages or the FAT., Interferes with a running application., Corrupts a program or overlay files.	**Size:** 1560	**See Also:**
Notes: The Alabama virus is a memory resident, encrypting, .EXE file infector. The virus contains the string, SOFTWARE COPIES PROHIBITED BY INTERNATIONAL LAW. Box 1055 Tuscambia ALABAMA USA. which is displayed after an hour of use on an infected machine. It hooks Crtl-Alt-Del and fakes a reboot when they are pressed, staying in memory. On Fridays, it does strange things like executing different files from those you selected. The following text on the screen, SOFTWARE COPIES PROHIBITED BY INTERNATIONAL LAW. Box 1055 Tuscambia ALABAMA USA. Executing one file and having a different one start running.		

MS-DOS/PC-DOS Computer Viruses

Name: Albania		
Aliases: Albania	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Direct acting.	
Damage:	**Size:** 429, 506, 575, 606	**See Also:**
Notes: The viruses contain the word "Albania".		

Name: Alex		
Aliases: Alex	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Direct acting.	
Damage:	**Size:** 368	**See Also:**
Notes:		

Name: Alexander		
Aliases: Alexander	**Type:** Program.	
Disk Location: COM application., EXE application., COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1951	**See Also:**
Notes: Alexander contains the following encrypted text: Apa depistata in microprocesor ! Functionarea poate fi compromisa ! Se recomandaoprirea calculatorului. citeva ore pentru uscare ! Alexander - Constanta, Romania.		

Name: Ambulance Car		
Aliases: Ambulance Car, REDX, Red Cross	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files., Interferes with a running application.	**Size:** 796 to .COM files	**See Also:**
Notes: When an infected application is run, the virus tries to find two .COM file victims which it randomly selects in the current directory or via the PATH variable in the environment. After some number of executions (110b), an ambulance car with a flashing light runs along the bottom of the screen accompanied by siren sounds. A flag is set, so the car will not run again until the next bootup. An ambulance car running along the bottom of the screen accompanied by siren sounds. almost every anti virus program almost every anti virus program		

MS-DOS/PC-DOS Computer Viruses

Name: Amoeba		
Aliases: Amoeba, 1392	**Type:** Program., Memory resident - TSR	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage: Machine can crash	**Size:** Every time attached to end of file, deletes a byte of, virus initialization code	**See Also:**
Notes: The Amoeba virus attaches to infected files in the front and end of the file. Each time the virus attaches to the end of a file, it drops a byte from the front of the virus initialization code, thus eventually after a few generations this virus will become unusable, and the machine will crash. When activated, the text "SMA Khetapunk - Nouvel Band A.M.O.E.B.A by Primesoft Inc." appears on the screen. To prevent reinfection, it uses F3 interrupt vector, if the value is CDCD it figures it is resident and won't infect. It was written with an unusual assembler. There is no trigger date, machine can crash. DDI's Data Physician Plus!, V 3.0C Data Physician Plus! v3.0C		

Name: Amstrad		
Aliases: Amstrad, Pixel, V-847, 847, V-847B, V-852	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 847	**See Also:**
Notes: Adds code to front of any .COM file in the current directory. The virus contains an advertisement for Amstrad computers. The program prints "Program sick error:Call doctor or buy PIXEL for cure description" with a 50-50 chance after the 5th infection. The virus contains the string "Program sick error:Call doctor or buy PIXEL for cure description". The string "IV" is at offset 3 in the COM file.		

Name: Andryushka		
Aliases: Andryushka	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application., EXE application., COMMAND.COM.	**Features:** Encrypted, Direct acting.	
Damage:	**Size:** Variable	**See Also:**
Notes:		

Name: Angarsk		
Aliases: Angarsk	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Direct acting.	
Damage:	**Size:** 238	**See Also:**
Notes:		

MS-DOS/PC-DOS Computer Viruses

Name: Anna		
Aliases: Anna	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application., COMMAND.COM.	**Features:** Encrypted, Direct acting.	
Damage:	**Size:** 742	**See Also:**
Notes: Anna is an encrypted virus, which contains the text: [ANNA] Slartibartfast, ARCV NuKE the French Have a Cool Yule from the ARcV xCept Anna Jones I hope you get run over by a Reindeer Santas bringin' you a Bomb All my Lurve - SLarTiBarTfAsT (c) ARcV 1992 - England Raining Again		

Name: Anthrax		
Aliases: Anthrax, Anthrax PT	**Type:** Boot sector.	
Disk Location: COM application., EXE application., Floppy disk boot sector., Hard disk boot sector.	**Features:**	
Damage: Trashes the hard disk	**Size:** 1024	**See Also:**
Notes: Infects both boot sectors and files. Trashes hard disks. MS-DOS 6's antivirus routine detects some, but not all infections by Anthrax.		

Name: Anti Pascal		
Aliases: Anti Pascal, Anti Pascal 529, Anti Pascal 605, AP 529, AP 605, C 605, V-605	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Deletes or moves files., Interferes with a running application., Corrupts a program or overlay files.	**Size:** 605	**See Also:**
Notes: May overwrite .BAK and .PAS files if not enough .COM files are available in a directory for it to infect. Infected files begin with "PQVWS". They also contain the string "combakpas???exe" at offset 0x17.0 VIRSCAN string....... BF00018B360C0103F7B95D021E07EA00, scan COM files only.		

Name: ANTI-PCB		
Aliases: ANTI-PCB	**Type:** Trojan.	
Disk Location: ANTI-PCB.COM	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: Apparently one RBBS-PC sysop and one PC-BOARD sysop started feuding about which BBS system is better, and in the end the PC-BOARD sysop wrote a trojan and uploaded it to the rbbs SysOp under ANTI-PCB.COM. Of course the RBBS-PC SysOp ran it, and that led to quite a few accusations and a big mess in general.		

MS-DOS/PC-DOS Computer Viruses

Name: AntiCAD		
Aliases: AntiCAD, Plastique-B, Plastique 2, Plastique 5.21, Plastique, Invader, HM2	**Type:** Boot sector.	
Disk Location: COM application., EXE application., COMMAND.COM. , Floppy disk boot sectors., Hard disk boot sectors.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 2576, 2900, 3004, 3012, 4096	**See Also:** Jerusalem
Notes: Story on first sighting May 1990 in virus-l, v5-059 plays tunes, infects both boot sectors and executable files. Derived from the Jerusalem virus. Targeted against the AutoCAD program. When ACAD.EXE is run the viruses will activate, overwriting data on floppy disks and hard disks, as well as garbling the contents of the CMOS.		

Name: Antimon		
Aliases: Antimon, Pandaflu	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Direct acting.	
Damage:	**Size:** 1450	**See Also:**
Notes: This virus is targeted against protection programs, Flushot and some programs from Panda Software.		

Name: AntiPascal		
Aliases: AntiPascal	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 605, 529	**See Also:**
Notes: This virus is supposed to have been written to take revenge against the former employer of the virus author.		

Name: AntiPascal II		
Aliases: AntiPascal II, Anti-pascal II, Anti-Pascal 400, Anti-Pascal 440, Anti-Pascal 480, AP-400, AP-440, AP-480	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 400, 440, 480	**See Also:** Anti-Pascal
Notes: A group of three viruses similar to the Anti-Pascal viruses, probably by the same author.		

MS-DOS/PC-DOS Computer Viruses

Name: Antitelifonica		
Aliases: Antitelifonica, A-VIR	**Type:** Boot sector., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application., EXE application., Floppy disk boot sectors., Hard disk boot sectors.	**Features:** Encrypted	
Damage: Corrupts boot sector, Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: A multi-partite virus, may be stealth too		

Name: April 1. EXE		
Aliases: April 1. EXE, Suriv 2, Suriv 2.01	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1488	**See Also:**
Notes: Same as the April 1. COM virus, displays APRIL 1ST HA HA HA YOU HAVE A VIRUS. on April 1st. Those two viruses were later combined into one, called SURIV 3, which evolved into the Jerusalem virus.		

Name: Arab		
Aliases: Arab	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 834	**See Also:**
Notes:		

Name: ARC513.EXE		
Aliases: ARC513.EXE, ARC514.COM	**Type:** Trojan.	
Disk Location: ARC513.EXE, ARC514.COM	**Features:**	
Damage: Corrupts boot sector, Corrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: ARC513.EXE This hacked version of ARC appears normal, so beware! It will write over track 0 of your [hard] disk upon usage, destroying the disk. ARC514.COM This is totally similar to ARC version 5.13 in that it will overwrite track 0 (FAT Table) of your hard disk. Also, I have yet to see an .EXE version of this program.		

Name: ARC533		
Aliases: ARC533	**Type:** Trojan.	
Disk Location: COMMAND.COM, ARC533.EXE	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: ARC533.EXE This is a new Virus program designed to emulate Sea's ARC program. It infects the COMMAND.COM		

Name: Armagedon		
Aliases: Armagedon, Armagedon the first, Armagedon the Greek	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1079	**See Also:**
Notes: If a Hayes modem is installed, the virus dials 081-141, which is the number of the "speaking clock" on the island of Crete.		

Name: Arriba		
Aliases: Arriba	**Type:** Program.	
Disk Location: COM application., EXE application., COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1590	**See Also:**
Notes:		

Name: Ash		
Aliases: Ash, Ash-743	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Direct acting.	
Damage:	**Size:** 280, 743	**See Also:**
Notes:		

Name: Astra		
Aliases: Astra	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 976	**See Also:**
Notes: Contains the text "(C) AsTrA, 1991".		

Name: AT		
Aliases: AT	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 132-149	**See Also:**
Notes: A group of 4 viruses that only run on an IBM AT computer.		

Name: AT II		
Aliases: AT II	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 108-122	**See Also:**
Notes: Group of small viruses that only work on an IBM AT computer.		

Name: Atas		
Aliases: Atas	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Direct acting.	
Damage:	**Size:** 384, 400	**See Also:**
Notes:		

Name: Athens

Aliases: Athens | **Type:** Program.

Disk Location: COM application., EXE application., COMMAND.COM. | **Features:** Memory resident; TSR.

Damage: | **Size:** 1463 | **See Also:**

Notes: This virus contains the following text message:

TROJECTOR II,(c) Armagedon Utilities, Athens 1992

Name: Attention

Aliases: Attention, Attention! | **Type:** Program.

Disk Location: COM application., COMMAND.COM. | **Features:** Memory resident; TSR.

Damage: | **Size:** | **See Also:**

Notes: This virus gets its name from the string "ATTENTION" which is near the beginning of infected files.

Name: Auto

Aliases: Auto | **Type:** Program.

Disk Location: COM application., COMMAND.COM | **Features:** Memory resident; TSR.

Damage: | **Size:** 129 | **See Also:**

Notes:

Name: AZUSA

Aliases: AZUSA, Azuza, Hong Kong | **Type:** Boot sector.

Disk Location: Floppy disk boot sectors., Hard disk partition tables. | **Features:** Memory resident; TSR above TOM.

Damage: Corrupts a program or overlay files., Disables com1 and lpt1, Corrupts a data file., Corrupts floppy disk boot sector, Corrupts hard disk partition table | **Size:** Overlays boot sector, no increase | **See Also:**

Notes: AZUSA is a boot sector and partition table infector that is at least as effective as the STONED and infects the boot sectors of floppies and the partition table of hard disks. It goes resident and takes 1k of memory from the TOM (CHKDSK "total bytes memory" is reduced by 1024 bytes - 640k machine will report 654336 instead of 655360). No stealth is involved and it may be recognized by the long jump (E9 8B) at the start of an infected sector. It causes bombs by disabling COM1 and LPT1.
Found on distribution disks of TVGA - 8916 (Trident Microsystems, Inc.) VGA software.
System crashes. The computer is not able to talk to COM1 and LPT1., Top of memory reduced by 1K. long jump (E9 8B) at the start of an infected sector. For floppies, boot with an uninfected disk and use the sys command to rewrite the boot blocks. A hard disk must have its partition table restored from a copy stored on a floppy. Most of the tools programs do this (PC Tools, Norton, etc.) though you must save the copy before the disk is infected.

MS-DOS/PC-DOS Computer Viruses

Name: Backfont		
Aliases: Backfont	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 905, 765, 900	**See Also:**
Notes: Appears to change the font on VGA/EGA displays. Font changes on VGA or EGA displays.		

Name: BACKTALK		
Aliases: BACKTALK	**Type:** Trojan.	
Disk Location: BACKTALK.???	**Features:**	
Damage: Overwrites sectors on the Hard Disk.	**Size:**	**See Also:**
Notes: This program used to be a good PD utility, but someone changed it to be trojan. Now this program will write/destroy sectors on your [hard] disk drive. Use this with caution if you acquire it, because it's more than likely that you got a bad copy.		

Name: Bad Boy		
Aliases: Bad Boy	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1000, 1001	**See Also:**
Notes: The virus contains the following text: Make me better! The Bad Boy virus, Version 2.0, Copyright (C) 1991.		

Name: Baobab		
Aliases: Baobab	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1635	**See Also:**
Notes:		

Name: Bebe		
Aliases: Bebe, Bebe-486	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Direct acting.	
Damage:	**Size:** 1004, 486	**See Also:**
Notes: This virus contains the following pieces of text: VIRUS! Skagi "bebe" Fig Tebe ! The variant, Bebe-486 is shorter and does not contain the text.		

Name: Best Wishes

Aliases: Best Wishes, Best Wishes-B, Best Wishes-970

Type: Program.

Disk Location: COM application., COMMAND.COM.

Features: Memory resident; TSR.

Damage:

Size: 1024, 970

See Also:

Notes: The virus contains the following text:

This programm ... With Best Wishes!

COMMAND.COM, will not work properly when infected.

The variant Best Wishes-970 , or Best Wishes-B is shorter and damages .EXE files trying to infect them.

Name: BetaBoys

Aliases: BetaBoys, Mud

Type: Program.

Disk Location: COM application., COMMAND.COM.

Features: Memory resident; TSR.

Damage:

Size: 575

See Also:

Notes: Written by the same authors who wrote the Swedish Boys viruses.

Name: Beware

Aliases: Beware, Monday 1st

Type: Program.

Disk Location: COM application., COMMAND.COM.

Features: Direct acting.

Damage: Overwrites sectors on a Floppy disk.

Size: 442

See Also:

Notes: The virus contains the text

BEWARE ME - 0.01, Copr (c) DarkGraveSoft - Moscow 1990

It activates Monday the 1st, overwriting the first sectors of any diskette in drive A:
Trashed Floppy disks on a Monday the 1st.

Name: BFD

Aliases: BFD, Boot-EXE

Type: Boot sector.

Disk Location: EXE application., Floppy disk boot sector., Hard disk boot sector.

Features: Memory resident; TSR.

Damage:

Size: 512

See Also:

Notes: The virus is very small, and infects .EXE files by inserting itself in the unused space between the file header
and the actual start of the code.

Name: Big Joke

Aliases: Big Joke | **Type:** Program.

Disk Location: COM application., COMMAND.COM. | **Features:** Direct acting.

Damage: | **Size:** 1068 | **See Also:**

Notes: The virus contains the text,

> At last ...... ALIVE !!!!!
>
> I guess your computer is infected by the Big Joke Virus.
>
> Release 4/4-91
>
> Lucky you, this is the kind version.
> Be more careful while duplicating in the future.
> The Big Joke Virus, killer version, will strike harder.
> The Big Joke rules forever

Name: BIO

Aliases: BIO | **Type:**

Disk Location: | **Features:**

Damage: | **Size:** | **See Also:**

Notes: Mac and pc version, attacks only Microsoft products

Name: Bit Addict

Aliases: Bit Addict | **Type:** Program.

Disk Location: COM application., COMMAND.COM. | **Features:** Memory resident; TSR.

Damage: Erases the Hard Disk. | **Size:** 477 | **See Also:**

Notes: This virus may trash hard disks, and then display the message:

> The Bit Addict says:
> "You have a good taste for hard disks, it was delicious !!!"

Name: Black Jec

Aliases: Black Jec, Sad, Digital F/X | **Type:** Program.

Disk Location: COM application., COMMAND.COM. | **Features:** Direct acting.

Damage: | **Size:** 231 to 440 | **See Also:**

Notes: A family of at least 11 small viruses.

The variant, Digital F/X crashes many machines.
The variant, Sad activates in Sept, and contains the text

> Sad virus - 24/8/91

Name: Black Monday		
Aliases: Black Monday, Borderline	**Type:** Program.	
Disk Location: COM application., EXE application., COMMAND.COM	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1055, 781 - Borderline veriant	**See Also:**

Notes: The virus contains the text,

Black Monday 2/3/90 KV KL MAL

The variant, Borderline can only infect .COM files.

Name: Blood		
Aliases: Blood, Blood 2	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Direct acting.	
Damage:	**Size:** 418	**See Also:**

Notes: Infected programs may occasionally display the following message when they are executed.

File infected by BLOOD VIRUS version 1.20

The variant, Blood-2, probably does not exist.

Name: BloodLust		
Aliases: BloodLust	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 302	**See Also:**

Notes: The virus contains the text,

Hi! This is the virus BloodLust striking!
Sorry to tell you, but your system is infected.

Name: Bloody!		
Aliases: Bloody!, Beijing, June 4th	**Type:**	
Disk Location:	**Features:**	
Damage: Corrupts boot sector	**Size:**	**See Also:**

Notes: The Bloody! virus (aka Beijing or June 4th) is a boot sector virus. You cannot get it by downloading files - you must try to boot from an infected diskette.

Name: Bloomington		
Aliases: Bloomington, NOINT, Stoned III, Stoned 3	**Type:** Boot sector., Direct acting. Activates when run.	
Disk Location: Floppy disk boot sectors., Hard disk boot sectors.	**Features:** Encrypted	
Damage: Corrupts boot sector	**Size:**	**See Also:**
Notes: "stealthy" MBR and boot sector infector. Not a very forgiving virus, if you look for the partition table you are likely to get garbage, and if DOS gets garbage, the disk is gone. CHKDSK will report 2k less "total bytes memory" (640k reporting 655360-653 or less is a danger sign) Named NoInt by Micke McCune when isolated in MAY 91 , it doesn't use interrupts to send commands to BIOS. McAfee calls it Stoned III for some random reason, Norton AntiVirus calls it Bloomington (town of its discovery)		

Name: Bob		
Aliases: Bob	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Direct acting.	
Damage:	**Size:** 718	**See Also:**
Notes: This virus activates in January 1993.		

Name: Bob Ross		
Aliases: Bob Ross, Beta	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:** Screaming Fist virus
Notes: Rumor: written by the group PHALCON/SKISM (like Screaming Fist virus) Polymorphic because it changes one byte in the middle of the decryption routine		

Name: Boojum		
Aliases: Boojum	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 334	**See Also:**
Notes:		

Name: Boys		
Aliases: Boys	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 500	**See Also:**
Notes: When this virus finds no more .COM files to infect, it starts deleting .EXE files.		

Name: Brain		
Aliases: Brain, Pakistani, Ashar, Shoe, Shoe_Virus, Shoe_Virus_B, Ashar_B, UIUC, UIUC-B, @BRAIN, Jork, Shoe B	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sector, Interferes with a running application., Corrupts a data file., Corrupts the file linkages or the FAT.	**Size:** Overlays boot sector, no increase	**See Also:**
Notes: This virus only infects the boot sectors of 360 KB floppy disks. It does no malicious damage, but bugs in the virus code can cause loss of data by scrambling data on diskette files or by scrambling the File Allocation Table. It does not tend to spread in a hard disk environment. Diskette volume labels changeto "(c) Brain".		

Name: Brasil Virus		
Aliases: Brasil Virus, Brazil	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector., Hard disk partition table.	**Features:** Memory resident; TSR., Encrypted	
Damage: Corrupts hard disk partition table, Corrupts floppy disk boot sector, Overwrites sectors on the Hard Disk., Overwrites part of the directory.	**Size:** Overlays boot sector, no increase, Overlays part of the directory	**See Also:**
Notes: The virus occupies three sectors of a disk. The first sector used is the boot sector in diskettes, or the master boot sector in hard disks. The first sector contains the initial activation code. The second sector contains the virus code that becomes memory resident, and that is responsible for propagating the virus. In the third sector the virus stores the original boot sector. In hard disks the virus uses sectors1, 2 and 3 of cylinder zero, head zero. To eliminate this virus, sector 3 (the original master boot) should to be copied back into sector 1. In 360k diskettes the virus uses DOS sectors 0, 10 and 11 (this means sector 1, cyl. 0, track 0 (boot), sec 2 cyl 0 tr. 1 (sector 10 and sect 3 cyl 0 tr. 1 (sector 11)). Sectors 10 and 11 are the end sectors of the root directory, and the virus may overwrite directory information during the infection process. To eliminate the virus sector 11 into should be copied back into sector 0. The virus handles correctly other diskette types (720k, 1.2M and1.44M), hiding his three sector always in the boot sector and in the last two directory sectors. The virus triggers by decrementing a counter once for every hour of operation. After 120 hours of effective use, the virus writes his message ("Brasil virus!"), writes random data in the first 50 cylinders of the hard disk and the "freezes" the computer. F-Prot 2.09D detects it. Scan 106 detects a non-standard boot sector. Virhunt 4.0B does not detect it.		

Name: Breeder		
Aliases: Breeder, Shield	**Type:** Companion and Trojan program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 5152, Adds File	**See Also:**
Notes: In addition to its operation as a regular "companion" type virus, this virus will append a 172 byte Trojan to COM files, which may display the message: I greet you user. I am COM-CHILD, son of The Breeder Virus. Look out for the RENAME-PROBLEM !		

Name: Brunswick		
Aliases: Brunswick, 910129	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors., Hard disk boot sectors.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sector	**Size:** Overlays boot sector, no increase	**See Also:**
Notes: The Brunswick virus infects the boot sector/master boot record of hard disks and floppies in drives A: and B: only. Once resident, this virus covertly infects all floppies and hard disks it contacts. An infected machine does not display any obvious indications of infection; therefore it can be very difficult to determine if your system is infected until the attack phase commences. During the attack phase, it overwrites the boot sector with random characters. None until it starts destroying boot records, then formerly bootable disks become unbootable. VIRHUNT v. 1.3D-1, VIRSCAN v.2.0.2 and others VIRHUNT v. 1.3D-1, VIRSCAN v.2.0.2 and others. Boot from an uninfected Floppy and rewrite the boot with the DOS SYS command.		

Name: Bryansk		
Aliases: Bryansk	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Direct acting.	
Damage:	**Size:** 673	**See Also:**
Notes: The virus activates on Fridays, before 3PM When activated, it makes files read-only. The virus contains the text, BRYANSK 1992, BITE 0.01 (C)		

Name: Budo		
Aliases: Budo	**Type:** Program.	
Disk Location: COM application., EXE application., COMMAND.COM	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 890	**See Also:**
Notes: The virus contains the strings, "FLOW LIKE A RIVER - STRIKE LIKE A THUNDER" "Run time error" "Run time error" is displayed if an infected program is run when the virus is already resident.		

Name: Bulgarian 800		
Aliases: Bulgarian 800, 800	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 800	**See Also:**
Notes:		

Name: BUPT		
Aliases: BUPT, Traveler	**Type:** Program.	
Disk Location: COM application., EXE application., COMMAND.COM	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1220, 1223	**See Also:**
Notes: The virus contains the following text, Traveller (C) BUPT 1991.4 Don't panic I'm harmless		

Name: Burger		
Aliases: Burger, 505, 509, 541, 909090H, CIA, Virdem 792, Virdem 2	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Direct acting.	
Damage:	**Size:**	**See Also:**
Notes: Not widespread at all		

Name: Burger		
Aliases: Burger, Burger 382, 382 Recovery, Burger 405, 405, Lima, Pirate, 560-A, 560-B, 560-C, 560-D, 560-E, 560-F, 560-G, 560-H	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 560, 382 - Burger 382, 382 Recovery, 405 - Burger 405, 609 - Pirate, Lima	**See Also:**
Notes: Overwrites .COM files At least eight 560 byte variants are known, named Burger 560-A, Burger 560-B etc. The variant, Burger 405 contains an error that allows it to reinfect files over and over.		

Name: Burghoffer		
Aliases: Burghoffer	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 525	**See Also:**
Notes:		

MS-DOS/PC-DOS Computer Viruses

Name: C-544		
Aliases: C-544, Paniker, vienna family	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage:	**Size:** 544 bytes	**See Also:**
Notes: see below in summary section 1st occurance mid 1990 in Leningrad, USSR On Friday the 13th, message appears Virus family: ideologically - Vienna Infection mechanism: Searching path and current directory, use standard int 21 file functions No Interrupts, no Special clues Detection: Use the message as a identification string, Prevention: Any active monitor Removal: Remove infected files, no fugs this time Direct detection: Infected files contain the readable strings: '*.COM', 'PATH=' and 'That could be a crash, crash, crash !' Marked files in the seconds field in directory.		

Name: Cancer		
Aliases: Cancer	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 740 or multiples of this actual length is only 228 bytes	**See Also:**
Notes: Cancer infects all .COM files in the current directory whenever an infected program is run. It will repeatedly infect a file. It adds 740 bytes to the beginning of a file. A variant of amsrad. Increasing file lengths. An infected file will contain the string "IV" at offset 3 in the COM file.		

Name: Cansu		
Aliases: Cansu, V, V-sign, Sigalit	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector., Hard disk partition table.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application., Corrupts hard disk partition table, Corrupts floppy disk boot sector	**Size:** Overlays boot sector, no increase	**See Also:** Brasil

Notes: Strange Video effects
Seen in Queensland Australia.

The virus has two parts, the boot sector and the virus body. The boot sector contains a short routine which loads the virus body into memory and transfers control to it. The virus body is located in:

Cylinder 0, Head 0, Sector 4 + 5	Harddisk
Track 0, Head 1, Sector 2 + 3	5.25" DD
Track 0, Head 1, Sector 13 + 14	5.25" HD
Track 0, Head 1, Sector 4 + 5	3.5" DD
Track 0, Head 1, Sector 14 + 15	3.5" HD

On floppy disks these sectors are the last two sectors of the root directory.

When executed, the virus goes memory resident and hooks interrupt vector 13 .

A bug causes floppy disks infected in drive B: to not work correctly. If you boot with such an infected disk, the virus try's to load the virus body from drive B: instead of A:. If there isn't an infected disk in drive B, your system hangs.

There are two variants which differ in the payload trigger. After 64 (variant 1) or 32 (variant 2) infections in a system that has not been shut down or rebooted, it will display a "V" (Victory) sign on screen and hang the computer.

To remove the virus from a hard disk use the undocumented FDISK /MBR command which writes a new partition record without changing the partition table.

Detect with Virhunt 4.0B, SCANV106

Name: Capital		
Aliases: Capital	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application., COMMAND.COM.	**Features:** Encrypted, Direct acting.	
Damage:	**Size:** 927	**See Also:**
Notes: Uses an encryption method similar to Cascade.		

Name: CARA		
Aliases: CARA	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1025	**See Also:**
Notes:		

Name: Carioca		
Aliases: Carioca	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 951	**See Also:** Faust
Notes: May be related to Faust		

Name: CARMEL TntVirus		
Aliases: CARMEL TntVirus	**Type:** Trojan.	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: This is a trojan suspect, Carmel Software Turbo Anti Virus package is a commercial package. If you did not purchase your copy or otherwise receive it directly from them, it could have a virus in it or otherwise be tampered. TAV has an "immunize" feature, if I recall correctly, that works by adding virus marker bytes (the signatures that viruses use to see if a file is infected) to the end of .COM and .EXE files. It could be that the files you immunized are self-checking and recognize that they have been modified.		

Name: Cascade		
Aliases: Cascade, 1704, 17Y4, 1704 B, 1704 C, Cascade A, Falling Tears, The Second Austrian Virus, Autumn, Blackjack, Falling Leaves, Cunning, Fall, Falling Letters, Herbst, Cascade YAP, YAP,Jo-Jo, Formiche	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.	**Features:** Encrypted, Stealth, Direct acting.	
Damage: Interferes with a running application., Corrupts a program or overlay files.	**Size:** 1704, 1701	**See Also:** 1701
Notes: Spreads between COM files. Occasionally causes odd screen behavior (the characters on the screen fall into a heap at the bottom of the screen!). One rare variant can destroy data on hard disks. see also 1701 Two different Cascade variants were called Cascade YAP. can be called YAP as well. Uses variable encryption, not polymorphic (virus-l, v5-097) The characters on the screen fall into a heap at the bottom of the screen!		

Name: Casino		
Aliases: Casino, Malta	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Corrupts the file linkages or the FAT.	**Size:** 2330	**See Also:**
Notes: The virus offers to let you play a game, if you loose, It destroys the FAT on your hard disk. An offer to play an uninstalled game.		

MS-DOS/PC-DOS Computer Viruses

Name: Casper		
Aliases: Casper	**Type:** Program.	
Disk Location:	**Features:** Encrypted, Direct acting., Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes: uses variable encryption		

Name: Catch 22		
Aliases: Catch 22, Catch-22	**Type:** Vaporware Virus; not real.	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: NOT A VIRUS! just a false report associated with Catch 2.2 loaded or resident. Was suspecious because it looked like it came from a Paint program.		

Name: CAZ		
Aliases: CAZ, CAZ-1159, Zaragosa	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1204, 1159	**See Also:**
Notes:		

Name: CC		
Aliases: CC	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 145	**See Also:**
Notes: Small virus that infects programs when they are executed.		

Name: CDIR		
Aliases: CDIR	**Type:** Trojan.	
Disk Location: CDIR.???	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: This program is supposed to give you a color directory of files on your disk, but it in fact will scramble your disk's FAT table.		

Name: Chad		
Aliases: Chad	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage:	**Size:** 751	**See Also:**
Notes: This virus contains the message, ... WOT!! No Anti - Virus		

Name: Chaos		
Aliases: Chaos	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors., Hard disk boot sectors.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sector, Interferes with a running application., Corrupts a program or overlay files., Corrupts the file linkages or the FAT.	**Size:** Overlays boot sector, no increase	**See Also:** Brain
Notes: Derivative of Brain		

Name: Chaos		
Aliases: Chaos, Faust	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1181	**See Also:**
Notes: This virus contains the following encrypted text. CHAOS!!! Another Masterpiece of Faust... It appears to be related to the Carioca virus,		

Name: Checksum		
Aliases: Checksum, Checksum 1.01	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1233, 1232, 1569 Variant infects COM and .EXE files	**See Also:**
Notes: A .COM file infector. The 1569 byte variant also infects .EXE files.		

Name: Cheeba		
Aliases: Cheeba	**Type:** Program.	
Disk Location:	**Features:** Encrypted, Direct acting.	
Damage:	**Size:**	**See Also:**
Notes: only virus that truely encrypts itself - uses a trivial kind of Vigenere cipher to encrypt its payload - V. Bontchev, v5-193		

Name: Chemnitz		
Aliases: Chemnitz	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 765	**See Also:**
Notes:		

Name: Christmas		
Aliases: Christmas, 1539, Father Christmas, Choinka, Tannenbaum, Christmas Tree, XA1, V1539	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Encrypted, Direct acting.	
Damage: Interferes with a running application., Corrupts boot sector	**Size:** 1539	**See Also:**
Notes: The virus infects .COM files when an infected application is executed. When an infected program is run between December 24th and 31st (any year), the virus displays a full screen image of a christmas tree and German seasons greetings. When an infected program is run on April 1st (any year), it drops a code into the boot- sectors of floppy A: and B: as well as into the partition table of the hard disk. The old partition sectors are saved but most likely destroyed since running another infected file will save the modified partition table to the same location. On any boot attempt from an infected hard disk or floppy, the text "April April" will be displayed and the PC will hang. "April April" printed at boot time then the machine hangs. A Christmas tree and German seasons greetings printed between 12/24 and 12/31. The virus contains the following German string: "Und er lebt doch noch : Der Tannenbaum !",0Dh, 0Ah,00h, "Frohe Weihnachten ...",0Dh,0Ah,07h, 00h (translated in English: "And he lives: the Christmas tree", "Happy Christmas")		

Name: Cinderella		
Aliases: Cinderella	**Type:** Program.	
Disk Location: COM application., infects files of .DOC and .CO extension + more	**Features:** Memory resident; TSR.	
Damage: None found	**Size:** 390 bytes	**See Also:**
Notes: Found in Finland on Sept. 1, 1991, seems to be common in Finland but not much of anywhere else Bug in virus: Can infect non executible files, but these files won't spread the virus. Can't survive a warmboot. Not sure if it has a payload at all, infects every file opened or executed. Virus is only 390 bytes long Will infect files opened with a *.CO? pattern. tester had trouble trying to infect .DOC files though (v5-044) The virus counts keystrokes, and after some number creates a hidden file named CINDEREL.LA and then resets the computer. Reports exist for the virus creating a file CINDEREL.LA after a certain number of keys have been pressed.		

Name: Cinderella		
Aliases: Cinderella	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 779	**See Also:**
Notes:		

Name: Clone		
Aliases: Clone	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:** Brain
Notes: Derivative of Brain		

Name: Clonewar		
Aliases: Clonewar	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Does no damage, doesn't affect any part of machine	**Size:** 247	**See Also:**
Notes:		

Name: Close		
Aliases: Close	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 656	**See Also:**
Notes: Attacks the system files IBMBIO.COM and IO.SYS. The system becomes unbootable.		

Name: Cls		
Aliases: Cls	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 853	**See Also:**
Notes: Occasionally clears the screen.		

Name: Cod		
Aliases: Cod	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage: Does no damage, doesn't affect any part of machine	**Size:** 572	**See Also:**
Notes:		

Name: Code Zero		
Aliases: Code Zero	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage:	**Size:**	**See Also:**
Notes: Similar to VCL viruses.		

Name: College		
Aliases: College	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: A virus that may have been developed at Algonquin college		

Name: Com2con		
Aliases: Com2con, USSR-311	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage:	**Size:** 311	**See Also:**
Notes:		

MS-DOS/PC-DOS Computer Viruses

Name: Comasp-472		
Aliases: Comasp-472	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 472	**See Also:**
Notes:		

Name: Commander Bomber		
Aliases: Commander Bomber	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Direct acting.	
Damage:	**Size:**	**See Also:**
Notes: Written by "Dark Avenger" this virus infects by putting parts of itself in between commands of the executible file. Basically, the virus code is split up and exists in various places within the infected file. Not encrypted, but you have to check the entire file for the virus. attacks against known virus scanning techniques		

Name: Como		
Aliases: Como	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: EXE application.	**Features:** Encrypted, Direct acting.	
Damage:	**Size:** 2019	**See Also:**
Notes: The virus contains the following text message: I'm a non-destructive virus developed to study the worldwide diffusion rate. I was released in September 1990 by a software group resident nearComo lake (north Italy). Don't worry about your data on disk. My activity is limited only to auto-transferring into other program files. Perhaps you've got many files infected. It's your task to find and delete them Best wishes		

Name: Compiler.1		
Aliases: Compiler.1	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:** 512
Notes: SCAN 97 says that Compiler.1 is the 512 virus (erroneously)		

Name: Cookie		
Aliases: Cookie, Animus	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Direct acting.	
Damage:	**Size:** 7360, 7392	**See Also:**
Notes: A large virus written in C or Pascal.		

Name: Copyright		
Aliases: Copyright, 1193	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 1193-1207 to COM files	**See Also:**

Notes: McAfee's program identifies it as Copyright [1193]
Has been distributed with a clone systems manufacturer along with some PD/shareware stuf & Jerusalem virus. Reported to infect .COM files incl COMMAND.COM, and load itself into RAM and remain resident, and directly or indirectly corrupt file linkages.
The virus contains the following fake copyright messages:

(C)1987 American Megatrends Inc.286-BIOS
(C)1989 American Megatrends Inc
(c) COPYRIGHT 1984,1987 Award Software Inc.ALL RIGHTS RESERVED

Infected executable will not run (giving a 'cannot execute' error or something similar) the first time an attempt is made, then will be either at that time or next time attempt is made, will delete it. CLEAN 86-B does not remove this virus

Name: Cossiga		
Aliases: Cossiga, Friends	**Type:** Program.	
Disk Location: EXE application.	**Features:** Direct acting.	
Damage:	**Size:** 883, 1361 - Friends variant	**See Also:**

Notes: The variant Friends contains the following text.

FRIENDS OF MAIS and CLAUDIA SAHIFFER

Name: Cpw		
Aliases: Cpw	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1459	**See Also:**

Notes: It contains the text

Este programa fue hecho en Chile en 1992 por CPW.

Name: Cracky		
Aliases: Cracky	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 546	**See Also:**

Notes: The virus contains the string,
"Cracky !"

Name: Crazy Eddie		
Aliases: Crazy Eddie	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application., EXE application.	**Features:** Encrypted, Direct acting.	
Damage: Erases the Hard Disk.	**Size:** Variable	**See Also:**
Notes:		

Name: Crazy Imp		
Aliases: Crazy Imp, Imp, Crazy	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.	**Features:** Encrypted, Direct acting.	
Damage:	**Size:** 1445	**See Also:**
Notes:		

Name: Creeper		
Aliases: Creeper, Creeping Tormentor, Creeper-425	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 475, 425	**See Also:**
Notes:		

Name: Crew-2048		
Aliases: Crew-2048	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 2048	**See Also:**
Notes: When infected programs are run, the 'European Cracking Crew' logo is sometimes displayed. The graphics screen contains the following text, This program is cracked by Notice this: TS ain't smart at all. Distribution since 11-06-1987 (or 06-11-1987) Press any key The variants have different messages.		

Name: Criminal		
Aliases: Criminal	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage:	**Size:** 2615	**See Also:** Ultimate Weapon
Notes: This virus contains the following text, Criminal, be a wiseguy and turn youreself in, if you don't I will The Ultimate Weapon has arrived, please contact the nearest police station to tell about the illegal copying of you This seems to be the same virus as the Ultimate Weapon listing, but the type is different.		

Name: Crooked		
Aliases: Crooked, Krivmous, Only	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 979	**See Also:**
Notes: This virus contains the text, Only God knows!		

Name: CryptLab		
Aliases: CryptLab	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting., Polymorphic	
Damage: Unknown, not analyzed yet.	**Size:** Polymorphic: each infection different	**See Also:**
Notes: Uses the MtE mutation engine.		

Name: CSL		
Aliases: CSL, Microelephant, CSL-V4, CSL-V5	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Does no damage, doesn't affect any part of machine	**Size:** 381, 517, 457	**See Also:**
Notes: This virus contains the text, 26.07.91.Pre-released Microelephant by CSL		

Name: CyberTech (rumored virus)		
Aliases: CyberTech (rumored virus)	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: only mentioned in May/June 1993 Infosecurity News, page 8 CIAC has article in full, believed that it displays message after Dec 31, 1992.		

Name: D-XREF60.COM		
Aliases: D-XREF60.COM	**Type:** Trojan.	
Disk Location: D-XREF60.COM	**Features:**	
Damage: Corrupts boot sector, Corrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: A Pascal Utility used for Cross-Referencing, written by the infamous `Dorn Stickel. It eats the FAT and BOOT sector after a time period has been met and if the Hard Drive is more than half full.		

Name: Dada		
Aliases: Dada, da,da, yes,yes	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1356	**See Also:**
Notes: Contains the text, da,da (yes,yes in Russian).		

Name: DANCERS		
Aliases: DANCERS, DANCERS.BAS	**Type:** Trojan.	
Disk Location: DANCERS.BAS	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: This trojan shows some animated dancers in color, and then proceeds to wipe out your [hard] disk's FAT table. There is another perfectly good copy of DANCERS.BAS on BBSs around the country.		

Name: Dark Avenger		
Aliases: Dark Avenger, Dark Avenger-B, Black Avenger, Diana, Eddie, Rapid Avenger, Apocalypse-2, CB-1530, Milana, MIR, Outland, Ps!ko, Zeleng, Rabid	**Type:** Program.	
Disk Location: COM application., EXE application., Program overlay files., COMMAND.COM	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files., Overwrites sectors on the Hard Disk.	**Size:** 1800	**See Also:** Zero Bug
Notes: Infects every executable file that is opened, .COM and EXE files are corrupted on any read attempt even when VIEWING!!! Every 16th infection, it overwrites a block of the hard disk with a copy of the boot block. The virus construction kit may have used the Dark Avenger as a basis. This virus may have been based upon the Zero Bug virus. Copies of the virus source code appear to have been passed out to others, resulting in the different variants. The Rabid virus swapped 2 instructions, located in the center of a search string used by a well known scanner. Damaged files with "Eddie lives...somewhere in time" in them. "Eddie lives...somewhere in time" at beginning and "This Program was written in the City of Sofia (C) 1988-89 Dark Avenger" near end of file		

Name: Dark Avenger 3		
Aliases: Dark Avenger 3, Dark Avenger II, V2000, Die Young, Travel, V2000-B, Eddie 3, v1024, Dark Avenger III	**Type:** Program.	
Disk Location: COM application., EXE application., COMMAND.COM.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files., Corrupts a data file., Interferes with a running application.	**Size:** 2000	**See Also:**
Notes: Every 16 executions of an infected file, the virus will overwrite a new random data sector on disk; the last overwritten sector is stored in boot sector. The system hangs-up, if a program is loaded that contains the string "(c) 1989 by Vesselin Bontchev"; V.Bonchev is a Bulgarian author of anti-virus programs. Hex dump strings in code, Two Strings : 1) "Copy me - I want to travel" (at beginning of virus-code) 2) "(c) 1989 by Vesselin Bontchev" (near end of virus code; but V.Bontchev is not the author!)		

Name: Dark End		
Aliases: Dark End	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1188	**See Also:**
Notes:		

Name: Darth Vader		
Aliases: Darth Vader	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:** 512
Notes: SCAN 97 says that Darth Vader virus is 512 virus (erroneously)		

Name: Dash-em		
Aliases: Dash-em	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1876	**See Also:**
Notes:		

Name: Datacrime		
Aliases: Datacrime, 1280, Columbus Day, DATACRIME Ib, Crime	**Type:** Program., Direct acting. Activates when run.	
Disk Location: COM application.	**Features:** Encrypted, Direct acting.	
Damage: Corrupts a program or overlay files., Attempts to format the disk., Corrupts the file linkages or the FAT.	**Size:** 1280	**See Also:**
Notes: Spreads between COM files. After October 12th, it displays the message "DATACRIME VIRUS RELEASE: 1 MARCH 1989", and then the first hard disk will be formatted (track 0, all heads). When formatting is finished the speaker will beep (end-less loop).		

Name: Datacrime II		
Aliases: Datacrime II, 1514, Columbus Day	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Encrypted, Direct acting.	
Damage: Corrupts a program or overlay files., Attempts to format the disk., Corrupts the file linkages or the FAT.	**Size:** 1514	**See Also:** 1168,1280
Notes: Spreads between both COM and EXE files. After October 12th, displays the message "* DATACRIME II VIRUS *", and damages the data on hard disks by attempting to reformat them.		

Name: Datacrime II-B		
Aliases: Datacrime II-B, 1917, Columbus Day, Crime-2B	**Type:** Program.	
Disk Location: COM application., EXE application., COMMAND.COM	**Features:** Encrypted, Direct acting.	
Damage: Corrupts a program or overlay files., Attempts to format the disk.	**Size:** 1917	**See Also:**
Notes: Spreads between both COM and EXE files. After October 12th, displays the message "* DATACRIME II VIRUS *", and damages the data on hard disks by attempting to reformat them.		

Name: Datacrime-B		
Aliases: Datacrime-B, 1168, Columbus Day, Datacrime Ia	**Type:** Program.	
Disk Location: COM application.	**Features:** Encrypted, Direct acting.	
Damage: Corrupts a program or overlay files., Attempts to format the disk., Corrupts the file linkages or the FAT.	**Size:** 1168	**See Also:** Datacrime II
Notes: Spreads between COM files. After October 12th, it displays the message "DATACRIME VIRUS RELEASE: 1 MARCH 1989", and then the first hard disk will be formatted (track 0, all heads). When formatting is finished the speaker will beep (end-less loop).		

Name: Datalock		
Aliases: Datalock, Datalock 1.00, V920, Datalock 2, Datalock-1043	**Type:** Program.	
Disk Location: COM application., EXE application., Only .COM files > 22999 bytes long	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 920, 1043 - Datalock-1043 variant	**See Also:**
Notes: It infects all EXE files but COM files must be greater than 22999 bytes long. If a file is opened that matches the selector *.?BF (.DBF files) is will give the message "Too many files open" and prevent access to the file. From a report in virus-l, v4-220: system lock-ups, drop out of application with no messages. Some programs would display the message "overlay not found" prior to dropping to DOS, a .EXE file grew by 920 bytes during first execution and after re-installation. Using debugger, found string "DataLock version 1.0". Datalock 2 variant found in wild in DC area that is buggy(virus-l, v5-092) DATALOCK 2 does NOT contain string "Datalock version 1.0" SCAN 89b and FPROT 2.03a don't find Datalock 2 variant in EXE files, but original datalock signatures are valid and can be used to identify this variant. For DATALOCK 2: C3 1E A1 2C 00 50 8C D8 48 8E D8 81 2E 03 00 80 00 40 8E D8		

Name: Day10		
Aliases: Day10, SYP	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Erases the Hard Disk.	**Size:** 674	**See Also:**
Notes: If the current date is divisible by 10, the virus trashes the hard disk.		

Name: Dbase		
Aliases: Dbase, DBF virus	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a data file., Interferes with a running application., Corrupts a program or overlay files., Corrupts the file linkages or the FAT.	**Size:** 1864	**See Also:**
Notes: Infects COM files. Registers all new .DBF files in a hidden file c:\BUGS.DAT. When any of those files are written, it reverses the order of adjacent bytes. When any of those files are read, it again reverses the bytes, making the file appear to be OK, unless it is read on an uninfected system or the file name is changed. When a file that is more than 3 months old is accessed, the virus attempts to destroy the FAT and root directory on drives D:, E;, ...Z:. Typical text in Virus body (readable with HexDump-utilities): "c:\bugs.dat"		

Name: Dedicated		
Aliases: Dedicated, Fear	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting., Polymorphic	
Damage: No damage, only replicates.	**Size:** Polymorphic: each infection different	**See Also:**
Notes: Uses the MtE mutation engine to hide.		

Name: Deicide		
Aliases: Deicide, Decide, Deicide II	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage:	**Size:** Overlays application, no increase, 1335 (Deicide II variant)	**See Also:**
Notes: When activated, the virus destroys the first 80 sectors on drive C: The virus contains the following text: DEICIDE! Glenn (666) says : BYE BYE HARDDISK!! Next time be carufull with illegal stuff. This experimental virus was written by Glenn Benton to see if I can make a virus while learning machinecode for 2,5 months. (C) 10-23-1990 by Glenn. I keep on going making virusses.		

Name: Demolition		
Aliases: Demolition	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.	**Features:** Encrypted, Direct acting.	
Damage:	**Size:** 1585	**See Also:**
Notes:		

Name: Demon		
Aliases: Demon	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** Overlays application, no increase	**See Also:**
Notes:		

Name: DenZuk		
Aliases: DenZuk, Venezuelan, Search, DenZuc B, Den Zuk, Mardi Bros, Sudah ada vaksin, Denzuko, Ohio, Hacker	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors.	**Features:** Memory resident; TSR above TOM.	
Damage: Interferes with a running application., Corrupts boot sector	**Size:** Overlays boot sector, no increase, Uses1 boot sector and 9 sectors on track 40	**See Also:**
Notes: Infects floppy disk boot sectors, and displays a purple DEN ZUK graphic on a CGA, EGA or VGA screen when Ctrl-Alt-Del is pressed. F-Prot calls it Mardi Bros (virus-1, v5-072), but viruSafe says it is a different virus Discovered July 1990 in France, this virus installs itself 7168 bytes above high memory. Infected diskettes have their volume lable changed to "Mardi Bros" Boot sector will contain the following message "Sudah ada vaksin" The label on an infected disk will read: "Y.C.1.E.R.P", where the "." is the F9h character.		

Name: Destructor		
Aliases: Destructor	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1150	**See Also:**
Notes: The virus contains the text, DESTRUCTOR V4.00 (c) 1990 by ATA		

Name: Devil's Dance		
Aliases: Devil's Dance, Mexican, 941, 951	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application., Corrupts a program or overlay files., Corrupts a data file., Corrupts the file linkages or the FAT., Overwrites sectors on the Hard Disk.	**Size:** 941, 951?	**See Also:**
Notes: Infects all .COM files in the current directory multiple times. Pressing Ctrl-Alt-Del displays DID YOU EVER DANCE WITH THE DEVIL IN THE WEAK MOONLIGHT ? PRAY FOR YOUR DISKS!! The Joker The virus counts keystrokes. After 2000 it activates, and and changes the screen colors, after 5000 it destroys the FAT The file date/time is set to the date/time of the infection (i.e. multiple infected files have the same file date/time). All characters typed will be displayed in a different color on a color card. If <CTRL>+<ALT>+<DEL> is pressed, the following message is displayed: "Have you ever danced with", "the devil under the weak light of the moon? ", "Pray for your disk! The_Joker...", "Ha Ha Ha Ha Ha Ha Ha Ha Ha Ha". Typical text in Virus body, readable with hexdump-utilities: "Drk", "*.com". If the high- bit of the displayed code is stripped, the message displayed at system reset time can be read. .COM files: the first three bytes (jmp) and the last three bytes are identical. The file date/time is set to the date/time of the infection (i.e. multiple infected files have the same file date/time).		

Name: Dewdz		
Aliases: Dewdz	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage:	**Size:** 601	**See Also:**
Notes: When this virus activates it displays the text Kewl Dewdz! The virus contains the string, Made in STL (c) '91		

Name: Diamond		
Aliases: Diamond, Italian Diamond, Damage, Damage-2, David, Greemlin, Lucifer, Rock Steady, Alfa, 1024	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage: Attempts to format the disk., Only the Rock Steady variant does this.	**Size:** 1024, 666 - Rock Steady Variant	**See Also:**
Notes: mentioned in Virus-l, v4-224, v5-006 Two variants were once uploaded to a BBS in Bulgaria. Relative of 1024/1024B The Rock Steady variant formats the hard disk on the 13th of any month.		

Name: Digger		
Aliases: Digger	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Direct acting.	
Damage:	**Size:** 1475 COM, 1478 EXE	**See Also:**
Notes:		

Name: Dima		
Aliases: Dima	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Direct acting.	
Damage:	**Size:** 1024	**See Also:**
Notes:		

Name: DIR		
Aliases: DIR	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Does no damage, doesn't affect any part of machine	**Size:** 691	**See Also:**
Notes: Only infects files when the DIR command is executed.		

Name: Dir II

Aliases: Dir II, Dir 2, MG series II, Creeping Death, DRIVER-1024, Cluster, D2

Type: Program., Memory resident., Encrypted/Stealth The virus actively hides.

Disk Location: COM application., EXE application., COMMAND.COM.

Features: Encrypted, Direct acting.

Damage: Encrypts the file directory., Corrupts the file linkages or the FAT., Overwrites sectors on the Hard Disk.

Size: Adds File 1024, places virus code in last cluster of infected disk and changes directory structure to have the cluster pointer of an executible file point to the viral executible.

See Also:

Notes: Cannot infect NetWare volumes, MS-Windows crashes upon infection
This virus modifies entries in the directory structure, causing the computer to jump to the virus code before execution of the program begins. This virus also uses stealth techniques to hide its existance in memory.
Initial infection occurs when a file with an infected directory is executed. The virus becomes memory resident by appearing to be a disk device driver, and puts a copy of itself on the last cluster defined as "good" in the disk. It then infects all .EXE and .COM file directory entries by scrambling the original cluster pointer, placing it in an unused section of the directory structure, and replacing the cluster with a pointer to the virus.
There are 5 variants (11/20/91). NOTE: This works on MS DOS ver 3.0-5.00.223-beta but does not work on true 5.0 version. and it has a bug in 3.31. At least one variant works under 5.0 With virus not active in memory, CHKDSK reports many cross-linked files and lost file chains, and copied infected files are only 1024 bytes long or the size one 1 cluster, usually 1 K; backups disks and other full disks can become corrupted when virus writes to the last cluster.
With virus not active in memory, CHKDSK -F or Norton Disk Doctor will destroy most executible files on the disk. DDI Data Physician V 3.0B, McAfee's CLEAN v84, Microcom's VIRx 1.8, F-PROT 2.01, Dr. Solomon's Anti-virus Toolkit V 5.13, Manual method described below.
These 4 detection steps are independant of each other:
1. Boot from a known clean floppy and run CHKDSK with no parameters. An indication of infection is a report of many cross-linked files and lost file chains.
2. WITH VIRUS ACTIVE IN MEMORY, perform a DIR. Now boot from a known clean floppy and perform a DIR. If the size of executible files changes between the two, it is fairly certain the virus is present.
3. With virus ACTIVE in memory, try to delete a file from a write protected diskette. If you don't get an error message, it is a sign of infection.
4. Format a new diskette and look at its map with PC Tools. If one cluster of the diskette is allocated (not bad) and it is at the end of the diskette, then it is probable the virus is resident and active in memory DDI Data Physician V 3.0B, McAfee's CLEAN v84, Bontchev's DIR2CLR
Use this 5-step process (Anti viral program versions prior to October 1991 are inadequate to find/eradicate this virus: 1. With DIR II active in memory, use the COPY command (RENAME command may also work, but COPY is more definitive) to copy all .EXE and .COM files to another file with a different extension. Example COPY file.EXE file.VXE
2. Reboot system from a clean, write protected diskette to ensure the system does NOT have the virus in memory. 3. Delete all files with extensions of .EXE and .COM. This will remove all pointers to the virus.
4. Rename all executibles to their original names. Example RENAME file.VXE file.EXE
5. Examine all these executibles you have just restored with the DIR command. if any are 1K in length, they are probably a copy of the virus and must be destroyed.
After eradication it may be desirable to now run CHKDSK /f or another disk optimization utility to ensure the virus is no longer anywhere on the disk.

Name: Disk Killer

Aliases: Disk Killer, Computer Ogre, Disk Ogre

Type: Boot sector.

Disk Location: Floppy disk boot sectors., Hard disk boot sectors.

Features: Memory resident; TSR.

Damage: Corrupts boot sector, Interferes with a running application., Corrupts a program or overlay files., Corrupts a data file., Encrypts the data on the disk.

Size: Overlays boot sector, no increase

See Also:

Notes: Infects floppy and hard disk boot sectors and after 48 hours of work time, it displays the following message

Disk Killer -- Version 1.00 by COMPUTER OGRE 04/01/1989

Warning !!
Don't turn off the power or remove the diskette while Disk Killer is
Processing!

PROCESSING

It then encrypts everything on the hard disk. The encryption is reversable. Word at offset 003Eh in the boot sector will contain the value 3CCBh.

Name: DISKSCAN

Aliases: DISKSCAN, SCANBAD, BADDISK

Type: Trojan.

Disk Location: DISKSCAN.EXE, , SCANBAD.EXE, BADDISK.EXE

Features:

Damage: Overwrites sectors on the Hard Disk.

Size:

See Also:

Notes: This was a PC-MAGAZINE program to scan a [hard] disk for bad sectors, but then a joker edited it to WRITE bad sectors. Also look for this under other names such as SCANBAD.EXE and BADDISK.EXE. A good original copy is availble on SCP Business BBS.

Name: Diskspoiler

Aliases: Diskspoiler

Type: Program., Encrypted/Stealth The virus actively hides.

Disk Location: COM application.

Features: Encrypted, Direct acting.

Damage:

Size: 1308

See Also:

Notes:

Name: Dismember

Aliases: Dismember

Type: Program., Encrypted/Stealth The virus actively hides.

Disk Location: COM application.

Features: Encrypted, Direct acting.

Damage:

Size: 288

See Also:

Notes:

Name: DM		
Aliases: DM, DM-310, DM-330	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: No damage, only replicates.	**Size:** 400, 310, 330	**See Also:**
Notes: The virus contains the following text: (C)1990 DM		

Name: DMASTER		
Aliases: DMASTER	**Type:** Trojan.	
Disk Location: DMASTER.???	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: This is yet another FAT scrambler.		

Name: Do Nothing		
Aliases: Do Nothing, Stupid Virus, 640K Virus	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 583	**See Also:**
Notes: Infects .COM files. The virus copies itself to 9800:100h, which means that only computers with 640KB can be infected. Many programs also load themselves to this area and erase the virus from the memory.		

Name: Doom		
Aliases: Doom, Doom II, Doom-2B	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application., EXE application.	**Features:** Encrypted, Direct acting.	
Damage:	**Size:** 1252	**See Also:**
Notes: virus-l, v4-131 says that a variant of the 512 and Doom-II virus can put executable code into video memory. The virus code contains the text, DOOM II (c) Dr.Jones, NCU.		

Name: Doomsday		
Aliases: Doomsday, Null Set, Scion	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Unknown, not analyzed yet.	**Size:** 733	**See Also:**
Notes: The virus contains the following texts, A scion to none Certainly no fun Total destruction when done Introducing DOOMSDAY ONE Written in Orlando, FL on 05/13/91 Your disk is dead! Long live DOOMSDAY 1.0		

Name: DOS-HELP		
Aliases: DOS-HELP	**Type:** Trojan.	
Disk Location: DOS-HELP.???	**Features:** Memory resident; TSR.	
Damage: Attempts to format the disk.	**Size:**	**See Also:**
Notes: This trojan, when made memory-resident, is supposed to display a DOS command for which the User needs help with. Works fine on a Diskette system but on a HARD DRIVE system tries to format the Hard Disk with every access of DOS-HELP.		

Name: DOShunt		
Aliases: DOShunt	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Trashes the hard disk.	**Size:** 483	**See Also:**
Notes: Activates on June 26 and trashes the hard disk.		

Name: DOSKNOWS		
Aliases: DOSKNOWS	**Type:** Trojan.	
Disk Location: DOSKNOWS.EXE	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:** 5376 Size of the real DOSKNOWS.EXE	**See Also:**
Notes: Apparently someone wrote a FAT killer and renamed it DOSKNOWS.EXE, so it would be confused with the real, harmless DOSKNOWS system-status utility.		

Name: Doteater		
Aliases: Doteater, Dot Killer, Point Killer	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Interferes with a running application.	**Size:** 944	**See Also:**
Notes: When activated, it removes all dots from the screen. All periods disappear from the screen.		

Name: DPROTECT		
Aliases: DPROTECT	**Type:** Trojan.	
Disk Location: DPROTECT.???	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: Apparently someone tampered with the original, legitimate version of DPROTECT and turned it into a FAT-table eater. A good version is available on SCP Business BBS.		

Name: DRAIN2		
Aliases: DRAIN2	**Type:** Trojan.	
Disk Location: DRAIN2.???	**Features:**	
Damage: Attempts to format the disk.	**Size:**	**See Also:**
Notes: There really is DRAIN program, but this revised program goes out does Low Level Format while it is playing the funny program.		

Name: DROID		
Aliases: DROID	**Type:** Trojan.	
Disk Location: DROID.EXE	**Features:**	
Damage:	**Size:** 54272 Size of DROID.EXE	**See Also:**
Notes: This trojan appears under the guise of a game. You are supposedly an architect that controls futuristic droids in search of relics. In fact, PC-Board sysops, if they run this program from C:\PCBOARD, will find that it copies C:\PCBOARD\PCBOARD.DAT to C:\PCBOARD\HELP\HLPX.		

Name: Dropper7		
Aliases: Dropper7, Dropper 7	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR., Stealth; actively hides from detection.	
Damage:	**Size:**	**See Also:** Dropper7 Boot
Notes: Can not be removed. Infected files must be deleted.		

Name: Dropper7 boot		
Aliases: Dropper7 boot	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector., Hard disk boot sector.	**Features:** Memory resident; TSR., Stealth; actively hides from detection.	
Damage:	**Size:**	**See Also:** Dropper7
Notes:		

Name: DRPTR		
Aliases: DRPTR, WIPEOUT	**Type:** Trojan.	
Disk Location: DRPTR.???	**Features:**	
Damage: Deletes or moves files.	**Size:**	**See Also:**
Notes: After running unsuspected file, the only things left in the root directory are the subdirectories and two of the three DOS System files, along with a 0-byte file named WIPEOUT.YUK. COMMAND.COM was located in a different directory; the file date and CRC had not changed.		

Name: DSZBREAK		
Aliases: DSZBREAK	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: Not sure if virus or trojan (v5-031) A program supposedly meant to break the registration requirement on Omen Software's DSZ (zmodem protocol). It works on some kind of a timer, so when you leave your machine running without using the keyboard, it will then make anything you attempt to enter from the keyboard a control character (DIR would become ^D^I^R). It appears to live in the boot sector, as reloading your .sys files fack to your dos directory or reformatting C: will get rid of it.		

Name: Dutch Tiny		
Aliases: Dutch Tiny, Dutch Tiny-124, Dutch Tiny-99	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: No damage, only replicates.	**Size:** 126, 124, 99	**See Also:**
Notes:		

Name: E. T. C.		
Aliases: E. T. C.	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: No damage, only replicates.	**Size:** 700	**See Also:**
Notes: The virus contains the text, E.T.C. VIRUS, Version 3.0, Copyright (c) 1989 by E.T.C. Co.		

Name: Ear		
Aliases: Ear, Quake, Suicide	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Direct acting.	
Damage:	**Size:** 1024, 960 - Quake variant, 2048 - Suicide variant	**See Also:**
Notes: The virus asks questions about the anatomy of the ear.		

Name: Eastern Digital		
Aliases: Eastern Digital	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1600	**See Also:**
Notes: The virus contains the text, MegaFuck from Eastern Digital It may affect Backup.com		

Name: Eddie 2		
Aliases: Eddie 2	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage: No damage, only replicates.	**Size:** 651	**See Also:**
Notes: Similar to the Eddie virus, it contains the string, Eddie Lives The seconds field of the time stamp contains 62. The virus hides its length change by trapping the DIR command and adjusting the length of any file with 62 in the seconds field of the time stamp.		

Name: EDV		
Aliases: EDV	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:** brain
Notes: Derivative of Brain, with the eighth bit set, using the ISO 8859-1 character table it will result in the swedish/finnish national characters in their major form and in alphabetical order. (virus-l, v5-73). This is just a coincidence, in the the EDV virus is French.		

Name: EDV		
Aliases: EDV, Cursy	**Type:** Boot sector., Activates once at boot time.	
Disk Location: Floppy disk boot sectors., Hard disk boot sectors.	**Features:** Memory resident; TSR.	
Damage:	**Size:** Overlays boot sector, no increase	**See Also:**
Notes: This virus hides in the upper memory block in any free memory below E800. It also issues a HLT instruction if ES or DS is pointing to it (indicating it is being scanned). The end of the boot sector contains the text EV. On a 360 K disk, the original boot sector is in the last sector of the last track. Contains an encrypted text string, That rings a bell,no ? from Cursy		

Name: EGABTR		
Aliases: EGABTR	**Type:** Trojan.	
Disk Location: EGABTR.???	**Features:**	
Damage: Deletes or moves files.	**Size:**	**See Also:**
Notes: BEWARE! Description says something like "improve your EGA display," but when run, it deletes everything in sight and prints, "Arf! Arf! Got you!"		

Name: Eight Tunes		
Aliases: Eight Tunes, 1971, 8-Tunes	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application., Corrupts a program or overlay files.	**Size:** 1971-1986 .COM applications bytes: (length -3) mod 16 = 0., 1971-1986 .EXE applications bytes: (length -3) mod 16 = 0.	**See Also:**
Notes: During load procedure, .COM and .EXE files are infected. 90 days after the infection, after 30 minutes, the virus will play one of eigth melodies (random selection). After a short time, the virus will play a melody again. The virus looks for and deactivates "BOMBSQAD.COM", an antivirus-tool controlling accesses to disks. The virus looks for "FSP.COM" (Flushot+), an antivirus tool controlling accesses to disks, files etc., and stops the infection if it is found. Your computer is randomly playing short tunes. Typical texts in Virus body (readable with HexDump-facilities):"COMMAND.COM" in the data area of the virus .Com files: the bytes 007h,01fh,05fh, 05eh,05ah,059h,05bh,058h,02eh,0ffh,02eh,00bh, 000h are found 62 bytes before end of file . .EXE files: the bytes 007h,01fh, 05fh,05eh,05ah,059h,05bh,058h,02eh,0ffh,02eh, 00bh,000h are found 62 bytes before end of file.		

Name: Eliza		
Aliases: Eliza	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 1193-1194 TO COM files, Destroys .EXE files	**See Also:**
Notes: Infected .COM files do not replicate. Infected .EXE files are destroyed. Lots of bugs in this virus.		

Name: EMF		
Aliases: EMF	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Unknown, not analyzed yet.	**Size:** 404, 625	**See Also:**
Notes: The virus contains the text Screaming Fist The screamer virus also contains this text, possibly indicating that they were written by the same author.		

Name: Emmie		
Aliases: Emmie	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 2702	**See Also:**
Notes:		

Name: Empire		
Aliases: Empire, Empire A, Empire C, Empire D, Stoned variant, Empire B.2, UofA	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors., Hard disk boot sectors.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sector	**Size:** Overlays boot sector, no increase	**See Also:** Azusa
Notes: Derived from the Stoned virus, originally from Univ. of Alberta. Last known variant released July 10, 1991, total of 18 variants identified to date. Variants have differences in the code, indicating separate prramming efforts on the part of the virus writer. Empire C gets around the simple "chkdsk" for boot sector viruses. Since most boot sector viruses have to reduce the number of "total bytes of memory" of a computer to hide at the top of memory, the virus can be detected by seeing whether "chkdsk" returns 1k or 2k less than it is supposed to return. Empire C didn't bother telling DOS that the virus was present in memory when it installed itself. It puts itself at 9000:0000 or 80000:0000 and functioned until something else used that memory location, then the system crashed. Empire D was a response to an installation of "Disk Secure". It recognized the presense of Disk Secure and removes it before infecting the computer. These are the most common viruses at the Univ. of Alberta and in Edmonton. See also listing for Empire B.2, or UofA virus McAfee Scan v80 may detect some Empire strains as Azusa		

Name: Empire B.2		
Aliases: Empire B.2, UofA, derived of Stoned	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors., Hard disk boot sectors.	**Features:** Memory resident; TSR above TOM.	
Damage: Corrupts boot sector	**Size:**	**See Also:**
Notes: Contains a data diddler routine. On any write to a floppy, the virus may randomly decide to alter one or more bytes being written, to a new random value. This variant does not announce its existence in any way. Does not use stealth, and can be detected using several virus scanners. Uses 1k of memory from "top of memory" and it tends to not work with 720k diskettes, they appear unreadablebecause DOS thinks they are 1.2Mb.		

Name: End of		
Aliases: End of	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:**	**See Also:**
Notes:		

Name: Enola		
Aliases: Enola	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 1864, 2430	**See Also:**
Notes:		

MS-DOS/PC-DOS Computer Viruses

Name: EUPM		
Aliases: EUPM, Year 1992, Apilapil	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage: Trashes the hard disk.	**Size:** 1731	**See Also:**
Notes: If the year is set to 1992, it overwrites the hard disk.		

Name: Europe '92		
Aliases: Europe '92, Dutch 424	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: No damage, only replicates.	**Size:** 421	**See Also:**
Notes: If the year is set to 1992, it displays the message, Europe/92 4EVER!		

Name: F-Soft		
Aliases: F-Soft, Frodo Soft, F-Soft 563	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Unknown, not analyzed yet.	**Size:** 458, 563 - F-Soft 563 variant	**See Also:**
Notes: The virus contains the text , (c) Frodo Soft The 563 variant is encrypted.		

Name: F-Word		
Aliases: F-Word, Fuck You, F-you	**Type:** Program.	
Disk Location: COM application., EXE application - 593 and 635 variants	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 417, 593, 635	**See Also:**
Notes: The virus contains the text, Fuck You		

Name: F1-337		
Aliases: F1-337	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: No damage, only replicates.	**Size:** 337	**See Also:**
Notes:		

Name: Fax Free		
Aliases: Fax Free, Mosquito, Topo, Pisello	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: EXE application.	**Features:** Encrypted, Direct acting.	
Damage: Unknown, not analyzed yet.	**Size:** 1024, 1536	**See Also:**
Notes: The virus contains the following text: Hello this is the core Rev 3 26/4/91 P 0.98c P. 0.98 Rev 4 24IX89 bye bye		

Name: FCB		
Aliases: FCB	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** Overlays application, no increase 384 bytes long	**See Also:**
Notes: Delete infected files		

Name: Feist		
Aliases: Feist	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 670	**See Also:**
Notes:		

Name: Fellowship		
Aliases: Fellowship, Better World	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 1019	**See Also:**
Notes: The virus contains the text: This message is dedicated to all fellow PC users on Earth Towards A Better Tomorrow And A Better Place To Live In The virus is actually not very friendly		

Name: FGT		
Aliases: FGT	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Unknown, not analyzed yet.	**Size:** 651	**See Also:**
Notes:		

Name: Fichv		
Aliases: Fichv, Fichv-EXE 1.0	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application., EXE application Fichv-EXE 1.0 variant	**Features:** Encrypted, Direct acting.	
Damage: Overwrites sectors on the Hard Disk.	**Size:** 903, 897 Fichv-EXE 1.0 variant	**See Also:**
Notes: The virus contains the text ***FICHV 2.1 vous a eu***** When activated, it overwrites the first 6 sectors of the track 0, head 1 of the current drive.		

MS-DOS/PC-DOS Computer Viruses

Name: Filedate 11		
Aliases: Filedate 11, Filedate 11-537	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 570, 537 - variant	**See Also:**
Notes:		

Name: FILES.GBS		
Aliases: FILES.GBS	**Type:** Trojan.	
Disk Location: FILES.GBS	**Features:**	
Damage: Bypasses OPUS BBS's security.	**Size:**	**See Also:**
Notes: When an OPUS BBS system is installed improperly, this file could spell disaster for the Sysop. It can let a user of any level into the system. Protect yourself. Best to have a sub-directory in each upload area called c:\upload\files.gbs (this is an example only). This would force Opus to rename a file upload of files.gbs and prevent its usage.		

Name: Filler		
Aliases: Filler	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors., Hard disk boot sectors.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** Overlays boot sector, no increase	**See Also:**
Notes: The virus code and the original boot sector are hidden on track 40, outside of the normal range of tracks.		

Name: Finnish		
Aliases: Finnish, Finnish-357	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: No damage, only replicates.	**Size:** 709	**See Also:**
Notes: The virus infects every .COM file run, or opened for any reason.		

Name: Fish		
Aliases: Fish, European Fish,Fish 6	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application., EXE application., COMMAND.COM.	**Features:** Encrypted, Direct acting.	
Damage: Corrupts a program or overlay files., Interferes with a running application., Corrupts a data file.	**Size:** 3584	**See Also:**
Notes: If (system date>1990) and a second infected .COM file is executed, a message is displayed: "FISH VIRUS #6 - EACH DIFF - BONN 2/90 '~Knzyvo}'" and then the processor stops (HLT instruction). The virus will attempt to infect some data files, corrupting them in the process. This is a variant of the 4096 virus. There is another virus named FISH that is a boot sector virus. (kp 2/26/93)		

Name: Flash		
Aliases: Flash, 688, Gyorgy	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application., EXE application., COMMAND.COM	**Features:** Encrypted, Direct acting.	
Damage: Corrupts a program or overlay files., Interferes with a running application.	**Size:** 688	**See Also:**
Notes: The memory resident virus infects applications when they are run. After June 1990, the virus makes the screen flash. This flash can only be seen on MDA, Hercules, and CGA adapters, but not on EGA and VGA cards. The Gyorgy variant contains the text "I LOVE GYÖRGYI". A flashing screen.		

Name: Flip		
Aliases: Flip, Omicron, Omicron PT	**Type:** Boot sector.	
Disk Location: COM application., EXE application., Hard disk boot sector.	**Features:** Polymorphic	
Damage:	**Size:** 2153 and 2343 strains exist, Polymorphic: each infection different/some strains	**See Also:**
Notes: Multi-partite virus. (infects both boot sectors and files) FProt finds Flip on two files of Central Point Anti-Virus: this is a false positive. The 2343 strain (the rarer one) patches COMMAND.COM 2nd Day of every month activates on a system with an EGA or VGA display between 1600 and 1659 and reverses the screen and characters.		

Name: Flower		
Aliases: Flower	**Type:** Program.	
Disk Location: EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 883	**See Also:**
Notes: This virus activates on Nov. 11th. Any infected file run on that date is overwritten wit a Trojan that displays the following text: FLOWER Support the power of women Use the power of man Support the flower of woman Use the word FUCK The word is love		

Name: FLUSHOT4		
Aliases: FLUSHOT4, FLU4TXT	**Type:** Trojan.	
Disk Location: FLUSHOT4.ARC	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: This Trojan was inserted into the FLUSHOT4.ARC and uploaded to many BBS's. FluShot is a protector of your COMMAND.COM. As to date, 05/14/88 FLUSHOT.ARC FluShot Plus v1.1 is the current version, not the FLUSHOT4.ARC which is Trojaned.		

Name: Forger		
Aliases: Forger	**Type:** Program.	
Disk Location: EXE application.	**Features:** Direct acting.	
Damage: Corrupts a data file.	**Size:** 1000	**See Also:**
Notes: Corrupts data when it is written to disk.		

Name: Form		
Aliases: Form, Form Boot, FORM-Virus, Forms	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors., Hard disk boot sectors.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files., Deletes or moves files.	**Size:** Overlays boot sector, no increase	**See Also:**
Notes: A boot sector virus that randomly destroys files. Dual acting; Attempts to infect the hard disk at boot time. Attempts to infect a floppy whenever the floppy is read. Does not infect the Master Boot Record (Partition table), but the boot record of the first logical drive (C:). It is also marks a cluster as bad, and stores the rest of the virus there. The command FDISK/MBR is ineffective against FORM because it is not in the MBR (v5-190) Versions of FPROT prior to 2.06a can't remove the virus. The SYS command removes the virus by rewriting the disks boot sector. It does not remobe the part stored in the bad sector, but that part won't hurt anything without the part in the boot sector. The virus makes the keys click and delays key action slightly. The boot sector will contain the following text(amongst others): "The FORM-Virus sends greetings to everyone who's read this text.". To remove it, boot from a clean disk and rewrite the boot sectors of an infected disk with the SYS command. Repeat for all infected disks. May have been on demo diskette of Clipper product. (virus-l V4-213)		

Name: Freddy		
Aliases: Freddy	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 1870	**See Also:**
Notes: The virus contains the text, Freddy Krg Nov 92, virus-! v5-188: CLEAN v97 and v99 may have trouble disinfecting Freddy, reports that Jeru virus was found. Clean corrupted the files, which hung user's computer. Since its not a Jer. variant, that won't work. Freddy appends itself to .COM files, DOESN'T add it's code to the beginning.		

Name: Freew		
Aliases: Freew	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 692	**See Also:**
Notes: Overwrites files with a Trojan that prints "Program Terminated Normally" when run.		

MS-DOS/PC-DOS Computer Viruses

Name: Friday 13 th COM		
Aliases: Friday 13 th COM, South African, 512 Virus, COM Virus, Friday The 13th-B, Friday The 13th-C, Miami, Munich, Virus-B, ENET 37	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 419, 613 - ENET 37 variant	**See Also:** number of the beast, Compiler.1, Darth Vader
Notes: Infects all .COM files except COMMAND.COM, and deletes the host program if run on Friday the 13th. Beast: SCAN 97 still says that "number of the beast" is the 512 virus, also says that Compiler.1 and Darth Vader viruses are also 512 virus (erroneously) Files disappear on Friday the 13th. Text "INFECTED" found near start of virus.		

Name: Frog's Alley		
Aliases: Frog's Alley	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: reported in Virus-l, v4-255, no more info		

Name: Frogs		
Aliases: Frogs, Frog's Alley	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.	**Features:** Encrypted, Direct acting.	
Damage: Unknown, not analyzed yet.	**Size:** 1500	**See Also:**
Notes: Files are infected when a DIR command is executed. The file contains the following encrypted text. AIDS R.2A - Welcome to Frog's Alley !, (c) STPII Laboratory - Jan 1990..		

Name: Fu Manchu		
Aliases: Fu Manchu, 2086, 2080, Fumanchu	**Type:** Program.	
Disk Location: COM application., EXE application., Program overlay files.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application., Corrupts a program or overlay files.	**Size:** 2086 Increase of .COM files, 2080-2095 Increase of .EXE files length mod 16 equals 0	**See Also:** Jerusalem, 1813
Notes: Infects .COM and .EXE files. The message 'The world will hear from me again! ' is displayed on every warmboot, and inserts insults into the keyboard buffer when the names of certain world leaders are typed at the keyboard. Occasionally causes the system to spontaneously reboot. Deletes certain 4 letter words when typed at the keyboard.		

Name: Funeral		
Aliases: Funeral	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 921	**See Also:**
Notes: Plays a tune		

MS-DOS/PC-DOS Computer Viruses

Name: FUTURE		
Aliases: FUTURE	**Type:** Trojan.	
Disk Location: FUTURE.???	**Features:**	
Damage: Attempts to erase all mounted disks.	**Size:**	**See Also:**
Notes: This "program" starts out with a very nice color picture and then proceeds to tell you that you should be using your computer for better things than games and graphics. After making that point, it trashes your A: drive, B:, C:, D:, and so on until it has erased all drives.		

Name: G-MAN		
Aliases: G-MAN	**Type:** Trojan.	
Disk Location: G-MAN.???	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: Another FAT killer.		

Name: GATEWAY		
Aliases: GATEWAY, GATEWAY2	**Type:** Trojan.	
Disk Location: GATEWAY.???	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: Someone tampered with the version 2.0 of the CTTY monitor GATEWAY. What it does is ruin the FAT.		

Name: Geek		
Aliases: Geek	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 450	**See Also:**
Notes:		

Name: Genb		
Aliases: Genb, genp	**Type:** Boot sector.	NOT ANY PARTICULAR VIRUS!!!
Disk Location: Hard disk boot sector.	**Features:**	
Damage:	**Size:**	**See Also:** Form, Brazil
Notes: This is NOT a particular virus! McAfee's SCAN program says identifies some boot sector viruses as the "genb" or "genp" viruses when it finds a suspicious scanning string in the boot sector . Viruses that have appeared that are identified as genb include FORM and Brazil. Eradication may occur if you run SYS C:, but backup your hard disk first!		

Name: Gergana		
Aliases: Gergana, Gergana-222, Gergana-300, Gergana-450, Gergana-512	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage:	**Size:** 182	**See Also:**
Notes: The virus contains the text "Gergana", and "Happy 18th Birthday"		

MS-DOS/PC-DOS Computer Viruses

Name: Ghost		
Aliases: Ghost	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts boot sector, Corrupts a program or overlay files.	**Size:** 2351	**See Also:**
Notes: Infects .COM files.		

Name: GhostBalls		
Aliases: GhostBalls, Ghost Boot; Ghost COM, Vienna, DOS-62	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts boot sector, Interferes with a running application., Corrupts a program or overlay files.	**Size:** 2351	**See Also:**
Notes: Variant of Vienna that puts a patched copy of the Ping Pong virus in the boot of drive A. It may infect floppy and hard disk boot sectors, sources differ on this. It contains the following text strings: GhostBalls, Product of Iceland Copyright (c) 1989, 4418 and 5F19 Bouncing ball on screen. COM files: "seconds" field of the timestamp changed to 62, as in the original Vienna virus. Infected files end in a block of 512 zero bytes. The string "GhostBalls, Product of Iceland" in the virus.		

Name: Gliss		
Aliases: Gliss	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Unknown, not analyzed yet.	**Size:** 1247	**See Also:**
Notes: Demonstration virus that announces its infections of programs.		

Name: Globe		
Aliases: Globe	**Type:** Program., DIET compressed	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 6610	**See Also:**
Notes:		

Name: Gosia

Aliases: Gosia | **Type:** Program.

Disk Location: COM application. | **Features:** Direct acting.

Damage: No damage, only replicates. | **Size:** Effective length of virus: 466 bytes | **See Also:**

Notes: Polish virus, first isolated in Poland in April 1991. It's rather primitive with logic similar to
W13. It only infects COM files. Infected files are marked by putting 44 in second field in file time stamp.

Not resident, does not use any stealth techniques. In one run it infects only 1 file in the current directory. COM files are recognized the extension of the name. It infects files with the length in the range
100-63,000 bytes. Write protected diskettes generate a write protect error.

Signature is: 5681C64401b90300BF0001FCF3A45E8BD6 - virus-l, v4-255
The name of the virus (Polish girl's nickname) is taken from a string inside the virus: "I love Gosia" where "love" is replaced by the heart character

This virus does not seem to contain any destructive code.

Name: Got You

Aliases: Got You | **Type:** Program.

Disk Location: EXE application. | **Features:** Direct acting.

Damage: Unknown, not analyzed yet. | **Size:** 3052 | **See Also:**

Notes:

Name: Gotcha

Aliases: Gotcha, Gotcha-D, Gotcha-E | **Type:** Program.

Disk Location: COM application., EXE application. | **Features:** Memory resident; TSR.

Damage: Unknown, not analyzed yet. | **Size:** 879, 881, 906, 627 - Gotcha-D variant | **See Also:**

Notes: Contains the text,
GOTCHA!
Of Dutch origin probably (the comments are in Dutch, yes the virus came to the researcher with original source.)

Name: GRABBER

Aliases: GRABBER | **Type:** Trojan.

Disk Location: GRABBER.COM | **Features:** Memory resident; TSR.

Damage: Deletes or moves files. | **Size:** 2583 Size of GRABBER.COM | **See Also:**

Notes: This program is supposed to be SCREEN CAPTURE program that copies the screen to a .COM file to be later run from a DOS command line. As a TSR it will attempt to do a DISK WRITE to your hard drive when you do not want it to. It will wipe out whole Directories when doing a normal DOS command. One sysop who ran it lost all of his ROOT DIR including his SYSTEM files.

MS-DOS/PC-DOS Computer Viruses

Name: Green Caterpillar		
Aliases: Green Caterpillar, 1590, 1591, 1575, 15xx	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1575	**See Also:**
Notes: fairly widespread A green catapillar with a yellow head crawls across the screen, munching letters then shifting margins to the right.		

Name: Groove		
Aliases: Groove	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR., Polymorphic	
Damage: Corrupts a data file.	**Size:** Polymorphic: each infection different	**See Also:**
Notes: Appears to be a mutation engine product that attacks anti-virus products by attacking their data files. v6-084: disables MSAV (MS DOS 6.0 antivirus program), targets checksum databases of some other products too (incl CPAV), the user may notice that something has happened.		

Name: Grower		
Aliases: Grower	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage:	**Size:** 267+	**See Also:**
Notes: When it is run it infects all .COM programs in the current directory, with the length of the first one increasing by 268 bytes, the second by 269 bytes, the third by 270 and so on.		

Name: Grune		
Aliases: Grune	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.	**Features:** Encrypted, Direct acting.	
Damage: Unknown, not analyzed yet.	**Size:** 1241	**See Also:**
Notes: The virus contains the encrypted text: Arbeiten Sie jetzt wirklich umweltfreundlich ? Sie haben nun viel Zeit darüber nachzudenken ! Es grüsst Sie die "Grüne Partei der Schweiz" !		

Name: Guppy		
Aliases: Guppy	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Unknown, not analyzed yet.	**Size:**	**See Also:**
Notes: Only infects files that start with a JMP instruction.		

Name: Gyro		
Aliases: Gyro	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 512, Overlays application, no increase	**See Also:**
Notes:		

Name: Ha!		
Aliases: Ha!, Ha	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application., EXE application.	**Features:** Encrypted, Direct acting.	
Damage: Interferes with a running application.	**Size:** 1456	**See Also:**
Notes: Prints: ha! on the screen in large letters.		

Name: Haddock		
Aliases: Haddock	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 1355	**See Also:**
Notes:		

Name: Hafenstrasse		
Aliases: Hafenstrasse	**Type:** Program.	
Disk Location: EXE application.	**Features:** Direct acting.	
Damage: Unknown, not analyzed yet.	**Size:** 809 - 1641	**See Also:** Ambulance
Notes: Some variants are droppers for the Ambulance virus.		

Name: Haifa		
Aliases: Haifa	**Type:** Program., loads itself to 8000:0100 (address fixed)	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR., Polymorphic	
Damage: Trashes the hard disk., Corrupts a data file.	**Size:** 2350 - 2400, Polymorphic: each infection different	**See Also:**
Notes: This virus has no stealth capabilities and can be picked out quickly by using any directory listing program. Will not infect overlay, .BIN or .SYS files. couldn't get to spread on a 386 machine or when invoked on a floppy drive on any of 7 PCs. Prints out messages, and adds text to .DOC, .TXT, and .PAS files. Adds code to .ASM files that will overwrite the hard disk if assembled and run. When HAIFA infacts a file, it will set the minutes field of the time stamp to an even value (it clears the 0 but) and sets seconds field to 38; Unusual numbers of programs with seconds set to 38 are a possible indication of this virus.		

Name: Halloechen		
Aliases: Halloechen, Hello_1a, Hello, Halloechn	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application., Corrupts a data file.	**Size:** 2011	**See Also:**
Notes: The virus slows the system down, and corrupts keyboard-entries (pressing an "A" produces a "B"). Does not infect files older than a month. The virus contains the text strings: "Hallöchen !!!!!!, Here I'm.. ", and " Acrivate Level 1.. "		

Name: Happy		
Aliases: Happy	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 412	**See Also:**
Notes: The virus contains the text: Thank you for running the Happy virus. Warning !!! COM-files in current directory and C:\DOS might be infected !!!!		

Name: Happy Halloween		
Aliases: Happy Halloween	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 10,000	**See Also:**
Notes: Non resident, required minimum file size to infect, discovered Dec 1991 in British Columbia, CANADA File infects on exection, appears to seek out single file for infection of length greater than xxxx bytes. Infected files grow by 10,000 decimal bytes. Virus infects all files as if .exe - infected .com files will not execute properly. Virus may have at one time been compressed with LZEXE. Embedded string ("All Gone") indicates file deletion/destruction may occur on Oct 31 of any year after 1991 or Dec 25. COMMAND.COM infection will make floppy boot necessary. not found by common scanners. string: 6c6c6f7765656e55		

Name: Happy Monday		
Aliases: Happy Monday	**Type:** Companion program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Unknown, not analyzed yet.	**Size:** varies	**See Also:**
Notes: A series of badly written companion viruses.		

Name: Happy New Year		
Aliases: Happy New Year, Bulgarian, Nina-2	**Type:** Program.	
Disk Location: COM application., EXE application., COMMAND.COM.	**Features:** Direct acting.	
Damage: Unknown, not analyzed yet.	**Size:** 1600, Command.com is overwritten	**See Also:**
Notes: Older virus (from around 1989 or 1990), this one was the first with the ability to infect device drivers, although it wasn't so easy to force it to infect them. Contains the text: "Dear Nina, you make me write this virus; Happy new year! "		

Name: Harakiri		
Aliases: Harakiri	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 5488 Overwriting	**See Also:**
Notes: Appears to have been written in Compiled Basic		

Name: Hary Anto		
Aliases: Hary Anto	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 981	**See Also:**
Notes:		

Name: Hate		
Aliases: Hate, Klaeren	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application., EXE application.	**Features:** Encrypted, Direct acting., Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 974, 978 - 1000	**See Also:**
Notes: Because of an error, destroys programs larger than 4K bytes. The virus contains the encrypted string: "Klaeren Haß, Haß! " Note: Haß it "Hate" in German Named after a teacher in a school in Germany Slightly stealth, as it hides the date May NOT infect COMMAND.COM		

Name: Helloween		
Aliases: Helloween	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 1376, 1182	**See Also:**
Notes:		

Name: Hero		
Aliases: Hero, Hero-394	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 506, 394	**See Also:**
Notes: Buggy virus that usually damages files while infecting them.		

Name: Hey You		
Aliases: Hey You	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 928	**See Also:**
Notes: This virus contains the following text: Hey, YOU !!! Something's happening to you ! Guess what it is ?! HA HA HA HA ...		

Name: HH&H		
Aliases: HH&H, GMB, Gomb	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 4091	**See Also:**
Notes: Contains the text "HARD HIT & HEAVY HATE the HUMANS !!".		

Name: Hi		
Aliases: Hi	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage: No damage, only replicates.	**Size:** 460	**See Also:**
Notes: Contains the text "Hi"		

Name: Hide and Seek		
Aliases: Hide and Seek	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage:	**Size:** 709	**See Also:**
Notes: The virus displays the message: Hi! boy. Do you know 'hide-and-seek' ? Let's play with me!!.		

Name: Highlander		
Aliases: Highlander	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 477	**See Also:**
Notes:		

Name: Hitchcock		
Aliases: Hitchcock	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.	**Size:** 1247	**See Also:**
Notes: Plays a tune from the Hitchcock TV series		

Name: Horror		
Aliases: Horror	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application., EXE application.	**Features:** Encrypted, Direct acting.	
Damage: Unknown, not analyzed yet.	**Size:** 1112, 1137, 1182	**See Also:**
Notes:		

Name: Horse		
Aliases: Horse, Naughty Hacker	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:**	**See Also:**
Notes: A family of 8 viruses		

Name: Horse Boot virus		
Aliases: Horse Boot virus	**Type:** Boot sector.	
Disk Location: Hard disk boot sectors., Floppy disk boot sectors.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sector	**Size:** Overlays boot sector, no increase	**See Also:** Horse virus
Notes: Same author as the Horse virus.		

Name: Horse II		
Aliases: Horse II, 1160, 512	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application., EXE application., Program overlay files., COMMAND.COM	**Features:** Encrypted, Direct acting.	
Damage: Corrupts a program or overlay files., Overwrites sectors on the Hard Disk.	**Size:** 1160	**See Also:**
Notes: The Horse II virus is a 1160 byte memory resident, stealth virus. It infects .COM applications including command.com, .exe applications, and program overlay files. We don't kown what the damage mechanism is yet. Similar in name but not function to Horse Boot virus 9 variants of Horse viruses, sometimes identifies it as 512, which is wrong. Most found in some schools in Sofia.		

Name: Hungarian		
Aliases: Hungarian, Hungarian-473	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Attempts to format the disk.	**Size:** 482, 473	**See Also:**
Notes: Activates on Nov 7 and formats the hard disk. The 473 variant activates on June 13.		

Name: Hydra		
Aliases: Hydra	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: No damage, only replicates.	**Size:** 340-736	**See Also:**
Notes: A series of 8 viruses		

Name: Hymn		
Aliases: Hymn	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v5-101: The Murphy and Hymn viruses are considered to be from separate families, although they include sections of code from the Dark Avenger (Eddie) virus.		

Name: Icelandic		
Aliases: Icelandic, Disk Eating Virus, Disk Crunching Virus, One In Ten, Saratoga 2	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application., Corrupts a program or overlay files., Corrupts the file linkages or the FAT.	**Size:** 656 -671 Length MOD 16 will always be 0.	**See Also:**
Notes: Infects every 10th .EXE file run, and if the current drive is a hard disk larger than10M bytes, the virus will select one cluster and mark it as bad in the first copy of the FAT. Diskettes and 10M byte disks are not affected. File length increases. Decreasing usable hard disk space. Infected .EXF files end in 18 44 19 5F (hex). System: Byte at 0:37F contains FF (hex)		

Name: Icelandic II		
Aliases: Icelandic II, One In Ten, System Virus, 642	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application., Corrupts a program or overlay files.	**Size:** 632-647 Length MOD 16 will always be 0.	**See Also:**
Notes: Every tenth program run is checked, and if it is an uninfected .EXE file it will be infected. The virus modifies the MCBs in order to hide from detection. This virus is a version of the Icelandic-1 virus, modified so that it does not use INT 21 calls to DOS services. This is done to bypass monitoring programs. EXE Files: Infected files end in 18 44 19 5F (hex). System: Byte at 0:37F contains FF (hex)		

Name: Icelandic III		
Aliases: Icelandic III, December 24th	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application., Corrupts a program or overlay files.	**Size:** 848 - 863	**See Also:**
Notes: It infects one out of every ten .EXE files run. If an infected file is run on December 24th it will stop any other program run later, displaying the message "Gledileg jol"		

Name: Invader		
Aliases: Invader, Plastic Boot	**Type:** Boot sector.	
Disk Location: COM application., EXE application., Hard disk boot sector., Floppy disk boot sector.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sector, Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: A multipartite virus: infects both files and boot area once the virus has become installed in memory The V101 virus is a multipartite virus too.		

Name: Invol		
Aliases: Invol	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes:		

Name: Involuntary		
Aliases: Involuntary	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: Device Driver infector		

Name: INVOLVE		
Aliases: INVOLVE	**Type:**	
Disk Location:	**Features:**	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: maybe this virus doesn't exist - v5-193 changes the date on files it has infected.		

Name: Israeli Boot		
Aliases: Israeli Boot, Swap	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sector	**Size:** Overlays boot sector, no increase	**See Also:**
Notes: It infects floppy disk boot sectors and reverses the order of letters typed creating typographical errors.		

Name: Jeff		
Aliases: Jeff	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: non resident com infector		

Name: Jerusalem		
Aliases: Jerusalem, Jerusalem A, Black Hole, Blackbox, 1808, 1813, Israeli, Hebrew University, Black Friday, Friday 13th, PLO, Russian, Kylie (variant), Scott's Valley, Mule, Slow,Timor	**Type:** Program.	
Disk Location: COM application., EXE application., Program overlay files.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application., Corrupts a program or overlay files., Deletes or moves files.	**Size:** 1813 Change in size of .COM files, 1808-1823 .EXE files: length mod 16 is 0, Multiple infections of .EXE files are possible	**See Also:**
Notes: Spreads between executable files (.COM or .EXE). On Friday the 13th, it erases any file that is executed, and on other days a two line black rectangle will appear at the bottom of the screen. Once this virus installs itself (once an infected COM or EXE file is executed), any other COM or EXE file executed will become infected. Kylie is difficult to spread. Mule variant uses encryption. EXE files too large to run, odd screen behavior and general slowdown, works well on LANs 1. "MsDos" and "COMMAND.COM" in the Data area of the virus 2. "MsDos" are the last 5 bytes if the infected program is a .COM file.		

MS-DOS/PC-DOS Computer Viruses

Name: Jerusalem-B		
Aliases: Jerusalem-B, Jerusalem-C, Jerusalem-D, Jerusalem-DC, Jerusalem-E, Jerusalem-E2, New Jerusalem, Payday, Skism-1, Anarkia, Anarkia-B, A-204, Arab Star, Mendoza, Park ESS, Puerto	**Type:** Program.	
Disk Location: COM application., EXE application., Program overlay files.	**Features:** Direct acting.	
Damage:	**Size:** 1808	**See Also:**
Notes: Works well on LANs		

Name: Joe's Demise		
Aliases: Joe's Demise, Joes Demise	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program file.	**Size:** 1 K, a 10 byte COM file was increased to 1928 bytes	**See Also:**
Notes: file infector, infects both .COM and .EXE files. It does not seem to effect .SYS or overlay files. File size shows a 1K increase when infected but the time and date stamps do not change. Stealth technique used: It detaches itself from the infected files when they are run. Windows may not load We identified the following as a valid search string for the new virus: 5A 5B 07 1F C3 1E 52 2E		

Name: Joker		
Aliases: Joker, Jocker	**Type:** Program.	
Disk Location: EXE application., DBF files	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** Overlays application, length changes	**See Also:**
Notes: Joker is a non-resident .EXE infector. It may also infect .DBF files. It overwrites the attacked file with the virus code. It was discovered in Poland in 1989. It is a poor replicator, and is probably extinct. There are many strange strings at the beginning of the file that are printed on the screen. It may cause system hangs. Some of the strings are: "END OF WORKTIME. TURN SYSTEM OFF!", "Water detect in Co-processor.", "I am hungry! Insert HAMBURGER into drive A:" Strange messages. .EXE files change length. File length changes, strange messages delete files		

MS-DOS/PC-DOS Computer Viruses

Name: JOKER-01		
Aliases: JOKER-01, Joker-01 Joker 01, Joker 2	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files., Interferes with a running application.	**Size:** 29233 to 29372, 29233	**See Also:**
Notes: A resident .EXE and .COM infector. It does not infect COMMAND.COM. The infection is at the end of the file. .EXE files are converted to .COM file signatures with a small loader inserted at the beginning of the file. The display may clear and the system may hang with this virus in memory. Random letters may appear on the screen. The string "JOKER-01" is in the file. The infection method is similar to VACSINA. System hangs. Strange letters on screen. File lengths change. String "JOKER-01" found in file. Scan file for string "JOKER-01" Delete files		

Name: Joshi		
Aliases: Joshi, Happy Birthday Joshi	**Type:** Boot sector.	
Disk Location: Hard disk boot sectors., Floppy disk boot sectors.	**Features:**	
Damage: Infects Master BooT record	**Size:**	**See Also:**
Notes: A new variant seems to be able to intercept BIOS calls. Will infect a second physical hard drive if it is present. FDISK/MBR will only clean up the first physical hard drive. on Jan 5 will ask you to type "happy birthday joshi" and only after you type it you can continue maybe came from India Virus exists in the partition table on HD, on Floppies it resides in the boot sector and on an additionally formatted tract (number 40 or 80, depending on diskette size)		

Name: Justice		
Aliases: Justice	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Direct acting.	
Damage:	**Size:**	**See Also:**
Notes: Once found in the wild in Bulgaria		

Name: Kamikazi		
Aliases: Kamikazi	**Type:** Program.	
Disk Location: EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: Rare virus. Overwrites the beginning of an infected file Damages the first four bytes of an infected file		

Name: Kamp		
Aliases: Kamp, Telecom 1, Telecom 2, Kamp-3700, Kamp-3784, Holo	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes:		

MS-DOS/PC-DOS Computer Viruses

Name: Kennedy		
Aliases: Kennedy, 333, Dead Kennedy, Danish Tiny, Stigmata, Brenda	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts the file linkages or the FAT.	**Size:** 333, 163, 1000 (Stigmata Variant), 256 (Brenda Variant)	**See Also:**
Notes: When an infected file is run, it infects a single .COM file in the current directory. On June 6th, November18th and November 22nd it displays the message: Kennedy er d¢d - længe leve "The Dead Kennedys" The Brenda variant contains the text: (C) '92, Stingray/VIPER Luv, Brenda		

Name: Keypress		
Aliases: Keypress	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1232-1247 in .COM file., 1472-1487 in .EXE file.	**See Also:**
Notes: Every 10 minutes, the virus looks at INT 09h (keyboard interrupt) for 2 seconds; if a keystroke is recognized during this time, it is repeated depending on how long the key is pressed; it thus appears as a "bouncing key"		

Name: Leapfrog		
Aliases: Leapfrog, 516	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: Does not change the file entry point. (other viruses that are similar are Voronezh 1600 and Brainy) Leapfrog modifies the instruction the initial JMP points to (for COM files) v6-084: will not be noticed by the integrity checking of MSAV (DOS 6.0 antivirus)		

Name: Lehigh

Aliases: Lehigh, Lehigh-2, Lehigh-B

Type: Program.

Disk Location: COMMAND.COM

Features: Memory resident; TSR.

Damage: Corrupts a program or overlay files., Corrupts the file linkages or the FAT., Corrupts boot sector

Size: Overlays application, no increase, 555 bytes inserted in stack area of COMMAND.COM.

See Also:

Notes: Spreads between copies of COMMAND.COM. After spreading four or ten times, it overwrites critical parts of a disk with random data. Displaying junk on the screen. Alters the contents and the date of COMMAND.COM. Spread will be detected by any good modification detector.

Name: Leningrad

Aliases: Leningrad

Type:

Disk Location:

Features:

Damage: Corrupts a program or overlay files.

Size:

See Also:

Notes: A friday the 13th time bomb virus that may or may not format the disk

Name: Liberty

Aliases: Liberty, Liberty-B, Liberty-C

Type: Program., Encrypted/Stealth The virus actively hides.

Disk Location: COM application., EXE application., Program overlay files.

Features: Encrypted, Direct acting.

Damage: Corrupts a program or overlay files., Corrupts boot sector

Size: 2862 bytes

See Also:

Notes: Self-encrypting, not known if destructive
floppy boot infection occurs rather rarely and is possible on PC XTs only
Scanners don't seem to report an infection when tested against an infected floppy.
INT 1CH is used to trigger. When triggered, the virus changes all characters being sent/received via INT 14H, printer via INT 17H and displayed via INT 10H (AH=09 or AH=0AH) toomake a string "MAGIC!!" for 512 timer ticks (approx 28 secs). After 10th triggering the virus swaps the upper line of a screen for blinking yellow-on-red sign "M A G I C !!!" (won't work on monochromes) then passes cotrol to ROM Basic. PCs without ROM Basic will either hang or reboot.
On self-encrypting: only self-encryps small piece of code used to infect COM files. Also encrypts first 120 bytes of infected COM file but this is NOT SELF-encrypting

Name: Lisbon		
Aliases: Lisbon, Vienna, Vienna 656, VHP related (?)	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 648 bytes added to the end of the file.	**See Also:**
Notes: Vienna Virus strain. The time stamp of an infected file is changed: the seconds are set to 62 (= 2 * 1Fh). When infected file is executed, .COM-files in the current directory as well as in the directories in the DOS-PATH are extended by appending the viral code; no infection if the file size<10 or file size>64000 bytes. A selected .COM-file is infected by "random" IF (system seconds AND 58h) <> 0 ELSE damaged! A selected .COM-file is damaged permanently by overwriting the first five bytes by "@AIDS" Damaged applications Easy identification.: Last five bytes of file = "@AIDS" (Ascii) The time stamp of an infected file is changed: the seconds are set to 62 (= 2 * 1Fh). Replace damaged files.		

Name: LZ		
Aliases: LZ	**Type:** A Companion virus	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: This companion virus makes a copy of itself with .com extension, and duplicates the name of all .exe files so it gets run first. Non-resident virus. Looks in current directory for an exe file. makes com file with same name, finds one at a time. Only one version (scan 86) finds it, it had too many false alarms so they took it out. LZ is a valid compression utility, that was causing lots of false alarms. Look in directory, see .com file there that has same name. (com file may be hidden) This one was tough to find, McAfee version should NOT be detecting it (too many false alarms)		

Name: Macho		
Aliases: Macho, MachoSoft, 3555, 3551	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application., EXE application., COMMAND.COM.	**Features:** Encrypted, Direct acting.	
Damage: Corrupts a program or overlay files., Corrupts a data file.	**Size:** 3550-3560 bytes are appended on a paragraph boundary	**See Also:**
Notes: Spreads between .COM and .EXE files. It scans through data on the hard disk, changing the string "Microsoft" (in any mixture of upper and lower case) to "MACHOSOFT". If the environment variable "VIRUS=OFF" is set, the virus will not infect. Use this as a temporary protection. Microsoft changes to MACHOSOFT Search for the string: 50,51,56,BE,59,00,B9,26,08,90,D1,E9,8A,E1,8A,C1,33,06,14,00,31,04,46,46,E2,F2,5E,59		

MS-DOS/PC-DOS Computer Viruses

Name: Maltese Amoeba		
Aliases: Maltese Amoeba, Irish, Grain of Sand	**Type:** Program., Memory resident - TSR	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR., Polymorphic	
Damage: Overwrites MBR/prints msg on 11/1 & 3/15	**Size:** Variable, dur to variable length of encryption header, Polymorphic: each infection different	**See Also:**
Notes: widespread in Ireland& UK, a dangerous polymorphic multi-partite fast infector (virus-l, v5-006) On Nov 1 or March 15 it replaces MBR of hard drive and displays a message that says something like "Amoeba virus by Hacker Twins...Just wait for Amoeba 2". The message refers to he University of Malta. This virus was probably very aware (or wrote) the Casino virus, as when it initially infects, it checks for the existance of the Casino, and if its there, it takes over INT 21 from it (thereby eradicating Casino) and places itself there instead. Signature scans don't work for this virus, an algorithmic check is the best way to locate it. None until activation date, at which point much text (see below) gets printed to the screen and the computer hangs. Not many anti-viral programs as of March 6, 1992. Data Physician Plus! v3.0D		

Name: MAP		
Aliases: MAP, FAT EATER	**Type:** Trojan.	
Disk Location: MAP.???	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: This is another trojan horse written by the infamous "Dorn Stickel." Designed to display what TSR's are in memory and works on FAT and BOOT sector. FAT EATER		

Name: Marauder		
Aliases: Marauder	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes:		

Name: MATHKIDS		
Aliases: MATHKIDS, FIXIT	**Type:** Trojan.	
Disk Location: FIXIT.ARC	**Features:**	
Damage: Cracks/opens a BBS to nonprivileged users.	**Size:**	**See Also:**
Notes: This trojan is designed to crack a BBS system. It will attemp to copy the USERS file on a BBS to a file innocently called FIXIT.ARC, which the originator can later call in and download. Believed to be designed for PCBoard BBS's.		

Name: Merritt

Aliases: Merritt, Alameda, Yale, Golden Gate, 500 Virus, Mazatlan, Peking, Seoul, SF Virus

Type: Boot sector.

Disk Location: Floppy disk boot sector.

Features: Memory resident; TSR.

Damage: Corrupts boot sector, Corrupts the file linkages or the FAT.

Size: Overlays boot sector, no increase

See Also:

Notes: Track 39 sector 8 is used to save the original boot record, and any file there will be overwritten. Destroys the FAT after some length of time. It spreads when the Ctrl-Alt-Del sequence is used with an uninfected diskette in the boot drive. The Golden Gate variation will reformat drive C: after n infections. Infects Floppies Only. Spreads between floppy disks. Unbootable disks, destroyed files. 80286 systems crash. Compare boot sector of infected disk with a "real" system disk. If different: check track 39, sector 8; if this contains the real boot blocks. Execute a SYS command to reinstall real boot block and system file from a clean disk.

Name: Mexican Stoned

Aliases: Mexican Stoned, stoned variant

Type: Memory resident; TSR., Activates once at boot time.

Disk Location:

Features: Memory resident; TSR.

Damage: Corrupts boot sector

Size:

See Also:

Notes: Prints out "No votes por el pri"
which is spanish for "Don't vote for el Pri" (a political party)

Name: Michelangelo

Aliases: Michelangelo, Michaelangelo, Mich

Type: Boot sector.

Disk Location: Floppy disk boot sectors., Hard disk boot sectors., Hard disk partition tables.

Features: Memory resident; TSR.

Damage: Corrupts boot sector

Size: Overlays boot sector, no increase, Moves orig. boot sector elsewhere, Uses Interrupts INT 13 and INT 1A

See Also:

Notes: First identified in the summer of 1991. This virus is similar to the Stoned, but utilizing some different techniques, so it's not simply a Stoned variant. It works for any version of MS DOS.

Triggers: Bootup from an infected disk will infect. Usage of floppy a: drive (read, write, or format) will cause infection of that medium. Payload: on March 6 (Michaelangelo's birthday) this virus will destroy data by overwriting the medium the computer was booted from. Hard disks will have sectors 1-17 on heads 0-3 of all tracks, floppies: sectors 1-9 or 1-14 on both heads and all tracks depending on the FAT type will be overwritten.

When Stoned and Michaelangelo both infect a disk, problems occur because they both try to hide the partition table in the same place. March 6th (Michaelangelo's birthday) data destruction. (see above long description) Upon bootup from an infected floppy the virus will go memory resident and infect the partition table. Any INT13 is intercepted thereafter. Any floppy A: operation will infect the disk in drive A: provided the motor was off (this cuts excessive infection testing). Most anti-viral utilities, when resident, CHKDSK will return a "total bytes memory" value 2048 less than normal. for a 640k PC normal=655,360; with virus: 653,312 Most anti-viral untilities: also, boot from a clean disk and move the original sector to its proper location (sector 1 head 0 track 0); on some systems FAT copy 1 might be damaged, so an additional copy of FAT 2 ont FAT 1 might be necessary

MS-DOS/PC-DOS Computer Viruses

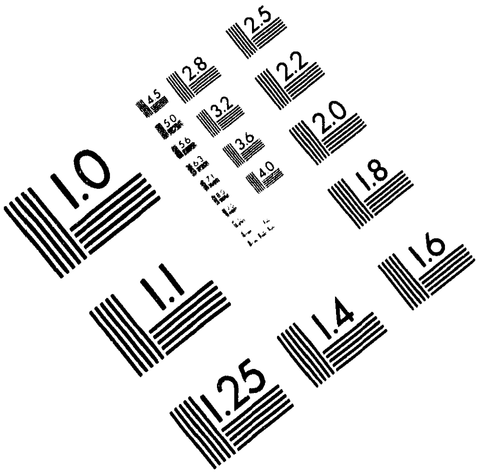
Name: Milena		
Aliases: Milena	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** increases by 1160	**See Also:**
Notes: Installs itself using standard Mem Alloc (DOS service 48) and INT 21 will be hooked by it. After becoming resident, and EXE or COM opened to create, open, chmod, load&exec, rename, or new file will be infected Opened TXT files will be overwritten at the end with the string "I Love Milena...". Infected files contain strings "LOVE" and "I Love Milena" A search string is 3D 21 25 74 0E 3D 21 35 74 15		

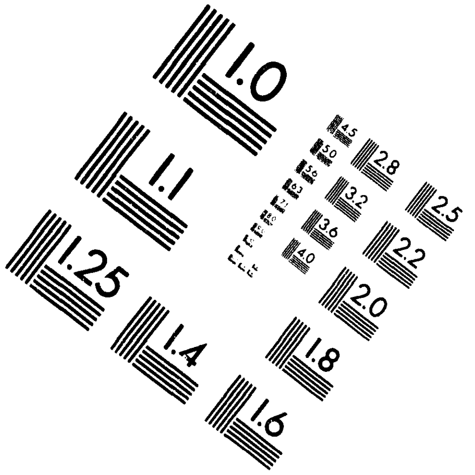
Name: minimal		
Aliases: minimal, minimal-45, 45	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 45 bytes!	**See Also:**
Notes: World's smallest virus. Only 45 bytes long. Non-resident program infoctor. No known damage. users of F-PROT can add the following line to SIGN.TXT to detect it. Minimal-45 dOT5v5ememVLstmMnMLdjSmmWtMpGfnBv2w7U7GFTBWdhvtgjLErsbwR71YJI1xfLd		

Name: Mirror		
Aliases: Mirror, Flip Clone	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application., Corrupts a program or overlay files.	**Size:** 925, 933	**See Also:**
Notes: When the virus is triggered, the screen will flip horizontally character for character.		

Name: Mix1		
Aliases: Mix1, MIX1, MIX/1, Mixer1	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application., Corrupts a program or overlay files.	**Size:** 1618-1634 length mod 16 equals 0	**See Also:**
Notes: The output is garbled on parallel and serial connections, after 6th level of infection booting the computer will crash the system (a bug), num-lock is constantly on, a ball will start bouncing on the screen. Garbled data from the serial or parallel ports. Bouncing ball on the screen. "MIX1" are the last 4 bytes of the infected file.		

Name: Moctzuma		
Aliases: Moctzuma, Moctzuma-B	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes:		



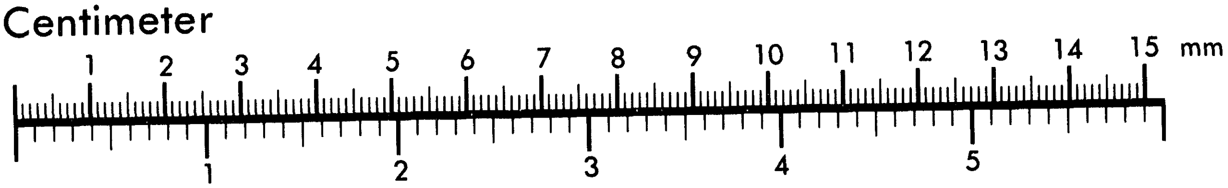


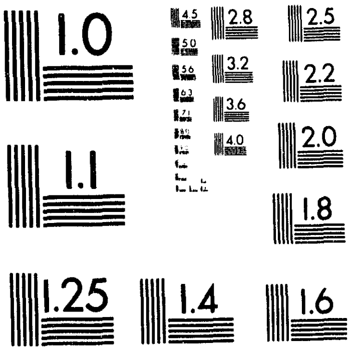
AIIM

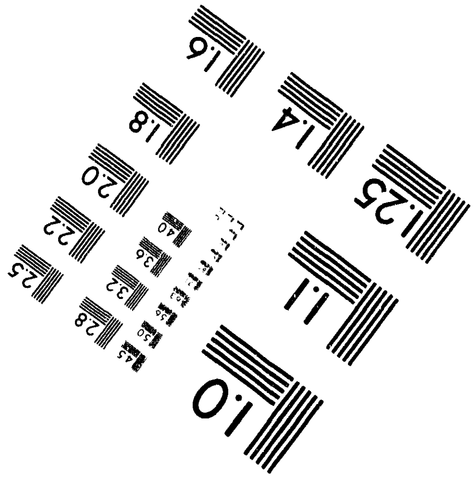
Association for Information and Image Management

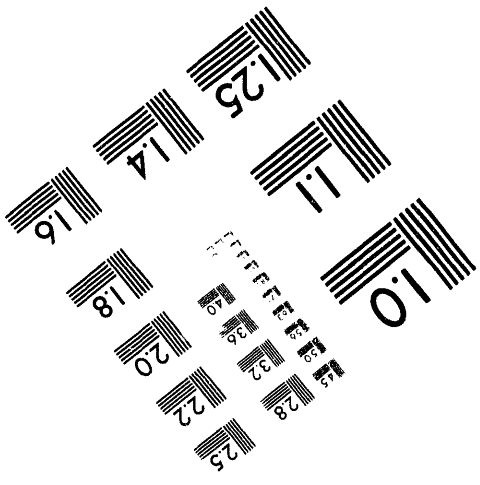
1100 Wayne Avenue, Suite 1100
Silver Spring, Maryland 20910

301/587-8202









MANUFACTURED TO AIIM STANDARDS
BY APPLIED IMAGE, INC.

2 of 2

MS-DOS/PC-DOS Computer Viruses

Name: Modem virus of 1989		
Aliases: Modem virus of 1989	**Type:** NONE, does not exist	
Disk Location:	**Features:**	
Damage: This virus is a myth!	**Size:**	**See Also:**
Notes: In December of 1989 there was a 'scare' about a modem virus being transmitted via a "sub-carrier" on 2400 bps modems. This is totally untrue, although reports of this mythical virus still occasionally occur. This information provided here to ensure that the myth goes no further.		

Name: Monkey		
Aliases: Monkey, Mon	**Type:** Boot sector.	
Disk Location: Hard disk boot sector.	**Features:** Stealth; actively hides from detection.	
Damage: Corrupts floppy disk boot sector, Corrupts hard disk boot sector, Corrupts boot sector	**Size:**	**See Also:** Int_10, Mon, Stoned.Empire.Monkey
Notes: Hides original partition table on cylinder 0, head 0, sector 3, and XOR's it with hex 2E (a "." character) SYS won't write a clean boot sector with Monkey, since it's a MBR infector. SYS works with floppies only Usually, most MBR viruses are removed with FDISK /MBR (dos 5.0 or up) but that doesn't work with Monkey because the Partition Table info in the MBR is not preserved. Program available (Nov 5, 1993) KillMonk v3.0 finds and removes the Monkey and Int_10 viruses. via ftp at ftp.srv.ualberta.ca, in the file pub/dos/virus/killmnk3.zip. The program claims it can also fix drives where the user has tried to use fdisk/mbr first. It's a very small virus, one sector, memory resident, MBR/stealth virus. it: 1. Tries to hide the virus infection - if you go to read the MBR, it redirects your inquiry and shows you the real MBR, not the virused one 2. Virus saves boot record, but masks it with character "2E" (which looks like a dot) and XOR's it, so to remove the virus you must un XOR (unmask) the real MBR. First version of Data Physician Plus! to find it is 3.1C 12/13/93: Karyn received one unconfirmed report that Data Physician Plus! 4.0B did not locate one variant of Monkey.		

Name: Monxla A		
Aliases: Monxla A, Monxla B, Time Virus, Vienna variant, VHP	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:**	**See Also:**
Notes: A virus with a time bomb: on the 13th of any month it damages the files it tries to infect on that day only. It is a Vienna variant, it infects only files in the current directory and in the directories inthe path variable. Also can be identified as Vienna [VHP] virus		

Name: Mummy		
Aliases: Mummy	**Type:**	
Disk Location: EXE application.	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: Infects .exe files only		

Name: Murphy HIV		
Aliases: Murphy HIV, AmiLia, Murphy variant	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** Overlays application, no increase	**See Also:**
Notes: FPROT 2.01 identifies it as Murphy HIV. A "fast file infector", it infects every file that is opened. No bounds have been found on the size of programs infected. The text string "AmiLia I Viri - [NukE] 1991" appears at the beginning of the infection. The text section also refers to "Released Dec91 Montreal". This indicates that the virus has spread extensively since its release. In vancouver, it appears toave been obtained in one instance from a BBS known as Abyss. Other indications that it has spread.		

Name: Murphy-1		
Aliases: Murphy-1, Murphy, V1277, April 15, Swami, Exterminator, Demon, Goblin, Patricia, Smack, Stupid Jack, Crackpot-272, Crackpot-1951	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.	**Size:** 1277	**See Also:**
Notes: Murphy is a program virus that appends itself to any COM or EXE file larger than 1277 bytes. COM files must be smaller than 64226 bytes, however if a COM file larger than 64003 is infected, it will not run. The virus also locates the original INT 13 handler and unhooks any other routines that have been hooked onto this interrupt and restores the interrupt to the original handler. It infects files on execution and opening. Between 10 and 11 AM, the speaker is turned on and off which produces a clicking noise. See Summary below for comments on some of the abovementioned aliases Between 10 and 11 AM, the speaker is turned on and off which produces a clicking noise. The virus contains the string: "Hello, I'm Murphy. Nice to meet you friend. I'm written since Nov/Dec. Copywrite (c)1989 by Lubo & Ian, Sofia, USM Laboratory."		

Name: Murphy-2		
Aliases: Murphy-2, Murphy, V1521	**Type:** Program.	
Disk Location: COM application., EXE application., COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.	**Size:** 1521	**See Also:**
Notes: A variant of Murphy-1, Murphy-2 is a program virus that appends itself to any COM or EXE file larger than 1521 bytes. COM files must be smaller than 63982 bytes. The virus also locates the original INT 13 handler and unhooks any other routinesthat have been hooked onto this interruptand restores the interrupt to the original handler. Files are infected on execution and opening. Between 10 and 11 AM a ball (character 07) bounces over the screen. Between 10 and 11 AM a ball (character 07) bounces over the screen. The virus contains the string: "It's me - Murphy. Copywrite (c)1989 by Lubo & Ian, Sofia, USM Laboratory."		

Name: Mutation Engine		
Aliases: Mutation Engine, Dark Avenger's Latest, Pogue, MtE, Sara, Sarah, Dedicated, Fear, Cryptlab, Groove, Questo, CoffeeShop, DAME (Dark Avenger Mutation Engine)	**Type:** Program., Virus Authoring Package	
Disk Location: COM application.	**Features:** Encrypted, Direct acting., Polymorphic	
Damage: Corrupts a program or overlay files.	**Size:** could be any size, Polymorphic: each infection different	**See Also:**
Notes: The MtE is a mutatuon engine that makes an existing virus difficult to detect by changing a virus with each infection. The first is the demo virus in the package (a silly, non-resident, COM file infector, infects only the files in the current directory) and a virus, called Pogue, wihch has been available on some VX BBSes in the USA. See notes below about the mutating engine. 11/2/92 virus-l, v5-186: announcement of MtE test reports, can be found via anonymous ftp from ftp.informatik.uni-hamburg.de:pub/virus/texts/tests/mtetests.zip and cert.org:pub/virus-l/docs/mtetests.zip none yet, but anti-virus researchers have it and are working hard -2/14/92		

Name: Net Crasher		
Aliases: Net Crasher	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:** Vienna
Notes:		

Name: NMAN		
Aliases: NMAN, NMAN B, NMAN C, C virus, Nowhere Man	**Type:** Program.	
Disk Location: EXE application., COM application.	**Features:** Direct acting., Not memory resident	
Damage: Corrupts a program or overlay files., Attempts to format the disk.	**Size:**	**See Also:**
Notes: Can get false positives because this virus was written in C and you might get the compiler to hit. Not memory resident, this virus is non-removable because it overwrites part of the infected file with itself, making recovery impossible. Mostly infects EXE files, although .COM files can be infected, the infection mechanism treats .COM files as .EXE files. NMAN B writes out a message, where NMAN does not. NMAN B also is nastier to the hard disk, and can erase the disk, but it is not certain if the erasure is intentional or not. It appears that this virus was written with the Borland Turbo C++ compiler, that's why this virus is sometimes called "C virus". Virus sample examined had a date of 9/24/91, so virus is at least that old.		

Name: Nomenklatura		
Aliases: Nomenklatura, 1024-B,	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:** Diamond
Notes: Diamond is a relative of this virus		

Name: NOTROJ		
Aliases: NOTROJ	**Type:** Trojan.	
Disk Location: NOTROJ.???	**Features:**	
Damage: Corrupts the file linkages or the FAT., Attempts to format the disk.	**Size:**	**See Also:**
Notes: All outward appearances indicate that the program is a useful utility used to FIGHT other trojan horses. Actually, it is a time bomb that erases any hard disk FAT table that IT can find on hard drives that are more than 50% full, and at the same time, it warns: "another program is attempting a format, can't abort! After erasing the FAT(s), NOTROJ then proceeds to start a low level format. Delete the NOTROJ.COM Application.		

Name: Novell		
Aliases: Novell, Jerusalem variant	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage: Deletes or moves files.	**Size:** 1806-1816	**See Also:**
Notes: This virus can infect Novell lans and defeat LAN privilages. It behaves like the Jerusalem B virus in stand alone mode, loads a TSR and hooks init 21. In a networked system it hooks init 21 and 8. Once in memory, it infects files when they are run. The virus infects NetWare 2.15C servers from infected nodes, dos server writing without write privileges, server deleting without delete privileges. Server deletion can be done from nodes with just ROS privileges (i.e. neither modify flags or write). On Friday the 13th, the program deletes any executed program instead of infecting it, even from nodew with no delete privilages on the server. Files increase by a little over 1800 bytes. Date and time stamps change on files on a server, even when the node does not have the modify privilage. "sUMsDos" string in executable file. Standard detectors will probably see it, it looks like Jeruseleam-B, "sUMsDos" string in virus. Standard eradicators that can fix Jeruseleam B, though you should replace .exe and .com files.		

Name: November 17		
Aliases: November 17, 855, Nov 17, Nov. 17, Nov 17-768, Nov 17-880, Nov 17-B, Nov 17-800, (not really) Simplistic File Infector	**Type:** Program.	
Disk Location: COM application., EXE application., COMMAND.COM.	**Features:** Memory resident; TSR above TOM.	
Damage: Erases the Hard Disk.	**Size:** 855, 786, 880, 928, 800	**See Also:**
Notes: The Nov. 17 virus is a memory resident virus that adds 855 bytes to .COM and .EXE files. It was discovered Dec, 1991 in Italy. On Nov. 17 it activates and trashes the hard disk. May target the McAfee programs SCAN and CLEAN to not infect those programs Use a scanner such as FPROT, ViruScan, IBM Scan, Novi, CPAV, NAV 2.1+, Vi-Spy, AllSafe, ViruSafe, Sweep, AVTK, VBuster, Trend, Iris, VNet, Panda, UTScan, IBMAV, NShld, Delete the file or repair with a scanner. Someone once (11/18/93) referred to this virus as "Simplistic File Infector" virus, but that is not a recognized alias for this virus.		

Name: November 30		
Aliases: November 30, Jerusalem variant	**Type:** same as Jerusalem	
Disk Location:	**Features:**	
Damage: same as Jerusalem	**Size:**	**See Also:**
Notes: a variant of Jerusalem with a trigger date of November 30, discovered in January 1992 Could be same virus found early last summer in Korea. (source: virus-l, v5-069)		

Name: Number of the Beast		
Aliases: Number of the Beast, Beast C, Beast D	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: Beast: 13 variants, all of them detected (inapproiately) as 512 by SCAN 97, some of the variants are not very widely spread in Bulgaria. Variants: Beast B, C, D, E , F, and X SCAN 97 still says that "number of the beast" is the 512 virus (erroneously)		

Name: Ohio		
Aliases: Ohio, Den-Zuk 2, Den Zuk 2	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sector	**Size:** Overlays boot sector, no increase	**See Also:**
Notes:		

Name: Omega		
Aliases: Omega	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: A friday the 13th time bomb virus		

Name: Ontario		
Aliases: Ontario	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different, It toggles one bit only	**See Also:**
Notes:		

Name: Oropax		
Aliases: Oropax, Music, Musician	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application., Corrupts a program or overlay files.	**Size:** 2756 -2806 Increase is divisible by 51	**See Also:**
Notes: Infects .COM files. After 5 minutes, the virus will start to play three melodies repeatly with a 7 minute interval in between. This can only be stopped with a reset. After 5 minutes, the virus will start to play three melodies repeatly with a 7 minute interval in between. This can only be stopped with a reset. Typical texts in Virus body (readable with HexDump facilities): "???????COM" and "COMMAND.COM"		

Name: Oulu		
Aliases: Oulu, 1008, Suomi	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Direct acting., Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes: Not very widespread in Finland		

Name: PACKDIR		
Aliases: PACKDIR	**Type:** Trojan.	
Disk Location: PACKDIR.???	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: This utility is supposed to "pack" (sort and optimize) the files on a [hard] disk, but apparently it scrambles FAT tables. (Possibly a bug rather than a deliberate trojan?? w.j.o.)		

Name: Paris		
Aliases: Paris, France	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Direct acting.	
Damage:	**Size:**	**See Also:**
Notes:		

Name: PC Flu 2		
Aliases: PC Flu 2	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes:		

Name: PCW271		
Aliases: PCW271, PC-WRITE 2.71	**Type:** Trojan.	
Disk Location: PCW271.???	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:** 98274 Size of bogus PC-WRITE normal is 98644 bytes.	**See Also:**
Notes: A modified version of the popular PC-WRITE word processor (v. 2.71) that scrambles FAT tables. The bogus version of PC-WRITE version 2.71can be identified by its size; it uses 98,274 bytes whereas the good version uses 98,644.		

Name: Pentagon		
Aliases: Pentagon	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sector	**Size:** Overlays boot sector, no increase	**See Also:**
Notes: It infects floppy disk boot sectors, and removes the Brain virus from any disk it finds. The virus can survive a warmboot. It appears that no anti-viral researchers can get this virus to replicate.		

Name: Perfume		
Aliases: Perfume, 765, 4711	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files., Interferes with a running application.	**Size:** 765	**See Also:**
Notes: It infects .COM files, and after 80 executions, it demands a password to run the application. The password is 4711 (the name of a perfume). A password request for a program that does not need one, or the printing of code on the screen when a program is run, much like using the DOS TYPE command with an excutable file. One version contains the following strings: "G-VIRUS V2.0",0Ah,0Dh, "Bitte gebe den G-Virus Code ein : $" <CRLF> 0Ah,0Dh,"Tut mir Leid !",0Ah,0Dh,"$"; (translated 2nd and 3rd strings: "please input G-virus code"; "sorry") Another version has a block of 88(dec) bytes containing 00h.		

Name: Phoenix		
Aliases: Phoenix, P1	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application., COMMAND.COM.	**Features:** Memory resident; TSR above TOM., Encrypted, Polymorphic	
Damage:	**Size:** 1704 All .COM files but COMMAND.COM, It overlays part of COMMAND.COM, Multiple infections are possible., Polymorphic: each infection different	**See Also:**
Notes: The Phoenix virus is of Bulgarian origin. This virus is one of a family of three (3) viruses which may be referred to as the P1 or Phoenix Family. The Phoenix virus is a memory resident, generic infector of .COM files, and will infect COMMAND.COM. Phoenix infects COMMAND.COM by overwriting part of the binary zero portion of the program, and changing the program's header information. COMMAND.COM will not change in file length. Phoenix is not able to recognize when it has previously infected a file, so it may reinfect .COM files several times. Each infection of a .COM file will result in another 1,704 bytes of viral code being appended to the file. Systems infected with the Phoenix virus will experience problems with executing CHKDSK.COM. Attempts to execute this program with Phoenix memory resident will result in a warm reboot of the system occurring, however the memory resident version of Phoenix will not survive the reboot. The Phoenix Virus employs a complex encryption mechanism, and virus scanners which are only able to look for simple hex strings will not be able to detect it. There is no simple hex string in this virus that is common to all infected samples. Also see: PhoenixD, V1701New A warmboot occurs when CHKDSK.COM is run. ViruScan V66+ Scan/D, or delete infected files		

Name: Phoenix D		
Aliases: Phoenix D, P1	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application., COMMAND.COM.	**Features:** Memory resident; TSR above TOM., Encrypted, Polymorphic	
Damage:	**Size:** 1704 All .COM files but COMMAND.COM, It overlays part of COMMAND.COM, Multiple infections are possible., Polymorphic: each infection different	**See Also:**
Notes: The Phoenix-D virus is of Bulgarian origin, and is a bug fixed version of Phoenix. This virus is one of a family of three (3) viruses which may be referred to as the P1 or Phoenix Family. The Phoenix virus is a memory resident, generic infector of .COM files, and will infect COMMAND.COM. Phoenix infects COMMAND.COM by overwriting part of the binary zero portion of the program, and changing the program's header information. COMMAND.COM will not change in file length. Phoenix is not able to recognize when it has previously infected a file, so it may reinfect .COM files several times. Each infection of a .COM file will result in another 1,704 bytes of viral code being appended to the file. Systems infected with the Phoenix virus will experience problems with executing CHKDSK.COM. Attempts to execute this program with Phoenix memory resident will result in a warm reboot of the system occurring, however the memory resident version of Phoenix will not survive the reboot. The Phoenix Virus employs a complex encryption mechanism, and virus scanners which are only able to look for simple hex strings will not be able to detect it. There is no simple hex string in this virus that is common to all infected samples. Also see: Phoenix, V1701New A warmboot occurs when CHKDSK.COM is run. ViruScan V66+ Scan/D, or delete infected files		

Name: Ping Pong		
Aliases: Ping Pong, Bouncing Ball, Italian, Bouncing Dot, Vera Cruz, Turin Virus	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector., Hard disk boot sector.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application., Corrupts boot sector	**Size:** Overlays boot sector, no increase	**See Also:**
Notes: Bouncing dot appears on screen. No other intentional damage. Spreads between disks by infecting the boot sectors. The bootsector contains at the offset 01FCh the word 1357h. Enter TIME 0, then immediately press any key and Enter; if the virus is present, the bouncing dot will be triggered		

Name: Ping Pong B		
Aliases: Ping Pong B, Boot, Falling Letters	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector., Hard disk boot sector.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application., Corrupts boot sector	**Size:** Overlays boot sector, no increase	**See Also:**
Notes: Bouncing dot appears on screen. No other intentional damage. Spreads between disks by infecting the boot sectors.		

Name: PKFIX361		
Aliases: PKFIX361	**Type:** Trojan.	
Disk Location: PKFIX361.EXE	**Features:**	
Damage: Attempts to format the disk.	**Size:**	**See Also:**
Notes: PKFIX361.EXE *TROJAN* Supposed patch to v3.61 - what it really does is when extracted from the .EXE does a DIRECT access to the DRIVE CONTROLLER and does Low-Level format. Thereby bypassing checking programs. (This would be only XT type disk drive cards. w.j.o.)		

Name: PKPAK/PKUNPAK 3.61		
Aliases: PKPAK/PKUNPAK 3.61, PK362, PK363	**Type:** Trojan.	
Disk Location: PK362.EXE, PK363.EXE, PKPAK/PKUNPAK v. 3.61	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: PKPAK/PKUNPAK *TROJAN* There is a TAMPERED version of 3.61 that when used interfers with PC's interupts. PK362.EXE This is a NON-RELEASED version and is suspected as being a *TROJAN* - not verified. PK363.EXE This is a NON-RELEASED version and is suspected as being a *TROJAN* - not verified.		

Name: PKX35B35		
Aliases: PKX35B35, PKB35B35	**Type:** Trojan.	
Disk Location: PKX35B35.ARC, PKB35B35.ARC	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: PKX35B35.ARC, PKB35B35.ARC This was supposed to be an update to PKARC file compress utility - which when used *EATS your FATS* and is or at least RUMORED to infect other files so it can spread - possible VIRUS?		

Name: PKZIP Trojan 1		
Aliases: PKZIP Trojan 1, ZIP Trojan, PKZ201.ZIP, PKZ201.EXE	**Type:** Program; activates when run.	
Disk Location: PKZ201.ZIP, PKZ201.EXE	**Features:** Direct acting.	
Damage: Alpha level software, anything is possible.	**Size:**	**See Also:** PKZIP Trojan 2
Notes: The PKZIP trojan 1 is PKZIP version 1.93 Alpha renamed as PKZIP version 2.01. The only danger, is that this is alpha level software, and may have bugs in it. There will never be a version of PKZIP numbered 2.01 though there may be a version 2.0 in the near future (6/92). The program has been found in the files PKZ201.ZIP, PKZ201.EXE and has been uploaded to several BBSs. Contact PKWARE if you see it. Voice at 414-354-8699, BBS at 414-354-8670, FAX at 414-354-8559 PKWARE Inc., 9025 N. Deerwood Drive, Brown Deer, WI 53223 USA See also PKZIP Trojan 2 Check the version number using PKUNZIP with the -l option to list the contents of the archive. If it is version 2.01 then delete it. Delete the file.		

Name: PKZIP Trojan 2		
Aliases: PKZIP Trojan 2, PKZIPV2.ZIP, PKZIPV2.EXE, ZIP Trojan	**Type:** Trojan.	
Disk Location: PKZIPV2.ZIP, PKZIPV2.EXE	**Features:**	
Damage: Erases the Hard Disk.	**Size:** The files are short, only a few lines of text.	**See Also:** PKZIP Trojan 1
Notes: The PKZIP trojan is a program masquareding as PKZIP version 2.2. It is actually just a short command file containing DEL C:\DOS\*.*, and DEL C:\*.* . When run, it attempts to erase the contents of the C:\DOS directory and the c:\ directory. There will never be a version of PKZIP numbered 2.2 though there may be a version 2.0 in the near future (6/92). The Trojan has been found in the files PKZIPV2.ZIP, PKZIPV2.EXE and has been uploaded to several BBSs. If you have had files deleted by this Trojan, you may be able to recover them with an unerase utility such as those supplied with Norton Utilities or PCTools. Contact PKWARE if you see it. Voice at 414-354-8699, BBS at 414-354-8670, FAX at 414-354-8559 PKWARE Inc., 9025 N. Deerwood Drive, Brown Deer, WI 53223 USA See also PKZIP Trojan 1 Your hard disk is erased. Type the file to see if it is a command file instead of an executable. The command file will contain instructions to delete files on the hard disk. Delete the file.		

Name: Plague		
Aliases: Plague	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: claim that it was created by either someone in Brisbane Austrailia, or USA. (virus-l, v5-189)		

Name: Plastique		
Aliases: Plastique, 3012, HM2, Plastique 1, Plastique 4.51	**Type:** Boot sector.	
Disk Location: COM application., EXE application., Hard disk boot sectors.	**Features:** Memory resident; TSR.	
Damage:	**Size:**	**See Also:**
Notes: Most variants play a melody, if you press Ctrl-Alt-del while melody is being played, it overwrites the beginning of the hard disk.		

Name: Plovdiv		
Aliases: Plovdiv, Plovdiv 1.1, Plovdiv 1.3, Damage 1.1, Damage 1.3, Bulgarian Damage 1.3	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR above TOM.	
Damage: Corrupts a program or overlay files., Attempts to format the disk.	**Size:** Overlays application, no increase1000 bytes in files, 1328 bytes in memory	**See Also:**
Notes: The virus identifies infection by the seconds field in file time. It allocates a memory block at high end of memory, 1344 bytes long Programs are infected at load time (using the functionload/execute of MS-DOS) and whenever a file is opened with the extension of .COM or .EXE The virus carries an evolution counter that is decreased every time the virus is executed. At 0, virus reads system timer, if the value of hundreds > 50 virus will format all available tracks on current drive (effectively 50% chance of destruction) The virus knocks out the transient part of COMMAND.COM forcing it to be reloaded and thereby infected, therefore it is a "fast infector" contains string "(c)Damage inc. Ver 1.3 1991 Plovdiv S.A."		

Name: Pogue		
Aliases: Pogue	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR., Polymorphic	
Damage: Unknown, not analyzed yet.	**Size:** Polymorphic: each infection different	**See Also:**
Notes: A variant of Gotcha that uses the MtE mutation engine.		

Name: Possessed		
Aliases: Possessed, Possessed A, Possessed B, Demon	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files., Deletes or moves files.	**Size:**	**See Also:**
Notes: Displays a low resolution picture of a demon on the screen with the words "Your computer is now Possessed" under it. Can delete files This virus has been falsely identified within one of the files on the DayStar Digital LT200 PC LocalTalk software disk (file DNET2.COM) by an older version of McAfee's SCAN82. If a "positive" reading is done on this file, please confirm by using a newer version of the software, or another scanning package.(virus-l, V4-214) standard detection/eradication packages		

Name: Proud		
Aliases: Proud, V1302, Phoenix related	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes:		

Name: QUIKRBBS		
Aliases: QUIKRBBS	**Type:** Trojan.	
Disk Location: QUIKRBBS.???	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: This Trojan horse advertises that it will install program to protect your RBBS but it does not. It goes and eats away at the FAT.		

Name: QUIKREF		
Aliases: QUIKREF	**Type:** Trojan.	
Disk Location: ARC513.COM	**Features:**	
Damage: Cracks/opens a BBS to nonprivileged users.	**Size:**	**See Also:**
Notes: This ARChive contains ARC513.COM. Loads RBBS-PC's message file into memory two times faster than normal. What it really does is copy RBBS-PC.DEF into an ASCII file named HISCORES.DAT.		

Name: RAM		
Aliases: RAM	**Type:** Program; activates when run.	
Disk Location:	**Features:** Direct acting.	
Damage:	**Size:**	**See Also:**
Notes: v6-081: There is no such thing as the RAM virus. Somebody gave Patty [Hoffman] a sample which was infected with two viruses - Cascade and Jerusalem, I think. This combination works perfectly together, but she did not realize the nature of the sample, and seemed to think this was one new virus. There are some other non-existing viruses in VSUM as well, but they are mostly for "copy protection" purposes.... - -frisk		

Name: RCKVIDEO		
Aliases: RCKVIDEO	**Type:** Trojan.	
Disk Location: RCKVIDEO.???	**Features:**	
Damage: Attempts to erase all mounted disks.	**Size:**	**See Also:**
Notes: After showing some simple animation of a rock star, the program erases every file it can find. After about a minute of this, it creates three ascii files that say "You are stupid to download a video about rock stars".		

MS-DOS/PC-DOS Computer Viruses

Name: Relzfu		
Aliases: Relzfu	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: A friday the 13th time bomb virus		

Name: RPVS		
Aliases: RPVS, 453, RPVS-B, TUQ	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files., Interferes with a running application.	**Size:** 453	**See Also:**
Notes: Whenever an infected application is run, at least one other .COM file in the default directory is infected.		

Name: Russian Mutant		
Aliases: Russian Mutant, 914	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes:		

Name: Saddam		
Aliases: Saddam, stupid	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 917-924	**See Also:**
Notes: This appears to be a variant of the Stupid virus. On every eigth infection, the string: "HEY SADAM"{LF}{CR} "LEAVE QUEIT BEFORE I COME" is displayed. The virus copies itself to [0:413]*40h-867h, which means that onl; computers with 640KB can be infected. Many large programs also load themselves to this area and erase the virus from the memory, or hang the system.		

Name: Saratoga		
Aliases: Saratoga, 632, Disk Eating Virus, One In Two	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application., Corrupts a program or overlay files., Corrupts the file linkages or the FAT.	**Size:** 642 to 657 Length MOD 16 will always be 0.	**See Also:**
Notes: Infects every 10th .EXE file run, and if the current drive is a hard disk larger than10M bytes, the virus will select one cluster and mark it as bad in the first copy of the FAT. Diskettes and 10M byte disks are not affected. Disk space on hard drives shrinking. .EXE files increasing in length. EXE Files: Infected files end in "PooT". System: Byte at 0:37F contains FF (hex)		

Name: Satan Bug

Aliases: Satan Bug | **Type:** Program.

Disk Location: EXE application., COM application., COMMAND.COM, Program overlay files.?, SYS System files.?

Features: Memory resident; TSR., Encrypted

Damage: Corrupts a program or overlay files.

Size: Polymorphic: each infection different, Files increase 2.9K to 5K

See Also:

Notes: The virus is a memory resident, non-stealth, encrypted, mutating, polymorphic virus that infects .COM, .EXE, .SYS, and .OVL files.
It hooks the file open and file execute commands and infects programs when they are opened or executed.

If Satan Bug is not already in memory, and if COMSPEC is not the first item in the environment (SET) the virus will not load into memory. If the virus is already in memory, this has no effect. If command.com is infected there is no way to make comspec last without having the virus load first. This appears to be how the virus writer protected his own system.
To move comspec from the first position, use something like the following at the beginning of your autoexec.bat file:

```
SET TEMP=C:\DOS
SET COMSPEC=C:\COMMAND.COM
```

This puts comspec into the second position. Note that if you redefine TEMP, comspec will move back into the first position.
The virus addes 100 years to the file's creation date. It probably uses this to check for an infection. You can't see this change with the DIR command, but must use a special utility. NAVCERT created the program CHKDATE to look for this change in the date.
Since the program infects .SYS files, network drivers tend to break after infection, making networks inaccessible. Note that I have not been able to get it to infect a .sys file, but it does infect emm386.exe which is usually installed high and could force the other drivers out.
Do not run an infected virus scanner on a disk, as it will then infect the whole disk.
Encrypted in the file is the text:

SATAN BUG virus - Little Loc

Locate with: DataPhysician Plus 4.0B, Scan V106, Norton AntiVirus 2.1 with August 1993 virus definitions.
Scan v106-109 do not see all infected files.

Name: SBC

Aliases: SBC, SBC-1024 | **Type:** Program.

Disk Location: COM application., EXE application., Program overlay files.

Features: Memory resident; TSR., Polymorphic

Damage: Corrupts a program or overlay files.

Size: 1024, min length of infectable files is 1536 bytes, Polymorphic: each infection different

See Also:

Notes: Fairly new as of Jan 1992, an encrypted, but not polymorphic virus, memory resident, uses
INT 21h/AX=4BFFh to detect its presence in memory, fast infector (infects both when copy and execute files)
.EXE files are padded up to the next multiple of 16 before they are infected.
Nothing obviously intentionally destructive in the virus code

Name: Scrambler		
Aliases: Scrambler, KEYBGR Trojan	**Type:** Trojan.	
Disk Location: KEYBGR.COM	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.	**Size:**	**See Also:**
Notes: About 60 minutes after the trojan KEYBGR.COM is started a smiley face moves in a random fashion about the screen displacing characters as it moves. The Trojan contains many copies of the string "nothing".		

Name: Screaming Fist .		
Aliases: Screaming Fist	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes: Rumor: Written by the group PHALCON/SKISM (like Bob Ross, aka Beta virus) Some debate whether it is polymorphic or not		

Name: SECRET		
Aliases: SECRET	**Type:** Trojan.	
Disk Location: SECRET.???	**Features:**	
Damage: Attempts to format the disk.	**Size:**	**See Also:**
Notes: BEWARE!! This may be posted with a note saying it doesn't seem to work, and would someone please try it; when you do, it formats your disks.		

Name: SECURE.COM		
Aliases: SECURE.COM	**Type:** Rumored virus, just password guesser	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: virus rumor in comp.sys.novell in July 1991. Inquiry in virus-l v4-128. From virus-l: There has been some discussion in comp.sys.novell about a new "virus" called SECURE.COM which opens up and damages netware binderies. No-one has seen it themselves yet, everyone has heard about it, so it may be another "urban legend". It is likely that if it does exist someone in this group will have heard of it, or be CERTAIN that it does not exist. It is a password guessing program		

Name: Sentinel		
Aliases: Sentinel	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: written in Pascal, created in Bulgaria		

Name: SIDEWAYS		
Aliases: SIDEWAYS, SIDEWAYS.COM	**Type:** Trojan.	
Disk Location: SIDEWAYS.COM	**Features:**	
Damage: Corrupts boot sector	**Size:** 3 KB SIDEWAYS.COM, 30 KB The legitimate SIDEWAYS.EXE application.	**See Also:**
Notes: Both the trojan and the good version of SIDEWAYS advertise that they can print sideways, but SIDEWAYS.COM trashes a [hard] disk's boot sector instead.		

Name: Simulation		
Aliases: Simulation	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes:		

Name: Slovakia		
Aliases: Slovakia	**Type:** Program.	
Disk Location: EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: Only activity is infecting files, sometimes displaying a message. Infects in current directory or path. Non-resident. Infected files get increased by 2000-2200 bytes. Last four bit of length are set to 1101binary. Virus remains inactive in infected program 10 days or til the end of the month. It's an encrypted virus. Decryption code has 8 mutations. On Monday, Wed, or Friday after March 1992, message displayed: "SLOVAKIA virus version 3.00 (c) 1991-1992 by??. All Rights Reserved. Greeting from Bratislava, SLOVAKIA.Type the word SLOVAKIA: ...."		

Name: STAR		
Aliases: STAR, STRIPES	**Type:** Trojan.	
Disk Location: STAR.EXE, STRIPES.EXE	**Features:**	
Damage: Cracks/opens a BBS to nonprivileged users.	**Size:**	**See Also:**
Notes: STAR.EXE Beware RBBS-PC SysOps! This file puts some stars on the screen while copying RBBS-PC.DEF to another name that can be downloaded later! STRIPES.EXE Similar to STAR.EXE, this one draws an American flag (nice touch), while it's busy copying your RBBS-PC.DEF to another file (STRIPES.BQS).		

Name: Stardot		
Aliases: Stardot, 805, V-801	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes:		

Name: Starship		
Aliases: Starship	**Type:** Stealth virus	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: Russian origin virus, infects device drivers (see also SVC 6.0 virus) Hard to get to replicate, but it will if you try hard enough can infect when copying files on diskettes, but is quite buggy		

Name: Stinkfoot		
Aliases: Stinkfoot, Paul Ducklin, Ducklin	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** Overlays application, no increase adds either 1254 bytes or 1273 bytes	**See Also:**
Notes: written (poorly) in assembler, found in South Africa virus tries to adjust INT 24h (Critical Error Handler) to its own code, author wrote non-working INT 24h code. Any critical errors after the virus has run bring down the system. When run, current directory is examined for .COM files; 1st uninfected one over 512 bytes is hit; IF the target .COM is the first one in its directory, virus hits it regardless of its size. If it was too small, it will no longer run (will hang PC) 1 version adds 1254 bytes to files, says "StinkFoot has arrived on your PC !", displayed in Black on Black if infected file is executed with DOS time minutes=seconds 2nd version adds 1273 bytes, says "StinkFoot: '(Eat this Paul Ducklin)'" displayed if hours=minutes (Black on Black) (Paul Ducklin is a South African anti-viral program developer)		

Name: Stoned		
Aliases: Stoned, Marijuana, Hawaii,New Zealand, Australian, Hemp, San Diego, Smithsonian, Stoned-B, Stoned-C, Zapper (variant)	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector., Hard disk boot sector., Hard disk partition table.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application., Corrupts boot sector, Corrupts the file linkages or the FAT.	**Size:** Overlays boot sector, no increase, 440 bytes	**See Also:** Michaelangelo
Notes: Spreads between boot sectors of both fixed and floppy disks. May overlay data. Sometimes displays message "Your PC is now Stoned!" when booted from floppy. Affects partition record on hard disk. No intentional damage is done. When Stoned and Michaelangelo both infect a disk, problems occur because they both try to hide the partition table in the same place. 'Your PC is now Stoned!.....LEGALISE MARIJUANA!' in the bootsector at offset 18Ah		

Name: SUG		
Aliases: SUG	**Type:** Trojan., Encrypted/Stealth The virus actively hides.	
Disk Location: SUG.???	**Features:** Encrypted	
Damage: Erases a Floppy Disk	**Size:**	**See Also:**
Notes: This program is supposed to unprotect copy protected program disks protectedby Softguard Systems, Inc. It trashes the disk and displays: "This destruction constitutes a prima facie evidence of your violation. If you attempt to challenge Softguard Systems Inc..., you will be vigorously counter-sued for copyright infringement and theft of services." It encrypts the Gotcha message so no Trojan checker can scan for it.		

Name: Sunday		
Aliases: Sunday, Sunday-B, Sunday-C	**Type:** Program.	
Disk Location: COM application., EXE application., Program overlay files.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application., Corrupts a program or overlay files.	**Size:** 1636, 1644, 1631, uses INT 21 subfunction FF to check for prior infections	**See Also:** Jerusalem
Notes: Infects .OVL, .COM and .EXE files. It is a memory resident virus. It can affect system run-time operations. It appears to be a "Jerusalem" variant, with modifications at the source code level to make this a separate and distinct virus (i.e. not a mutation of Jerusalem). First discovered in Seattle, WA in November 1989. Three variants exist. FAT damage has been reported, but not confirmed. Each of the three variants adds a different amount of bytes to files, it is not yet known which size is for which variant. One variant only is damaging; it activates on Sundays and displays a message. The other two variants have a bug which stops this action, and do not cause FAT damage. Works well on LANs Activation on Sundays and displays message "Today is Sunday! Who do you work so hard? All work and no play make you a dull boy. C'mon let's go out and have fun!" then may cause FAT damage Find with standard detection/eradication packages FPROT 2.00, probably earlier versions, most commercial scanners.		

Name: Suriv-01		
Aliases: Suriv-01, April-1-COM, April 1st, Suriv A, sURIV 1.01	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application., Corrupts a program or overlay files.	**Size:** 897	**See Also:**
Notes: Spreads between COM files. On April 1st, 1988, writes the message: "APRIL 1ST HA HA HA HA YOU HAVE A VIRUS" and hangs the system. After that, simply writes a message every time any program is run. If day is greater than 1st April, only "YOU HAVE A VIRUS !!!" is displayed. Typical text in Virus body (readable with HexDump-utilities): "sURIV 1.01"		

Name: Suriv-03		
Aliases: Sufiv-03, Suriv03, Suriv 3.00,Suriv 3.00, Suriv B, Jerusalem (B), Israeli #3	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application., Corrupts a program or overlay files.	**Size:** 1813 bytes increase in length of .COM files, 1808-1823 bytes increase in length of .EXE files	**See Also:**
Notes: The system is infected if function E0h of INT 21h returns value 0300h in the AX-register. .Com files: program length increases by 1813; files are infected only once; COMMAND.COM is not infected. .EXE files: program length increases by 1808 - 1823 bytes, and no identification is used; therefore, .EXE files can be infected more than once. Programs are infected at load time. 30 seconds after the 1st infected program was run, the virus scrolls up 2 Lines in a small window of the screen (left corner 5,5; right corner 16,16). The virus slows down the system by about 10 %. Suriv 3.00 compares the system-date with "Friday 13th", but is not able to recognize "Friday 13th", because of a "bug"; if it correctly recognized this date, it would delete any program started on "Friday 13th". Increase in the length of .EXE files. Lines scrolling in a small window. General slowdown of a machine. Typical texts in Virus body (readable with HexDump facilities): "sURIV 3.00"		

Name: SVC 6.0		
Aliases: SVC 6.0	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:** Starship
Notes: Russian origin virus, infects device drivers (see also Starship virus)		

Name: Swap Boot		
Aliases: Swap Boot, Falling Letters Boot	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sector	**Size:** Overlays boot sector, no increase	**See Also:**
Notes: The virus overwrites the boot with a loader that loade the rest of the virus stored near the end of track 39. The virus makes letters fall down the screen.		

Name: Sylvia V2.1		
Aliases: Sylvia V2.1,Holland Girl	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 1332	**See Also:**
Notes: The virus infects only COM-files with less than 30 KB; it does not infect COMMAND.COM, IBMBIO.COM, IBMDOS.COM. 1301 bytes of the virus-code are written in front of and 31 bytes are written behind the original code; files are only infected once, because the virus checks the existence of its signature (808h) at the beginning of the file. When an infected file is started, the virus tries to infect 5 COM-files on default drive. The virus displays the following message : "FUCK YOU LAMER !!!! (CRLF) system halted..." and stops system by jumping into an endless loop. The message is encoded in the program. In this version (V2.1), the message typical for original Sylvia virus ("This program is infected by a HARMLESS ... ") is NOT displayed. After being activated, the virus checks itself by creating a check-sum of the first 144 words. When the check-sum is incorrect (# 46A3h) the damaging part of the virus is activated. "FUCK YOU LAMER !!!! (CRLF) system halted", displayed on screen. Typical texts in Virus body (readable with Hexdump-facilities) : 1. "39 38 39 38 4F 45 4F 52 61 59 1E 56 5D 5A 52 61 62" (encoded text) 2. 'Text-Virus V2.1' 3. 'Sylvia Verkade' 808h at beginning of file.		

Name: Syslock		
Aliases: Syslock, Macrosoft	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application., EXE application., COMMAND.COM.	**Features:** Encrypted, Direct acting.	
Damage: Corrupts a program or overlay files., Corrupts a data file.	**Size:** 3550-3560 bytes are appended on a paragraph boundary	**See Also:**
Notes: Spreads between .COM and .EXE files. It scans through data on the hard disk, changing the string "Microsoft" (in any mixture of upper and lower case) to "MACROSOFT". If the environment variable "SYSLOCK=@" is set, the virus will not infect. A variant of Advent. Microsoft changes to MACROSOFT		

Name: Telefonica		
Aliases: Telefonica, Spanish Telecom, Telecom Boot, Anti-Tel, A-Tel, Campanja, Campana, (see also Antitelefonica)	**Type:** Boot sector.	
Disk Location: COM application., EXE application., Floppy disk boot sector., Hard disk boot sector.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sector, Corrupts the file linkages or the FAT., Attempts to format the disk.	**Size:**	**See Also:**
Notes: The Telefonica COM/EXE file infector can contain the Campana boot sector virus. Campana only affects the bootblock of floppies and partition table of hard disks. To eradicate from HD boot from clean floppy, and with DOS 5, type FDISK /MBR to rebuild the partition table. Or try most anti-viral utilities, they should clean it. Campana may try to format the hard disk. If the virus has trashed the disk, probably can't recover the Antitelefonica variant is a multi-partite virus (see record of that virus for more info)		

Name: Terror		
Aliases: Terror, Dark Lord	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: a new version was found recently in Bulgaria in the wild, does not seem to work properly, mentioned in virus-l, v4-224		

Name: The Basic Virus		
Aliases: The Basic Virus, 5120, V Basic Virus	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Direct acting.	
Damage:	**Size:** 5120-5135 bytes change in length. Code added at a paragraph boundary.	**See Also:**
Notes: The virus infects programs at run time (it is not memory resident) by searching through the directories recursively starting on paths "C:\", "F:\" as well as the current drive. All .EXE and .COM files it can find are infected. EXE files will be infected if the length as reported by DOS is less that the file length as reported by the EXE header plus one page. COM files will be infected if the file length is less than 60400 bytes. The virus will infect any time it is executed after the 6th of July 1989. However, an infected file will infect before this date, if it has already been executed once. On any date after the 1st of June, 1992, any infected file will terminate with the message "Access denied" (this comes from the virus, not from DOS). After 1/1/92, executed programs terminate with an "Access denied" error. The following texts are contained in the virus: "BASRUN", "BRUN", "IBMBIO.COM", "IBMDOS.COM", "COMMAND.COM", "Access denied"		

MS-DOS/PC-DOS Computer Viruses

Name: Tiny 163		
Aliases: Tiny 163, V 163, V-163	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Direct acting.	
Damage:	**Size:** 163 Added to .COM files. that start with a JMP instruction	**See Also:**
Notes: When an infected file is executed, the virus attempts to infect other .COM files in the local directory. Files increase in length.		

Name: Tiny virus		
Aliases: Tiny virus, Tiny 134, Tiny 138, Tiny 143, Tiny 154, Tiny 156, Tiny 158, Tiny 159, Tiny 160, Tiny 169, Tiny 198, Tiny 133	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:** tiny
Notes: see tiny		

Name: TIRED		
Aliases: TIRED	**Type:** Trojan.	
Disk Location: TIRED.???	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: Another scramble the FAT trojan by Dorn W. Stickel.		

Name: Toothless		
Aliases: Toothless, W13, W13-A, W13-B	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 534, 507	**See Also:**
Notes: Infects .COM files. Infected programs are first padded so their length becomes a multiple of 512 bytes, and then the 637 bytes of virus code is added to the end. It then intercepts any disk writes and changes them into disk reads.		

Name: TOPDOS		
Aliases: TOPDOS	**Type:** Trojan.	
Disk Location: TOPDOS.???	**Features:**	
Damage: Attempts to format the disk.	**Size:**	**See Also:**
Notes: This is a simple high level [hard] disk formatter.		

Name: TPWORM		
Aliases: TPWORM	**Type:** Companion program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage:	**Size:**	**See Also:**
Notes: A companion virus (v4-121)		

Name: Traceback		
Aliases: Traceback, 3066, 3066-B, 3066-B2, Traceback-B, Traceback-B2	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files., Interferes with a running application.	**Size:** 3066	**See Also:**
Notes: Spreads between COM and EXE fles. Based on a rather complicated set of criteria, it will sometimes cause the text displayed on the screen to fall to the bottom, and then rise back up. One hour after system infection, the characters will fall down the screen. After 1 minute, screen is automaticly restored. During damage, INT 09h will be hooked. Characters typed during damage will move "fallen-down" characters back to their start position. Damage repeats every hour. Typical text in Virus body (readable with hex-dump-utilities): 1. "VG1" in the data area of the virus 2. "VG1" is found at offset of near-jmp- displacement if program is a .COM file. 3. The complete name of the file, which infected the currently loaded file, is in the code. 4. Search the last 16 bytes of a .COM or .EXE files for the hex-string: 58,2B,C6,03,C7,06,50,F3,A4,CB,90,50,E8,E2,03, 8B		

Name: Traceback II		
Aliases: Traceback II, 2930, 2930-B, Traceback II-B	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 2930	**See Also:**
Notes: This appears to be an earlier version of Traceback. Spreads between .COM and .EXE files. Based on a rather complicated set of criteria, it will sometimes cause the text displayed on the screen to fall to the bottom, and then rise back up. Text falls down the screen.		

Name: Trackswap		
Aliases: Trackswap, VB Trackswap	**Type:**	
Disk Location:	**Features:**	
Damage: Corrupts boot sector	**Size:**	**See Also:**
Notes: Swaps tracks from the front with end of floppy tracks, making it real difficult to disinfect Not seen in wild by DDI		

Name: Tremor		
Aliases: Tremor	**Type:** Memory resident; TSR.	
Disk Location:	**Features:** Memory resident; TSR.	
Damage:	**Size:**	**See Also:**
Notes: Polymorphic, stealth, tunneling, direct attacks some anti-virus software big in Europe Disables VSAFE from DOS 6.0 (the resident antivirus program)(v6-084) Find with: FPROT 2.08 TBCLEAN, ANTISER, Vi-Spi		

Name: Troi		
Aliases: Troi, Best Wishes, Best Wish (may be wrong), Troi Two	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** Adds 322-324 bytes to infected .com files	**See Also:**
Notes: Hinders execution of some programs. Virus code is located at the end of the orig. .com file and is jmp - ed toas a FAR procedure. Attempt to infect a file on a write prot. disk will produce "Abort, retry, fail?" message SCAN 86B says its the Best Wishes virus, but this may be wrong. Programs monitoring disk activity will trap the infection requests. Easy to detect as it changes the times and dates for infected files to outrageous times and dates. Approximately fifty-six YEARS are added to the date. HEX search string: 2AC0CF9C80FCFC75, also scan for string "The Troi Virus" FPROT 2.03a		

Name: TSRMAP		
Aliases: TSRMAP	**Type:** Trojan.	
Disk Location: TSRMAP.???	**Features:**	
Damage: Corrupts boot sector	**Size:**	**See Also:**
Notes: TSRMAP *TROJAN* This program does what it's supposed to do: give a map outlining the location (in RAM) of all TSR programs, but it also erases the boot sector of drive "C:".		

Name: Twin-351		
Aliases: Twin-351	**Type:** Companion program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 351 bytes	**See Also:**
Notes: Unlike the other two companion viruses (AIDS II and TPWORM) it stays resident in memory, intercepting the Findfirst/FindNext calls. As the files containing the virus are also marked as "hidden", the virus is able to hide quite efficiently, unless a program reads the directory directly. Suspected not found outside of Norway		

Name: Typo		
Aliases: Typo, Type Boot	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors., Hard disk boot sectors.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sector, Interferes with a running application.	**Size:** Overlays boot sector, no increase	**See Also:**
Notes: Infects floppy and hard disk boot sectors. Infects data disks as well as system disks. Attempting to boot with an infected data disk in the drive loads the virus then asks for a system disk. Every 50 printed characters, the virus inserts a typo. Typos in printed output. 80286 and 80386 machines hang when booted with an infected disk. You can detect infected diskettes by running Chkdsk . If you get 1k of bad sectors, that's a good sign of Typo (or Italian virus), as FORMAT marks an entire track (5k on a 360k diskette) as bad if it finds a defect. Treatment consists of simply copying all the files off an infected diskette (using "COPY *.*"; do not use Diskcopy or any image copier), and reformatting the diskette		

Name: Typo		
Aliases: Typo, Fumble, Typo COM, 867, Mistake	**Type:** Program.	
Disk Location: COM application., COMMAND.COM.	**Features:** Direct acting.	
Damage: Interferes with a running application., Corrupts a program or overlay files.	**Size:** 867	**See Also:**
Notes: Infects .COM files. The virus replaces the keyboard handler, and if it is in place, it occasionally replaces the key that is typed, with the key immediately to the right. The fumble only activates if you type at better than six characters per second (approximately 60 wpm). If you type at that speed, after not using the keyboard for five seconds, you get a fumble. Typed characters are not what you pressed.		

Name: ULTIMATE		
Aliases: ULTIMATE	**Type:** Trojan.	
Disk Location: ULTIMATE.ARC, ULTIMATE.EXE	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:** 3090 size of ULTIMATE.EXE, 2432 Size of ULTIMATE.ARC	**See Also:**
Notes: Another FAT eater		

Name: Ultimate Weapon		
Aliases: Ultimate Weapon, Smulders's virus, Criminal	**Type:** Program.	
Disk Location: COM application., EXE application., COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: A Dutch virus, activated after Jan 1, 1992, after boot a message is displayed (sic): The Ultimate Weapon has arrived, please contact the nearest police station to tell about the illegal copying of you The system will hang, after boot from floppy in A: all files and directories in the root and the next directory-level renamed to CRIMINAL.001, CRIMINAL.002 etc See also Criminal virus signature given in virus-l v5-011: MF00EVKUR		

Name: USSR		
Aliases: USSR, USSR 516, USSR 600, USSR 707, USSR 711, USSR 948, USSR 1049, USSR 1689, USSR 2144, USSR 1594	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different, (USSR-1594 only alters one byte)	**See Also:**
Notes:		

Name: V-299		
Aliases: V-299, Amstrad	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 299	**See Also:**
Notes: Adds code to front of any .COM file in the current directory. The virus contains an advertisement for Amstrad computers. The program prints "Program sick error:Call doctor or buy PIXEL for cure description" with a 50-50 chance after the 5th infection. The virus contains the string "Program sick error:Call doctor or buy PIXEL for cure description". The string "IV" is at offset 3 in the COM file.		

Name: V-345		
Aliases: V-345, Amstrad	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 345	**See Also:**
Notes: Adds code to front of any .COM file in the current directory. The virus contains an advertisement for Amstrad computers. The program prints "Program sick error:Call doctor or buy PIXEL for cure description" with a 50-50 chance after the 5th infection. The virus contains the string "Program sick error:Call doctor or buy PIXEL for cure description". The string "IV" is at offset 3 in the COM file.		

Name: V08-15		
Aliases: V08-15	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1322 -1337 virus is placed on even paragraphs	**See Also:**
Notes: A .COM and .EXE file infector. After the 11th of November 1990 the virus will intercept INT 09 and count the keystrokes. If the number of keystrokes reaches 3000 the virus will display the message "CRITICAL ERROR 08/15: TOO MANY FINGERS ON KEYBOARD ERROR". and halt the system. Counting starts as soon as the first infected file is started. CRITICAL ERROR 08/15: TOO MANY FINGERS ON KEYBOARD ERROR. printed on screen. Infected files contain the readable string: 'CRITICAL ERROR 08/15: TOO MANY FINGERS ON KEYBOARD ERROR.' EXE-type files are marked infected by 4D54h at offset 12h (that is the EXE header checksum). COM-type files are marked by the same 16bit value but at offset 3 in file (that is 103h when loaded). Boot from a clean disk and delete infected files.		

Name:V1701New		
Aliases: V1701New, V1701New-B, Evil, Evil-B, P1, Phoenix related	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application., COMMAND.COM	**Features:** Memory resident; TSR above TOM., Encrypted, Polymorphic	
Damage:	**Size:** 1701 All .COM files but COMMAND.COM, It overlays part of COMMAND.COM, Multiple infections are possible., Polymorphic: each infection different	**See Also:**
Notes: The V1701-New virus is of Bulgarian origin, a variant of Phoenix. The V1701-New virus is a memory resident, generic infector of .COM files, and will infect COMMAND.COM. V1701-New infects COMMAND.COM by overwriting part of the binary zero portion of the program, and changing the program's header information. COMMAND.COM will not change in file length. V1701-New is not able to recognize when it has previously infected a file, so it may reinfect .COM files several times. Each infection of a .COM file will result in another 1,701 bytes of viral code being appended to the file. Systems infected with the V1701-New virus will experience problems with executing CHKDSK.COM. Attempts to execute this program with V1701-New memory resident will result in a warm reboot of the system occurring, however the memory resident version of V1701-New will not survive the reboot. The V1701-New Virus employs a complex encryption mechanism, and virus scanners which are only able to look for simple hex strings will not be able to detect it. There is no simple hex string in this virus that is common to all infected samples. Also see: PhoenixD, Phoenix A warmboot occurs when CHKDSK.COM is run. ViruScan V66+ Scan/D, or delete infected files		

Name:V2P2		
Aliases: V2P2	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes:		

Name:V2P6		
Aliases: V2P6, Vienna Variant, V2P6 Trash, V2P6Z, Adolph \	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting., Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes: A polymorphic virus, the decryption routine and infection length vary lots, so its hard to locate all infected files. Otherwise, it is a vienna-related virus, non-resident, and infects only COM files in the current directory and in the directories listed in the PATH. VIRx has reported some false positives for this virus, in older versions of mem.com, popdrop.com, and HP.com. Virx21.zip should have fixed these false positives: reported in virus-l, v5-065 MS-DOS 6's antivirus routine detects some, but not all infections by V2P6.		

Name: V-299		
Aliases: V-299, Amstrad	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 299	**See Also:**
Notes: Adds code to front of any .COM file in the current directory. The virus contains an advertisement for Amstrad computers. The program prints "Program sick error:Call doctor or buy PIXEL for cure description" with a 50-50 chance after the 5th infection. The virus contains the string "Program sick error:Call doctor or buy PIXEL for cure description". The string "IV" is at offset 3 in the COM file.		

Name: V-345		
Aliases: V-345, Amstrad	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 345	**See Also:**
Notes: Adds code to front of any .COM file in the current directory. The virus contains an advertisement for Amstrad computers. The program prints "Program sick error:Call doctor or buy PIXEL for cure description" with a 50-50 chance after the 5th infection. The virus contains the string "Program sick error:Call doctor or buy PIXEL for cure description". The string "IV" is at offset 3 in the COM file.		

Name: V08-15		
Aliases: V08-15	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1322 -1337 virus is placed on even paragraphs	**See Also:**
Notes: A .COM and .EXE file infector. After the 11th of November 1990 the virus will intercept INT 09 and count the keystrokes. If the number of keystrokes reaches 3000 the virus will display the message "CRITICAL ERROR 08/15: TOO MANY FINGERS ON KEYBOARD ERROR". and halt the system. Counting starts as soon as the first infected file is started. CRITICAL ERROR 08/15: TOO MANY FINGERS ON KEYBOARD ERROR. printed on screen. Infected files contain the readable string: 'CRITICAL ERROR 08/15: TOO MANY FINGERS ON KEYBOARD ERROR.' EXE-type files are marked infected by 4D54h at offset 12h (that is the EXE header checksum). COM-type files are marked by the same 16bit value but at offset 3 in file (that is 103h when loaded). Boot from a clean disk and delete infected files.		

Name: V1701New		
Aliases: V1701New, V1701New-B, Evil, Evil-B, P1, Phoenix related	**Type:** Program., Encrypted/Stealth The virus actively hides.	
Disk Location: COM application., COMMAND.COM	**Features:** Memory resident; TSR above TOM., Encrypted, Polymorphic	
Damage:	**Size:** 1701 All .COM files but COMMAND.COM, It overlays part of COMMAND.COM, Multiple infections are possible., Polymorphic: each infection different	**See Also:**
Notes: The V1701-New virus is of Bulgarian origin, a variant of Phoenix. The V1701-New virus is a memory resident, generic infector of .COM files, and will infect COMMAND.COM. V1701-New infects COMMAND.COM by overwriting part of the binary zero portion of the program, and changing the program's header information. COMMAND.COM will not change in file length. V1701-New is not able to recognize when it has previously infected a file, so it may reinfect .COM files several times. Each infection of a .COM file will result in another 1,701 bytes of viral code being appended to the file. Systems infected with the V1701-New virus will experience problems with executing CHKDSK.COM. Attempts to execute this program with V1701-New memory resident will result in a warm reboot of the system occurring, however the memory resident version of V1701-New will not survive the reboot. The V1701-New Virus employs a complex encryption mechanism, and virus scanners which are only able to look for simple hex strings will not be able to detect it. There is no simple hex string in this virus that is common to all infected samples. Also see: PhoenixD, Phoenix A warmboot occurs when CHKDSK.COM is run. ViruScan V66+ Scan/D, or delete infected files		

Name: V2P2		
Aliases: V2P2	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes:		

Name: V2P6		
Aliases: V2P6, Vienna Variant, V2P6 Trash, V2P6Z, Adolph \	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting., Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes: A polymorphic virus, the decryption routine and infection length vary lots, so its hard to locate all infected files. Otherwise, it is a vienna-related virus, non-resident, and infects only COM files in the current directory and in the directories listed in the PATH. VIRx has reported some false positives for this virus, in older versions of mem.com, popdrop.com, and HP.com. Virx21.zip should have fixed these false positives: reported in virus-l, v5-065 MS-DOS 6's antivirus routine detects some, but not all infections by V2P6.		

Name: Vacsina		
Aliases: Vacsina, TP04VIR, TP05VIR, TP06VIR, TP16VIR, TP23VIR, TP24VIR, TP25VIR	**Type:** Program.	
Disk Location: COM application., EXE application., Program overlay files.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application., Corrupts a program or overlay files.	**Size:** 1206 - 1221 Added to a .COM file length mod 16 equals 0, 132+ Added to .EXE file then like a com file.	**See Also:** Yankee Doodle
Notes: It infects .COM and .EXE files when they are loaded, old versions of the virus will be replaced by newer ones. System beep when running a program. The string 'VACSINA' in the virus code the last 4 bytes of an infected file show F4 7A 05 00		

Name: Vcomm		
Aliases: Vcomm, 637	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 637	**See Also:**
Notes:		

Name: VDIR		
Aliases: VDIR	**Type:** Trojan.	
Disk Location: VDIR.???	**Features:**	
Damage: Attempts to erase all mounted disks.	**Size:**	**See Also:**
Notes: This is a disk killer that Jerry Pournelle wrote about in BYTE Magazine.		

Name: VHP		
Aliases: VHP, VHP-348, VHP-353, VHP-367, VHP-435, Faggot	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Direct acting.	
Damage:	**Size:**	**See Also:**
Notes: File infector, Faggot is somewhat of a virus/trojan, if its the first infection, it trashes the hard disk, but if it's not the first infection, it just sits there. May be related to VHP. It is probably a hack on the Vienna, but very poorly written.		

Name: Vienna		
Aliases: Vienna, 648, Lisbon, Vienna-B, Austrian, Dos-62, Unesco, The 648 Virus, The One-in-Eight Virus, 62-B, DOS-68, Vien6, Vienna-B645, 648-B	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files., Deletes or moves files.	**Size:** 648	**See Also:**
Notes: The virus infects one .COM file every time it is run. 7/8 of the time it infects the .COM file and 1/8 of the time it inserts a jump to the BIOS initialitation routines that reboot the machine. To mark a file as infected, the virus sets the seconds field of the timestamp to 62 which most utilities (including DIR) skip. Damaged files, file lengths increase. The second-entry of the time stamp of an infected file is set to 62 dec.		

Name: Vienna 348		
Aliases: Vienna 348	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files., Interferes with a running application.	**Size:** 348	**See Also:**
Notes: The time stampof an infected file is changed: the seconds are set to 62 (= 2 * 1Fh). When infected file is executed, .COM-files in the current directory as well as in the directories in the DOS-PATH are extended by appending the viral code; no infection if the filesize<10 or filesize>64000 bytes. A selected .COM-file is infected by "random" IF (system seconds AND 7) <> 0 ELSE damaged! INT 24h diverted to own error-handler only during virus-runtime to suppress error-messages send out by DOS. A selected .COM-file is damaged permanently: Overwriting the first five bytes with a far jump to the HD-low-level-format- routine (XT only). The virus ignores READ-ONLY and HIDDEN attributes; A branch to the low level format routine on an XT when a program is run. Bytes found in virus = EAh,06h,00h,00h,C8h; text found: "*.COM",00h,"PATH=". Seconds time stamp changed to 62		

Name: Vienna 353		
Aliases: Vienna 353, Vienna 367, Vienna 435, Vienna 623, Vienna 627	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application., Corrupts a program or overlay files.	**Size:** 353, 367, 435, 623, 627	**See Also:**
Notes: The time stampof an infected file is changed: the seconds are set to 62 (= 2 * 1Fh). When infected file is executed, .COM-files in the current directory as well as in the directories in the DOS-PATH are extended by appending the viral code; no infection if the filesize<10 or filesize>64000 bytes. A selected .COM-file is infected by "random" IF (system seconds AND 7) <> 0 ELSE damaged! INT 24h diverted to own error-handler only during virus-runtime to suppress error-messages send out by DOS. A selected .COM-file is damaged permanently: Overwriting the first five bytes with a far jump to the HD-low-level-format- routine (XT only). The virus ignores READ-ONLY and HIDDEN attributes; Bytes found in virus = EAh,06h,00h,00h,C8h; text found: "*.COM",00h,"PATH=". The time stamp of an infected file changes to 62		

Name: Viki		
Aliases: Viki, V-277, Amstrad	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 277	**See Also:**
Notes: Adds code to front of any .COM file in the current directory. The virus simulates a RAM parity error. The program terminates with a simulated RAM parity error with a 50-50 chance after the 5th infection. The string "UM" at offset 3 in the COM file		

Name: Virus 101		
Aliases: Virus 101	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes:		

Name: Virus Creation Lab		
Aliases: Virus Creation Lab, VCL	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: The VCL is a program which creates viruses. It has a menuing routine which allows for easy creation of new viruses, using various selection criteria. It has been wide distributed on various bulletin boards. sometimes difficult, some antivirus products have only a 90% success rate in finding it. Data Physician Plus! claims over a 99% success rate Once found, it is easy to eradicate viruses created as all viruses are .exe and .com infectors		

Name: Virus-90		
Aliases: Virus-90	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 857	**See Also:**
Notes:		

Name: Vlad the Inhaler		
Aliases: Vlad the Inhaler	**Type:** Not a virus/worm/other destructive procedure	
Disk Location:	**Features:**	
Damage: Does no damage, doesn't affect any part of machine	**Size:**	**See Also:**
Notes: NOT A VIRUS! This phrase was a false alert, a task titled "Vlad the Inhaler" shows up in the file NWRES.DLL which is part of the Norton Desktop program. Occasionally it appears to show up when upgrading to Windows 3.1. It is included here in case anyone sees it and thinks it may be a destructive piece of code.		

Name: Voice Master		
Aliases: Voice Master	**Type:** Trojan.	
Disk Location: Voice Master	**Features:**	
Damage: Corrupts boot sector, Corrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: Since the IBM PC speaker could make a very poor microphone but the system electronics is designed only for sound output, the programs claims (see below) could be evidence of malicious purpose. Found on a BBS in Virginia, USA Will attempt to overwrite the Boot record, both FATs and a portion of the root dir on all disks using Interrupt 26. At this time not known if it will occur on each activation or if their is a discriminator in use (disassembly is 54 pages long)		

Name: Voronezh		
Aliases: Voronezh, Voronezh B, Voronezh-1600	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: Voronezh-1600 places a Far CALL to its body at the EXE file's entry point This virus does not change the file entry point, as does Leapfrog and Brainy		

Name: Warrier		
Aliases: Warrier, Brainy	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 1531	**See Also:**
Notes: Brainy related to "Warrier" (not "Warrior"), mentioned virus-l, v4-224 Warrier may be broken, as virus-l writer was not able to infect anything, but Brainy may work OK. It may insert itself into the middle of a .COM program, without changing the beginning of the file, a trick which is only used by few other viruses (Leapfrog, and Voronezh-1600)		

MS-DOS/PC-DOS Computer Viruses

Name: Whale		
Aliases: Whale, Mother Fish, Z The Whale	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes:		

Name: Wordswap 1485		
Aliases: Wordswap 1485, Wordswap 1504, Wordswap 1385, 1391	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes: 1385 and 1391 won't work at all for one researcher		

Name: Yankee Doodle		
Aliases: Yankee Doodle, Five O'Clock, TP33VIR, TP34VIR, TP38VIR, TP41VIR, TP42VIR, TP44VIR, TP45VIR, TP46VIR, Yankee Doodle 44, Enigma, Old Yankee	**Type:** Program.	
Disk Location: COM application., EXE application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application., Corrupts a program or overlay files.	**Size:** 1961, 1624, 1755, 2772 Yankee Doodle-B	**See Also:** vacsina
Notes: One day in about 8 at 5 pm it can play the "Yankee Doodle" tune This virus also uses hamming codes to check itself and repair itself if someone had modified it. TP44 virus: at 15 seconds before 5 pm it plays the Yankee Doodle tune Yankee Doodle coming from the computer's speakers. One of the easier viruses to disinfect, lots of softwar will do it.		

Name: Zero Bug		
Aliases: Zero Bug, Agiplan, 1536. Palette, ZBug	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application., Corrupts a program or overlay files.	**Size:** 1536	**See Also:** Dark Avenger
Notes: Infects .COM files. All characters "0" (zero) will be exchanged with other characters. Exchange characters are 01h, 2Ah, 5Fh, 3Ch, 5Eh, 3Eh and 30h, in which case the attribute is set to back- ground color (i.e. the character is invisible). This routine uses about 10% of CPU-time (system is slowed down accordingly). The Dark Avenger may be a descendant of this virus. Typical text in Virus body (readable with HexDump-utilities): "ZE","COMSPEC=C:", "C:\COMMAND.COM". In infected .COM files the "seconds" field of the timestamp is changed to 62 sec (similar to GhostBalls original Vienna viruses).		

Name: ZeroHunt		
Aliases: ZeroHunt, Minnow	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-084: preserves the file's date, time, attributes, AND file length. Will not be detected by the integrity checking of MSAV or VSafe.		

Windows Computer Virus Table

Name: WinVir14		
Aliases: WinVir14, Win14, Windows virus	**Type:** Windows virus	
Disk Location:	**Features:**	
Damage: no damage, doesn't affect any part of machine	**Size:**	**See Also:**
Notes: From an article in Network World, November 23, 1992 (see article text below) if an infected program is run from dos prompt, it doesn't infect. Only if run from in windows The string MK92 is found in the virus, not used as actual data. After infecting all other programs in the dir, it deletes itself from the host program so it seems that the user simply mis-double-clicked the file, and the user doesn't knwo a virus has attacked.		

Amiga Computer Virus Table

Name: EM-Wurm		
Aliases: EM-Wurm, EuroMail Bomb	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: Apparently the virus edits startup-sequence to execute a program with the single letter name $A0. A file of this name is created in c:. Effects as described in the file: Damage routine: + Works only when devices [directories] EM or EUROMAIL or EUROSYS are available. + overwrites all Files in these directories with memory from MsgPort. + In damaged files: from $BC text 'clipboard.device'. + After that a pause of 3mins using dosdelay $259A + After pause damage routine is called again.		

Name: Saddam		
Aliases: Saddam	**Type:** Memory resident; TSR.	
Disk Location:	**Features:** Memory resident; TSR.	
Damage:	**Size:**	**See Also:**
Notes: Infects amiga's memory as soon as you insert an infected disk Disguises itself as the Disk-Validator, and sets about randomly altering all your vectors so that the disk becomes read-error happy. It eventually trashes your disk at some given trigger. A LINK virus VirusScan 5.32, Disaster Master 2		

Name: Smiley Cancer		
Aliases: Smiley Cancer	**Type:**	
Disk Location:	**Features:**	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: Not a bootblock-virus, but not a link-virus. It uses method similar to PC Dir II virus, because it changes some info in the file headers		

Atari Computer Virus Table

Name:(Atari virus info)		
Aliases: (Atari virus info)	**Type:** Not a virus/worm/other destructive procedure	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: This record contains some Atari virus info in the Summary section, taken from virus-l, v5-187 About two dozens of them are described in the Atari ST section of the Computer Virus Catalog, published by VTC-Hamburg. Get the file ftp.informatik.uni-hamburg.de:/pub/virus/texts/catalog/atarivir.zip		

Name: Batman		
Aliases: Batman	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: virus-l, v5-187 talks about it (see summary section)		

Name: Frankie		
Aliases: Frankie	**Type:**	
Disk Location: Applications and the Finder	**Features:**	
Damage:	**Size:**	**See Also:**
Notes:		

Name: Ghost		
Aliases: Ghost, Mouse Inversion	**Type:**	
Disk Location:	**Features:**	
Damage: Corrupts boot sector	**Size:**	**See Also:**
Notes: Does not check boot sectors to determine if they are already executable. It hooks itself into the ST operating system and writes a copy of itself onto every disk the ST reads or writes. It will overwrite any boot sector, rendering other booting disks useless. ST Virus Killer was able to clean up the affected disk and the virus apparently has not spread on the test system. It acts by counting how man copies of itself it has written. After 5 copies are made it starts attacking. Every 5 times the boot sector of either floppy is accessed, it reverses the vertical orientation of the mouse.		

In-Process Table

Viruses to be Described in Subsequent Update Bulletins

1381, 1605, 2131, 646, Vienna C, Christmas in Japan, Xmas in Japan, Cursy, Dot Killer, 944, Point Killer, Durban, Saturday the 14th, Eddie 3, V651, Fere Jacques, Fere, Groen, Groen Links, Green Left, Halloechen, Holocaust, India, Itavir, 3880, JOJO, July 13th, June 16th, Pretoria, Kemerovo, Korea, LBC Boot, Kukac,Turbo Kukac, Polish 2, Leprosy, Leprosy 1.00, Leprosy-B, News Flash, Live After Death, V800, V800M, Lozinsky, MGTU, Microbes, Music, Music Bug, Music Boot, Number 1, Number One, Ping Pong-C, Polimer, Polimat Tapeworm, Polish 217, 217, Polish Stupid, Polish 529, 529, Polish 529, Polish 583, Polish 961, Stone '90, Print Screen, 8920, EB-21, Print Screen 2, PrtSc, Prudents Virus, 1210, PSQR, 1720, Recovery Virus, 382, 382 Recovery Virus, Red Diavolyata, Scott's Valley, 2133, Shake, Slow, Slowdown, Solano 2000, Dyslexia, Dyslexia 2.00, Dyslexia 2.01, Sorry, G-Virus V1.3, Spyer, Subliminal 1.10, Sverdlov, SVir, SVir-A, SVir-B, Taiwan, Taiwan 2, Taiwan-B, Taiwan 3, Taiwan 4, 2576, Ten Bytes, 1554, 1559, 9300:0000, V-Alert, Tequila, Turbo 448, @ Virus, Turbo @, Polish 2, UScan Virus, V2100, 2100, VFSI, 437, VHP2, 623, VHP-623, VHP-627, Victor, Violator, Violator Strain B, VP, Westwood, Wisconsin, Death to Pascal, Wolfman, Yankee 2, 1624, 1961, Yankee go Home

MS-DOS/PC-DOS Cross Reference Table

This is the PC-DOS/MS-DOS virus name cross reference table. Use it to locate virus descriptions in the PC-DOS/MS-DOS virus description table. Locate the virus by name in the first column of this table then use the name in the second column to locate the virus description.

Virus Name/Alias	Name in Description
10 past 3	10 past 3
100 Years Virus	4096
1008	Oulu
1024	Diamond
1024-B	Nomenklatura
1024PrScr	1024PrScr
109 Virus	109 Virus
1160	Horse II
1168	Datacrime-B
1193	Copyright
12-TRICKS Trojan	12-TRICKS Trojan
1226	1226
1226D	1226
1226M	1226
1260	1260
1280	Datacrime
1391	Wordswap 1485
1392	Amoeba
1514	Datacrime II
1536	Zero Bug
1539	Christmas
1575	Green Caterpillar
1590	Green Caterpillar
1591	Green Caterpillar
15xx	Green Caterpillar
1701	1701
1704	Cascade
1704 B	Cascade
1704 C	Cascade
1704-Format	1704-Format
17Y4	Cascade
1808	Jerusalem
1813	Jerusalem
1917	Datacrime II-B
1971	Eight Tunes
2080	Fu Manchu
2086	Fu Manchu
2387	2387
2761	Advent
2930	Traceback II
2930-B	Traceback II
3012	Plastique
3066	Traceback
3066-B	Traceback
3066-B2	Traceback
333	Kennedy
3551	Macho
3555	Macho
382 Recovery	Recovery Virus
3X3SHR	3X3SHR
405	405
4096	4096
45	minimal
453	RPVS

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description
4711	Perfume
4870 Overwriting	4870 Overwriting
500 Virus	Merritt
505	Burger
509	Burger
512	Friday 13 th COM
512 Virus	Friday 13 th COM
512-A	512
512-B	512
512-C	512
512-D	512
5120	The Basic Virus
516	USSR
541	Burger
560-A	Burger
560-B	Burger
560-C	Burger
560-D	Burger
560-E	Burger
560-F	Burger
560-G	Burger
560-H	Burger
62-B	Vienna
632	Saratoga
637	Vcomm
640K Virus	Do Nothing
642	Icelandic II
648	Vienna
648-B	Vienna
66a	66a
688	Flash
765	Perfume
8-Tunes	Eight Tunes
800	Bulgarian 800
805	Stardot
847	Amstrad
855	November 17
867	Typo
909090H	Burger
910129	Brunswick
914	Russian Mutant
941	Devil's Dance
951	Devil's Dance
99%	99%

Virus Name/Alias	Name in Description
99 percent	99%
A-204	Jerusalem-B
A-Tel	Telefonica
A-VIR	Antitelifonica
Ada	DenZuk
Adolf	Adolf
Adolph\	V2P6
Advent	Advent
Agiplan	Zero Bug
AIDS	AIDS
AIDS II	AIDS II
AIDS-II	AIDS II
Aircop	Aircop
Akuku	Akuku
Alabama	Alabama
Alabama-B	Alabama
Alameda	Merritt
Albania	Albania
Alex	Alex
Alexander	Alexander
Alfa	Diamond
Ambulance Car	Ambulance Car
AmiLia	Murphy HIV
Amoeba	Maltese Amoeba
Amstrad	Amstrad
Anarkia	Jerusalem-B
Anarkia-B	Jerusalem-B
Andryushka	Andryushka
Angarsk	Angarsk
Animus	Cookie
Anna	Anna
Anthrax	Anthrax
Anthrax PT	Anthrax
Anti Pascal 529	Anti Pascal
Anti Pascal 605	Anti Pascal
Anti-Pascal 400	AntiPascal II
Anti-Pascal 440	AntiPascal II
Anti-Pascal 480	AntiPascal II
Anti-pascal II	AntiPascal II
ANTI-PCB	ANTI-PCB
Anti-Tel	Telefonica
AntiCAD	AntiCAD
Antimon	Antimon
AntiPascal	AntiPascal

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description
AntiPascal II	AntiPascal II
Antitelifonica	Antitelifonica
AP 529	Anti Pascal
AP 605	Anti Pascal
AP-400	AntiPascal II
AP-440	AntiPascal II
AP-480	AntiPascal II
Apilapil	EUPM
Apocalypse-2	Dark Avenger
April 1. EXE	April 1. EXE
April 15	Murphy-1
April 1st	Suriv-01
April-1-COM	Suriv-01
Arab	Jerusalem-B
Arab Star	Jerusalem-B
ARC513.EXE	ARC513.EXE
ARC514.COM	ARC513.EXE
ARC533	ARC533
Armagedon	Armagedon
Armagedon the first	Armagedon
Armagedon the Greek	Armagedon
Arriba	Arriba
Ash	Ash
Ash-743	Ash
Ashar	Brain
Ashar_B	Brain
Astra	Astra
AT	AT
AT II	AT II
Atas	Atas
Athens	Athens
Attention!	Attention
Australian	Stoned
Austrian	Vienna
Auto	Auto
Autumn	Cascade
AZUSA	AZUSA
Azuza	AZUSA
Backfont	Backfont
BACKTALK	BACKTALK
Bad Boy	Bad Boy
BADDISK	DISKSCAN
Baobab	Baobab
Beast C	Number of the Beast
Beast D	Number of the Beast
Bebe	Bebe
Bebe-486	Bebe
Beijing	Bloody!
Best Wish	Troi
Best Wishes	Best Wishes
Best Wishes-970	Best Wishes
Best Wishes-B	Best Wishes
Beta	Bob Ross
BetaBoys	BetaBoys
Better World	Fellowship
Beware	Beware
BFD	BFD
Big Joke	Big Joke
BIO	BIO
Bit Addict	Bit Addict
Black Avenger	Dark Avenger
Black Friday	Jerusalem
Black Hole	Jerusalem
Black Jec	Black Jec
Black Monday	Black Monday
Blackbox	Jerusalem
Blackjack	Cascade
Blood	Blood
Blood 2	Blood
BloodLust	BloodLust
Bloody!	Bloody!
Bloomington	Bloomington
Bob	Bob Ross
Bob Ross	Bob Ross
Boojum	Boojum
Boot	Ping Pong B
Boot-EXE	BFD
Borderline	Black Monday
Bouncing Ball	Ping Pong
Bouncing Dot	Ping Pong
Boys	Boys
Brain	Brain
@BRAIN	Brain
Brainy	Warrier

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description
Brasil Virus	Brasil Virus
Brazil	Brasil Virus
Breeder	Breeder
Brenda	Kennedy
Brunswick	Brunswick
Bryansk	Bryansk
Budo	Budo
Bulgarian	Plovdiv
Bulgarian 800	Bulgarian 800
Bulgarian Damage 1.3	Plovdiv
BUPT	BUPT
Burger	Burger
Burger 382	Burger
Burger 405	Burger
Burghoffer	Burghoffer
C 605	Anti Pascal
C virus	Cascade
C-544	C-544
Camouflage	1260
Campana	Telefonica
Campanja	Telefonica
Cancer	Smiley Cancer
Cansu	Cansu
Capital	Capital
CARA	CARA
Carioca	Carioca
CARMEL TntVirus	CARMEL TntVirus
Cascade	Cascade
Cascade A	Cascade
Cascade B	Cascade
Cascade Format	1704-Format
Cascade YAP	Cascade
Casino	Casino
Casper	Casper
Catch 22	Catch 22
Catch-22	Catch 22
CAZ	CAZ
CAZ-1159	CAZ
CB-1530	Dark Avenger
CC	CC
CDIR	CDIR
Century	4096
Century Virus	4096
Chad	Chad
Chameleon	1260
Chaos	Chaos
Checksum	Checksum
Checksum 1.01	Checksum
Cheeba	Cheeba
Chemnitz	Chemnitz
Choinka	Christmas
Christmas	Christmas
Christmas Tree	Christmas
CIA	Burger
Cinderella	Cinderella
Clone	Mirror
Clonewar	Clonewar
Close	Close
Cls	Cls
Cluster	Dir II
Cod	Cod
Code Zero	Code Zero
CoffeeShop	Mutation Engine
College	College
Columbus Day	Datacrime
COM Virus	Friday 13 th COM
Com2con	Com2con
Comasp-472	Comasp-472
Commander Bomber	Commander Bomber
Como	Como
Compiler.1	Compiler.1
Computer Ogre	Disk Killer
Cookie	Cookie
Copmpl	Akuku
Copyright	Copyright
Cossiga	Cossiga
Cpw	Cpw
Crackpot-1951	Murphy-1
Crackpot-272	Murphy-1
Cracky	Cracky
Crazy	Crazy Eddie
Crazy Eddie	Crazy Eddie
Crazy Imp	Crazy Imp
Creeper	Creeper
Creeper-425	Creeper

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description
Creeping Death	Dir II
Creeping Tormentor	Creeper
Crew-2048	Crew-2048
Crime	Datacrime
Crime-2B	Datacrime II-B
Criminal	Ultimate Weapon
Crooked	Crooked
CryptLab	Mutation Engine
CSL	CSL
CSL-V4	CSL
CSL-V5	CSL
Cunning	Cascade
Cursy	Cursy
CyberTech	CyberTech (rumored virus)
D-XREF60.COM	D-XREF60.COM
D2	Dir II
da	Dada
Dada	Dada
Damage	Plovdiv
Damage 1.1	Plovdiv
Damage 1.3	Plovdiv
Damage-2	Diamond
DAME (Dark Avenger Mutation Engine)	Mutation Engine
DANCERS	DANCERS
DANCERS.BAS	DANCERS
Danish Tiny	Kennedy
Dark Avenger	Dark Avenger
Dark Avenger 3	Dark Avenger 3
Dark Avenger II	Dark Avenger 3
Dark Avenger III	Dark Avenger 3
Dark Avenger's Latest	Mutation Engine
Dark Avenger-B	Dark Avenger
Dark End	Dark End
Dark Lord	Terror
Darth Vader	Darth Vader
Dash-em	Dash-em
Datacrime	Datacrime
Datacrime Ia	Datacrime-B
DATACRIME Ib	Datacrime
Datacrime II	Datacrime II
Datacrime II-B	Datacrime II-B
Datacrime-B	Datacrime-B
Datalock	Datalock
Datalock 1.00	Datalock
Datalock 2	Datalock
Datalock-1043	Datalock
David	Diamond
Day10	Day10
Dbase	Dbase
DBF virus	Dbase
Dead Kennedy	Kennedy
December 24th	Icelandic III
Decide	Deicide
Dedicated	Mutation Engine
Deicide	Deicide
Deicide II	Deicide
Demolition	Demolition
Demon	Murphy-1
Den Zuk	DenZuk
Den Zuk 2	Ohio
Den-Zuk 2	Ohio
DenZuc B	DenZuk
DenZuk	DenZuk
Denzuko	DenZuk
derived of Stoned	Empire B.2
Destructor	Destructor
Devil's Dance	Devil's Dance
Dewdz	Dewdz
Diamond	Diamond
Diana	Dark Avenger
Die Young	Dark Avenger 3
Digger	Digger
Digital F/X	Black Jec
Dima	Dima
DIR	Dir II
Dir 2	Dir II
Dir II	Dir II
Disk Crunching Virus	Icelandic
Disk Eating Virus	Icelandic
Disk Eating Virus	Icelandic
Disk Killer	Disk Killer
Disk Ogre	Disk Killer

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description
DISKSCAN	DISKSCAN
Diskspoiler	Diskspoiler
Dismember	Dismember
DM	DM
DM-310	DM
DM-330	DM
DMASTER	DMASTER
Do Nothing	Do Nothing
Doom	Doom
Doom II	Doom
Doom-2B	Doom
Doomsday	Doomsday
DOS-62	Vienna
Dos-62	Vienna
DOS-68	Vienna
DOS-HELP	DOS-HELP
DOShunt	DOShunt
DOSKNOWS	DOSKNOWS
Dot Killer	Dot Killer
Doteater	Doteater
DPROTECT	DPROTECT
DRAIN2	DRAIN2
DRIVER-1024	Dir II
DROID	DROID
Dropper 7	Dropper7
Dropper7	Dropper7
Dropper7 boot	Dropper7 boot
DRPTR	DRPTR
DSZBREAK	DSZBREAK
Ducklin	Stinkfoot
Dutch 424	Europe '92
Dutch Tiny	Dutch Tiny
Dutch Tiny-124	Dutch Tiny
Dutch Tiny-99	Dutch Tiny
E. T. C.	E. T. C.
Ear	Ear
Eastern Digital	Eastern Digital
Eddie	Dark Avenger
Eddie 2	Eddie 2
Eddie 3	Dark Avenger 3
EDV	EDV
EGABTR	EGABTR
Eight Tunes	Eight Tunes
Eliza	Eliza
EMF	EMF
Emmie	Emmie
Empire	Empire
Empire A	Empire
Empire B.2	Empire
Empire C	Empire
Empire D	Empire
End of	End of
ENET 37	Friday 13 th COM
Enigma	Yankee Doodle
Enola	Enola
EUPM	EUPM
Europe '92	Europe '92
European Fish	Fish
Evil	V1701New
Evil-B	V1701New
Exterminator	Murphy-1
F-Soft	F-Soft
F-Soft 563	F-Soft
F-Word	F-Word
F-you	F-Word
F1-337	F1-337
Faggot	VHP
Fall	Cascade
Falling Leaves	Cascade
Falling Letters	Ping Pong B
Falling Letters Boot	Ping Pong B
Falling Tears	Cascade
FAT EATER	MAP
Father Christmas	Christmas
Faust	Chaos
Fax Free	Fax Free
FCB	FCB
Fear	Mutation Engine
Feist	Feist
Fellowship	Fellowship
FGT	FGT
Fichv	Fichv
Fichv-EXE 1.0	Fichv
Filedate 11	Filedate 11
Filedate 11-537	Filedate 11
FILES.GBS	FILES.GBS
Filler	Filler

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description
Finnish	Finnish
Finnish-357	Finnish
Fish	Fish
Fish 6	Fish
Five O'Clock	Yankee Doodle
FIXIT	MATHKIDS
Flash	Flash
Flip	Flip
Flip Clone	Mirror
Flower	Flower
FLU4TXT	FLUSHOT4
FLUSHOT4	FLUSHOT4
Forger	Forger
Form	Form
Form Boot	Form
FORM-Virus	Form
Formiche	Cascade
Forms	Form
France	Paris
Freddy	Freddy
Freew	Freew
Friday 13 th COM	Friday 13 th COM
Friday 13th	Jerusalem
Friday The 13th-B	Friday 13 th COM
Friday The 13th-C	Friday 13 th COM
Friends	Cossiga
Frodo	4096
Frodo Soft	F-Soft
Frog's Alley	Frog's Alley
Frogs	Frogs
Fu Manchu	Fu Manchu
Fuck You	F-Word
Fumanchu	Fu Manchu
Fumble	Typo
Funeral	Funeral
FUTURE	FUTURE
G-MAN	G-MAN
GATEWAY	GATEWAY
GATEWAY2	GATEWAY
Geek	Geek
Genb	Genb

Virus Name/Alias	Name in Description
genp	Genb
Gergana	Gergana
Gergana-222	Gergana
Gergana-300	Gergana
Gergana-450	Gergana
Gergana-512	Gergana
Ghost	Ghost
Ghost Boot	GhostBalls
Ghost COM	GhostBalls
GhostBalls	GhostBalls
Gliss	Gliss
Globe	Globe
GMB	HH&H
Goblin	Murphy-1
Golden Gate	Merritt
Gomb	HH&H
Gosia	Gosia
Got You	Got You
Gotcha	Gotcha
Gotcha-D	Gotcha
Gotcha-E	Gotcha
GRABBER	GRABBER
Grain of Sand	Maltese Amoeba
Greemlin	Diamond
Green Caterpillar	Green Caterpillar
Groove	Mutation Engine
Grower	Grower
Grune	Grune
Guppy	Guppy
Gyorgy	Flash
Gyro	Gyro
Ha	Ha!
Hacker	DenZuk
Haddock	Haddock
Hafenstrasse	Hafenstrasse
Hahaha	AIDS
Haifa	Haifa
Halloechen	Halloechen
Halloechn	Halloechen
Happy	Joshi
Happy Birthday Joshi	Joshi
Happy Halloween	Happy Halloween
Happy Monday	Happy Monday

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description
Happy New Year	Happy New Year
Harakiri	Harakiri
Hary Anto	Hary Anto
Hate	Hate
Hawaii	Stoned
Hebrew University	Jerusalem
Hello	Halloechen
Hello_1a	Halloechen
Helloween	Helloween
Hemp	Stoned
Herbst	Cascade
Hero	Hero
Hero-394	Hero
Hey You	Hey You
HH&H	HH&H
Hi	Hi
Hide and Seek	Hide and Seek
Highlander	Highlander
Hitchcock	Hitchcock
HM2	Plastique
Holland Girl	Sylvia V2.1
Holo	Kamp
Hong Kong	AZUSA
Horror	Horror
Horse	Horse II
Horse Boot virus	Horse Boot virus
Horse II	Horse II
Hungarian	Hungarian
Hungarian-473	Hungarian
Hydra	Hydra
Hymn	Hymn
Icelandic	Icelandic
Icelandic II	Icelandic II
Icelandic III	Icelandic III
IDF	4096
Imp	Crazy Imp
Invader	Invader
Invol	Invol
Involuntary	Involuntary
INVOLVE	INVOLVE
Irish	Maltese Amoeba
Israeli	Jerusalem
Israeli #3	Suriv-03
Israeli Boot	Israeli Boot
Italian	Ping Pong
Italian Diamond	Diamond
Jeff	Jeff
Jerusalem	Jerusalem
Jerusalem A	Jerusalem
Jerusalem (B)	Suriv-03
Jerusalem-B	Jerusalem-B
Jerusalem-C	Jerusalem-B
Jerusalem-D	Jerusalem-B
Jerusalem-DC	Jerusalem-B
Jerusalem-E	Jerusalem-B
Jerusalem-E2	Jerusalem-B
Jo-Jo	Cascade
Jocker	Joker
Joe's Demise	Joe's Demise
Joes Demise	Joe's Demise
Joker	Joker
Joker 2	JOKER-01
JOKER-01	JOKER-01
Joker-01 Joker 01	JOKER-01
Jork	Brain
Joshi	Joshi
June 4th	Bloody!
Justice	Justice
Kamikazi	Kamikazi
Kamp	Kamp
Kamp-3700	Kamp
Kamp-3784	Kamp
Kennedy	Kennedy
KEYBGR Trojan	Scrambler
Keypress	Keypress
Klaeren	Hate
Krivmous	Crooked
Kylie (variant)	Jerusalem
Leapfrog	Leapfrog
Lehigh	Lehigh
Lehigh-2	Lehigh
Lehigh-B	Lehigh
Leningrad	Leningrad
Liberty	Liberty
Liberty-B	Liberty
Liberty-C	Liberty

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description
Lima	Burger
Lisbon	Vienna
Lucifer	Diamond
LZ	LZ
Macho	Macho
MachoSoft	Macho
Macrosoft	Syslock
Malta	Casino
Maltese Amoeba	Maltese Amoeba
MAP	MAP
Marauder	Marauder
Mardi Bros	DenZuk
Marijuana	Stoned
MATHKIDS	MATHKIDS
Mazatlan	Merritt
Mendoza	Jerusalem-B
Merritt	Merritt
Metal Thunder	Akuku
Mexican	Devil's Dance
Mexican Stoned	Mexican Stoned
MG series II	Dir II
Miami	Friday 13 th COM
Mich	Michelangelo
Michaelangclo	Michelangelo
Michelangelo	Michelangelo
Microelephant	CSL
Milana	Dark Avenger
Milena	Milena
minimal	minimal
minimal-45	minimal
Minnow	ZeroHunt
MIR	Dark Avenger
Mirror	Mirror
Mistake	Typo
MIX/1	Mix1
MIX1	Mix1
Mixer1	Mix1
Moctzuma	Moctzuma
Moctzuma-B	Moctzuma
Modem virus of 1989	Modem virus of 1989
Mon	Monkey
Monday 1st	Beware
Monkey	Monkey

Virus Name/Alias	Name in Description
Monxla A	Monxla A
Monxla B	Monxla A
Mosquito	Fax Free
Mother Fish	Whale
MtE	Mutation Engine
Mud	BetaBoys
Mule	Jerusalem
Mummy	Mummy
Munich	Friday 13 th COM
Murphy	Murphy-1
Murphy HIV	Murphy HIV
Murphy variant	Murphy HIV
Murphy-1	Murphy-1
Murphy-2	Murphy-2
Music	Oropax
Musician	Oropax
Mutation Engine	Mutation Engine
Naughty Hacker	Horse
Net Crasher	Net Crasher
New Jerusalem	Jerusalem-B
New Zealand	Stoned
Nina-2	Happy New Year
NMAN	NMAN
NMAN B	NMAN
NMAN C	NMAN
NOINT	Bloomington
Nomenklatura	Nomenklatura
NOTROJ	NOTROJ
Nov. 17	November 17
Nov 17-768	November 17
Nov 17-800	November 17
Nov 17-880	November 17
Nov 17-B	November 17
Novell	Novell
November 17	November 17
November 30	November 30
Nowhere Man	NMAN
Null Set	Doomsday
Number of the Beast	Number of the Beast
Ohio	DenZuk
Old Yankee	Yankee Doodle
Omega	Omega
Omicron	Flip

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description
Omicron PT	Flip
One In Ten	Icelandic
One In Two	Saratoga
Only	Crooked
Ontario	Ontario
Oropax	Oropax
Oulu	Oulu
Outland	Dark Avenger
P1	Phoenix
PACKDIR	PACKDIR
Pakistani	Brain
Palette	Zero Bug
Pandaflu	Antimon
Paniker	C-544
Paris	Paris
Park ESS	Jerusalem-B
Patricia	Murphy-1
Paul Ducklin	Stinkfoot
Payday	Jerusalem-B
PC Flu 2	PC Flu 2
PC-WRITE 2.71	PCW271
PCW271	PCW271
Peking	Merritt
Pentagon	Pentagon
Perfume	Perfume
Phoenix	1226
Phoenix D	Phoenix D
Ping Pong	Ping Pong
Ping Pong B	Ping Pong B
Pirate	Burger
Pisello	Fax Free
Pixel	Amstrad
PK362	PKPAK/PKUNPAK 3.61
PK363	PKPAK/PKUNPAK 3.61
PKB35B35	PKX35B35
PKFIX361	PKFIX361
PKPAK/PKUNPAK 3.61	PKPAK/PKUNPAK 3.61
PKX35B35	PKX35B35
PKZ201.EXE	PKZIP Trojan 1
PKZ201.ZIP	PKZIP Trojan 1
PKZIP Trojan 1	PKZIP Trojan 1

Virus Name/Alias	Name in Description
PKZIP Trojan 2	PKZIP Trojan 2
PKZIPV2.EXE	PKZIP Trojan 2
PKZIPV2.ZIP	PKZIP Trojan 2
Plague	Plague
Plastic Boot	Invader
Plastique	Plastique
Plastique 1	Plastique
Plastique 2	AntiCAD
Plastique 4.51	Plastique
Plastique 5.21	AntiCAD
Plastique-B	AntiCAD
PLO	Jerusalem
Plovdiv	Plovdiv
Plovdiv 1.1	Plovdiv
Plovdiv 1.3	Plovdiv
Pogue	Mutation Engine
Point Killer	Dot Killer
Possessed	Possessed
Possessed A	Possessed
Possessed B	Possessed
Proud	Proud
PrSc	1024PrScr
PrScr	1024PrScr
Ps!ko	Dark Avenger
Puerto	Jerusalem-B
Quake	Ear
Questo	Mutation Engine
QUIKRBBS	QUIKRBBS
QUIKREF	QUIKREF
Rabid	Dark Avenger
RAM	RAM
Rapid Avenger	Dark Avenger
RCKVIDEO	RCKVIDEO
Red Cross	Ambulance Car
REDX	Ambulance Car
Relzfu	Relzfu
Rock Steady	Diamond
RPVS	RPVS
RPVS-B	RPVS
Russian	Jerusalem
Russian Mutant	Russian Mutant
Sad	Black Jec
Saddam	Saddam
San Diego	Stoned

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description
Sara	Mutation Engine
Sarah	Mutation Engine
Saratoga	Icelandic
Saratoga 2	Icelandic
Satan Bug	Satan Bug
SBC	SBC
SBC-1024	SBC
SCANBAD	DISKSCAN
Scion	Doomsday
Scott's Valley	Jerusalem
Scrambler	Scrambler
Screaming Fist	Screaming Fist
Search	DenZuk
SECRET	SECRET
SECURE.COM	SECURE.COM
(see also Antitelefonica)	Telefonica
Sentinel	Sentinel
Seoul	Merritt
SF Virus	Merritt
Shield	Breeder
Shoe	Brain
Shoe B	Brain
Shoe_Virus	Brain
Shoe_Virus_B	Brain
SIDEWAYS	SIDEWAYS
SIDEWAYS.COM	SIDEWAYS
Sigalit	Cansu
Simplistic File Infector	November 17
Simulation	Simulation
Skism-1	Jerusalem-B
Slovakia	Slovakia
Slow	Jerusalem
Smack	Murphy-1
Smithsonian	Stoned
Smulders's virus	Ultimate Weapon
South African	Friday 13 th COM
Spanish Telecom	Telefonica
STAR	Jerusalem-B
Stardot	Stardot
Starship	Starship
Stealth	4096
Stigmata	Kennedy
Stinkfoot	Stinkfoot
Stoned	Stoned
Stoned 3	Bloomington
Stoned III	Bloomington
Stoned-B	Stoned
Stoned-C	Stoned
STRIPES	STAR
stupid	Do Nothing
Stupid Jack	Murphy-1
Stupid Virus	Do Nothing
Sudah ada vaksin	DenZuk
SUG	SUG
Suicide	Ear
Sunday	Sunday
Sunday-B	Sunday
Sunday-C	Sunday
Suomi	Oulu
sURIV 1.01	Suriv-01
Suriv 2	April 1. EXE
Suriv 2.01	April 1. EXE
Suriv 3.00	Suriv-03
Suriv A	Suriv-01
Suriv B	Suriv-03
Suriv-01	Suriv-01
Suriv-03	Suriv-03
Suriv03	Suriv-03
SVC 6.0	SVC 6.0
Swami	Murphy-1
Swap	Israeli Boot
Swap Boot	Israeli Boot
Sylvia V2.1	Sylvia V2.1
SYP	Day10
Syslock	Syslock
System Virus	Icelandic II
Tannenbaum	Christmas
Taunt	AIDS
Telecom 1	Kamp
Telecom 2	Kamp
Telecom Boot	Telefonica
Telefonica	Telefonica
Terror	Terror
The 648 Virus	Vienna

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description
The Basic Virus	The Basic Virus
The One-in-Eight Virus	Vienna
The Second Austrian Virus	Cascade
Time Virus	Monxla A
Timor	Jerusalem
Tiny 133	Tiny virus
Tiny 134	Tiny virus
Tiny 138	Tiny virus
Tiny 143	Tiny virus
Tiny 154	Tiny virus
Tiny 156	Tiny virus
Tiny 158	Tiny virus
Tiny 159	Tiny virus
Tiny 160	Tiny virus
Tiny 163	Tiny 163
Tiny 169	Tiny virus
Tiny 198	Tiny virus
Tiny virus	Tiny virus
TIRED	TIRED
Toothless	Toothless
TOPDOS	TOPDOS
Topo	Fax Free
TP04VIR	Vacsina
TP05VIR	Vacsina
TP06VIR	Vacsina
TP16VIR	Vacsina
TP23VIR	Vacsina
TP24VIR	Vacsina
TP25VIR	Vacsina
TP33VIR	Yankee Doodle
TP34VIR	Yankee Doodle
TP38VIR	Yankee Doodle
TP41VIR	Yankee Doodle
TP42VIR	Yankee Doodle
TP44VIR	Yankee Doodle
TP45VIR	Yankee Doodle
TP46VIR	Yankee Doodle
TPWORM	TPWORM
Traceback	Traceback II
Traceback II	Traceback II
Traceback II-B	Traceback II
Traceback-B	Traceback
Traceback-B2	Traceback
Trackswap	Trackswap
Travel	Dark Avenger 3
Traveler	BUPT
Tremor	Tremor
Tricks	12-TRICKS Trojan
Troi	Troi
Troi Two	Troi
TSRMAP	TSRMAP
TUQ	RPVS
Turin Virus	Ping Pong
Twelve Tricks Trojan	12-TRICKS Trojan
Twin-351	Twin-351
Type Boot	Typo
Typo	Typo
Typo COM	Typo
UIUC	Brain
UIUC-B	Brain
ULTIMATE	ULTIMATE
Ultimate Weapon	Ultimate Weapon
Unesco	Vienna
UofA	Empire
USSR	USSR
USSR 1049	USSR
USSR 1594	USSR
USSR 1689	USSR
USSR 2144	USSR
USSR 516	USSR
USSR 600	USSR
USSR 707	USSR
USSR 711	USSR
USSR 948	USSR
USSR-311	Com2con
V	The Basic Virus
V 163	Tiny 163
V Basic Virus	The Basic Virus
V-163	Tiny 163
V-277	Viki
V-299	V-299
V-345	V-345
V-605	Anti Pascal
V-801	Stardot
V-847	Amstrad

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description
V-847B	Amstrad
V-852	Amstrad
V-sign	Cansu
V08-15	V08-15
v1024	Dark Avenger 3
V1226	1226
V1226D	1226
V1226DM	1226
V1277	Murphy-1
V1302	Proud
V1521	Murphy-2
V1539	Christmas
V1701New	V1701New
V1701New-B	V1701New
V2000	Dark Avenger 3
V2000-B	Dark Avenger 3
V2P1	1260
V2P2	V2P2
V2P6	V2P6
V2P6 Trash	V2P6
V2P6Z	V2P6
V920	Datalock
Vacsina	Vacsina
Variable	1260
VB Trackswap	Trackswap
VCL	Virus Creation Lab
Vcomm	Vcomm
VDIR	VDIR
Venezuelan	DenZuk
Vera Cruz	Ping Pong
VGA2CGA	AIDS
VHP	Monxla A
VHP related (?)	Lisbon
VHP-348	VHP
VHP-353	VHP
VHP-367	VHP
VHP-435	VHP
Vien6	Vienna
Vienna	Vienna
Vienna 348	Vienna 348
Vienna 353	Vienna 353
Vienna 367	Vienna 353
Vienna 435	Vienna 353
Vienna 623	Vienna 353
Vienna 627	Vienna 353
Vienna 656	Lisbon
vienna family	C-544
Vienna-B	Vienna
Vienna-B645	Vienna
Viki	Viki
Virdem 2	Burger
Virdem 792	Burger
Virus 101	Virus 101
Virus Creation Lab	Virus Creation Lab
Virus-90	Virus-90
Virus-B	Friday 13 th COM
Vlad the Inhaler	Vlad the Inhaler
Voice Master	Voice Master
Voronezh	Voronezh
Voronezh B	Voronezh
Voronezh-1600	Voronezh
W13	Toothless
W13-A	Toothless
W13-B	Toothless
Warrier	Warrier
Whale	Whale
WIPEOUT	DRPTR
Wordswap 1385	Wordswap 1485
Wordswap 1485	Wordswap 1485
Wordswap 1504	Wordswap 1485
XA1	Christmas
Yale	Merritt
Yankee Doodle	Yankee Doodle
Yankee Doodle 44	Yankee Doodle
YAP	Cascade
Year 1992	EUPM
yes	Dada
Z The Whale	Whale
Zapper	Stoned
Zaragosa	CAZ
ZBug	Zero Bug
Zeleng	Dark Avenger
Zero Bug	Zero Bug
ZeroHunt	ZeroHunt
ZIP Trojan	PKZIP Trojan 1

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description	Virus Name/Alias	Name in Description

Type Definitions Table

Type definitions: The type of a computer virus is a classification based on how it operates, how it infects files, or where it hides in memory.

Types	Description
Program.	A program virus attaches itself to a program and is activated when that program is run.
Boot sector.	A boot sector virus hides in the boot sectors of a floppy or hard disk. Viruses of this type also include those that hide in a hard disks partition table. A boot sector virus is activated whenever a machine is booted with an infected disk.
Companion program.	A companion program is a virus program with the same name as a .EXE program but with the .COM extension. Since .COM programs are run before .EXE programs, the virus is executed first. After executing, the virus program runs the .EXE program to make it appear that nothing is wrong.
Directory structure.	A directory structure virus hides in the sectors normally used by a disks directory.
Bogus CODE resource.	The virus is added as a new CODE segment on the Macintosh, and the jump table is patched to point to that new segment. For example when an application is infected with nVIR, the virus attaches a CODE 256 resource to the end of the application and changes the CODE 0 resource (the jump table) to jump to and execute the CODE 256 resource before executing the application. Most Macintosh viruses (today) are of this type for example: Scores, nVIR, INIT29.
Patched CODE resource.	The virus code is added to the end of the main code segment on the Macintosh, and either the first program instruction or the jump table is patched to point to the virus code.
Bogus INIT.	A system INIT on the Macintosh is executed at boot time before the operating system takes over. They are used to patch the system and change its functionality, which makes them ideal for a virus.

TYPE DEFS

Type Definitions Table

Bogus resource.	Mac viruses of this type install a changed version of a standard system resource in the call chain between a program and the system. When a program needs a resource, it looks in the last opened file first, and then proceeds to the first opened file (the system) until it finds the resource it wants. The last opened file is usually a document, followed by the application, the desktop file, the finder, and the system. A viral resource placed on any of these files will be used in place of the one in the system file.
Trojan.	This isn't a virus, but a program that does damage of some sort that masquerades as something else. For example, DRAIN2 erases your hard disk while you play the game.
Worm.	This isn't a virus or a Trojan. A worm is a stand-alone program whose only property is to creates as many copies of itself as possible.
Virus Authoring Package (VAP).	A package that can be used to create new and different viruses.
Vaporware Virus; not real.	This is a reported virus that turned out to be a hardware or software malfunction or a normal program acting in a suspicious way.
Other:	Programs that don't fit any of the other categories.

Features Definitions Table

Features definitions: The following table contains descriptions of virus special features such as how it hides from detection.

Features Types	Description
Direct acting.	A direct acting virus is one that only infects other files when the infected program is run. Trojans are also of this type. This is in contrast to memory resident programs that watch for triggers.
Memory resident; TSR.	A memory resident virus that loads as a TSR (Terminate and Stay Resident) program. A memory resident virus usually hooks some of the event traps from the operating system and uses those events to activate itself.
Memory resident; TSR above TOM.	A memory resident virus that loads at the TOM (Top of Memory). Most of these viruses then move the TOM down to make room for themselves, but a few don't. A memory resident virus usually hooks some of the event traps from the operating system and uses those events to activate itself.
Encrypted.	An encrypted virus has a small decryption segment, with the balance of the virus encrypted so key searches don't work.
Stealth; actively hides from detection.	A stealth virus uses one or more methods to hide from detection programs. A common method is to encrypt the programs with a changing encryption key, making it difficult to use key search programs. Another is to make infected files appear normal when they are accessed by other programs such as DIR, or a virus checker (the 4096 virus is this type). Another method is to hide in bad blocks on the disk, or in unused portions of COMMAND.COM so that file lengths don't change.
Polymorphic; each infection different.	Polymorphic viruses use different methods to hide for each infection. They will use variable encryption, and both boot sector and program virus infection methods. Viruses of this type are the most active stealth viruses.

Features Definitions Table

Disk Locations Definitions Table

Disk locations definitions: The following table describes where viruses hide on disk.

Disk Locations	Description
Floppy disk boot sector.	The virus hides in the boot sectors of a floppy disk. The original boot sector is moved and executed by the virus after the virus finishes running. Data disks can also spread boot sector viruses.
Hard disk boot sector.	The virus hides in the boot sectors of a hard disk. The original boot sector is moved and executed by the virus after the virus finishes running.
EXE application.	The virus hides in .EXE executable files, usually by attaching to the end of the application and placing a jump to the attached code at the beginning. After the virus code runs, it jumps back and executes the applications code.
COM application.	The virus hides in .COM executable files, but not necessarily COMMAND.COM, usually by attaching to the end of the application and placing a jump to the attached code at the beginning. After the virus code runs, it jumps back and executes the applications code.
COMMAND.COM	The virus hides in the COMMAND.COM system files, usually by attaching to the end of the application and placing a jump to the attached code at the beginning. Afte: the virus code runs, it jumps back and executes the applications code. COMMAND.COM viruses also have hidden in some of the blank areas within the application, so they don't increase its length.
Program overlay files.	The virus hides in .OVL overlay files, usually by attaching to the end of the application and placing a jump to the attached code at the beginning. After the virus code runs, it jumps back and executes the applications code.
Directory.	The virus hides in the sectors that normally contain the directory.

DISK LOCATION DEFS

Disk Locations Definitions Definitions Table

Hard disk partition table.	The virus hides in the partition table of a hard disk. The original partition data is usually stored in the virus or elsewhere and accessed by the virus when needed.
File Allocation Table (FAT)	The virus hides in the sectors that normally contain the file allocation table.
Bad blocks.	The virus stores itself on disk then marks the blocks where it hides as bad. A small fragment of the virus must be outside of the bad blocks to cause a jump to the code stored there.
Application programs and the Finder.	Most Mac viruses are transmitted by attaching to general applications, or to the Finder.
System program.	Most Mac viruses are passed from an infected application to the System, which then infects other applications.
INIT program.	INIT programs on the Macintosh run just after system startup to add functionality to the system. A virus posing as an INIT adds its own special functionality.
Desktop file.	Some Mac viruses (WDEF) attached to the Desktop file, and intercept system resource requests, replacing them with the viral resource. These viruses can be passed without running an application, but merely by inserting an infected disk in a Mac (the Finder opens and reads the Desktop file whenever a disk is inserted).
Document files.	A virus attaches to a document file (this works only in a Mac, so far).
HyperCard Stack.	The virus hides in a HyperCard Stack (Mac).
SYS System files.	The virus hides in .SYS files, usually by attaching to the end of the application and placing a jump to the attached code at the beginning. After the virus code runs, it jumps back and executes the applications code.

Damage Definitions Table

Damage definitions: These are the types of damage that a virus may inflict on the attacked system. This damage in not necessarily intentional on the part of the virus writer, but often is caused by bugs in the virus program. Damage does not always occur, as most viruses rely on a damage trigger of some sort, since immediate damage prevents the spread of the virus. Triggers include dates, and the number of times an infected program is run.

Damage Types	Description
Corrupts a program or overlay files.	Most viruses spread themselves by attaching to an application, damaging it. Viruses may actively seek to destroy specific applications (SCORES). Other viruses write information to a specific block on a disk, which destroys any file that might already be using that block.
Attempts to format the disk.	This is usually an intentional attempt to destroy all information on a disk.
Interferes with a running application.	Interference can be intentional or caused by bugs in the virus. Intentional interference consists of things like making the letters fall in a heap at the bottom of the screen (Cascade), playing music at odd times (Oropax), or inserting typos when specific keys are pressed (Typo). Unintentional interference consists of bugs in the virus code that cause things like printing problems or crashes (nVIR, SCORES).
Corrupts a data file.	Data files are corrupted either by changing their contents, overwriting them with viral code, or deleting them.
Corrupts the file linkages or the FAT.	The file linkages, the File Allocation Table (FAT), and the file directory control where a file is on disk, and how the blocks of data that make up the file are linked together. Some viruses actively overwrite the FAT, since it is an easy way to corrupt a disk. Others, actually hide the viral code in the directory.
Attempts to erase all mounted disks.	If files are simply erased, only the directory entries are lost and the files re recoverable. Other viruses encrypt the disk, which makes it unrecoverable (Disk Killer).
Encrypts the file directory.	The files themselves are still OK, but the directory entries are gone. The files are probably recoverable.

DAMAGE DEFS

Damage Definitions Table

Erases the Hard Disk.	If files are simply erased, only the directory entries are lost and the files re recoverable. Other viruses encrypt the disk, which makes it unrecoverable (Disk Killer).
Overwrites sectors on the Hard Disk.	Some viruses store things in specific sectors on the hard disk. If another file already used that sector, the file is destroyed. If the sector contains the FAT, directory or is the boot sector, all files may be lost.
Deletes or moves files.	The virus deletes or moves files on the disk.
Cracks/opens a BBS to nonprivileged users.	This is usually a Trojan with an inviting name that copies the user directory and password file to a directory where the virus writer can download it.
Erases a Floppy Disk	If files are simply erased, only the directory entries are lost and the files re recoverable. Other viruses encrypt the disk, which makes it unrecoverable (Disk Killer).
Corrupts floppy disk boot sector	Boot sector viruses place their virus code in the boot area of a floppy disk, and usually move the boot code somewhere else. This can also occur on a nonsystem disk.
Corrupts hard disk boot sector	Boot sector viruses place their virus code in the boot area of a floppy disk, and usually move the boot code somewhere else.
Corrupts hard disk partition table	The partition table tells the system where the logical disk drive is on the physical hard disk. The partition table includes code to be loaded into memory and used to do the actual partitioning of the disk. This code is loaded even before the system is booted, so a virus placed there gains control of the system before any virus protection software can be installed.
Corrupts boot sector	Boot sector viruses place their virus code in the boot area of a floppy disk, and usually move the boot code somewhere else.
OTHR This code is used for non-standard messages.	The code OTHR is used for non-standard messages where appropriate. It is not defined in this file so anything inserted as a description will not be replaced.
Does no damage.	This code does no damage at all, to any part of a machine.
No damage, only replicates.	This code does no damage either intentionally or unintentionally. It only replicates.
Unknown, not analyzed yet.	Unknown. The code has not been analyzed in sufficient detail to know if it can do damage.
Trashes the hard disk.	Trashes the hard disk in some way. Probably by overwriting, encrypting, or formatting.
Trashes the floppy disk.	Trashes the floppy disk in some way. Probably by overwriting, encrypting, or formatting.

DATE
FILMED
6 / 16 / 94

END