10_Past_3
Aircop
Akuku
Alabama
Albania
Ambulance
Amoeba
Anthrax
Anti-Pascal
Anti-Pascal_II
AntiCMOS
AntiMon
Arab
Aragon
Armagedon
Arusiek
Ash
Attention
Attitude
BUPT
BackFont
Backform
Bad_Boy
Bebe
Beech
Beer
Best_Wishes
Beta_Boys
Better_World
Beware
Billboard
Bing_Bang
Bizarre
Black_Jec
Black_Monday
Blood
Bomber
Boys
Brainy
Burger
Burghofer
Butterfly
CARA
CAZ
CLI
COM_Virus
CSL
Carioca
Casino
Casper
Chaos
Checksum
Cheeba
Cinderella

Cod
Coffe_Shop_MtE
Comasp
Copyright
Corrected_MtE
Crazy_Imp
Creeper
Crepate
Crew
Czech_Happy
DataCrime
Dedicated_MtE
Digger
Ear
Eight_Tunes
Encroacher_MtE
Explosion
Fear_MtE
Fifo
Finnish
Flip
Freew
Friday_13th
Frodo
Fumble
Geld_wasch
Groove_MtE
Haifa
Helloween
Howard_Stern
Hydra_II
J&M
Justice
KWZ
Kampana
Klepavka
Lao_Doung
Letter_H
Level_3
Lisa
MSK
Mange-tout
Minsk
Monika
Murphy
Nina
Number_of_the_Beast
On_64
One_Half
Page
Phi
Pieck
Pivrnec
Pixel
Plastic_Pizza

Pogue_MtE
Pojer
Poledne
Prague
Predator
Questo_MtE
Rage
Raptor
Relzfu
Sampo
Saturday_14th
Semtex
Ser_No
Seventh_son
Simulate
Slovakia
Slovakia_II
Smeg
Socha
StarDot
Susan
TPE
Tack
Ten_Bytes
Tequila
Thanksgiving
Tiny
Tiny-GM
Tiso
Tremor
Uruguay
V-Sign
Vic
Vienna
Vietnam
Voronezh
Yale
Yog-Sothoth
ZP

Virus Tremor

Tremor is one of the most interesting viruses around. It is strongly polymorphic, uses perfect stealth techniques, can defend itself from some antivirus programs and can place itself in HMA (High Memory Area).

The history of its spread is also worth mentioning. A program infected by Tremor was distributed through the data channel of the TV station PRO-7. Because Murphy's Law really works - the infected program was actually a popular antivirus program.

Contains coded text which sometimes displays:

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

Virus TPE

TPE is not actually a virus, but a code library used for making viruses. Usually contains this text:

```
[ MK / TridenT ]

[TPE 1.3]
```

Virus Aircop

Attacks BOOT the sector on diskettes. When attacking every eighth diskette the flashing text is displayed:

```
.RED STATE, Germ offensing  --Aircop
```

Virus Akuku

Family of non-resident viruses which usually attack COM and EXE files. For the most part they are not destructive.

Variant Akuku.899.B

Contains text `A kuku, Nastepny komornik !!!`, which it displays when started between 32nd and 35th minute of each hour. This mutation attacks COM files only.

Virus Alabama

Resident virus which attacks EXE files. Controls access from keyboard and if it detects the combination Ctrl+Alt+Del it restarts computer, but stays in memory and after approximately 30 seconds takes control again. If it stays in memory long enough for the system to increment the hour then it erases the screen and displays red flashing text:

```
+-------------------------------------------------------------------------+
¦SOFTWARE COPIES ARE PROHIBITED BY INTERNATIONAL LAW  XÛ¸DELnåÚÉ¢DEL 00009 ¦
¦                                                                         ¦
¦     °iødý}¸·DELDEL_É¢É¢É¢ DELDELDELDELDELBox 1055 Tuscambia ALABAMA USA      ¦
+-------------------------------------------------------------------------+
```

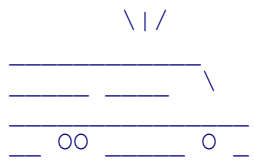
The number in the top left corner is the number of virus generation. It is not clear whether unsensible characters make any sense with peculiar type of display adaptor, or whether copy of the virus is damaged.

Virus Albania

Family of simple non-resident viruses which attach themselves to the end of COM files. They contain the text albania or ALBANIA. The virus does not display this text but uses it to identify already infected files.

Virus Ambulance

Simple non-resident viruses which attack COM files. From time to time they attract attention by driving an ambulance across the screen with the siren sounding.



Virus Amoeba

Resident virus which attacks COM and EXE files. Contains primitively coded text which sometimes displays on the bottom line of screen:

```
SMA KHETAPUNK - NOUVEL Band  A.M.O.E.B.A.  by  PrimeSoft Inc
```

Virus Anthrax

Multi-partite virus, which attacks the MBR of hard disks and EXE and COM files. Contains uncoded text:

```
(c) Damage, Inc.

1990

ANTHRAX
```

Anthrax tries to find original service of disk operations and uses many other undocumented operating system services to reduce the possibility of its discovery.

Virus AntiCMOS

This virus attacks the boot sector on diskettes and the partition table on hard disks. Sometimes erases the CMOS memory.

Variant AntiCMOS.LiXi

Contains the text:

```
I am Li Xibin!
```

Virus AntiMon

Non-resident virus attacking COM files. It tries to destroy computer protection programs. Their list is not coded in the virus body:

```
FLUSHOT3.COM
C:\PANDA
MONITOR.COM
TSRMON.COM
TSRMONEZ.COM
C:\BAT
```

Virus Anti-Pascal

Family of simple non-resident viruses which attack COM files.
Virus deletes files *.PAS and *.BAK.

Virus Anti-Pascal_II

Simple non-resident virus which attacks COM files and destroys files with extension ?A? (e.g. PAS, BAK). Most likely written by the same author as Anti-Pascal.

Virus Arab

Resident virus which attacks executed COM files. Occasionally destroys the MBR of hard disks so the operating system can be started from diskette only.

Virus Aragon

Virus of Czech origin which attacks the BOOT sector of diskettes and the MBR on hard disks. Contains text JMH which apparently are the initials of a tutor in the computer department at Brno University. Aragon is a stealth virus and is not destructive.

Virus Ash

Family of simple non-resident viruses which attack COM files only.

Variant Ash.1604

Occasionally bothersome with these texts:

```
I'm hungry!  Insert PIZZA & BEER into drive A: and
Strike any key when ready...

Impotence error reading user's dick

Program too big to fit in memory

Cannot load COMMAND, system halted

I'm sorry, Dave.... but I'm afraid I can't do that!

Format another? (Y/N)?

Damn it!  I told you not to touch that!

Suck me!'

Cocksucker At Keyboard error reading device CON:

I'm sorry, but your call cannot be completed as dialed.
Please hang up & try your call again.

No!

Panic kernal mode interrupt

CONNECT 1200

Okay, okay!  Be patient! ...

And if I refuse?

Fuck the world and its followers!

You are pathetic, man... you know that?

Cum on!  Talk DIRTY to me !!!

Your coprocessor wears floppy disks!

Joker! ver ÓÓ by TBSI!
Remember!  EVERYTHING's bigger in Texas!
```

Virus Attention

Simple resident virus which attacks COM files only. At the beginning of victim files it inserts the uncoded text:

```
ATTENTION  !
```

If an error occurs accessing a disk, Attention tries (regardless where the error occurred) to reset the floppy drive A:.

Virus Attitude

Variant Attitude.827

A simple virus which looks for and attacks COM files.
Occasionally erases the first sector of disk C:, alternatively
destroys files `C:\CONFIG.SYS`, `C:\AUTOEXEC.BAT` and `C:\COMMAND.COM`.
Sometimes overwrites file `C:\DOS\KEYB.COM`.

Contains this message:

```
I hereby annex this sector as the property of IR!
Red Mercury (c) '94 The Unforgiven/Immortal Riot
```

Virus BackFont

Family of resident viruses attacking EXE files when opened. Some play non-destructively with the video card only and some occasionally destroy system regions of hard disk.

Variant BackFont.905

Beginning twenty seconds after this mutation is loaded into memory and every ten seconds thereafter it turns around characters on the screen. This effect is performed only if you have an EGA graphics card and the virus has been present on your computer at least three months.

Virus Backform

Resident virus which attacks COM and EXE files while copied to diskette. It tries to attack only COMMAND.COM immediately, so the chances of spreading are increased. It does not attach to this file but writes in it's data areas so the size is not increased.

When attacking COM files which begin with a jump instruction then the beginning is left alone and a jump to itself is written where the first jump points to.

Backform does not attack files beginning with letters AI.

This text is visible in the body of the virus:

```
c:\command.com
```

Backform controls diskette operations and when formatting the order of sectors is changed. If it survives to the twentieth generation then this function is turned off in the first half of a year.

Virus Bad_Boy

Family of simply encrypted viruses, which attack COM files when opened. Occasionally display this text and halts the system:

```
The bad boy halt your system .....
```

Contain uncoded text:

```
The Bad Boy virus, Copyright (C) 1991.
```

Bad_Boy is (although in an unusual way) polymorphic. It can randomly organise its eight parts, which are then called through a "table of services".

Virus Number_of_the_Beast

Resident stealth virus which attacks COM files. It is programmed in a very interesting way, uses many undocumented MS-DOS services, and is very small for what it does. Originally it was written for MS-DOS 3.30 only and could not function properly with other versions of DOS. Nevertheless there are many variants, which differ in their details and allow its spread under other DOS versions. Some variants contain the text `666`, which is only visible when the virus is not resident.

No destructive mutation function is known but the way it attacks files can lead to unrecoverable damage.

Virus Bebe

Family of simple non-resident viruses which attack all files in the current directory.

Variant Bebe.1004

This variant installs a small resident part which is sometimes bothersome with the message:

```
+------ VIRUS! ------+
¦ Skagi "bebe" >     ¦
+--------------------+
```

If you answer with requested word the virus will explain:

```
+------ VIRUS! ------+
¦     Fig Tebe !     ¦
+--------------------+
```

Bebe contains several errors which prevent it spreading to new types of computer and which can cause the system to hang after opening an infected program.

Virus Beech

Resident virus which attacks COM files currently opened or being opened. Contains neither text nor any destructive action. It is an ideal example of a virus which cannot be properly described.

Virus Beer

Family of resident viruses of Russian origin. Attacks EXE and COM files. Part of the virus is trivially encoded. It occasionally plays some music and destroys files used by antivirus software.

Variant Beer.3192

Contain coded text `Ceøšac íÛ »šóàa`, which it occasionally displays while playing music. With this text it overwrites some files:

```
DISKDATA.DTL
VIRUSES.INF
A-DINF-_.___
DIRINFO
```

Does not attack `COMMAND.COM` and `AIDSTEST.EXE`.

Virus Best_Wishes

Family of resident viruses which attack both EXE and COM files.
Sometimes destroys hard disk system regions.

Variant Best_Wishes.1024

Every fifth generation of this virus reduces information returned about hard disk size. On Friday 13th it sets the size to zero and displays message:

```
With Best Wishes!
```

This text is visible at the end of virus body:

```
This programm ... With Best Wishes!
```

Virus Beta_Boys

Resident viruses which attack opened COM files. The way it resides in the memory is far from being good mannered and can cause the system to hang.

Variant Beta_Boys.Mud

Every time an infected program is run the grey colour on the screen is darkened by one degree (on VGA card only). Contains simply coded text, which is never displayed:

```
Mexican Mud (c)1992 MaZ
The BetaBoys Development Corp.
+Sweden+
```

Variant Beta_Boys.Rattle

If active between 24.00h and 01.00h it starts in a never ending loop very quickly shifting the contents of the screen to left and right. Contains simply coded text which is never diplayed:

```
DEATH RATTLE V1.OO
(c)1992 The BetaBoys Development Corp.
+S+W+E+D+E+N+
```

Virus Beware

This virus attacks COM files in the current directory. If the first day of the month is a Monday it tries to overwrite diskette in drive A:. Contains , but does not display, uncoded text:

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

Virus Bing_Bang

Simple virus which looks for and attacks COM files. If it is activated on 1st January, then it destroys the hard disk partition table. (The author probably wanted to mark the disk as not accessible, but did not "hit" the correct places of the MBR).

Contains (but does not use) these texts:

```
[Big Bang]
(c) 1993 Evil Avatar
```

Virus Billboard

Simply coded virus which looks for and attacks COM files. Contains these powerful messages:

```
Billboard 1.0, (c)1993 SlþþzþÞ [Nuke].
Jeff K. - You are a lying prick, just like all politicians
Patty   - This was written from the ground up, in Australia
Alan    - You are wasting your time chasing Rock Steady
Frisk   - Pull your head out of your ass, [NuKE] is way ahead
          of you AV wankers
Johnny  - Scan is just too lame to worry about ha ha
```

Virus Bizarre

Resident polymorphic stealth virus which attacks COM files.
In the body of the virus the following text:

```
Bizarre by Dreamer
```

Virus Black_Jec

Family of simple viruses attacking all COM files in the current directory. In the body of virus there is usually the text `*?.com`.

This is another virus which has nothing of interest about it.

Variant Black_Jec.Sad.307

If activated in September it displays:

```
Sad virus - 24/8/91
```

and tries to format first sector of the current disk.

Virus Black_Monday

Unpleasant resident virus attacking both COM and EXE files.
Contains code to format disks which is not activated on a Monday
but depends on an internal counter of infected files.

Variant Black_Monday.Black_Monday.A

Contains this uncoded text:

```
Black Monday 2/3/90 KV KL MAL
```

Virus Blood

Non-resident virus which attacks all COM files in current directory. Contains uncoded text:

```
File infected by BLOOD VIRUS version 1.20
```

Which it displays with a 25% probability when an infected file is opened.

Virus Boys

Simple non-resident virus which attacks COM files in the current directory. For reasons known only to the author, it marks the first EXE file as a system file.

Contains this uncoded text:

```
The good and the bad boy.
```

Virus Brainy

Resident virus which attacks loaded COM files. It is trivially encoded and contains the text `The WARRIER!`. If the victim begins with a jump instruction Brainy does not insert itself at the beginning of the file but at the place where this jump points to.

Virus Butterfly

Primitive non-resident virus which attacks COM files. Contains but does not display this text:

```
Hurray The Crusades
```

Virus BUPT

Resident virus which attacks opened COM and EXE files. Contains uncoded text which it sometimes displays for a moment:

```
!!!-->> Traveller (C) BUPT  1991.4  Don't  panic I'm harmless <<--!!!
```

If any program looks for free hard disk space, BUBT takes this as request to attack more files and complies.

Virus Burger

Family of very trivial non-resident viruses which overwrite COM files. Ralf Burger published the source code of this virus in his book in 1986 and so a large number of uninteresting mutations with small differences were made.

Variant Burger.Pirate

Contains uncoded text:

```
1989 / 1990 Software Pirates - Fast Serial - Portugal
```

Virus Burghofer

Resident virus which attacks loaded COM files. Does not contain any destructive action but nonetheless contains an error which can cause the system to hang. At the beginning of attacked files it inserts text `GS/02`, which is visible.

Virus CARA

Resident virus which attacks COM files while opening or executing. At the beginning of the virus body is the visible text `CARA` . CARA is a curious virus. When started it tries to identify typical signs of BOOT virus and if successful beeps and displays:

```
Virus es en memoria!

Clandestino
Auto-
Reproductivo
Anti-virus
```

It also checks diskettes and if it locates a BOOT virus of the Ping-Pong , Stoned, Brain, Microbes or Pentagon families, it will destroy it. An attempt to load the operating system from a diskette treated this way results in a beep and message:

```
Disco es infectado. Reemplaza "Boot".

Clandestino
Auto-
Reproductivo
Anti-virus
```

Virus Carioca

Resident virus which attacks loaded COM files. Does not attack files with an extension ending with a E (eg EXE) but does not check the contents of victims, so an infected program may be incapable of starting. Also does not attack COMMAND.COM and this text can be seen in the virus body. In the second half of November and December Carioca overwrites the contents of counter (used for memory refresh) every time a key is pressed. which serves for renovation of memory contents. This can cause memory errors and system to hang.

Virus Casino

Resident virus attacking COM files. If an infected program is started on 15th of January, April or August, the contents of your hard disk can be gambled for:

```
                DISK DESTROYER ¨ A SOUVENIR OF MALTA

            I have just DESTROYED the FAT on your Disk !!
   However, I have a copy in RAM, and I`m giving you a last chance
                     to restore your precious data.
  WARNING: IF YOU RESET NOW, ALL YOUR DATA WILL BE LOST - FOREVER !!
                Your Data depends on a game of JACKPOT

                    CASINO DE MALTE JACKPOT

                      +-+     +-+     +-+
                      Î¼Î     Î?Î     ÎŠÎ
                      +-+     +-+     +-+
                          CREDITS : 5


                      ¼¼¼ = Your Disk
                      ??? = My Phone No.

                      ANY KEY TO PLAY
```

If you manage to win in five goes, Casino congratulates you and recommends that you leave your computer switched off for the rest of the day. It is good advice, the second time you will probably not be so lucky.

```
BASTARD ! You`re lucky this time - but for your own sake, now
SWITCH OFF YOUR COMPUTER AND DON`T TURN IT ON TILL TOMORROW !!!
```

If you see these texts:

```
No Fuckin` Chance; and I`m punishing you for trying to trace me down !
HA HA !! You asshole, you`ve lost: say Bye to your Balls ...
```

This means that first 40KB of your hard disk is overwritten for ever.

Visible in the virus body are these texts:

```
*.COM
C:\COMMAND.COM
COMMAND .COM
```

Virus Casper

A simple virus which looks for and attacks COM files. If an infected file is started on 1st April, Casper tries to format your hard disk. This is promised by the text:

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

Virus CAZ

Resident virus which attacks both EXE and COM files when loading or opening. If it manages to locate COMMAND.COM in the root directory it attacks it first. When CLEAN is run it displays:

```
Virus anti-McAfee v1.0 (C) SEPTEMBER 1991  Made in SPAIN
```

Over-writing of the first hard disk's MBR follows.

The following texts are visible in the virus body:

```
EXECOM
C:\COMMAND.COM
CLEAN.
```

Variant CAZ.1204

Approximately thirty minutes after being loaded into memory it begins to rapidly (18 times per second) shift the screen left to right. The result is an unpleasant flicker which gives the impression that monitor is faulty.

Virus Chaos

Resident virus which attacks both COM and EXE files when loaded.

Variant Chaos.1241

When this virus is loaded the time is checked and if it matches a certain condition it decides to be naughty. (Probability that the condition is met is approx. 4.2%). It then monitors disk operations and with every fifth disk access overwrites few sectors. If all this happens in September and the disk is destroyed it introduces itself:

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

and ends in never ending loop.

Variant Chaos.1181

If the virus is activated on the 13th day in month, every fifth disk access overwrites several sectors and after 100 key presses it introduces itself:

```
CHAOS!!! Another Masterpiece of Faust...
```

In the last six days in the year the virus changes a value which is used to recognise whether a file has been infected, so one file can be attacked several times.

Virus Checksum

Family of resident viruses, possibly of Russian origin. All attack loaded COM files, some variants EXE files also.

Checksums uses self-checking and does not spread if it feels that it was somehow damaged.

Virus Cheeba

Resident virus which changes in an usual way and attacks both COM
and EXE files. Follows its creation (eg unpacking from archive
or copying), and while closing, attacks them. If it finds that
a program writes to disk characters containing part of word victim, then it leaves it alone. If
Cheeba finds that someone
manipulates files with name corresponding to complicated controlling
addition, uses this name as a key for decoding of special function.
The correct name is USERS.BBS and this file virus damages.
Unpleasant side effect of this method is, that it is possible
to find names which correspond with controlling addition, but when
used as a key, instead of correct code, only pack of noncece
instruction is created. Their execution can then lead to suspension
of operating system.

Variant Cheeba.A

Contains coded text:

```
CHEEBA Makes Ya High Harmlessly. F**K THE LAMERS
```

Variant Cheeba.B

Contains coded text:

```
CHEEBA Makes Ya High Harmlessly-1.1 F**K THE LAMERS
```

Virus Cinderella

Resident virus which attacks COM files when loading and opening. Occasionally creates file CINDERELLA and reboots computer. It is not destructive but the way it occupies memory can cause the system to hang.

The following text is visible in the virus body:

```
cInDeReL.la
```

Virus Cod

Simple resident virus which attacks loaded EXE files and is not at all interesting.

Virus Comasp

Simple resident virus. Attacks COM files when opening and loading.
The way it installs itself in memory is incorrect and can cause
the system to hang. In the viruses body is this uncoded text:

```
ASP
```

Virus COM_Virus

A simple virus which attacks COM files on diskettes. If an infected program is run, COM_Virus attracts attention with the following text:

```
This file infected with COMVIRUS 1.0
```

Virus Copyright

Resident viruses, which attack loaded COM files. It celebrates
important anniversaries by displaying a picture in text mode.
Copyright does not spread on computers with following BIOSes:

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

Variant Copyright.1193

As a reason to celebrate considers this dates:

23/2, 7/3, 22/4, 30/4 and 6/11
On these days the virus does not spread but slows down the screen
with stripes, waits for a key press and starts original program.
Apart from texts used for identification of computer BIOS it also
contains also text COM.

Virus Crazy_Imp

Family of resident viruses which attack COM files when opening or closing. They use stealth techniques when an infected file is being opened or closed, cure it, and once finished the virus attacks it again. The size of the infected file is distorted so at a glance it seems that everything is OK.

Variant Crazy_Imp.1445.A

In virus body is this text:

```
Crazy imp   v2.0
```

Virus Creeper

Family of resident viruses which attack COM files on being opened.

Variant Creeper.475

This variant monitors the screen and when it detects the word
`TORMENTOR!` (sign of some viruses of the Murphy family)
it reacts with overwriting the beginning of the hard disk.

Virus Crepate

Resident multi-partite virus of Italian origin. Attacks EXE, COM and OV? files when being loaded, opened, created or renamed. It ignores files which end with '`AN`' (eg SCAN) or '`LD`' (VSHIELD).

The virus body is encrypted, only three bytes from the end is the visible text '`cs`', with which Crepate recognises infected files. The decryption loop is constant, but contains large amount of random data, so at first glance it can be confused with polymorphic virus.

Crepate is written very well, which, unfortunately, applies to its destructive capabilities also. It is not satisfied with formatting the beginning of a hard disk but it makes an effort to find the disks parameters and tries to format the whole hard disk. Destruction is planned for 16th and 17th day of every month.

In the virus body are these texts:

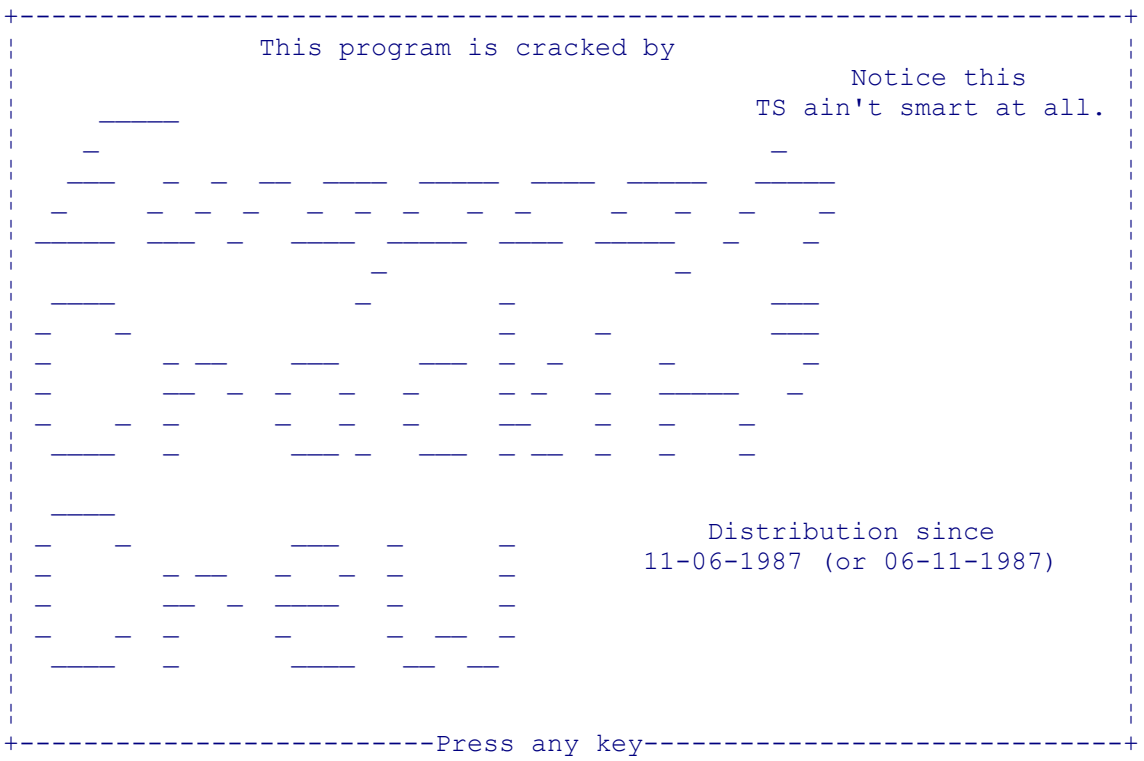
```
Crepate  (c)1992/93-Italy-(Pisa)

Crepa(c) bye R.T.

COMcomEXEexeOV?ov?
```

P.S.
Crepa means death.

Virus Crew

Family of non-resident viruses which attack COM files in current directory. To hide their presence they do nothing when activated with a probability of 70%.

From June to December they are sometimes bothersome with the text (which differs marginally in each mutation):



Virus CSL

Family of simple resident viruses which attack COM files when loaded and try to attack COMMAND.COM. These viruses are usually not destructive but the way they manage memory can conflict with the operating system.

Variant CSL.Pre_Release

This variant contains text:

```
26.07.91.Pre-released Microelephant by CSL
```

Variant CSL.V4

This variant contains text:

```
Microelephant V4ò by CSL
```

If activated on 1/1, 2/2, 3/3 etc it then erases the hard disk parameters in CMOS memory.

Variant CSL.V5

This variant contains text:

```
Microelephant V5 by CSL
```

Virus Czech_Happy

Resident virus of Czech origin which attacks both EXE and COM files when being opened. It contains trivially encoded childish texts with which it bothers in January from 1994:

```
* * * VY ZIRATE MY ZIRAME !!! * * *
Sorry, ale zbal to !
* Más slizkej Hárd, nemám ho rád, zkus to tak brát Baby *
A nyní nekolik pozdravu :
FUCK OFF AMIGA !  FUCK OFF ATARI ST !  FUCK OFF O.K.!
>> PRESS ANY KEY TO CONTINUE <<
```

On 1st January it always bothers, on any other day only after a certain number of calls to the operating system have been made.

Czech_Happy tries to avoid traps set by antivirus programs by not attacking files with the current date.

Virus DataCrime

Non-resident file virus which attacks COM files. Just before formatting the hard disk it introduces itself:

```
DATACRIME VIRUS
RELEASED: 1 MARCH 1989
```

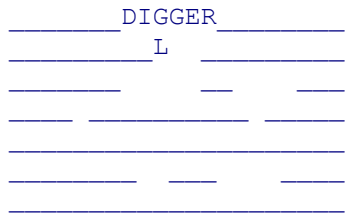
Then beeps in a never ending loop.

Virus Digger

Variant Digger.600

A simple resident virus which attacks loaded COM files. The way it installs itself in memory can lead to frequent hanging of the system. Due to an error, about 1% of files are attacked incorrectly.

Always at 10:00h and 17:00h it starts flashing in the top left corner of the monitor:



It contains the text:

```
DIGGER IS MY LOVE!
```

Virus Ear

A simple non-resident virus which attacks both COM and EXE files. Its source code was published in the 40Hex - an underground electronic magazine.

It is bothersome on the first day of every month when it asks where certain part of an ear is located:

```
PHALCON/SKISM 1992 [Ear-6] Alert!
Where is the  * located?
 1. External Ear
 2. Middle Ear
 3. Inner Ear
( )
```

In place of * one of the following is substituted:

```
Auditory Canal
Lobe
Anvil
Eustachian Tube
Auditory Nerve
Cochlea
```

It waits for a reply. If the reply is correct then:

```
Wow, you know your ears!  Please resume work.
```

is displayed.

An incorrect answer results in:

```
You obviously know nothing about ears.
Try again after some study.
```

and infected program does not run.

Apart from texts, which are part of the test, it contains the "signature" of author:

```
[Ear-6]
Dark Angel
```

The body of the virus is trivially encoded.

Virus Fifo

A simple resident virus which attacks COM files. It is not destructive but the way it installs itself in memory and the way it uses drives can lead to frequent system crashes. It contains but does not display:

```
FIFO
```

Virus Finnish

Variant Finnish.709

Resident virus which attacks COM files when loaded or opened. Contains many errors and oversights, which can lead to operating system crashes.

Virus Flip

Resident polymorphic virus which attacks loaded COM files (COM and EXE) and the hard disk partition. By tracing they try to find and use the original address of operating system services and in this way avoid some monitoring programs. They demonstrate their presence by 'flipping' the screen. Contains encoded text:

```
OMICRON by PsychoBlast
```

Variant Flip.2343

Displays itself on the second day of each month between 10:00h and 11:00h. It looks for a sequence of instructions which it modifies. It seems that the goal is to mask the increased size of the infected file. Considering that this sequence can be found in many files (eg COMMAND.COM and DEBUG.COM in MS-DOS 3.30 or DEBUG.EXE and CHKDSK.EXE in MS-DOS 5.00) this amendment can lead to occasional system crashes.

Same ending happens to amended files when loaded, if virus is not active in the memory.

Variant Flip.MBR

Introductor of some Flip virus.

Variant Flip.2153

Displays itself on the second day of each month between 10:00h and 11:00h, if the computer had been switched of at least twelve times since infection.

Virus Freew

Family of non-resident, relatively unpleasant viruses which attack COM files.

Variant Freew.718.A

Attacks COM files in all directories. Avoids programs `MKS_VIR.COM` and `COMMAND.COM`.

From 1993, always in January, it does not infect files created in even numbered hour, but destroys them. The destroyed program, when loading, displays:

```
Program terminated normally
```

and exits

Virus Friday_13th

Family of simple viruses which attack COM files (exept COMMAND.COM) in the current directory.

On Friday 13th they remove them selves from infected files together with their original contents.

Virus Fumble

A simple non-resident virus which attacks COM files in the current directory.

Although virus is not resident, it installs a stub in memory, which monitors keyboard activity and sometimes substitutes the pressed key with a neighbouring key.

In the virus body the keyboard map is visible:

```
`1234567890-=\
~!@#$%^&*()_+|
qwertyuiop[]
[asdfghjkl;'
zxcvbnm,./
QWERTYUIOP{}
ASDFGHJKL:";
ZXCVBNM<>?.
```

Also visible is virus mark 'V1' and the mask used to seek its victims, '`*.COM`'.

Virus Haifa

Family of resident polymorphic viruses which monitor directory searches and not only attack COM and EXE files, but also damage some data files.

Variant Haifa.B

The author of this virus probably had a hard disk with volume label AT_286. Providing it finds this label, it does not spread and does not attack data files. It demonstrates its presence on 8th April and 24th April, when while an infected program is opening, it displays with 1% probability:

```
HAIFA VIRUS V1.01
WRITTEN BY Y.S.
GUEST STARS: T.S. & I.F.
MADE IN ISRAEL
I AM TIRED. PLEASE WAKE ME UP ON TUE 12.4.3456
PRESS RESET TO CONTINUE...
```

At the beginning of files with extension PAS it inserts:

```
CONST VIRUS='HAIFA';
```

ASM files are modified with this text:

```
.model  small
.code
s:      mov     ax,310h
xor     cx,cx
mov     dx,80h
int     13h
end     s
```

In the middle of files with extension DOC and TXT it inserts:

```
OOPS! Hope I didn't ruin anything!!!
Well, nobody reads those stupied DOCS anyway!
```

Virus Helloween

Family of viruses of Czech origin. Resident file viruses which attack both COM and EXE files. Mostly they are not destructive. They do not attack files containing any of the following text groups:

```
3P.E, AHEL, ALIK, ASTA, AZOR, BOOT,
CLEA, COMM, DISK, F-PR, INI., KERN,
MAND, NAV., NC.E, PAST, PCC., REX.,
SCAN, SHIE, TRAP, TSAF, UCOM, UEXE,
VCOP, VIRT, VIRU, VS.E, WIN.
```

This table changes marginally in each variant, in some it is not included at all. Viruses from the Holloween family usually contain simply encoded text, which on a specified day (differs according to mutation) RESETS the system.

Variant Helloween.1684

Does not attack COM files and does not avoid antivirus programs. Contains this text:

```
Do you work with DOS ?
Do you like free memory ?
Do you like space on disk ?
YOUR    SOLUTION    IS
The Volkov Commander
You can drive it like Norton Commander 4.0
The SIZE of Volkov Commander is ONLY 62 KB!
The VC brings many new functions!
All actions of VC are very quick!
The VC is ShareWare but please
don't make black copies, it's not fair.
```

Variant Helloween.2470

Every month on 5th and 24th it displays this text:

```
                                        -m
                                        -Ï-Ï-Ï-   zdrojovy
                                         ¦ ¦ ¦     text:
                                        -ð-ð-ð-  867 radku

                                        & spol.

              (c) 1993 II.A 1988

          Specialne pro ucitele SPS Prostejov:
 Ing. M. Zaka, Ing. J. Melku, Ing. P. Cizka, Ing. K. Kabrhela
 Ing. M. Blahu, Ing. M. Pavlovskeho a dalsi vyucujici.
```

```
            Specialni podekovani patri:
   Macrosoftu (sorry Microsoftu)  za MeSsy DOS
   Borlandu                       za TASM, TLINK, TD
   Zdenku Breitenbacherovi        za EDDIE 1.17
```

Variant Helloween.1063

Does not attack COM files and does not try to avoid antivirus programs.

Variant Helloween.1376.A

First (and most widely spread) mutation of Helloween. It contains simply encoded text which is displayed on 1st November:

```
  Nesedte porad u pocitace a zkuste jednou delat neco rozumneho!

                      ******************

     !! Poslouchejte HELLOWEEN - nejlepsi metalovou skupinu !!
```

Variant Helloween.1376.B

Marginally modified Halloween.1376.A. On 21st February it displays this text:

```
  Zdravim uzivatele pocitacu hlavne vsechny LENKY a nejvic tu nasi!

        Preji ti vsechno nejlepsi k tvemu svatku ahoj
```

Variant Helloween.1839

A wide-spread mutation. Contains text which it never displays:

```
           Virus napsany specialne pro inzenyra ZAKA ze SPS
                         ******************
        Nepodlehejte panice, mate nakazeno jen par souboru...
                         (c) 1993 II.A 1988

             Tak a ted si vyzkousime treba: RESET

Kdyby kazdy nespokojeny student napsal virus, tak v nasich skolach by
       ani jiny software nekoloval a McAfee by se divil...
```

Virus Howard_Stern

Exceptionally stupid non-resident virus which attacks COM files.
If an infected program is opened between 06:00h and 11:00h it displays:

```
I'm not working until Howard Stern is done @ 11:00 am !
Bow down before the King      Smile ... [NuKE] loves you
```

and hangs the system.

The virus is overloaded with huge errors, which are very likely to crash the system even before it can spread.

Howard_Stern contains these texts:

```
I'm not working until Howard Stern is done @ 11:00 am !
```

(This is not mistake, this text is really there twice!)

```
1234567890!@#$%^&*()ascii  (c) Ba Ba Stupid...
Remember Studderin' John  Robin, I love You!  Long Live [NuKE] ....
Georgia needs Howard Stern
```

Virus J&M

Simple viruses, which attack diskette BOOT sectors and the MBR of hard disks. Virus body is trivially encoded and at its end the visible text `J&M`.

Contains unpleasant destructive action - formats the beginning of C: drive.

Variant J&M.A

Destructive action is planned for 15th November.

Variant J&M.B

This variations sequence of instructions in the decryption loop are just swapped around and its destructive action is postponed until 15th April. Otherwise is identical to J&M.A.

Variant J&M.C

This variations sequence of instructions in the decryption loop are just swapped around, the text `J&M` is changed to `R&Z` and its destructive action is postponed until 12th November.

Virus Justice

Resident virus which attacks COM files when loading or opening. It is written specifically for MS-DOS versions 3.10 and 3.30. Due to this it can called constant addresses for secure calling of some operating system services (and avoid thus monitoring programs). Under newer versions of MS-DOS the virus doesn't spread.

Attaches itself to the end of its victim, but COMMAND.COM is attacked by inserting itself into the data regions thereby not changing its size.

Infected files start with two instructions NOP (90h).

In the virus body are these texts:

```
AND.BIO.DOS..COM.EXE\COMMAND

...AND JUSTICE FOR ALL
```

Contains extremely unpleasant destructive action. Monitors writing to the disk and with probability of about 0.4% writes not only to the correct place but also "one track lower".

Virus Kampana

An interesting family of Spanish origin which comment on the quality of Spanish Telecom services. Kampana is not a multi-partite virus in its true meaning. It attacks COM files and releases a bootvirus, which lives its own life and is not capable of infecting files.

Kampana masks the increased length of infected files and attacks loaded (in some versions even opening) programs. It tries to trace original addresses of DOS services of some system functions (int 13h and 21h) and then use them. By taking over interrupt 21h it tries to mask itself by having in its body several different bridges leading to the real access point of service and it randomly selects which one to use. The body of the virus (only part in variant Kampana.3445) is encoded and it contains (but doesn't use) a short text.

The bootvirus calculates how many times the system has started and once a set value is reached , the hard disk overwritten.

Variant Kampana.MBR.A

Contains text:

```
Campaòa Anti-TELEFONICA (Barcelona)
```

Destruction begins after 400 boots from an infected hard disk.

Variant Kampana.MBR.B

Contains text:

```
Anti-TELEFONICA 2 (CSFR)
```

Destruction begins after 400 boots from an infected hard disk.

This variant was probably created by modification of the bootvirus. We do not have information about the existence of a file virus which would be the carrier of this bootvirus variant.

Variant Kampana.MBR.C

Contains text:

```
Campaòa Anti-TELEFONICA (Barcelona)
```

Destruction begins after 333 boots from an infected hard disk.

Variant Kampana.3445

Contains text:

```
(C) 1990 Grupo HOLOKAUSTO (Barcelona, Spain)
Kampaòa Anti-TELEFONICA: Mejor servicio, Menores tarifas...
```

It is a carrier of the bootvirus Kampana.MBR.A.

Variant Kampana.3784

Contains text:

```
Virus Anti - C.T.N.E. v2.10a. (c)1990 Grupo Holokausto.
Kampanya Anti-Telefonica. Menos tarifas y mas servicio.
Programmed in Barcelona (Spain). 23-8-90. - 666 -
```

It is a carrier of the bootvirus Kampana.MBR.C.

Variant Kampana.3700

Contains text:

```
Virus Anti - C.T.N.E. (c)1990 Grupo Holokausto.
Kampanya Anti-Telefonica. Menos tarifas y mas servicio.
Programmed in Barcelona (Spain). 23-8-90. - 666 -
```

It is a carrier of the bootvirus Kampana.MBR.A.

Virus Klepavka

Resident virus of Czech origin, which attacks COM files when loading and the first three when locating.

On 18th February it displays:

```
        KLEPAVKA VIRUS
        **************
  Thank you for reproduction
```

and starts to shake the computer screen.

Virus Lao_Doung

This virus attacks the BOOT sector on diskettes and the MBR of hard disks. An infected computer, with a probability of 0.8%, plays a melody.

Virus Letter_H

Variant Letter_H.446

Short resident virus which attacks loaded COM files (except COMMAND.COM). Victims are marked by substituting the character 'H' for the forth byte in the file.

It is not destructive function and does not contain text. The way the timer is used makes tracing of infected file more difficult.

Virus Level_3

Resident polymorphic virus of Slovak origin. It seems that it is another creation from the author of One_Half which is very successfully spreading all over the world).

Level_3 attacks loaded EXE and COM files. It monitors files and attacks when a new file is closed.

It recognises victims by the odd (but variable) date and time of their creation and masks their size increase so that DIR reports the original size. To detect similar viruses a simple program can be used, which controls the date and time of files. This method is not very reliable, but as a last resort can be helpful. The author probably took this into account as not every infected file is marked, about 4% keep the correct values.

This is not the only way of hiding itself. The resident parts of some well known antivirus programs are detected and switched off. It does not attack files which begin with:

`SCAN`, `VSHIELD`, `CLEAN`, `FINDVIRU`, `GUARD`, `VIVERIFY`, `TB`, `-V`, `VIRSTOP`
`NOD`, `HIEW`, `PASCA`, `NETENVI` nebo `F-PROT`

When F-PROT or CHKDSK is loaded, the virus retreats, stops attacking and masks the size of already infected files.
If something starts to check memory , it learns that its owner is COMMAND and the beginning of the viruses body contains the text `* EMM 1.0 *`, which could convince that it is a correct part of system. Part of its fight against simple defence mechanisms is the way with which it finds its presence in the memory. Doesn't use any system services calls, to which answer can be made by its resident copy, but also short simple program. (this would obviously prevent further spread.)

Every 25th generation displays on the seventh day in the month:

```
Welcome to the Explosion's Mutation Machine !
Dis is level 3.
```

In the body is also coded this string which it uses to recognise resident parts of antivirus program TBAV:

```
TBMEMXXXTBCHKXXXTBDSKXXXTBFI
```

Virus Lisa

Simply coded virus which looks for and attacks COM files.

Contains (but doesn't use) this loving nonsense:

```
love.girl.LISA.forever.666
(c) Metal Militia / Immortal Riot Sweden 24/12/93
Thunderclouds pass the sky, dreams & thoughts goes thrue
my mind.. winds of love, floods of hope, until the day,
when you'll be mine!.... Dedicated to Lisa Olsson who will
always be my passion my obsession and my infinite dream.
All i ever wanted, all i ever asked for.
Happy new year, yours Metal.....
```

Virus Mange-tout

This resident virus keeps most of its body in memory in encoded form. If any program tries to find free disk space, Mange-tout attacks a file of COM or EXE type in the current directory.

If the keyboard is untouched for at least an hour, the virus considers this unforgivable laziness and teaches you a lesson by formatting a randomly selected track on hard drive C:.

Virus Minsk

Resident virus which attacks both EXE and COM files when opening. When access to a .DBF file is detected it starts playing up. Every twentieth reading, instead of the correct contents, empty spaces are returned. Minsk inserts into the system table text, VO. Unfortunately in the place which other programs sometimes use. This could crash the system.

Whats more, it has several trivial errors, which possibly happened by misstyping the source code. (eg using number 21 instead of 21h and ignoring the NOT operator) These mistakes can cause infected programs to crash and considerably reduce the chances of spreading.

Virus MSK

Family of silly overwriting viruses. Liquidates EXE files in the current directory (some mutations also COM files) and attracts attention with some text.

Variant MSK.284

Contains text:

```
The Eternal Blaze Virus has been unleashed...Beware!       [JD]
```

Variant MSK.272.A

Contains text:

```
The Midnight Serial Killer is roaming in your computer...Beware! [JD]
```

Virus Coffe_Shop:MtE

Variant Coffe_Shop:MtE

Resident virus coded with the help of the MtE library. Attacks EXE files while opening and copying. If the name of the file begins with any of the following pairs of characters it prefers not to act:

```
SC
CL
VS
NE
HT
TB
VI
RA
FE
MT
BR
```

Virus contains these texts:

```
Amsterdam = COFFEESHOP!
MK1992

MtE 0.90ß
```

If activated on a Friday then, with 1/60 probability, it draws with semi-graphical characters a large sign LEGALIZE CANNABIS and a leaf.

Virus Corrected:MtE

Variant Corrected:MtE

Resident virus coded with MtE library . Attacks both EXE and COM files while opening. After at least half an hour of residing in memory it celebrates file infection with the text:

```
We dedicate this little virus to Sara Gordon,
who wanted to have it corrected--
learn to program before you touch M_t_e
```

Obviously contains this text:

```
MtE 0.90ß
```

This virus probably developed from the Groove variant. It contains code for file deletion but it is never used, and list I should use is substituted with empty spaces.

Virus Dedicated:MtE

Variant Dedicated:MtE.Cryptlab

This virus coded with the MtE library and attacks COM files in current directory. If it does not find any suitable file it can overwrite a randomly selected sector. It contains these texts:

```
CryPtLAB:  THE SELECT CHOICE FOR ALL YOUR  VIRUS
AND TROJANRESEARCH NEEDS! -URNST KOUCH.
*.*

MtE 0.90ß
```

Variant Dedicated:MtE.A

This virus is coded with the MtE library and attacks COM files in the current directory. If it cannot find any suitable file it can overwrite the contents of a randomly chosen sector. It contains these texts:

```
We dedicate this little virus to Sara Gordon
who wanted to have a virus named after her.

*.COM

MtE 0.90ß
```

Virus Encroacher:MtE

Variant Encroacher:MtE.A

This virus is coded with the MtE library and attacks COM files in current directory. It does not like 'Central Point Antivirus' and tries to erase its files (`C:\CPAV\CPAV.EXE` and `C:\CPAV\VSAFE.COM`). It messes up additional files created by this program (`chklist.cps`) by deleting them in such way that their renewal is difficult.

If started in the afternoon it locates and damages `*.EXE` files. Infected files reboot the system when executed. Apart from already mentioned texts it contains:

```
ENCROACHER is here

MtE 0.90ß
```

Virus Fear:MtE

Variant Fear:MtE

This virus is coded the MtE library and attacks COM files in the current directory. If it cannot locate any suitable file, it waits for key to be pressed. The author's intention was probably to display the following text, but it calls an incorrect operating system function:

```
You have nothing to fear except FEAR itself...
```

It also contains these texts:

```
Fear VirusCreated on 2-5-92 by PkaHerONEhpY

*.COM

MtE 0.90ß
```

Virus Groove:MtE

Variant Groove:MtE

Resident virus encoded with the MtE library. Attacks both EXE and COM files when started. If at least half an hour has passed since virus occupied memory it celebrates file infection with text:

```
Dont wory, you are not alone at this hour...
This Virus is NOT dedicated to Sara
its dedicated to her Groove (...Thats my name)
This Virus is only a test Virus therefor
be ready for my   Next  Test ....
```

Obviously it also contains the text:

```
MtE 0.90ß
```

In the virus body is list of files, which it tries to destroy:

```
C:\NAV_._NO
C:\NOVIRCVR.CTS
C:\NOVIPERF.DAT
C:\CPAV\CHKLIST.CPS
C:\TOOLKIT\FILES.LST
C:\UNTOUCH\UT.UT1
C:\UNTOUCH\UT.UT2
C:\VS.VS
```

Virus Pogue:MtE

Variant Pogue:MtE

Resident virus coded the MtE library. Attacks COM files when opening or copying. Contains this text:

```
TNX2DAV

Pogue Mahone!

MtE 0.90ß
```

If activated before 08:00h it plays music. On 1st May it celebrates with "International" song , regardless at what time it is opened.

Virus Questo:MtE

Variant Questo:MtE

Another out of many variants created by making small changes to
a demonstration virus which was distributed with the MtE library.
It attacks COM files in the current directory, if no suitable victim
can be found, it can try to erase a randomly selected sector.
If this happens on a Friday, the BOOT sector of disk C: is
overwritten with the text:

```
Questo sistema Å stato infettat
```

It also contains texts:

```
*.COM

MtE 0.90ß
```

Virus Murphy

Resident viruses which attack both EXE and COM files. Many marginally different mutations exist. Viruses from this family try to locate and use original disk services in ROM. That can prevent some resident guard programs from detecting suspicious activities (eg overwriting or formatting disks). Most mutations contain at the beginning, short uncoded text, which is sometimes displayed on the screen. Some show small faces running across the screen and some destroy data by overwriting or formatting part of the hard disk.

Variant Murphy.Delyrium.1778

In June it tries to erase files, damage data on hard disk and displays text:

```
Delyrium Virus - Created by Cracker Jack 1991
Copyright by Italian Virus Research Laboratory 1991

.....because the dead is not so far
....and the horror will be with you
```

Contains also text (c) IVRL 1991 (Ivrl Head Quarter, Milan Italy), which it never displays.

Variant Murphy.HIV

This text is displayed if started on a Saturday:

```
HIV Virus - Release 1.0
Created by Cracker Jack
(C) 1991 Italian Virus Laboratory
```

If it survives in memory at least sixteen hours, displays moving small face on screen.

Variant Murphy.Pest

If you try to open any EXE file on a Friday the virus displays:

```
Your PC is infected with the Intergalactic Pest!
```

If a COM file is opened on a Friday this text is displayed:

```
What a horrible program, i wish not execute it!
```

Opening COM file on Saturday leads to the following message:

```
I'm hungry!! Why don't you buy me a Cheesburger??
```

Also contains (but doesn't display) these texts:

```
(c) by Cracker Jack 1991 Italian Virus Research Laboratory
Created,Developed and Written by Cracker Jack, All rights reserved
Con questo virus dichiaro guerra a tutti i POVERI (ahhh quanto
sono poveri!) cosiddetti 'Virus Researchers' del globo...
provate a prendermi..ahahahah l'IVRL e'forte.....vincer.!!!!
Virus Writers di tutte le nazioni...uniamci!
```

Opening programs which end with either AN.EXE or HK.EXE will be understood as a polite request to format the hard disk, and virus will comply.

Variant Murphy.Finger

On Saturday displays:

```
Cannot remember what I was doing!!
Insert fingers in ears and reboot please
```

and tries to format several sectors of the hard disk.

Variant Murphy.Amilia.A

This text is displayed if started on Sunday:

```
AmiLiA I Virii - [NukE]
Released Dec91 Montreal
(C) NukE Development Software Inc
```

This text is also visible in the virus body, but is never displayed:

```
AmiLiA I Virii  -  [NukE] i99i   By Rock Steady/NukE
```

After surviving in memory for at least sixteen hours a small moving face is shown on screen.

Variant Murphy.AntiChrist

Does not contain or display text. Deletes files with extension ZIP.

Variant Murphy.Bad_Taste

On Mondays it displays:

```
Bad Taste Ltd.
'(C) 1991 by Odrowad Trow.....who am I???
```

and tries to format several sectors of the hard disk.

Variant Murphy.Cemetery

Contains the text `CEMETERY`, which it never displays. After surviving in memory for at least sixteen hours a small moving face is shown on screen. Serial links are monitored and if the character '1' is found a re-boot is attempted.

Variant Murphy.Diabolik

On Mondays displays:

```
Diabolik Ltd.
(C) 1991 by OdrowadŠTrow
```

and tries to format several sectors of the hard disk.

Variant Murphy.Erasmus

On Thursday it displays:

```
Gli Dei si mostreranno agli uomini,
Quando essi saranno autori di grande conflitto,
Prima il Cielo visto sarÏ con spada e lancia,
Che verso la mano sinistra porterÏ piÚ grande afflizione.

Alla rivoluzione del grande numero sette,
ApparirÏ ai tempi giochi d'Ecatombe,
Non lontano dalla grande etÏ del millennio
Coloro che entrarono usciranno dalle loro tombe.

Saint-Rémi, 14 dicembre 1533
```

and tries to format few sectors on the hard disk.

Variant Murphy.Murphy.1521

Contains this text which it never displays:

```
It's me - Murphy.
Copywrite (c)1990 by Lubo & Ian, Sofia, USM Laboratory.
```

After surviving in memory for at least ten hours a small moving face is shown on screen.

Variant Murphy.Murphy.1480

Contains text which it never displays:

```
It's me - Murphy.
Copywrite (c)1990 by Lubo & Ian, Sofia, USM Laboratory.
```

After surviving in memory for at least ten hours a small moving face is shown on screen.

Variant Murphy.Murphy.1284

Contains text which it never displays:

```
Hello, I'm Murphy.
Nice to meet you friend.
I'm written since Nov/Dec.
Copywrite (c)1989 by Lubo & Ian, Sofia, USM Laboratory.
```

Variant Murphy.Murphy.1277

Contains text which it never displays:

```
Hello, I'm Murphy.
Nice to meet you friend.
I'm written since Nov/Dec.
Copywrite (c)1989 by Lubo & Ian, Sofia, USM Laboratory.
```

Variant Murphy.Kamasya

On Tuesdays it displays:

```
Kamasya nendriya pritir
labho jiveta yavata
jivasya tattva jijnasa
nartho yas ceha karmabhih
```

Variant Murphy.Migram.A

On Saturdays iy displays:

```
+--------------------+
¦  MIGRAM VIRUS 1.0  ¦
¦    (C) 1991 IVL    ¦
+--------------------+
```

and tries to format a few sectors of the hard disk.

Variant Murphy.Migram.B

On Saturday it displays:

```
+--------------------+
¦  MIGRAM VIRUS 1.0  ¦
¦    (C) 1991 IVL    ¦
+--------------------+
```

and tries to format a few sectors of the hard disk.

Variant Murphy.Smack.1835

On Friday it asks `Is today Friday? (Y/N)` and if the answer is 'Y', displays `Sorry but on Fridays I wish not work!!` and finishes. Any other answer treats you to - `You are untruthful!! For punishment I` format your HD Fat!! and then formats parts of the hard disk. The contains but does not use these texts:

```
This virus was written in Italy by Cracker Jack 1991 IVRL
All rights reserved, please don't crack this virus!!
Special message to Patricia Hoffman: I love you!!!!!!!! SmackSmack!!
Can you give me your telephone number??? Ciao bellissima!
```

Variant Murphy.Swami.A

On 15th April it displays:

```
Bhaktivedanta Swami Prabhupada (1896-1977)
```

and tries to erase some files.

Variant Murphy.Tormentor.B

On 31st day in the month it tries to overwrite data on the hard disk. Contains uncooked texts:

```
NUKE! Mutation by Lixo, Sweden!
```

and

```
[Thanks DAv!] DEMORALIZED YOUTH!
```

which it never displays.

Variant Murphy.Tormentor.D

On 24th day in the month it tries to overwrite data on disk.

Virus On_64

Simple non-resident virus attacking COM files. If activated
at least sixty four times it destroys infected files and
the beginning of the hard disk.

Virus Page

Resident viruses attacking both COM and EXE files when loading, opening, renaming or changing attributes. They are the creation of a member of the group NuKE, an association of virus authors.

Variant Page.1206

Masks the increased size of its victims and contains a simple trick, which is supposed to prevent tracking of infected program.

Contains this text:

```
Let's EnSlave Australia Agian! - pAgE!
[NuKE] The Domination of old Australia
```

Variant Page.1221

This variant is polymorphic and masks the increased size of its victims. Tries to defend itself against antivirus programs. Does not attack SCAN, TBAV and F-PROT. Contains a simple trick, which is supposed to prevent tracking of infected programs. Looks for checksum files and erases them:

```
ANTI-VIR.DAT
MSAV.CHK
CHKLIST.CPS
CHKLIST.MS
```

Contains these texts:

```
[NuKE '95]  by pAgE!
[VIP v0.01]
```

Virus Phi

Attacks diskette BOOT sector and MBR of hard disk. If on booting, CapsLock is on and NumLock is off, the contents of the window in the middle of the screen is shifted down by one row and NumLock is switched on. When a diskette is attacked it displays the character Ý.

Virus Pieck

Polish resident multi-partite stealth viruses. Apart from COM and EXE files it also attacks the hard disk partition table.

Under certain conditions Pieck removes itself from the MBR and cures infected files.

Variant Pieck.2016

Removes itself from hard disk if some program calls disk services (Int 13h) and in registers AX and BX passes text `mgre`. Cures programs opened from diskette.

3rd March asks for password:

```
Podaj haslo ?
```

If the password is correct (`pieck`), the virus is polite:

```
Pozdrowienia dla wychowankow Pieck'a
```

Incorrect password gets this reply:

```
Blad !
```

and hangs the system.

Variant Pieck.4444

This variant obtains tracking them and it tries to prevent its detection by coding itself in memory.

If the word test is typed while the computer starts, then the virus displays some information about itself. For example:

```
Wersja.........2
Kodowanie......8
Licznik HD...112
```

If word `kaczor` is written then virus displays:

```
Zrobione.
```

and cures disk.

Infected files cures when loaded from diskette.

From 1995 installs on 3rd March function, which increases significantly system time speed and slowly splits monitor picture.

Similar effect can be achieved even without computer - by consuming sufficient level of alcohol.

Virus Pixel

Family of simple viruses attacking COM files in the current directory. Some mutations introduce themselves only after a set number of activations (text is visible in the virus body), destructive variants exist.

Viruses Pixel.Hydra represent unique chronicle. They are in reality development stages of simple virus.

Variant Pixel.257

Second generation, displays with 50% probability:

```
Fucking hell:You wet pussy
```

Variant Pixel.779

Fifth generation, with 50% probability, beeps when activated.

Variant Pixel.837

Fifth generation, with 50% probability, beams:

```
I love you so much!!!
                    -- Francis
```

Variant Pixel.847.RV1

Fifth generation, with 50% probability, displays:

```
En tu PC hay un virus RV1, y ésta es su quinta generación
```

Variant Pixel.852

Third generation, with 50% probability, displays:

```
ž¦ò Ôá éÀáòà« š °Òú«óš+ _á_à« !  ÂšÒ ó_šÌàš _ÈÒ Ôá »_Ò¦___«ø__ó« !
```

Text is probably Bulgarian, unfortunately due to unavailability of character composition the above text is not accurate.

Variant Pixel.Cancer

This is a "slimed down" mutation. It is not destructive contains no text.

Variant Pixel.Hydra.495

Contains this uncoded text:

```
HyDra-8   Beta - Not For Release.
Copyright (c)  1991 by C.A.V.E.
```

Overwrites EXE files with a short program, which when activated, displays:

```
Who is John Galt?
```

Variant Pixel.275

Second generation, displays with 50% probability:

```
Fucking hell:You wet pussy
```

Variant Pixel.277

Fifth generation, with 50% probability, reprograms internal counter of computer in such way, that it leads to system crash and message being displayed about hardware memory error.

Variant Pixel.283

Tenth generation, with 50% probability it displays after start up:

```
What a stupid you are !!!!!!!!
```

Variant Pixel.295

Fifth generation, with 50% probability, displays:

```
Program sick error:Call doctor or buy PIXEL for cure description
```

Variant Pixel.299

Fifth generation, with 50% probability, displays:

```
Program sick error:Call doctor or buy PIXEL for cure description
```

Variant Pixel.345.A

Fifth generation, with 50% probability, displays:

```
Program sick error:Call doctor or buy PIXEL for cure description
```

Variant Pixel.345.B

Fifth generation, with 50% probability, displays:

```
Program sick error:Call doctor or buy PIXEL for cure description
```

Variant Pixel.847.Pixel

Fifth generation, with 50% probability, displays:

```
Program sick error:Call doctor or buy PIXEL for cure description
```

Variant Pixel.847.Advert

Fifth generation, with 50% probability, displays advert:

```
Buy AMSTRAD it is THE CHEAPEST COMPUTER thatyou can buy
```

Variant Pixel.847.Hello

Fifth generation, with 50% probability, displays:

```
Hello, John Mcafee,please uprade me.Bests regards,Jean Luz.
```

Variant Pixel.847.Near_End

Fifth generation, with 50% probability, displays:

```
THE END IS NEAR!!  THE SIGNS OF THE BEAST ARE EVERYWHERE!!
```

Variant Pixel.850

Fifth generation, with 50% probability, displays:

```
Program sick error:Call doctor or buy PIXEL for cure description
```

Variant Pixel.854

Fifth generation, with 50% probability, displays:

```
ž¦ò Ôá éÀáòà« š °Òú«óš+ _á_à« !  ÂšÒ ó_šÌàš _ÈÒ Ôá »_Ò¦___«ø__ó« !
```

Text is probably Bulgarian, unfortunately due to unavailability
of character composition the above text is not accurate.

Variant Pixel.877

Ninth generation, with 50% probability, displays:

```
Sector not found error fucking defoult drive!
Please buy me a new disk drive!
```

Variant Pixel.899

After 1st April, with 50% probability, displays:

```
Fucking Hell: What a smelly ass hole!!Do you want to fuck it!!!
```

and tries to format beginning of diskette in A: drive.

Variant Pixel.892

Third generation, with 50% probability, displays:

```
Fucking Hell: What a smelly ass hole!!Do you want to fuck it!!!
```

and tries to format beginning off diskette in A: drive.

Variant Pixel.936

After 1st April, with 50% probability, displays:

```
Fucking Hell: What a smelly ass hole!!Do you want to fuck it!!!
 HaHaHa... What a Good Friday!!
```

and tries to format beginning off diskette in A: drive.

Variant Pixel.Hydra.340

Contains this uncoded text:

```
HyDra-4   Beta - Not For Release.
Copyright (c)  1991 by C.A.V.E.
```

Tries to restore address of control of disk operations.

Variant Pixel.Hydra.342

Contains this uncoded text:

```
HyDra-2   Beta - Not For Release.
Copyright (c)  1991 by C.A.V.E.
```

Tries to restore address of control of disk operations.

Variant Pixel.Hydra.343

Contains this uncoded text:

```
HyDra-2   Beta - Not For Release.
Copyright (c)  1991 by C.A.V.E.
```

Sets a sign in the area of memory dedicated to Microsoft Basic and immediately after that calls for a disk reset. Could be that it tries to interact with another virus.

Variant Pixel.Hydra.368

Contains this uncoded text:

```
HyDra-7   Beta - Not For Release.
Copyright (c)  1991 by C.A.V.E.
```

Destroys EXE files in current directory.

Variant Pixel.Hydra.372

Contains this uncoded text:

```
HyDra-6   Beta - Not For Release.
Copyright (c)  1991 by C.A.V.E.
```

After file is attacked tries to destroy COMMAND.* files.

Variant Pixel.Hydra.391

Contains this uncoded text:

```
HyDra-5   Beta - Not For Release.
Copyright (c)  1991 by C.A.V.E.
```

After attacking files it directly calls some services of older types of disk controller. Its exact meaning was not identified.

Variant Pixel.Hydra.403

Contains this uncoded text:

```
HyDra-1   Beta - Not For Release.
Copyright (c)  1991 by C.A.V.E.
```

Introduces itself when attacking files:

```
HYDRA
Copyright (c)  1991 by C.A.V.E.
```

and amends the interrupt table so that system could crash.

Variant Pixel.Hydra.736

Contains this uncoded text:

```
HyDra     Beta - Not For Release.
Copyright (c)  1991 by C.A.V.E.

Coalition of American Virus Engineers
-=-=-
Dedicated to supporting the anti-virus
industry without recognition or reward.
-=-=-
```

After attacking files displays:

```
HYDRA
Watch for the many heads.
The first eight are easy to find and kill.
Their replacements will be more sophisticated.
(c) 1991  -  C. A. V. E.
```

Virus Plastic_Pizza

Resident virus attacking loaded COM files. Part of the data in its body is boot virus Stoned.Michelangelo.E, which Plastic_Pizza inserts into BOOT sector of hard disk.

Virus Pojer

Family of viruses of Czech origin. Attack both EXE and COM files when loading. Body of the virus is simply coded and decoding loop contains changeable parts. Just at the end of the virus is uncoded text "XmY?!&", which Pojer uses to recognise already infected files.

Variant Pojer.1941

17th November and 6th February displays:

```
   **  B R A I N  2  v1.00  **

WARNING ! Your PC has been WANKed !

>> 17.11.1989 <<

Viruses against political extremes , for freedom and
parliamentary democracy.

>> STOP LENINISM , STOP KLAUSISM , STOP BLOODY DOGMATIC IDEOLOGY !! <<

Remarks:
 - for John McAfee: John,your SCAN = good program.

 - for CN and his company:
   Boys,the best ANTI-VIRUSES are Zeryk,Saryk and Vorisek !

 - for F : Girls are better than computers and programming !

This program is copyright by  SB SOFTWARE  All rights reserved.

O.K. Your PC is now ready !
```

Sometimes flashes in top left corner character '_'.

Variant Pojer.1919

On 17th November and 6th February displays:

```
   **  B R A I N  2  v1.40  **

WARNING ! Your PC has been WANKed !

>> 17.11.1989 <<

Viruses against political extremes , for freedom
and parliamentary democracy.

>> STOP LENINISM , STOP KLAUSISM , STOP BLOODY DOGMATIC IDEOLOGY !! <<

Remarks:
```

```
 - for John McAfee: John,your SCAN = good program.

 - for CN and his company:
   Boys,the best ANTI-VIRUSES are Zeryk,Saryk and Vorisek !

 - for F : Girls are better than computers and programming !

This program is copyright by  SB SOFTWARE  All rights reserved.

O.K. Your PC is now ready !
```

Sometimes flashes in top left corner character '_'.

Variant Pojer.1935

17th November and 6th February displays:

```
   **  B R A I N  2  v1.00  **

WARNING ! Your PC has been WANKed !

>> 17.11.1989 <<

Viruses against political extremes , for freedom and
parliamentary democracy.

>> STOP LENINISM , STOP KLAUSISM , STOP BLOODY DOGMATIC IDEOLOGY !! <<.

Remarks:
 - for John McAfee: John,your SCAN = good program.

 - for CN and his company:
   Boys,the best ANTI-VIRUSES are Zeryk,Saryk and Vorisek !

 - for F : Girls are better than computers and programming !

This program is copyright by  SB SOFTWARE  All rights reserved.

O.K. Your PC is now ready !
```

Sometimes flashes in top left corner character '_'.

Variant Pojer.1949

17th November and 6th February displays:

```
   **  B R A I N  2  v1.60  **

WARNING ! Your PC has been WANKed !

>> 17.11.1989 <<

Viruses against political extremes , for freedom and parliamentary
democracy.
```

```
>> STOP LENINISM , STOP KLAUSISM , STOP BLOODY DOGMATIC IDEOLOGY !! <<

Remarks:
 - for John McAfee: John,your SCAN = good program.

 - for CN and his company:
   Boys,the best ANTI-VIRUSES are Zeryk,Saryk and Vorisek !

 - for F : Girls are better than computers and programming !
```

Sometimes displays in white on red background text:

```
Zruste armadu a jdete domu!!
```

Virus Poledne

Resident virus of Czech origin. Attacks both EXE and COM files when loading. Contains coded text Ja jsem Karlik2 which it uses to recognise already infected files.

At 12:00h clears screen and displays:

```
Casove znameni oznami dvanact hodin.
```

Waits several seconds, beeps and displays:

```
Casove znameni oznamilo dvanact hodin.
```

To avoid some checking programs, Poledne tries to find and use the original address of interrupt 21h.

Virus Prague

Family of resident viruses attacking loaded COM files and mutations differ in their external appearance only.

Variant Prague.BackTime

Contains text:

```
BackTime
```

If virus is in memory, system time goes backwards.

Variant Prague.Blinker

Contains text:

```
Blinker
```

Sets display card register display cards ignore this setting.

Variant Prague.Joker

Contains text:

```
Joker
```

Every 14 seconds it damages the contents of one processor register. The results of this vandalism are unpredictable. Ranging from "odd" program behaviour to an operating system crash.

Variant Prague.Shaker

Contains text:

```
Shake
```

Randomly amends the contents of display card register "Vertical Total Adjust". Modern display cards ignore this.

Virus Predator

Resident virus attacking COM files when loading and opening. If active in memory, masks increased size and data change of its victims. In the body is coded text which is never used:

```
Predator virus  (c) Mar. 93  Priest
```

Predator monitors reading from disk and occasionally changes value of a randomly selected bit.

Virus Rage

Variant Rage.575

This virus attacks COM files in both the root and current directory. Stops spreading if it detects the presence of 'FluShot'. When activated, with 5% probability, displays:

```
Pray for death - RABID '91
```

On the thirteenth day in the month it displays:

```
Rage - RABID Int'nl Development Corp.
By Data Disruptor - Thanks to Zodiac
```

and destroys beginning of disk C:.

Virus Raptor

Resident virus of Czech origin. Attacks EXE files when loading or opening. If day value equals month value (eg 1st January, 2nd February etc) and it is not December then the text is displayed.

Variant Raptor.B

Displays this text:

```
                The Raptor virus version 1.7
           Copyright 3.12.1993 - Hacker club Brno - Czech republic
  Don`t panic!! This virus doesn`t destroy data! I am most kindly virus!!
I should inform you that soon comes Raptor2.0 with special sealth systems
           You can be sure that Raptor2 will be totally untouchable!
```

Variant Raptor.C

Displays this text:

```
                The Raptor virus version 1.4
           Copyright 3.12.1993 - Hacker club Brno - Czech republic
  Don`t panic!! This virus doesn`t destroy data! I am most kindly virus!!
I should inform you that soon comes Raptor2.0 with special sealth systems
           You can be sure that Raptor2 will be totally untouchable!
```

Thirteenth day in a month, approximately 55 minutes after starting, moving blue rectangles appear on screen.

Variant Raptor.A

Displays this text:

```
                The Raptor virus version 1.5
           Copyright 3.12.1993 - Hacker club Brno - Czech republic
  Don`t panic!! This virus doesn`t destroy data! I am most kindly virus!!
I should inform you that soon comes Raptor2.0 with special sealth systems
           You can be sure that Raptor2 will be totally untouchable!
```

(Due to an error this text is displayed also in December.)

Thirteenth day in a month, approximately 55 minutes after starting, moving blue rectangles appear on screen.

Virus Relzfu

Simple non-resident virus, which attacks COM files in the current directory. On Friday 13th it displays text in the top left corner:

```
VirX 3/90
```

and starts beeping in an endless loop.

(This text is trivially coded in the virus body - incidentally, a coded part looks like this: `ufzleR`. Thats where the name comes from.)

Virus Sampo

A very interesting virus which attacks MBR of hard disks and boot sector of diskettes. When started it checks memory for some older boot viruses (Joshi, Stoned) and destroys them. Tries to survive a warm reboot (Ctrl+Alt+Del).

The fact that it cannot infect a write protected diskette is taken as an insult. For revenge it pretends that the diskette is infected with another boot virus (Kamana.A).

On 30th November, about one or two hours after starting, displays:

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

Virus Saturday_14th

A resident virus which attacks both EXE and COM files. Just at the end of its body is visible text `ECV`, which is being used for recognition of already infected files.

On Saturday 14th it attempts to overwrite the beginning of disks.

Virus Semtex

Resident virus of Czech origin. Attacks COM files when opening or loading. Sometimes demonstrates its presence by filling the screen with random data.

Variant Semtex.1000.A

Shows off after each hour in memory. Contains, but does not display, this text:

```
S E M T E X  by Dusan Toman, CZECHOSLOVAKIA (7)213-040 or (804)212-23
```

Variant Semtex.1000.B

Shows off between 24:00h and 03:00h, on the hour. Contains, but does not display, this text:

```
S E M T E X  by Dusan Toman, CZECHOSLOVAKIA ***  Have a nice day  ***
```

Virus Ser_No

This virus looks for and attacks EXE files. he body of the virus is coded and the decoding loop changes in parts. Does not attack files with names beginning with any of these characters:

`SC`, `CL`, `NO`, `AS`, `FI` nebo `TO`

Ser_No is equipped with a very insidious destructive action. Occasionally it randomly selects a sector and within this sector changes a random byte. If its presence is detected late, not only data on the disk can be damaged, but also their backups, which no doubt you make regularly.

It announces itself with this text:

```
V1.01 ser.No :
```

behind which is proudly displayed a five digit number of its generation.

Virus Simulate

A polymorphic non-resident virus, which looks for and attacks COM files. Occasionally displays randomly selected text and finishes in an endless loop:

```
ALIVE... Your system is infected by the SIMULATION virus.
                    Have a nice day!.
```

Four of its texts lead you to suspect another virus is present:

```
HA HA HA YOU HAVE A VIRUS

FRODO LIVES!

Have you ever danced with the Devil in the pale moonlight?

DATACRIME VIRUS RELEASED: 1 MARCH 1989
```

Virus Slovakia_II

Variant Slovakia_II.3584.1_0

Resident virus attacking both EXE and COM files. When resident in memory it masks the increased size of infected files. Does not like antivirus programs, preferring not to attack:

`scan`, `avg`, `vir`, `asta`, `alik`, `rex`, `msav`, `cpav`, `nod`, `clean`, `f-prot`, `tbav`, `tbutil`, `avast`, `nav`, `vshield` a `vsafe`

Checksum control files (`chklist.ms`, `chklist.cps` or `smartchk.cps`) are erased. Resident defensive program Vsafe is switched off immediately. When attacking files they are renamed first to svl.svl so as not to attract attention. If activated between 1st and 4th August, it politely introduces itself:

```
I'am SLOVAKIA virus  Version 1.0 Copyright (c) 19.1.1994 SVL
```

Also contains (but never displays) this text:

```
(C) 26.1.1994 SVL
Technické paramete:
MENO: Slovakia v.1.0.
TYP: Rezidentny COM&EXE infektor.
KRYPTOVANIE
```

Variant Slovakia_II.1024

A simple resident virus, which attacks loaded EXE files. If activated in the first week in the year it displays:

```
HAPPY NEW YEAR,SLOVAKIA
```

Then waits about two and half minutes and restarts the original program. In this period it does not spread.

Variant Slovakia_II.3584.1_1

Marginally modified version of Slovakia_II.3584.1_0. List of files avoided is extended by name dizz and displayed text is:

```
I'am SLOVAKIA virus  Version 1.1 Copyright (c) 29.1.1994 SVL
```

Virus Slovakia

Family of viruses attacking EXE files in current directory and in the path. Slovakia sometimes greets:

```
Greeting from Bratislava, SLOVAKIA.
```

and introduces itself:

```
SLOVAKIA virus version 2.00 (c) 1991 by ??. All Rights Reserved.
```

and then:

```
Type the word SLOVAKIA :
```

If you type a different word it explains:

```
Type word SLOVAKIA, not CZECH, YUGOSLAVIA or SLOVENIA !! Press Esc.
```

and will not let you go until the correct answer is received.

Slovakia does not attack files with names beginning with `SC`, `CP`, `NO`, `DC`, `AS`, `TN`, `PK` and `LH`.

Variant Slovakia.Slon

This variant descends from the original virus Slovakia, but uses functions, which are encoded and decoded while the program is running. When the main loop is decoded the following text can be seen:

```
Msg #0 to Slon! & Kuko.  Hi _, pleased to meet your program.
Enjoy new version of S. :-)  Bye ??.
```

Virus Smeg

Group of British polymorphic viruses which use a very good generator of encoding loops.

Variant Smeg.Queeg

Resident virus attacking both COM and EXE files. Avoids programs with names beginning with:

F-, SC, TB, VI, FS, VP, VS, CL, SM nebo FL

Tracks down safe addresses of some system functions and tries to avoid some checking programs.

Every 32nd generation 12:00h and 13:00h and introduces itself:

```
+---------------------------+
¦         -» QUEEG «-       ¦
¦            ~~~~~          ¦
¦ (C)  The Black Baron 1994 ¦
¦                           ¦
¦   Featuring:  SMEG v0.2   ¦
¦                           ¦
¦   Better than life.....   ¦
+---------------------------+
```

It then overwrites randomly selected hard disk sectors.

Variant Smeg.Pathogen

Resident virus attacking both EXE and COM files when loading. Avoids programs with name beginning with:

F-, SC, TB, VI, FS, VP, VS, CL, SM nebo FL

Tracks down safe addresses of some system functions and tries to avoid some checking programs.

On every 32nd generation it between 05:00h and 06:00h, deletes the hard disk parameters from
CMOS memory then introduces itself:

```
Your hard-disk is being corrupted, courtesy of PATHOGEN!

  Programmed in the U.K. (Yes, NOT Bulgaria!) [C] The Black Baron 1993-4

    Featuring SMEG v0.1:  Simulated Metamorphic Encryption Generator!

      'Smoke me a kipper, I`ll be back for breakfast.....'

        Unfortunately some of your data won`t!!!!!
```

It then starts overwriting randomly chosen hard disk sectors.

Variant Smeg.V3

A simple virus which looks for and attacks COM files in the current directory. On Friday 13th infected programs cannot be opened and instead this message appears:

```
This program requires Microsoft Windows.
```

Virus Socha

Resident virus which attacks COM files when loading. Spreads only if the year is set to 1981. Does not attack programs which are part of Norton Commander. Avoids also programs (could not be identified by us) using file `me$.ovl`. Contains th is text:

```
Socha
C:\m_edit\me$.ovl
```

which serve for identification of files not to be attacked.

Virus StarDot

Non-resident viruses which look for and attack both EXE and COM files. Contains short uncoded text:

```
AMZ
```

Sometimes overwrite beginning of disks.

Variant StarDot.801

Destructive action is planned for 13th February after 13:00h.

Variant StarDot.600

Destructive action is started at random.

Variant StarDot.789.A

Overwrites contents of hard disk on 24th September after 19:00h.

Virus Susan

One of a few interesting overwriting viruses. It is resident (!) and uses undocumented operating system call to take over control of the DIR command. When this command is used the virus attacks files and if more than sixteen have been infected, begins to erase the contents of current directory.

Opening an infected file ends with a simulation of an MS-DOS error message (from COMMAND.COM):

```
Bad command or file name
```

Other texts are visible in the virus body:

```
Susan
*.*
*.EXE
DIR
```

Virus Tack

Family of simple non-resident viruses which attack COM files. Individual variants differ only very little and contain an error which prevents their treatment (at the beginning of a file six bytes are amended, but only five bytes are stored).

Variant Tack.411

When an infected file is opened, this text is displayed:

```
Infected file.
```

Variant Tack.449

When an infected file is opened, this text is displayed:

```
----------------- Hello, I am virus ! ------------
```

Variant Tack.460

When an infected file is opened, this text is displayed:

```
----------------- Hello, I am virus ! ------------
```

Variant Tack.477

When an infected file is opened, this text is displayed:

```
----------------- Hello, I am virus ! ------------
```

Variant Tack.635

This variant is supplemented with an encoding loop and damages only five bytes at the beginning of the file, so it is possible to remove the virus.

Infected files are increased in size by the size of the virus plus up to 255 random bytes.

When attacking it displays:

```
-- I am virus ! --
```

Virus Ten_Bytes

Resident viruses attacking both COM and EXE files when loading. They install themselves into a fixed memory address, so frequent operating system crashes can be expected.

From September until December Ten_Bytes monitors writes to the disk and amends them by shifting the pointer ten bytes forward.

Virus Tequila

Resident virus attacking EXE files and MBR of hard disk. Belongs among the best written viruses and to date its occurrence has been reported from many places. The first time Tequila loads it tries to find the original address of disk services (and thus avoid checking programs), attacks MBR, but does not start spreading. Only after re-starting the computer do it attack loaded EXE files. Files names containing the characters "SC" and "V" are avoided and checksums attached by SCAN to guarded programs are damaged.

When the virus is in memory, it amends the size of infected files to pretend that everything is OK. The body of the virus is encoded in complicated way and the decoding part is changeable. There are four basic types and altogether it can take about 25000 different forms.

Tequila occasionally, when a program is closing, paints a fractal on screen and displays the text:

```
Execute: mov ax, FE03 / int 21. Key to go on!
```

When a program containing the above mentioned instructions is loaded, the virus introduces itself:

```
Welcome to T.TEQUILA's latest production.
Contact T.TEQUILA/P.o.Box 543/6312 St'hausen/Switzerland.
Loving thoughts to L.I.N.D.A

BEER and TEQUILA forever !
```

Virus Thanksgiving

One of the first multi-partite viruses. Attacks loaded COM files, hard disk partition table and diskette boot sector. Contains visible text `V-1L` which it uses to identify already infected files. Furthermore, there is coded text in the virus body:

```
Disk error
```

This is displayed if it cannot read its own data.

After 24th December 1990 it overwrites contents of hard disk.

Virus Tiny

Family of resident viruses, which usually attack loaded COM files. It is possibly an attempt to create the smallest, fully functional virus.

Virus Tiny-GM

Simple viruses, which look for and attack COM files. They do not check if a victim has already been infected and can therefore infect the same file several times.

Virus Tiso

Variant Tiso.846

Resident virus, which attacks loaded COM files and the hard disk partition table. When attached to a file, its body is simply encoded. Sometimes displays in white on blue background:

```
Nech zije Jozef Tiso, prvy slovensky prezident !
```

Virus Uruguay

A family of polymorphic resident viruses, which attack both COM and EXE files when loading or opening. It tries to track down the original addresses of important operating system services and so avoid some antivirus programs. With the same intention it does not change table of interrupt services, but directly overwrites the beginning of the relevant code with jump instruction to the virus.

Uruguay does not attack COMMAND.COM and some variants avoid F-PROT, SCAN and others with names starting with 'AI' and containing 'V'.

Other characteristics appearing in some variants are:

- Monitoring of Ctrl+Alt+Del and attempt to survive the reboot

- Uses ROM checksum as a simple means for identifying infected files

- Announcement of successful installation into memory. For example:

```
    Uruguay-#8 installed (seg=9CDF)
```

When an infected program is loaded it will announce itself with a text message(0.4% probability),wait five seconds and then continue. The message differs from version to version.

Variant Uruguay.6

```
'Uruguay-#6' Virus
Programmed in Montevideo (URUGUAY) by F3161. 11/92.
This is a research virus - DO NOT DISTRIBUTE.
```

Variant Uruguay.1

```
The BEATLEMANIA is alive!
THE BEATLES, for ever, the best.
John, Paul, George and Ringo, ladies and gentlemen, here they are!
PLEASE, PLEASE ME. WITH THE BEATLES. A HARD DAY'S NIGHT.
BEATLES FOR SALE. HELP. RUBBER SOUL. REVOLVER.
SGT.PEEPERS LONELY HEARTS CLUB BAND. THE BEATLES. YELLOW SUBMARINE.
ABBEY ROAD. LET IT BE. MAGICAL MISTERY TOUR.
Other LP and singles available...

Virus 'Uruguay-#1'
Programmed in Montevideo (URUGUAY) by F3161. 03/92.
This is a research virus - DO NOT DISTRIBUTE.
```

Variant Uruguay.2

```
I love ROXETTE !!!

Virus 'Uruguay-#2'
```

```
Programmed in Montevideo (URUGUAY) by F3161. 04/92.
This is a research virus - DO NOT DISTRIBUTE.
```

Variant Uruguay.3

```
'Uruguay-#3' Virus
Programmed in Montevideo (URUGUAY) by F3161. 06/92.
This is a research virus - DO NOT DISTRIBUTE.
```

Variant Uruguay.4

```
'Uruguay-#4' Virus
Programmed in Montevideo (URUGUAY) by F3161. 07/92.
This is a research virus - DO NOT DISTRIBUTE.
```

Variant Uruguay.5

```
'Uruguay-#5' Virus
Programmed in Montevideo (URUGUAY) by F3161. 08/92.
This is a research virus - DO NOT DISTRIBUTE.
```

Variant Uruguay.8

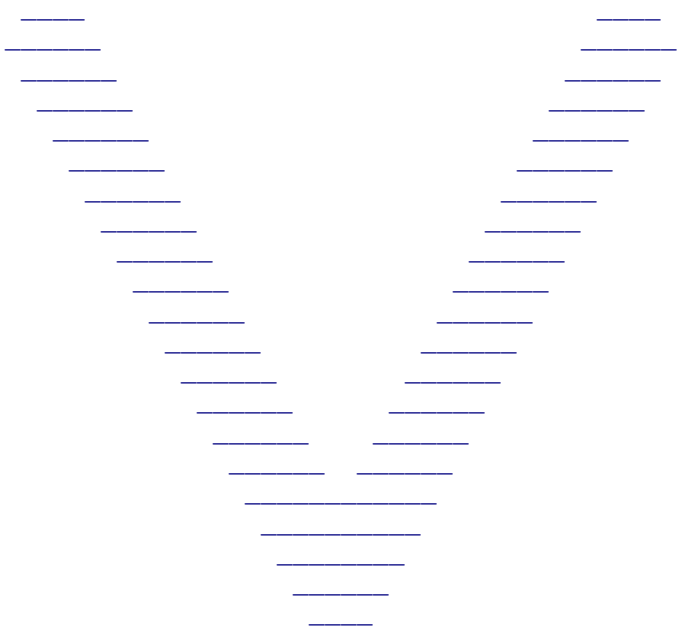
```
Uruguay-#8 Virus
Programmed in Montevideo (URUGUAY). 03/93.
This is a research virus - DO NOT DISTRIBUTE.
```

Variant Uruguay.7

```
Uruguay-#7 Virus
Programmed in Montevideo (URUGUAY). 02/93.
This is a research virus - DO NOT DISTRIBUTE.
```

Virus V-Sign

This virus attacks diskette BOOT sectors and the MBR of hard disks. After infecting the 32nd diskette it celebrates with slow display of a large V and ends in a loop.



Virus Vic

Resident virus of Czech origin which attack both COM and EXE files when opening and loading. The body is encoded and the decryptive loop is modified. When active in memory it causes the clock to go backwards. Vic contains, but does not use:

```
VZDY MAS O JEDEN VIRUS VIC, NEZ SI MYSLIS.
```

Virus Vienna

A family of simple non-resident viruses which attack COM files. Thanks to the fact that source of this virus was published, there are now large number of mutations, which differ only in detail. Some mutations occasionally damage the infected program beyond repair.

Virus Vietnam

Variant Vietnam

Attack diskette BOOT sectors and hard disk MBR. Its source text was distributed in electronic magazines published by hackers groups.

Between 17th and 30th June Vietnam overwrites the hard disk.

Virus Voronezh

A family of resident viruses of Russian origin, which usually attack only COM files.

Variant Voronezh.1600

This variant does not contain text and is not destructive. Attacks files not only when loaded, but also when opened. Attacks also EXE files. Tries to ignore COMMAND.COM.

Variant Voronezh.650

If an infected file is opened in the third minute, the screen is switched to 40x25 character mode and displays:

```
Video mode 80x25 not supported
```

Also contains uncoded text:

```
16.01.91, v1.00, ÓšÈšà & žÀ«°
```

Virus Yale

One of the oldest viruses. Spreads by attacking BOOT sector in drive A: on Ctrl+Alt+Del.

Several variants exist, but most of them cannot spread on modern computers.

Virus Yog-Sothoth

Silly resident virus. When activated it attacks all COM files in the current directory.

At ten o'clock exactly it attracts attention with:

```
Ha! Jsem virus Yog-Sothoth a mam te rad.
Kdyz budes hodnej, nezacnu ti hned formatovat hardisk.
Ale treba az za chvili. Ha, ha, ha...!
```

then resets the computer.

It is not directly destructive, but the way it handles the operating system and memory can cause regular system crashes.

The body of the virus is encoded and Yog-Sothoth contains some form of polymorphism - it has two different (but very similar) decryption loops and swaps between them regularly.

Virus ZP

A small resident virus, which attacks EXE files when loaded or opened. On thirteenth day in any month, after few hours from being loaded into memory, it restarts the computer.

Virus 10_Past_3

Family of memory resident viruses which attack COM files. They are not destructive but can cause much annoyance. Contain code which should obstruct their tracing.

Variant 10_Past_3.748

This variant does not contain any text. On being loaded in to memory on 22nd of a month it resets the computer. On some other days it switches off some important operating system functions. After fifteen hours and ten minutes from starting the computer it takes over keyboard control and occasionally and Shift.

Virus Seventh_son

Family of simple non-resident viruses attacking COM files. Contain uncoded text:

```
Seventh son of a seventh son
```

This text is displayed when the seventh copy of seventh copy of the original virus is loaded.

Virus Eight_Tunes

Resident virus which attacks both EXE and COM files. It sometimes plays one of eight tunes and contains uncoded text `COMMAND.COM`.
If it detects the presence of the program FLUSHOT it stops spreading.
It seems that it can detect and de-activate one more antivirus program, but we could not find out which one.

Virus Armagedon

Family of resident viruses of Greek origin. Attacks only COM files and interestingly with help of a modem they try to dial telephone numbers.

Variant Armagedon.1079

Between 17.00h and 18.00h it tries to dial 081-141 (apparently the speaking clock in Greece). Contains uncoded text:

```
Armagedon the GREEK
```

Also the command to dial the telephone number with Hayes compatible modems can be detected:

```
+++aTh0m0s7=35dp081,,,,141
```

Variants Armagedon.1709.B and Armagedon.1079.C are try to dial number 911 (emergency number in USA) and contain the text:

```
Support Your Police
```

Virus Arusiek

Resident viirus which attacks both COM and EXE files. In the body of the virus is a table of files which it preferably ignores:

```
MKS
NAV
CLEAN
COMMAND
```

It also contains the text Arusiek R., which is visible in the file in the form:

```
9A r u s i e k% 9R .4
```

Virus Better_World

Resident virus attacking EXE files when opened. Contains uncoded text which if activated in Septemeber, displays with pride:

```
This message is dedicated to
all fellow PC users on Earth
  Towards A Better Tomorrow
And A Better Place To Live In
```

Virus Bomber

This virus attacks COM files in an awkward way. It inserts itself
at a random place in the victim and in the rest randomly spreads
created intruction management. Last one then starts own code in the body of virus.

Body of the virus is not encoded and contains this text:

```
COMMANDER BOMBER WAS HERE a [DAME] [DAME].
```

Virus Explosion

Resident virus which attacks both EXE and COM files. It does not attack files with names SCAN, CLEAN, FINDVIRU AND GUARD. On the seventh day in the month (subject to extra more complex conditions) it displays:

```
Dis is one virus.
Leave the room IMMEDIATLY !!!
Your PC is about to EXPLODE within 20 sec !
```

It begins to beep and starts to count from nineteen to zero, then displays:

```
EXPLOSION
What did you expect ?
```

After the show is over, it remains in memory, but stops attacking files.

Virus Frodo

Family of resident viruses which attack both EXE and COM files. Almost certainly one of the most technically perfect viruses. The complexity of their stealth techniques is worth mentioning. Apart from masking themselves when old DOS functions are called (which is not usual), they remove themselves completely from infected files which are opened for writing into or under the control of a debugger.

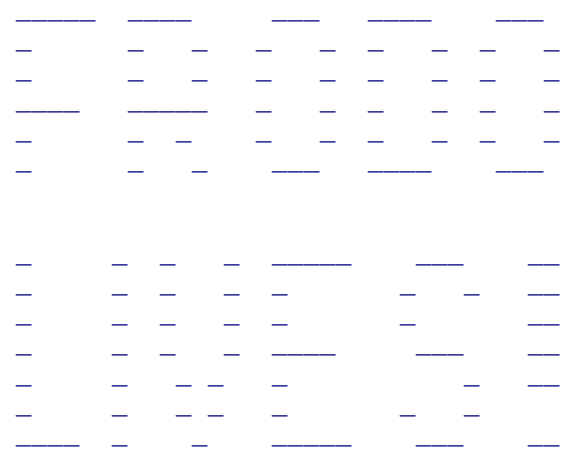
By trying to detect the original address of most important system services and using those services directly they avoid antivirus programs.

The Frodo family does not check the extension of its victim directly, but with a help of checksums. The side effect is that data files can be attacked as well (from common files eg BMP, CDX, DIR, FAX and PIF). Thanks to its stealth techniques the change of these files does not appear until after the virus is removed from memory.

Variant Frodo.Frodo.A

Frodo.Frodo tests memory usage and, should better place be free, it can easily move itself there.

From 22nd September the virus is destructive (the birthday of Frodo, a character from J.R.R. Tolkien's books). This feature is unfortunately in all the samples available to us. It seems that its task was to overwrite the BOOT sector of disk or diskette in a way so that after reboot it displays text in a frame in the form of "lit snake":



Variant Frodo.Fish_6.A

Frodo.Fish is derived from the Frodo.Frodo virus. Unlike its ancestor it is encoded (not only in infected files but also in memory) and contains many tricks, which make its analysis

more difficult.

After 1991 they introduce themselves when an infected program is started:

```
FISH VIRUS #6 - EACH DIFF - BONN 2/90 '~knzyvo}'
```

In the encoded virus body are the texts:

```
COD, SHARK, CARP, BASS, TROUT, FIN, MUSKY, SOLE, FISH, PIKE
MACKEREL, FISH a TUNA
```

Just at the end of the virus is this encoded text:

```
FISH FI
```

Virus Geld_wasch

Resident virus which attacks EXE files when loaded. After 1991 and always on 25th in even months it displays:

```
Ihr Geld wasch ich sauber, schnell und prompt !
Ganz geil ich werde, wenn es von Drogen kommt !
Ihr korruptes Wirtschaftsschwein Hans W. Kopp !
```

It then destroys the contents of hard disks.

Virus Hydra_II

Resident viruses which attack EXE files. From 1995 if activated on 1st January, 5th May or 9th September it demonstrates its presence. On these days it does not spread.

Variant Hydra_II.A

Introduces itself with this text:

```
This is Hydra v1.0.
Don`t panic, I will not destroy your data.
```

Variant Hydra_II.B

In an interesting way it scrolls the screen and displays:

```
This is Hydra v1.1.
Don`t panic, I will not destroy your data.
```

Virus KWZ

Resident virus which attacks COM files when loaded. From 25th until end of the month it decreases the systems performance and, when attempting to create a new directory, resets the computer.

The author of the virus probably wished not to be bothered with his own creation, so KWZ does not spread if it identifies a computer with BIOS number:

```
01/15/8808/30/9006/06/9207/07/91
```

At the end of the victim is uncoded text, which the virus uses to identify already infected files:

```
K  WZ
```

Virus Monika

Resident virus of Czech origin which attacks COM files. It attaches itself in classic way at the end of its victim, but damages also two bytes in the body. It probably tries to prevent its removal by some programs which control file integrity.

On 8th October the screen is overwritten with the text `Monika` and regrettably, the beginning of the hard disk.

Virus Nina

Simple resident virus attacking COM files. In its body is coded the text `Nina` which is never displayed.

Variant Nina.D

Text Nina is in this variant substituted by: `RIOT!`.

Virus One_Half

Resident polymorphic multi-partite virus of Slovak origin. When active in memory it uses stealth techniques to mask changes to the MBR and the reduced size of infected files. Some checking programs are avoided by tracing system services. Also does not attack some antivirus programs.

One_Half insidiously and unpleasantly destructive. Every time the computer is started two tracks are written to the hard disk. Once more then 50% of the hard disk capacity is damaged it begins to attract attention. Displays:

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

Then beeps and waits for a key press.

Under normal conditions nothing can be recognised. One_Half sits in memory, controls access to the hard disk and decodes data according to need. An amateurish attempt to remove this virus (eg FDISK/MBR) will destroy the virus but also information needed to decode the contents of the hard disk.

Variant One_Half.3544

Contains text:

```
Did you leave the room ?
```

Does not attack these programs:

```
SCAN
CLEAN
FINDVIRU
GUARD
NOD
VSAFE
MSAV
```

If `CHKDSK` is loaded the virus prefers not to use stealth to conceal the infected file size.

Variant One_Half.3577

Contains text:

```
DidYouLeaveTheRoom?
```

Does not attack these programs:

```
SCAN
CLEAN
```

```
FINDVIRU
GUARD
EMM
```

If `CHKDSK` is loaded the s prefers not to use stealth to conceal infected file size.

Variant One_Half.3570

Contains text:

```
Did you leave the room ?
```

Does not attack these programs:

```
SCAN
AIDS
FINDVIRU
WEB
NOD
VSAFE
MSAV
```

If `CHKDSK` is loaded the s prefers not to use stealth to conceal infected file size.

Virus Pivrnec

Simple virus attacking loaded COM files.

On 10th October it destroys the hard disk partition table (MBR),
and introduces itself:

```
Mé jméno je Pivrnec a chtìl bych
Vám podìkovat za poskytnutí
podmínek potøebných pro moji
inkubaci a zdárný vývoj mé
osobnosti ...!?...

                    Pivrnec `95

PS: Doufám, že Vás nepøešla ŽåZEÒ !?
```

and ends in a never ending loop.

Virus CLI

Simple resident virus which attacks COM files when loading
or opening. Does not attack COMMAND.COM.

On 2nd of February 1997 it will destroy the CMOS data and after
a key is pressed it overwrites the hard disk partition table (MBR).