

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
Dropper
Ear
Eight Tunes
Encroacher MtE
Explosion
FCB
Fear MtE
Fifo
Finnish
Flip
Freew
Friday 13th
Frodo
Fumble
Geld wasch
Groove MtE
Haifa
Halloween
Howard Stern
Hydra II
J&M
Justice
KWZ
Kampana
Klepavka
Lao DOUNG
Letter H
Level 3
Lisa
Lock Show
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 je jedním z nejzajímavějších virů vůbec. Je silně polymorfní, používá dokonalou stealth techniku, umí se bránit před některými antivirovými programy a umí se uložit do HMA (High Memory Area).

Za zmínku stojí i historie jeho šíření. Program napadený Tremorem byl odvysílán v datovém kanálu televizní stanice PRO-7. A protože Murphyho zákony opravdu pracují - tím napadeným programem byl populární antivirus.

Obsahuje zakódovaný text, který oběs vypíše:

```
* 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 není přímo konkrétní virus, ale knihovna určená a používaná pro kódování virů. Obvykle obsahuje tyto texty:

[MK / Trident]

[TPE 1.3]

Virus Aircop

Napadá BOOT sektor disket. Při napadení každé osmé diskety vypíše blikající text:

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

Virus Akuku

Rodina nerezidentních virù, které obvykle napadají soubory COM a EXE. Většinou neobsahují žádnou destruktivní činnost.

Varianta Akuku.899.B

Obsahuje text `A kuku, Nastepny komornik !!!`, který napíše jestliže je spuštěn mezi 32. a 35. minutou v hodině.
Tato mutace napadá pouze COM soubory.

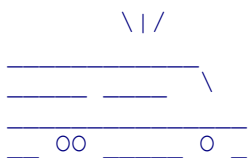
Virus Albania

Rodina jednoduchých nerezidentních virů, které se připojují na konec COM souborů. Obsahují text *albania* resp. *ALBANIA*.

Tento text virus nikdy nevypíše. Používá ho pro identifikaci souborů, které už napadl.

Virus Ambulance

Jednoduché nerezidentní viry napadající COM soubory. Občas na sebe upozorní touto sanitkou projíždící za zvuku sirény přes obrazovku:



Virus Amoeba

Rezidentní virus, který napadá COM a EXE soubory. Obsahuje triviální zakódovaný text, který občas napíše na dolní řádek obrazovky:

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

Virus Anthrax

Multipartitní virus, který napadá kromě MBR pevného disku také EXE a COM soubory. Obsahuje nezakódované texty:

(c) Damage, Inc.

1990

ANTHRAX

Anthrax se snaží najít původní obsluhu diskových operací a používá řadu dalších nedokumentovaných služeb operačního systému, aby snížil pravděpodobnost, že bude zpozorován.

Virus AntiCMOS

Tyto viry napadají boot sektor disket a tabulku rozdělení pevného disku. Oběs smažou obsah paměti CMOS.

Varianta AntiCMOS.LiXi

Obsahuje text:

```
I am Li Xibin!
```

Virus AntiMon

Nerezidentní virus napadající COM soubory. Snaží se ničit obecné programy pro ochranu počítače. Jejich seznam není v tìle viru zakódován:

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

Virus Anti-Pascal

Rodina jednoduchých nerezidentních virů, které napadají COM soubory.
Virus maže soubory *.PAS a *.BAK.

Virus Anti-Pascal_II

Jednoduché nerezidentní viry, které napadají COM soubory a ničí soubory jejichž přípona odpovídá masce ?A? (např. PAS, BAK). Pravděpodobně pochází od stejného autora jako viry Anti-Pascal.

Virus Arab

Rezidentní virus, který napadá spouštiné COM soubory. Občas poškodí MBR pevného disku tak, že je možné operační systém zavést pouze z diskety.

Virus Aragon

Virus českého původu, který napadá BOOT sektor disket a MBR pevného disku. Obsahuje text [JMH](#), což jsou (prý) iniciály jednoho z pedagogů katedry počítačů VUT Brno.

Aragon je stealth virus a neprovádí žádnou destruktivní činnost.

Virus Ash

Rodina jednoduchých nerezidentních virù, které napadají pouze COM soubory.

Varianta Ash.1604

Obèas obtìžuje tímto texty:

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

Jednoduchý rezidentní virus, který napadá pouze COM soubory. Na začátek oběti vkládá nezakódovaný text:

ATTENTION !

Pokud dojde k chybě při přístupu na disk, Attention se pokusí (bez ohledu na to kde se stala) resetovat disketovou mechaniku A:.

Virus Attitude

Varianta Attitude.827

Jednoduchý virus, který hledá a napadá soubory typu COM.
Obèas maže první sektor disku C:, pøípadnì nièí soubory C:\CONFIG.SYS,
C:\AUTOEXEC.BAT a C:\COMMAND.COM. Nìkdy také pøepisuje soubor
C:\DOS\KEYB.COM.

Obsahuje tento výkøik:

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

Virus BackFont

Rodina rezidentních virů napadajících EXE soubory při jejich spuštění. Některé obsahují pouze neškodné hrátky s videokartou, některé občas poškodí systémové části disku.

Varianta BackFont.905

Dvacet sekund poté co se tato mutace usadí v paměti, začne každých deset sekund otáčet znaky na obrazovce. Tento efekt provádí pouze pokud máte grafickou kartu EGA a virus už na vašem počítači strávil alespoň tři měsíce.

Virus Backform

Rezidentní virus, který napadá soubory typu COM a EXE při jejich kopírování na disketu. Pouze COMMAND.COM se snaží najít a napadnout okamžitě, aby tak zvýšil své šance na šíření. K tomuto souboru se nepřipojuje, ale vepisuje do jeho datových oblastí, takže nezvětšuje jeho délku.

Pokud napadá soubor typu COM začínající instrukcí skoku, tak ponechá jeho začátek netknutý a odkaz na sebe vepíše až do místa, kam tato instrukce ukazuje.

Backform nenapadá soubory, jejichž jméno začíná na AI.

V těle viru je viditelný tento text:

`c:\command.com`

Backform kontroluje operace s disketami a při jejich formátování mění pořadí sektorů na stopě. Jestliže dospěje alespoň do dvacáté generace, tak tuto destrukci v prvním polovině roku vypíná.

Virus Bad_Boy

Rodina jednoduše kódovaných virù, které napadají spouštìné COM soubory. Obèas vypíše tento text a zastaví èinnost poèítaèe.

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

Obsahují nezakódovaný text:

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

Bad_Boy je (i když poněkud kuriózním způsobem) polymorfní. Umí náhodně uspořádat osm svých částí, které pak volá přes jakousi "tabulku služeb".

Virus Number_of_the_Beast

Rezidentní stealth virus, který napadá COM soubory. Je nesmírně zajímavě naprogramován, používá velké množství nedokumentovaných služeb MS-DOSu a na to co všechno dělá je až neuvěřitelně krátký. Původně byl napsán pouze pro MS-DOS 3.30 a s jinými verzemi operačního systému nedokázal správně fungovat. Existuje ovšem řada variant, které se většinou liší právě jenom v detailech a umožňují jeho šíření i pod jinými verzemi DOSu. Některé varianty obsahují text 666, který je ovšem viditelný pouze pokud virus není přítomen v paměti. Není známa žádná mutace obsahující nějakou vysloveně destruktivní akci, ale způsob jakým napadá soubory může vést k jejich neopravitelnému poškození.

Virus Bebe

Rodina jednoduchých nerezidentních virů, napadajících všechny soubory v aktuálním adresáři.

Varianta Bebe.1004

Tato varianta instaluje malou rezidentní část, která občas obtěžuje výzvou:

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

Pokud odpovíte požadovaným slovem, virus vám to vysvětlí:

```
+----- VIRUS! -----+
|      Fig Tebe !      |
+-----+
```

Bebe obsahuje několik chyb, které mu brání se šířit na novějších typech počítačů a které mohou způsobit pád operačního systému bezprostředně po spuštění napadeného programu.

Virus Beech

Rezidentní virus, který napadá spouštěcí nebo otevírané COM soubory. Neobsahuje žádný text ani žádnou destruktivní akci. Je přímo ideálním vzorkem viru o kterém se nedá nic rozumného napsat.

Virus Beer

Rodina rezidentních virů ruského původu. Napadají EXE i COM soubory
Část viru je triválním způsobem zakódována, občas hraje nějakou melodii
a ničí některé soubory používané antivirovými programy.

Varianta Beer.3192

Obsahuje zakódovaný text `Ceøšac íÛ »šóàa`, který občas napíše a zahraje
melodii. Tímto textem také přepisuje některé soubory:

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

Nenapadá `COMMAND.COM` a `AIDSTEST.EXE`.

Virus Best_Wishes

Rodina rezidentních virů, které napadají EXE i COM soubory. Oběs poškozují systémovou část pevného disku.

Varianta Best_Wishes.1024

Každá pátá generace tohoto viru zmenší údaj o velikosti pevného disku. V pátek třináctého virus toto číslo rovnou vynuluje a napíše:

```
With Best Wishes!
```

Tento text je viditelný na konci těla viru:

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

Virus Beta_Boys

Rezidentní viry, které napadají spouštěcí COM soubory. Způsob jakým se usazují v paměti má daleko k dobrému vychování a může způsobit pád operačního systému.

Varianta Beta_Boys.Mud

Při každém spuštění napadeného programu stmaví šedou barvu o jeden stupeň (samozřejmě pouze na VGA karti).

Obsahuje jednoduše zakódovaný text, který ale nikdy nezobrazí:

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

Varianta Beta_Boys.Rattle

Pokud je virus aktivní mezi půlnocí a jednou hodinou, začne v nekonečné smyčce velmi rychle posouvat obsah obrazovky doleva a doprava.

Obsahuje jednoduše zakódovaný text, který ale nikdy nezobrazí:

```
DEATH RATTLE V1.00  
(c)1992 The BetaBoys Development Corp.  
+S+W+E+D+E+N+
```

Virus Beware

Tento virus napadá COM soubory v aktuálním adresáři. Pokud první den v měsíci připadne na pondělí, pokusí se přepsat disketu v mechanice A:. Obsahuje nezakódovaný text, ale nezobrazuje ho:

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

Virus Bing_Bang

Jednoduchý virus, který hledá a napadá soubory typu COM.

Jestliže je spuštěn 1.1., poškodí tabulku rozdělení pevného disku.
(Autor zřejmě chtěl označit jednotlivé disky jako nepřístupné, ale "netrefil" se do správných míst MBR).

Virus obsahuje (ale nepoužívá) tyto texty:

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


Virus Billboard

Jednoduše kódovaný virus, který hledá a napadá soubory typu COM.
Obsahuje tyto silácké vzkazy:

```
Billboard 1.0, (c)1993 Slp̂p̂ẑp̂ [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

Rezidentní polymorfní stealth virus, který napadá COM soubory.
V těle viru je obsažen tento zakódovaný text:

`Bizarre by Dreamer`

Virus Black_Jec

Rodina jednoduchých virů napadajících všechny COM soubory v aktuálním adresáři. V těle viru je obvykle viditelný text `*?.com`.

Další z mnoha rodin virů o kterých se nedá nic zajímavého napsat.

Varianta Black_Jec.Sad.307

Pokud je spuštěn v zářít, napíše:

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

A pokusí se naformátovat první stopu aktuálního disku.

Virus Black_Monday

Nepøíjemné rezidentní viry, napadající COM i EXE soubory. Je v nich pokus o formátování disku, který ovšem není aktivován v pondělí, ale v závislosti na vnitřním èítaèi napadených souborù.

Varianta Black_Monday.Black_Monday.A

Obsahuje tento nezakódovaný text:

Black Monday 2/3/90 KV KL MAL

Virus Blood

Nerezidentní virus, který napadá všechny COM soubory v aktuálním adresáři. Obsahuje nezakódovaný text:

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

Který s 25% pravděpodobností vypíše při spuštění napadeného souboru.

Virus Boys

Jednoduchý nerezidentní virus, který při spuštění napadne COM soubor v aktuálním adresáři. Z důvodů známých pravděpodobně pouze autorovi také označí první EXE soubor, který najde, jako systémový. Obsahuje tento nezakódovaný text:

The good and the bad boy.

Virus Brainy

Rezidentní virus, který napadá spouštěcí COM soubory. Je triviálním způsobem zakódován a obsahuje text [The WARRIER!](#).

Pokud obě začíná instrukcí skoku, Brainy se nevloží na začátek souboru, ale na místo, kam tento skok vede.

Virus Butterfly

Primitivní nerezidentní virus, který napadá soubory typu COM.
Obsahuje, ale nevypisuje, tento text:

Hurray The Crusades

Virus BUPT

Rezidentní viry, které napadají spouštěcí soubory COM i EXE. Obsahují nezakódovaný text, který občas na chvíli zobrazí:

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

Pokud nějaký program začne zjišťovat velikost volného místa na disku, virus to pochopí jako žádost o napadení dalších souborů a vyhoví.

Virus Burger

Rodina velmi triviálních nerezidentních virů, které přepisují COM soubory. Ralf Burger publikoval v roce 1986 zdrojový kód tohoto viru ve své knize a tak vzniklo velké množství nepatrně se lišících a zcela nezajímavých mutací.

Varianta Burger.Pirate

Obsahuje nezakódovaný text:

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

Virus Burghofer

Rezidentní virus, který napadá spouštiné COM soubory. Neobsahuje žádnou destrukční akci, ale stejně je v něm chyba, která může způsobit pád operačního systému. Na začátek napadeného souboru vkládá text `GS/02`, který je také viditelný na začátku těla viru.

Virus CARA

Rezidentní virus, který napadá COM soubory při jejich spuštění nebo otevírání. Na začátku napadeného souboru je viditelný text `CARA`, který můžete najít i v těle viru.

CARA patří mezi kuriozity. Snaží se při svém spuštění zjistit příznaky typické pro BOOT virus a pokud se to podaří, pípne a napíše:

```
Virus es en memoria!
```

```
Clandestino  
Auto-  
Reproductivo  
Anti-virus
```

Také kontroluje diskety se kterými pracujete a pokud najde BOOT virus z rodin Ping-Pong, Stoned, Brain, Microbes nebo Pentagon, tak ho zničí. Pokus o zavedení operačního systému z takto ošetřené diskety skončí pípnutím a nápisem:

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

```
Clandestino  
Auto-  
Reproductivo  
Anti-virus
```

Virus Carioca

Rezidentní virus, který napadá spouštěcí COM soubory. Nenapadá soubory jejichž přípona končí písmenem E (například .EXE), ale nekontroluje skutečný obsah oběti, takže program nemusí být po napadení virem schopen spuštění. Také nenapadá [COMMAND.COM](#) a tento text je v těle viru vidět.

Ve druhé polovině listopadu a prosince Carioca při každém stisku klávesy přepisuje obsah řádku, který slouží k řízení obnovování obsahu paměti.

To může způsobit chybu paměti a zhroutení operačního systému.

Virus Casino

Rezidentní virus napadající COM soubory. Pokud je napadený program spuštěn patnáctého ledna, dubna nebo srpna, můžete si zahrát o obsah vašeho disku:

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

Jestliže se vám podaří na pít pokusů vyhrát, Casino vám poblahopřeje a doporučí nechat už dnes počítač vypnutý. A je to dobrá rada, podruhé už takové štěstí asi nebudete mít.

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

Pokud si budete moct přečíst tyto texty:

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 ...

Znamená to, že prvních 40 kB vašeho disku je nenávratně přepsáno.

V těle viru jsou viditelné tyto texty:

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

Virus Casper

Jednoduchý virus, který vyhledává a napadá soubory typu COM.
Pokud je napadený soubor spuštěn prvního dubna, Casper se pokusí
o formátování. To ostatně slibuje i text, který obsahuje:

```
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

Rezidentní virus, které napadá EXE i COM soubory při jejich spuštění nebo otevírání. Pokud se mu podaří najít v kmenovém adresáři disku C: soubor COMMAND.COM, napadne ho jako první. Při pokusu o spuštění programu CLEAN virus napíše:

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

Následuje přepsání MBR prvního pevného disku.

V těle viru jsou viditelné tyto texty:

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

Varianta CAZ.1204

Přibližně třicet minut poté, co se usadí v paměti počítače, začne velmi rychle (18 krát za vteřinu) posunovat obsah obrazovky doleva a doprava. Výsledkem je nepříjemné kmitání obrazu, které má zřejmě vzbudit dojem, že došlo k poruše monitoru.

Virus Chaos

Rezidentní viry, které napadají spuštěné soubory typu COM a EXE.

Varianta Chaos.1181

Jestliže je virus spuštěn třináctý den v měsíci, tak při každém pátém přístupu na disk přepíše několik sektorů a po stisku stejné klávesy se představí:

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

Posledních šest dní v roce má nízkou hodnotu, podle které poznává, zda nějaký soubor už napadl, takže pak může napadnout jeden soubor několikrát.

Varianta Chaos.1241

Při spuštění si tento virus zkontroluje datum a pokud odpovídá složitě vyjádřené podmínce, tak se rozhodne, že bude zlobit. (Pravděpodobnost, že datum bude odpovídat podmínkám je cca 4.2%).

V tom případě sleduje operace s diskem a při každém pátém přístupu přepíše několik sektorů. Pokud se tohle dění odehrává v září, tak se po zničení kousku disku představí:

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

a skončí v nekonečné smyčce.

Virus Checksum

Rezidentní viry, pravděpodobně ruského původu. Všechny napadají spouštěcí COM soubory, některé varianty i EXE soubory.

Checksum používá kontrolní součty a nešíří se, pokud získá pocit, že byl nějak poškozen.

Virus Cheeba

Rezidentní virus, který ménì obvyklým zpùsobem napadá COM i EXE soubory. Sleduje jejich vytváøení (napø. rozbalení z archívu nebo okopírování) a pøi uzavírání je napadne. Pokud ovšem zjistí, že nijaký program píše na disk texty obsahující znaky 'iru' (zøejmì èást slova 'virus'), nebo se tyto znaky vyskytují ve vyhlédnuté obìti, tak dá raději pokoj. Jestliže Cheeba zjistí, že nikdo manipuluje se souborem, jehož název odpovídá složitým kontrolním souètùm, použije tento název jako klíè pro dešifrování speciální funkce. Správné jméno je USERS.BBS a tento soubor virus poškodí. Nepøíjemným vedlejším efektem tohoto postupu je, že lze nalést jména, která sice kontrolním souètùm vyhovují, ale pøi jejich použití jako klíèe vznikne místo správného kódu pouze balík nesmyslných instrukcí. Jejich vykonání pak může vést ke zhroucení operaèního systému.

Varianta Cheeba.A

Obsahuje zakódovaný text:

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

Varianta Cheeba.B

Obsahuje zakódovaný text:

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

Virus Cinderella

Rezidentní virus, který napadá spouštěcí a otevírané COM soubory. Oběs vytvoří soubor CINDEREL.LA a provede restart počítače. Neobsahuje žádnou destrukční funkci, ale způsob, kterým se usidluje v paměti může vést ke zhroutilí operačního systému. V tle viru je viditelný tento text:

`cInDeReL.la`

Virus Cod

Jednoduchý rezidentní virus, který napadá spouštěné EXE soubory a není vůbec ničím zajímavý.

Virus Comasp

Jednoduchý rezidentní virus. Napadá spouštěcí a otevírané COM soubory. Způsob kterým se instaluje do paměti je nekorektní a může vést ke zhroucení operačního systému. V těle viru je tento nezakódovaný text:

ASP

Virus COM_Virus

Jednoduchý virus, který napadá COM soubory na disketách.
Pokud je spuštěn napadený program, COM_Virus na sebe upozorní tímto textem:

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

Virus Copyright

Rezidentní viry, napadající spouštěné COM soubory. Významná výročí oslaví obrázkem (namalovaným v textovém režimu z mezer a znaků '_'). Virus Copyright se nešíří na počítačích osazených tímto BIOSy:

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

Varianta Copyright.1193

Za důvod k oslavě považuje tato výročí:

23.2., 7.3., 22.4., 30.4. a 6.11.

V tyto dny se virus nešíří, ale pomaluje obrazovku proužky, počká na stisk klávesy a spustí původní program.

Kromě textů, které virus používá pro identifikaci BIOSu počítače také obsahuje text COM.

Virus Crazy_Imp

Rodina rezidentních virů, které napadají COM soubory při jejich zavírání nebo po jejich spuštění. Používají stealth techniku - pokud zjistí, že je otevírán nebo spuštěn napadený soubor, vyléčí ho a po skončení práce s ním opět zaútočí. U napadených souborů lžou o jejich délce, takže se na první pohled zdá, že je všechno v naprostém pořádku.

Varianta Crazy_Imp.1445.A

V těle viru je viditelný tento text:

`Crazy imp v2.0`

Virus Creeper

Rodina rezidentních virů, které napadají spouštěcí soubory typu COM.

Varianta Creeper.475

Tato varianta sleduje obrazovku a jakmile zjistí, že nikdo napsal slovo **TORMENTOR!** (projev některých virů z rodiny Murphy) reaguje přepsáním začátku pevného disku.

Virus Crepate

Rezidentní multipartitní virus italského původu. Napadá EXE, COM a OV? soubory při jejich spouštění, otevírání, vytváření a přejmenování. Souborům, jejichž název končí na 'AN' (např. SCAN) a na 'LD' (VSHIELD), se raději vyhne.

Tělo viru je zakódováno, pouze tři bajty před koncem je viditelný text 'cs', podle kterého Crepate poznává napadené soubory. Dekryptovací smyčka je sice konstantní, ale je proložena velkým množstvím náhodných dat, takže se na první pohled může zdát, že jde o polymorfní virus.

Virus je napsán velmi kvalitně, což se bohužel týká i destrukce akce, která se nespokojí s přeformátováním začátku disku, ale dá si tu práci se zjištěním konkrétních parametrů a pokusí se ho přeformátovat celý. Destrukce je naplánována na 16. a 17. den v libovolném měsíci.

V těle viru jsou tyto texty:

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

```
Crepa(c) bye R.T.
```

```
COMcomEXEexeOV?ov?
```

P.S.

Crepa znamená smrt.

Virus Crew

Rodina nerezidentních virů, které napadají COM soubory v aktuálním adresáři. Aby nebyly tak nápadné, s pravděpodobností 70% neudílají při svém spuštění vůbec nic.

Od června do prosince občas obtížují textem (který se v jednotlivých mutacích nepatrně liší):

```
+-----+
|                                         |
|                This program is cracked by                |
|                                                         |
|            _____            Notice this            |
|            -_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_- |
|            -_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_- |
|            -_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_- |
|            _____            TS ain't smart at all.   |
|            -_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_- |
|            -_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_- |
|            -_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_- |
|            -_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_- |
|            -_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_- |
|            -_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_- |
|            _____            Distribution since        |
|            -_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_- |
|            -_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_- |
|            -_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_- |
|            -_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_- |
|            _____            11-06-1987 (or 06-11-1987) |
|            -_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_- |
|            -_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_- |
|            -_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_- |
|            _____            Press any key            |
|            -_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_- |
|            -_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_- |
|            -_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_- |
|            _____            |
+-----+
```

Virus CSL

Rodina jednoduchých rezidentních virů, které napadají spouštěcí soubory typu COM a snaží se napadnout příkazový interpret operačního systému. Tyto viry sice obvykle neobsahují žádnou destruktivní akci, ale způsob, jakým zacházejí s pamětí, lze chápat jako žádost o konflikt s operačním systémem.

Varianta CSL.Pre_Release

Tato varianta obsahuje text:

`26.07.91.Pre-released Microelephant by CSL`

Varianta CSL.V4

Tato varianta obsahuje text:

`Microelephant V4 by CSL`

Pokud je spuštěna 1.1., 2.2., 3.3. atd., tak v paměti CMOS vynuluje informace o typech pevných disků.

Varianta CSL.V5

Tato varianta obsahuje text:

`Microelephant V5 by CSL`

Virus Czech_Happy

Rezidentní virus českého původu, který napadá spouštěcí soubory typu COM a EXE. Obsahuje triviálně zakódované dětské texty, kterými od roku 1994 obtěžuje v lednu:

```
* * * 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 <<
```

Prvního ledna otravuje vždy, v ostatních dnech až po určitém počtu volání služeb operačního systému.

Czech_Happy se snaží obejít "udičky" různých antivirových programů tím, že nenapadá soubory s dnešním datem.

Virus DataCrime

Nerezidentní souborový virus, který napadá soubory typu COM.
Tisňi pøed pokusem o formátování disku se pøedstaví:

DATA CRIME VIRUS
RELEASED: 1 MARCH 1989

Pak zaène v nekoneèné smyèce pípát.

Virus Digger

Varianta Digger.600

Jednoduchý rezidentní virus, který napadá spouštěcí COM soubory. Způsob jakým se instaluje do paměti může mít za následek časté pády operačního systému. Díky chybě také cca 1% souborů nenapadne správně.

Vždy v 10:00 a v 17:00 rozblíká v levém horním rohu obrazovky:

```
_____DIGGER_____
_____L_____
_____
_____
_____
_____
_____
_____
```

Obsahuje také text:

```
DIGGER IS MY LOVE!
```


Virus Dropper

Varianta Dropper

Tento program není napaden virem, ale slouží k instalaci bootviru na disketu. Přestože je "slušný" a vyžaduje potvrzení této operace, bylo by asi lepší ho smazat.

Virus Ear

Jednoduchý nerezidentní virus, který útočí na soubory typu COM a EXE. Jeho zdrojový text byl publikován v undergroundovém elektronickém časopise 40Hex.

Virus sám není nijak zajímavý, za zmínku stojí jenom způsob, kterým obtěžuje uživatele vždy první den v měsíci. Zeptá se na polohu některé z částí ucha:

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

Místo znaku * uveďte některou z těchto částí:

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

A poeká si na odpovědi. Pokud je odpovědi správná, napíše:

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

Špatnou odpovědi komentuje takto:

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

A napadený program nespustí.

Kromě textů, které jsou součástí kvízu obsahuje ještě "podpis" autora:

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

Tělo viru je triviálním způsobem kódováno.

Virus FCB

Nerezidentní přepisující virus, který ničí soubory typu EXE i COM.
Je zajímavý snad jedině tím, že používá výhradně zastaralých funkcí pro přístup k souborům (tzv. FCB služby).
Obsahuje tento text:

```
401 File Virus.  
Infects any .COM or .EXE file on any writeable Device
```

Virus Fifo

Jednoduchý rezidentní virus, který napadá soubory typu COM. Neobsahuje žádnou destruktivní činnost, ale způsob jakým se instaluje do paměti a jak používá zásobník nutně povede k častým haváriím systému. Fifo obsahuje, ale nepoužívá, slovo:

FIFO

Virus Finnish

Varianta Finnish.709

Rezidentní virus, který napadá spouštěcí nebo otevírané COM soubory. Obsahuje větší množství chyb a opomenutí, kterým mohou vést k pádu operačního systému.

Virus Flip

Rezidentní polymorfní viry, které napadají spouštěné soubory (COM i EXE) a tabulku rozdělení pevného disku.

Snaží se trasováním zjistit a používat původní adresu obsluhy služeb operačního systému a obejít tak některé monitorovací programy.

Svou přítomnost demonstrují převrácením obrazu na monitoru.

Obsahují zakódovaný text:

OMICRON by PsychoBlast

Varianta Flip.2153

Předvádí se druhý den v měsíci mezi desátou a jedenáctou hodinou, jestliže byl počítan po napadení alespoň dvanáctkrát zapnut.

Varianta Flip.2343

Předvádí se druhý den v měsíci mezi desátou a jedenáctou hodinou.

Ve spouštěných souborech vyhledává skupinu instrukcí, kterou modifikuje tak aby byla při jejich vykonávání zavolána zvláštní funkce viru.

Zdá se, že cílem je maskovat zvětšení délky napadeného souboru.

Vzhledem k tomu, že tuto sekvenci je možné najít v mnoha souborech (např. COMMAND.COM a DEBUG.COM z MS-DOSu 3.30 nebo DEBUG.EXE a CHKDSK.EXE z MS-DOSu 5.00), může tato úprava vést k oběsným pádům operačního systému. Stejně skoně spuštění takto upraveného programu, jestliže virus nebude aktivní v paměti.

Varianta Flip.MBR

Zavadiě některého z virů kmene Flip.

Virus Freew

Skupina nerezidentních, poměrně nepříjemných virů, které napadají soubory typu COM.

Varianta Freew.718.A

Prochází všechny adresáře a napadá v nich soubory typu COM. Programům [MKS_VIR.COM](#) a [COMMAND.COM](#) se raději vyhne.

Od roku 1993 vždy v lednu soubory se sudou hodinou vzniku nenapadá, ale nic není. Zničený program pak při svém spuštění napíše:

```
Program terminated normally
```

a skončí.

Virus Friday_13th

Rodina jednoduchých virů, které napadají soubory typu COM v aktuálním adresáři. Souboru [COMMAND.COM](#) se raději vyhnou.

V pátek třináctého se z napadených souborů odstraní. I s jejich původním obsahem.

Virus Fumble

Jednoduché nerezidentní viry, které útočí na soubory typu COM v aktuálním adresáři.

Přestože virus sám není rezidentní, instaluje do paměti krátkou funkci, která sleduje čtení z klávesnice a občas přečtený znak zamění za sousední.

V těle viru je viditelná "mapa" klávesnice,

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

značka viru 'v1' a maska, kterou používá pro hledání obětí: '* .COM'.

Virus Haifa

Rezidentní polymorfní viry, které sledují prohledávání adresářů a při té příležitosti se snaží nejen zaútočit na soubory typu COM a EXE, ale také poškodit některé datové soubory.

Varianta Haifa.B

Autor viru má pravděpodobně svůj disk C: označen labelem `AT_286`. Pokud virus takový label najde, nešíří se ani neútočí na datové soubory. Svou přítomnost demonstruje 8.4. a 24.8., kdy při spuštění napadeného programu s pravděpodobností 1% napíše:

```
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...
```

Na začátek souborů s příponou PAS vkládá:

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

ASM soubory vyšperkuje tímto úryvkem:

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

Doprostřed souborů s příponou DOC a TXT vkládá:

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

Virus Halloween

Rodina virù èeského pùvodu. Rezidentní souborové viry napadající spouštiné soubory typu COM a EXE. Většinou neobsahují žádnou destruktivní akci.

Nenapadají soubory, jejichž jméno obsahuje některý z následujících znaků:

```
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.
```

V jednotlivých variantách se tato tabulka nepatrně mění, v několika není vůbec.

Viry z rodiny Halloween obvykle obsahují jednoduše zakódovaný text, který v konkrétní den (liší se u jednotlivých mutací) zobrazí a provedou RESET počítače.

Varianta Halloween.1063

Nenapadá COM soubory a nesnaží se vyhýbat antivirovým programům.

Varianta Halloween.1376.A

První (a dosud nejrozšířenější) mutace viru Halloween. Obsahuje jednoduše zakódovaný text, kterým vás potěší 1.listopadu:

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

```
*****
```

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

Varianta Halloween.1376.B

Nepatrně modifikovaný Halloween.1376.A. 21.února vypíše tento text:

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

```
Preji ti vsechno nejlepsi k tvemu svatku ahoj
```

Varianta Halloween.1684

Nenapadá COM soubory a nesnaží se vyhýbat antivirovým programům. Obsahuje tento text:

Virus Howard_Stern

Mimořádně stupidní nerezidentní virus, který napadá COM soubory. Pokud je napadený program spuštěn mezi šestou a jedenáctou hodinou dopoledne, virus napíše:

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

a zastaví počítač.

Virus je plně hrubými chybami, které s vysokou pravděpodobností povedou k havárii systému ještě dříve, než se stihne nijak rozšířit.

Dále obsahuje Howard_Stern tyto texty:

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

(To není chyba, skutečně je tam tento výkřik dvakrát !)

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

Virus J&M

Napadá BOOT sektor disket a MBR pevného disku. Obsahuje nezakódovaný text **J&M**. Patnáctého listopadu se pokusí přeformátovat začátek disku C:. Tělo tohoto viru je triviálně kódováno.

Varianta J&M.B

Tato varianta má přehozeno pořadí některých instrukcí v dekryptovací smyčce. Jinak je zcela totožná s J&M.A.

Virus Justice

Rezidentní virus, který napadá soubory typu COM při jejich otevírání a spouštění. Je napsán speciálně pro MS-DOS verze 3.10 a 3.30. Díky tomu může používat konstantní adresy pro bezpečné volání některých služeb operačního systému (a vyhnout se tak monitorovacím programům). Pod novějšími verzemi MS-DOSu se Justice nešíří.

Připojuje se na konec své oběti, ale COMMAND.COM napadá tak, že se vloží do datových oblastí v něm a proto ho neprodlouží. Nakažené soubory začínají dvěma instrukcemi NOP (90h).

V těle viru jsou čitelné tyto texty:

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

```
...AND JUSTICE FOR ALL
```

Obsahuje velmi nepříjemnou destruktivní akci. Sleduje zápisy na disk a s pravděpodobností cca 0.4% provede zápis nejen na správné místo, ale také "o stopu níž".

Virus Kampana

Skupina zajímavých virů španělského původu, komentujících kvalitu služeb tamní telekomunikační společnosti. (V této souvislosti se nabízí otázka, co by autor těchto virů spáchal, kdyby byl obeznámen s těmito službami u nás. Raději nejmenovaný kolega tvrdí, že asi sebevraždu.)

Kampana není multipartitní viru v pravém slova smyslu. Napadá soubory typu COM a vypouští bootvirus, který pak ovšem žije svým vlastním životem a není schopen útočit na soubory.

Kampana maskuje prodloužení souborů v adresáři a na spouštěné (některé verze i na otevírané) programy útočí. Snaží se trasováním zjistit původní adresy obsluhy některých systémových funkcí (Int 13h a 21h) a ty pak používá. To že sám přebírá přerušení 21h se snaží maskovat tím, že má ve svém tile několik různých můstků vedoucích ke skutečnému vstupnímu bodu obsluhy a náhodně vybírá, který z nich bude používat. Tilo viru (u varianty Kampana.3445 pouze jeho část) je zakódováno a obsahuje (ale nepoužívá) krátký text.

Bootvirus poěta kolikrát byl poětaè spuštìn a po dosažení nastavené hodnoty se pøedstaví a zaène pøepisovat obsah disku.

Varianta Kampana.MBR.A

Obsahuje text:

`Campaða Anti-TELEFONICA (Barcelona)`

Destrukci zahájí při 400 startu poětaèè z napadeného disku.

Varianta Kampana.MBR.B

Obsahuje text:

`Anti-TELEFONICA 2 (CSFR)`

Destrukci zahájí při 400 startu poětaèè z napadeného disku.

Tato varianta pravděpodobně vznikla modifikací samotného bootviru. Nemáme informace o existenci nějakého souborového viru Kampana, který by byl nosičem této varianty bootviru Kampana.

Varianta Kampana.MBR.C

Obsahuje text:

`Campaða Anti-TELEFONICA (Barcelona)`

Destrukci zahájí při 333 startu poětaèè z napadeného disku.

Varianta Kampana.3445

Obsahuje text:

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

Je nosièem bootviru Kampana.MBR.A.

Varianta Kampana.3784

Obsahuje 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 -

Je nosièem bootviru Kampana.MBR.C.

Varianta Kampana.3700

Obsahuje 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 -

Je nosièem bootviru Kampana.MBR.A.

Virus Klepavka

Rezidentní virus českého původu, který napadá COM soubory při jejich spuštění a první tři při jejich hledání.

Osmnáctého února se představí:

```
KLEPAVKA VIRUS  
*****
```

```
Thank you for reproduction
```

a zaène "tøepat" s obrazem na monitoru poèítaèe.

Virus Lao_Doung

Tento virus napadá BOOT sektor disket a MBR pevného disku. Při spuštění napadeného počítače zahraje s pravděpodobností 0.8% melodii.

Virus Letter_H

Krátký rezidentní virus, který napadá spouštěné soubory typu COM (mimo COMMAND.COMu). Své oběti označuje znakem 'H' umístěným ve čtvrtém bajtu souboru.

Neobsahuje žádnou destrukční akci ani žádný text. Je zajímavý pouze způsobem použití časovače, kterým se snaží znesnadnit trasování napadeného souboru.

Virus Level_3

Rezidentní polymorfní virus slovenského původu. Zdá se, že je dalším dílkem autora viru One_Half. (Ten se svého času velmi úspěšně šířil i mimo území střední Evropy.)

Level_3 napadá spouštěcí soubory typu EXE a COM. Sleduje také vytváření souborů a jakmile zjistí, že vaše práce s novým souborem skončila, využije příležitost a zaútočí.

Své oběti poznává podle zvláštního (proměnného) nastavení data a času vzniku souboru a maskuje jeho prodloužení tak, aby příkaz DIR vypsal původní délku. U podobných virů lze pro jejich rychlé nalezení použít jednoduchý program, kontrolující datum a čas souborů. Tato metoda sice není nijak zvlášť spolehlivá, ale v nouzi se jistě může hodit. Autor tohoto viru s tím zřejmě počítal a tak Level_3 neoznačuje všechny napadené soubory, ale cca u 4% obětí ponechá původní hodnoty.

To ovšem není jediný způsob jak se virus brání před odhalením. Detekuje přítomnost rezidentních částí některých antivirových programů a vypíná je. Napadá soubory jejichž jména začínají na:

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

Při spuštění programů F-PROT nebo CHKDSK se virus stáhne do "ilegality" a přestane napadat soubory a maskovat prodloužení délky již napadených programů.

Pokud si bude nějaký zvědavce prohlížet oblast paměti obsazenou virem, dozví se že jejím majitelem je COMMAND a na začátku těla viru najde text * EMM 1.0 *, který by mohl slabší povahy přesvědčit, že jde o korektní část systému.

Součástí boje viru proti jednoduchým metodám obrany je i způsob jakým zjišťuje svou přítomnost v paměti. Nepoužívá žádné volání systémové služby, na které mu může smlouvenou odpověď poskytnout nejen jeho rezidentní kopie, ale i krátký jednoúhelový program. (To by samozřejmě zabránilo dalšímu šíření na takto chráněném systému.)

Každá 25. generace viru se sedmý den v měsíci představí:

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

V těle jsou ještě zakódovány tyto řetězce, které virus používá pro rozpoznání rezidentních částí antivirového programu TBAV:

TBMEMXXXTBCHKXXXTBDSKXXXTBFI

Virus Lisa

Jednoduše kódovaný virus, který hledá a napadá soubory typu COM.

Obsahuje (ale nepoužívá) toto zamilované blábolení:

```
love.girl.LISA.forever.666  
(c) Metal Militia / Immortal Riot Sweden 24/12/93  
Thunderclouds pass the sky, dreams & thoughts goes thru  
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 Lock_Show

Jednoduchý virus, který napadá COM soubory v aktuálním a v kmenovém adresáři. Napadení souboru oslaví blikáním s kontrolkami na klávesnici. Neprovádí žádnou destrukční akci a neobsahuje žádný viditelný text.

Virus Mange-tout

Tento rezidentní virus si v paměti udržuje většinu svého těla v zakódovaném tvaru. Jestliže nějaký program požádá o zjištění volného místa na disku, Mange-tout vyhoví a při té příležitosti se pokusí napadnout jeden soubor typu COM nebo EXE v aktuálním adresáři disku.

Pokud se nikdo alespoň hodinu nedotkne klávesnice, virus to považuje za neodpuštělnou lenost a revanšuje se přeformátováním náhodně vybrané stopy disku C:.

Virus Minsk

Rezidentní virus, který napadá otevírané soubory typu EXE a COM. Pokud zjistí přístup k souboru s příponou DBF, začne si hrát. Při každém dvacátém čtení vrátí místo správného obsahu samé mezery. Pro své rozpoznání v paměti si Minsk zapíše do systémové tabulky text `vo`. Bohužel na místo, které občas používají i jiné programy, což lze hodnotit jako žádost o zhrucení operačního systému.

Virus navíc obsahuje několik pozoruhodně triviálních chyb, které pravděpodobně vznikly drobnými překlepy ve zdrojovém textu. (Například použití čísla 21 místo správného 21h, nebo vynechání operátoru NOT.) Tyto chyby mohou vést k havárii napadeného programu a výrazně omezují šance Minsku na šíření.

Virus MSK

Rodina hloupouèkých pøepisujících virù. Likvidují EXE soubory v aktuálním adresáři (níkteré mutace nièí i soubory typu COM) a upozoròují na sebe níjakým textem.

Varianta MSK.272.A

Obsahuje text:

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

Varianta MSK.284

Obsahuje text:

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

Virus Coffe_Shop:MtE

Varianta Coffe_Shop:MtE

Rezidentní virus kódovaný pomocí knihovny MtE. Napadá EXE soubory při jejich spuštění a kopírování. Pokud jméno souboru začíná některou z těchto dvojic znaků, tak se mu raději vyhne:

SC
CL
VS
NE
HT
TB
VI
RA
FE
MT
BR

Virus obsahuje tyto texty:

Amsterdam = COFFEESHOP!
MK1992

MtE 0.90B

Pokud je spuštěn v pátek, tak s pravděpodobností 1/60 poskládá ze semigrafických znaků velký nápis LEGALIZE CANNABIS a javorový list.

Virus Corrected:MtE

Varianta Corrected:MtE

Rezidentní virus kódovaný pomocí knihovny MtE. Napadá EXE i COM soubory při jejich spuštění. Jestliže uplynulo alespoň půl hodiny od okamžiku, kdy se virus dostal do paměti, oslaví napadení souboru textem:

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

Samozřejmě také obsahuje tento text:

```
MtE 0.90B
```

Tento virus je pravděpodobně odvozen od varianty Groove. Obsahuje funkci pro mazání souborů, ale tato funkce není nikdy volána a seznam který by měla používat je vyplněn mezerami.

Virus Dedicated:MtE

Varianta Dedicated:MtE.A

Tento virus je kódován pomocí knihovny MtE a napadá COM soubory v aktuálním adresáři. Jestliže se mu nepodaří žádný vhodný soubor najít, může přepsat obsah náhodně vybraného sektoru disku. Obsahuje tyto texty:

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

```
*.COM
```

```
MtE 0.90B
```

Varianta Dedicated:MtE.Cryptlab

Tento virus je kódován pomocí knihovny MtE a napadá COM soubory v aktuálním adresáři. Jestliže se mu nepodaří žádný vhodný soubor najít, může přepsat obsah náhodně vybraného sektoru disku. Obsahuje tyto texty:

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

```
*.*
```

```
MtE 0.90B
```

Virus Encroacher:MtE

Varianta Encroacher:MtE.A

Tento virus je kódován pomocí knihovny MtE a napadá COM soubory v aktuálním adresáři. Nemá rád program Central Point Antivirus, snaží se smazat jeho soubory `C:\CPAV\CPAV.EXE` a `C:\CPAV\VSAFE.COM`. Soubory kontrolních souětů vytváøené tímto programem (`chklist.cps`) maže tak, aby jejich pøípadná obnova byla ztížena. Pokud je spuštìn odpoledne, hledá a poškozujè soubory `*.EXE`. Takto ošetøené programy pøi svém spuštìní provedou reset poèítaèe. Kromì uží uvedených textù obsahuje virus toto:

```
ENCROACHER is here
```

```
MtE 0.90B
```

Virus Fear:MtE

Varianta Fear:MtE

Tento virus je kódován pomocí knihovny MtE a napadá COM soubory v aktuálním adresáři. Jestliže se mu nepodaří žádný vhodný soubor najít, počká na stisk klávesy. Původním záměrem autora viru zřejmě bylo vypsát tento text ale volá špatnou funkci operačního systému:

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

Dále virus obsahuje tyto texty:

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

```
*.COM
```

```
MtE 0.90B
```

Virus Groove:MtE

Varianta Groove:MtE

Rezidentní virus kódovaný pomocí knihovny MtE. Napadá EXE i COM soubory při jejich spuštění. Jestliže uplynulo alespoň půl hodiny od okamžiku, kdy se virus dostal do paměti, oslaví napadení souboru textem:

```
Dont worry, 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 ....
```

Samozřejmě také obsahuje tento text:

```
MtE 0.90B
```

V těle viru je seznam souborů, které se pokouší zničit:

```
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

Varianta Pogue:MtE

Rezidentní virus kódovaný pomocí knihovny MtE. Napadá COM soubory při jejich spuštění, nebo kopírování. Obsahuje tyto texty:

`TNX2DAV` (Poděkování autoru MtE, který si říká Dark Avenger)

`Pogue Mahone!`

`MtE 0.90B`

Pokud je spuštěn před osmou ráno, zahraje melodii. První máj oslaví internacionálou bez ohledu na to, v kolik hodin je spuštěn.

Virus Questo:MtE

Varianta Questo:MtE

Další z mnoha variant vzniklých nepatrnými úpravami demonstarèního viru, který byl distribuován s knihovnou MtE. Napadá COM soubory v aktuálním adresáři a pokud nenajde žádnou vhodnou obì, může se pokusit smazat obsah náhodnì vybraného sektoru. Pokud se to stane v pátek, pøepíše BOOT sektor disku C: tímto textem:

```
Questo sistema Å stato infettat
```

Dále obsahuje tyto texty:

```
*.COM
```

```
MtE 0.90B
```

Virus Murphy

Rezidentní viry napadající EXE i COM soubory. Existuje velké množství nepatrně se lišících mutací.

Viry z této rodiny se snaží najít a používat původní obsluhu diskových operací z ROM počítače. To může některým rezidentním hlídačům zabránit v detekci podezřelých aktivit (třeba přepisování nebo formátování disku).

Většina mutací má na začátku krátký nezakódovaný text, který občas vypisují na obrazovku. Některé nechají po obrazovce běhat "ksichtík" a některé se snaží zničit vaše data mazáním souborů nebo přepisem, případně formátováním, části disku.

Varianta Murphy.Finger

V sobotu napíše:

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

a pokusí se naformátovat několik sektorů vašeho disku.

Varianta Murphy.Tormentor.D

Jestliže je 24. den v měsíci, pokusí se přepsat vaše data na disku.

Varianta Murphy.Tormentor.B

Jestliže je 31. den v měsíci, pokusí se přepsat vaše data na disku.
Obsahuje nezakódované texty

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

a

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

které ale nikdy nevypíše.

Varianta Murphy.Erasmus

Ve čtvrtek napíše:

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

```
Alla rivoluzione del grande numero sette,  
Apparirà ai tempi giochi d'Ecatombe,
```

Non lontano dalla grande et  del millennio
Coloro che entrarono usciranno dalle loro tombe.

Saint-R mi, 14 dicembre 1533

a pokus  se naform tovat nikolik sektor  va eho disku.

Varianta Murphy.Delyrium.1778

V  ervnu se pokus  smazat soubory, po kodit data na disku
a napsat 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

Obsahuje tak  text (c) IVRL 1991 (Ivrl Head Quarter, Milan Italy),
kter  ale nikdy nepou ije.

Varianta Murphy.Diabolik

V pond l  nap še:

Diabolik Ltd.
(C) 1991 by Odrowad Trow

a pokus  se naform tovat nikolik sektor  va eho disku.

Varianta Murphy.Cemetery

Obsahuje text CEMETERY, ketr  nikdy nevyp še.
Pokud vydr z  v pam ti alespo  16 hodin, nech  po obrazovce b hat
ksicht k. Sleduje s riov  linky a pokud p ijde znak '1', pokus 
se prov st restart po  ta e.

Varianta Murphy.Bad_Taste

V pond l  nap še:

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

a pokus  se naform tovat nikolik sektor  va eho disku.

Varianta Murphy.AntiChrist

Neobsahuje a nevypisuje  adn  text. Pokud naraz  na soubor
s p  ponou ZIP, sma e ho.

Varianta Murphy.Amilia.A

Tento text vypíše pokud je spuštěn v neděli:

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

Tento text je také viditelný v těle viru, ale nikdy není vypsán:

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

Pokud vydrží v paměti alespoň 16 hodin, nechá po obrazovce běhat ksichtík.

Varianta Murphy.Murphy.1521

Obsahuje text, který nikdy nevypisuje:

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

Pokud vydrží v paměti alespoň 10 hodin, nechá po obrazovce běhat ksichtík.

Varianta Murphy.Swami.A

Patnáctého dubna napíše:

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

a pokusí smazat nějaký soubor.

Varianta Murphy.Smack.1835

V pátek se zeptá `Is today Friday? (Y/N)` a pokud odpovíte 'Y' napíše `Sorry but on Friday I wish not work!!` a skončí. Jakákoliv jiná odpověď se zjeví viru dotkne a odmítní ji vypsáním textu `You are untruthful!! For punishment I format your HD Fat!!` a formátováním části disku.

Dále virus obsahuje (ale nepoužívá) tyto texty:

```
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!
```

Varianta Murphy.Pest

Pokud se v pátek pokusíte spustit nějaký EXE soubor, virus napíše:

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

Při spuštění COM souboru vás v pátek potíší textem:

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

Za pokus o spuštění COM souboru v sobotu bude odmítní takto:

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

Obsahuje (ale nezobrazuje) také tyto texty:

```
(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!
```

Spuštění programu jehož jméno končí AN.EXE nebo HK.EXE bude chápáno jako zdvořilá žádost o formátování disku a virus jí vyhoví.

Varianta Murphy.Migram.B

V sobotu napíše:

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

a pokusí se naformátovat několik sektorů vašeho disku.

Varianta Murphy.Migram.A

V sobotu napíše:

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

a pokusí se naformátovat několik sektorů vašeho disku.

Varianta Murphy.Murphy.1480

Obsahuje text, který nikdy nevypisuje:

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

Pokud vydrží v paměti alespoň 10 hodin, nechá po obrazovce bítat ksichtík.

Varianta Murphy.Murphy.1284

Obsahuje text, který nikdy nevypíše:

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

Varianta Murphy.Murphy.1277

Obsahuje text, který nikdy nevypíše:

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

Varianta Murphy.Kamasya

V úterý napíše:

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

Varianta Murphy.HIV

Tento text vypíše pokud je spuštěn v sobotu:

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

Pokud vydrží v paměti alespoň 16 hodin, nechá po obrazovce bítat ksichtík.

Virus On_64

Jednoduchý nerezidentní virus, který napadá soubory typu COM.
Jestliže je spuštěn alespoň 64 krát, zničí napadený soubor a přepíše začátek pevného disku.

Virus Page

Rezidentní viry, který napadají soubory typu COM i EXE při jejich spouštění, otevírání, přejmenování a při nastavování atributů. Jsou výtvozem jednoho z členů skupiny NuKE, která sdružuje autory virů.

Varianta Page.1206

Maskuje zvětšení délky svých obětí a obsahuje jednoduchý trik, který má zabránit trasování napadeného programu.

Obsahuje texty:

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

Varianta Page.1221

Tato varianta je polymorfní a maskuje zvětšení délky svých obětí. Snaží se bránit proti antivirovým programům. Nenapadá SCAN, TBAV a F-PROT. Obsahuje jednoduchý trik, který má zabránit trasování napadeného programu. Vyhledává soubory kontrolních souětů a maže je:

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

Obsahuje texty:

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

Virus Phi

Napadá BOOT sektor disket a MBR pevného disku. Jestliže je při startu napadeného počítače zapnutý CapsLock a vypnutý NumLock, Phi posune obsah okna ve středu obrazovky o řádek dolů a zapne NumLock. Při napadení diskety vypíše znak Ÿ.

Virus Pieck

Polské rezidentní multipartitní stealth viry. Kromě souborů typu COM a EXE napadají také tabulku rozdělení pevného disku.

Za určitých okolností je virus Pieck ochoten se odstranit z MBR a vyléčit napadené soubory.

Varianta Pieck.2016

Z pevného disku se odstraní, jestliže nějaký program zavolá obsluhu disků (Int 13h) a v registrech AX a BX předá text `mgre`.
Programy spuštěné z diskety vyléčí.

Třetího března požádá o zadání hesla:

```
Podaj haslo ?
```

Pokud odpovíte správným heslem (`pieck`), tak slušně pozdraví:

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

Na špatné heslo odpoví

```
Blad !
```

a zastaví počítač.

Varianta Pieck.4444

Tato varianta získává "bezpečné" adresy systémových služeb jejich trasováním a snaží se zabránit odhalení tím, že virus je i v paměti zakódován.

Jestliže při zapnutí napadeného počítače napíšete slovo `test`, virus o sobě napíše nějaké informace. Například:

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

Pokud napíšete slovo `kaczor`, virus napíše:

```
Zrobione.
```

a vyléčí disk.

Napadené soubory vyléčí při jejich spuštění z diskety.

Po roce 1995 instaluje vždy 3. března funkci, která výrazně zrychluje běh systémového času a zvolna rozdvouje obraz na monitoru. Podobného efektu lze dosáhnout i bez počítače, konzumací dostatečného množství alkoholu.

Virus Pixel

Rodina jednoduchých virů, které napadají soubory typu COM v aktuálním adresáři. Některé mutace se pouze po určitém počtu spuštění představí (text je v těle viru čitelný), ale existují i varianty vybavené destrukční funkcí.

Viry Pixel.Hydra představují svým způsobem unikátní kroniku. Jsou to vlastně jednotlivé vývojové fáze jednoduchého viru.

Varianta Pixel.257

Druhá generace se s 50% pravděpodobností při spuštění představí:

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

Varianta Pixel.275

Druhá generace se s 50% pravděpodobností při spuštění představí:

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

Varianta Pixel.277

Pátá generace s 50% pravděpodobností přeprogramuje interní čítač počítače tak, že dojde k havárii systému s hlášením o hardwarové chybě paměti.

Varianta Pixel.283

Desátá generace s 50% pravděpodobností při spuštění napíše:

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

Varianta Pixel.295

Pátá generace se s 50% pravděpodobností při spuštění představí:

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

Varianta Pixel.299

Pátá generace se s 50% pravděpodobností při spuštění představí:

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

Varianta Pixel.345.A

Pátá generace se s 50% pravděpodobností při spuštění představí:

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

Varianta Pixel.345.B

Pátá generace se s 50% pravděpodobností při spuštění představí:

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

Varianta Pixel.779

Pátá generace s 50% pravděpodobností při spuštění napadeného programu pípne.

Varianta Pixel.837

Pátá generace se s 50% pravděpodobností při spuštění sviøí:

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

Varianta Pixel.847.Advert

Pátá generace s 50% pravděpodobností při spuštění dílá reklamu:

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

Varianta Pixel.847.Hello

Pátá generace s 50% pravděpodobností při spuštění napíše:

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

Varianta Pixel.847.Near_End

Pátá generace s 50% pravděpodobností při spuštění napíše:

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

Varianta Pixel.847.Pixel

Pátá generace se s 50% pravděpodobností při spuštění představí:

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

Varianta Pixel.847.RV1

Pátá generace se s 50% pravděpodobností při spuštění představí:

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

Varianta Pixel.850

Pátá generace se s 50% pravděpodobností při spuštění představí:

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

Varianta Pixel.852

Třetí generace s 50% pravděpodobností při spuštění vypíše tento text:

```
ž!ò Ôá éÀáòà« š °òú«óš+ _á_à« ! Âšò ó_šìàš _Èò Ôá »_ò!___«ø__ó« !
```

Text je pravděpodobně bulharský, bohužel zatím nemáme k dispozici popis rozložení znaků, takže není zobrazen zcela přesně.

Varianta Pixel.854

Pátá generace při spuštění vypíše s 50% pravděpodobností text:

```
ž!ò Ôá éÀáòà« š °òú«óš+ _á_à« ! Âšò ó_šìàš _Èò Ôá »_ò!___«ø__ó« !
```

Text je pravděpodobně bulharský, bohužel zatím nemáme k dispozici popis rozložení znaků, takže není zobrazen zcela přesně.

Varianta Pixel.877

Devátá generace s 50% pravděpodobností při spuštění obtěžuje textem:

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

Varianta Pixel.892

Třetí generace při spuštění vypíše s 50% pravděpodobností text:

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

a pokusí se formátovat začátek diskety v mechanice A:

Varianta Pixel.899

Po 1.4. s 50% pravděpodobností při spuštění vypíše text:

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

a pokusí se formátovat začátek diskety v mechanice A:

Varianta Pixel.936

Po 1.4.1991 s 50% pravděpodobností při spuštění vypíše text:

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

a pokusí se formátovat začátek diskety v mechanice A:

Varianta Pixel.Cancer

Toto je "odtušená" mutace. Neobsahuje žádný text, ani žádnou destrukční akci.

Varianta Pixel.Hydra.340

Obsahuje tyto nezakódované texty:

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

Pokouší se obnovit adresu obsluhy disketových operací.

Varianta Pixel.Hydra.342

Obsahuje tyto nezakódované texty:

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

Pokouší se obnovit adresu obsluhy disketových operací.

Varianta Pixel.Hydra.343

Obsahuje tyto nezakódované texty:

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

Nastavuje prázdný znak v oblasti paměti určené pro původní Microsoft Basic a bezprostředně poté volá službu pro reset disku. Může se jednat o nějakou interakci s jiným virem.

Varianta Pixel.Hydra.368

Obsahuje tyto nezakódované texty:

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

Níeí soubory typu EXE umístíne v aktuálním adresáři.

Varianta Pixel.Hydra.372

Obsahuje tyto nezakódované texty:

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

Po napadení souboru se pokusí znièit soubory COMMAND.*

Varianta Pixel.Hydra.391

Obsahuje tyto nezakódované texty:

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

Po napadení souboru pøímó zavolá nijakou službu starších modelù øadièe disku. Její pøesný význam se nepodaøilo identifikovat.

Varianta Pixel.Hydra.403

Obsahuje tyto nezakódované texty:

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

Pøi napadení souboru se pøedstaví:

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

a zmíní tabulku obsluhy pøerušení tak, že systém může havarovat.

Varianta Pixel.Hydra.495

Obsahuje tyto nezakódované texty:

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

EXE soubory pøepisuje krátkým programem, který pøi jejich spuštění zobrazí text:

Who is John Galt?

Varianta Pixel.Hydra.736

Obsahuje tyto nezakódované texty:

```
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.  
-----
```

Po napadení souboru se představí:

```
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

Rezidentní virus napadající spouštěcí COM soubory.
Součástí dat v jeho těle je boot virus Stoned.Michelangelo.E,
který Plastic_Pizza vkládá do BOOT sektoru vašich disket.

Virus Pojer

Rodina virù èeského pùvodu. Napadají spouštìné COM a EXE soubory. Vlastní tělo viru je jednoduchým způsobem zakódováno a dekodovací smyčka obsahuje proměnné části.

Tisni pøed koncem viru je nezakódovaný text "XmY?!&", podle kterého Pojer pozná, že soubor už byl napaden.

Varianta Pojer.1919

17.11. a 6.2. napíše:

```
** 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 !
```

Občas bliká v levém horním rohu obrazovky znakem ' _ '

Varianta Pojer.1935

17.11. a 6.2. napíše:

```
** 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 !

Obèas bliká v levém horním rohu obrazovky znakem ' _ '

Varianta Pojer.1941

17.11. a 6.2. napíše:

```
** 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 !

Obèas bliká v levém horním rohu obrazovky znakem ' _ '

Varianta Pojer.1949

17.11. a 6.2. napíše:

```
** 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 !

Obèas napíše bílým písmem na èerveném podkladu text:

Zruste armadu a jdete domu!!

Virus Poledne

Rezidentní virus českého původu. Napadá spouštěné EXE a COM soubory. Obsahuje zakódovaný text `Ja jsem Karlik2.` podle něj poznává, které soubory už napadl.

Ve dvanáct hodin smaže obrazovku a napíše:

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

Počká několik vteřin, napodobí zvuk časového znamení a napíše:

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

Aby obešel některé kontrolní programy, snaží se Poledne zjistit a používat původní adresu přerušení 21h.

Virus Prague

Rodina rezidentních virů, které napadají spouštěcí soubory typu COM a liší se pouze svými vnějšími projevy.

Varianta Prague.BackTime

Obsahuje text:

`BackTime`

Pokud je virus v paměti, jdou systémové hodiny pozpátku.

Varianta Prague.Blinker

Obsahuje text:

`Blinker`

Registr videokarty 'Interlace Mode' nastavuje na hodnotu 1. Moderní videokarty toto nastavení ignorují.

Varianta Prague.Joker

Obsahuje text:

`Joker`

Každých 14 vteřin poškodí obsah jednoho z registrů procesoru. Následky tohoto vandalizmu jsou nepředvídatelné. Začínají někde u "divného" chování programů a koně u zhroutení operačního systému.

Varianta Prague.Shaker

Obsahuje text:

`Shake`

Náhodně mění obsah registru videokarty 'Vertical Total Adjust'. Moderní videokarty to stejně nezajímá.

Virus Predator

Rezidentní virus, který napadá spouštěcí a otevírané COM soubory. Pokud je aktivní v paměti, maskuje nárůst délky a změnu data svých obětí.

V těle má zakódován text, který nikdy nepoužívá:

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

Predator sleduje čtení z disku a občas změní hodnotu náhodně vybraného bitu.

Virus Rage

Varianta Rage.575

Tento virus napadá soubory typu COM v aktuálním a kmenovém adresáři disku. Pokud zjistí přítomnost kontrolního programu FluShot, přestane se raději šířit.

Při spuštění napíše s 5% pravděpodobností text:

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

Třináctý den v měsíci se představí:

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

a zničí začátek disku C:.

Virus Raptor

Rezidentní virus českého původu. Napadá EXE soubory při jejich otevření nebo spuštění. Jestliže je den roven měsíci (tedy 1.1., 2.2. atd.) a není prosinec, tak vypíše text.

Varianta Raptor.A

Píše tento 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 stealth systems
You can be sure that Raptor2 will be totally untouchable!
```

(Díky chybì, je tento text vypisován i v prosinci.)

Třináctého dne v měsíci, přibližně 55 minut po spuštění, začne přesouvat modré obdélníky na obrazovce.

Varianta Raptor.B

Píše tento 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 stealth systems
You can be sure that Raptor2 will be totally untouchable!
```

Varianta Raptor.C

Píše tento 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 stealth systems
You can be sure that Raptor2 will be totally untouchable!
```

Třináctého dne v měsíci, přibližně 55 minut po spuštění, začne přesouvat modré obdélníky na obrazovce.

Virus Relzfu

Jednoduchý nerezidentní virus, který napadá soubory typu COM v aktuálním adresáři. V pátek třináctého napíše do levého horního rohu obrazovky text:

VirX 3/90

a zaèene v nekoneènè smyèce pípát.

(Tento text je v tile viru triviálním způsobem zakódován a shodou okolností jeho èást po zakódování vypadá takto: `ufzleR`. Odtud zøejmì pochází jeho název.)

Virus Sampo

Velmi zajímavý virus, který napadá MBR disků a boot sektor disket. Při svém startu kontroluje paměť na přítomnost několika starších boot virů (Joshi, Stoned) a případně je ničí. Snaží se přežít teplý start počítače (Ctrl-Alt-Del).

To že nemůže napadnout disketu chráněnou proti zápisu považuje tento virus zřejmě za urážku. Oplácí předstíráním, že disketa je napadena jiným boot virem (Kampana.A).

30. listopadu se hodinu až dvě po startu počítače představí:

```
+-----+
|           |
|   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

Rezidentní virus, který napadá spouštiné soubory typu COM a EXE. Tisň před koncem jeho těla je viditelný text [ECV](#), který používá pro rozpoznání již napadených souborů.

V sobotu ètrnáctého se pokusí pøepsat zaèátky disků.

Virus Semtex

Rezidentní virus českého původu. Napadá spouštěné a otevírané soubory typu COM. Občas demonstruje svou přítomnost zaplněním obrazovky náhodnými daty.

Varianta Semtex.1000.A

Každou hodinu, kterou vydrží v paměti počítače se předvádí. Obsahuje, ale nevypisuje, tento text:

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

Varianta Semtex.1000.B

Předvádí se mezi půlnocí a třetí hodinou ráno, vždy v celou hodinu. Obsahuje, ale nevypisuje, tento text:

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

Virus Ser_No

Tento virus hledá a napadá soubory typu EXE. Tělo viru je kódováno a dekodovací smyčka se děláte ním.

Nenapadá soubory, jejichž název začíná některou z těchto dvojic znaků:

SC, CL, NO, AS, FI nebo TO

Ser_No je vybaven velmi zákeřnou destrukční funkcí. Občas si náhodně vybere sektor a v něm změní náhodný bajt. Pokud je jeho výskyt zjištěn pozdě, mohou už být poškozena nejen data na disku, ale i jejich záložní kopie, které zajišťují pravidelně vytváříte.

Svou přítomnost oznamuje textem:

V1.01 ser.No :

za který hrdě popisuje číselné číslo své generace.

Virus Simulate

Polymorfní nerezidentní virus, který hledá a napadá soubory typu COM.
Občas se představí náhodně vybraným textem a skončí v nekonečné smyčce.

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

Ětyři z jeho textů mají připomínat prezentaci jiných virů:

```
HA HA HA YOU HAVE A VIRUS
```

```
FRODO LIVES!
```

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

```
DATA CRIME VIRUS RELEASED: 1 MARCH 1989
```

Virus Slovakia_II

Varianta Slovakia_II.1024

Jednoduchý rezidentní virus, který napadá spouštiné EXE soubory. Pokud je spuštěn první týden v roce, napíše:

```
HAPPY NEW YEAR, SLOVAKIA
```

Pak počká cca dvě a půl minuty a spustí původní program. V tomto období se také nešíří.

Varianta Slovakia_II.3584.1_0

Rezidentní virus, který napadá spouštiné COM a EXE soubory. Jestliže je přítomen v paměti, maskuje zvětšení délky napadených souborů. Nemá rád antivirové prostředky. Tyto programy raději nenapadá:

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

Pokud najde soubory kontrolních součástí (`chklist.ms`, `chklist.cps` nebo `smartchk.cps`), tak je smaže. Rezidentní ochranný program Vsafe rovnou vypíná. Když útočí na nějaký soubor, tak ho raději nejprve přejmenuje na `sv1.sv1`, aby na sebe zbytečně neupozoroval.

Je-li spuštěn prvního až čtvrtého srpna, tak se zdvojnásobí představitel:

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

Také obsahuje (ale nikdy nevypisuje) tento text:

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

Varianta Slovakia_II.3584.1_1

Nepatrně modifikovaná verze viru Slovakia_II.3584.1_0. Seznam nenapadených souborů je dolní o jméno `dizz` a vypisovaný text zní:

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

Virus Slovakia

Rodina virù, které napadají EXE soubory v aktuálním adresáři a v cestì.
Slovakia obèas pozdraví,

Greeting from Bratislava, SLOVAKIA.

pøedstaví se

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

a zviditelòuje Slovensko:

Type the word SLOVAKIA :

Pokud napíšete jiné slovo, virus vám to vysvìtlí

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

a nedá pokoj, dokud se nedoèká správné odpovìdi.

Slovakia nenapadá soubory, jejichž název zaèíná SC, CP, NO, DC,
AS, TN, PK nebo LH.

Varianta Slovakia.Slon

Tato varianta vychází z pùvodních virù Slovakia, ale používá funkce,
které se dekodují a kódují za bìhu programu.

Po rozkódování hlavní smyèky je v tomto viru vidìt následující text:

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

Virus Smeg

Skupina britských polymorfních virù, které používají velmi kvalitní generátor kódovacích smyèek.

Varianta Smeg.Pathogen

Rezidentní virus, který napadá spuštìné soubory typu COM i EXE. Vyhne se tím programùm, jejichž název zaèíná na:

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

Zjišuje bezpečné adresy některých systémových funkcí jejich trasováním (snaží se tak vyhnout některým kontrolním programùm).

Každá 32 generace viru v pondělí mezi pátou a šestou hodinou odpoledne zablokuje klávesnici, zruší v CMOS paměti nastavený typ disketové mechaniky, představí se:

`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!!!!`

a pak začne přepisovat obsah náhodně vybraných sektorů pevných disků.

Varianta Smeg.V3

Jednoduchý virus, který v aktuálním adresáři hledá a napadá soubory typu COM. V pátek třináctého nedovolí napadený program spustit a místo toho napíše:

`This program requires Microsoft Windows.`

Varianta Smeg.Queeg

Rezidentní virus, který napadá spuštìné soubory typu COM i EXE. Vyhne se tím programùm, jejichž název zaèíná na:

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

Zjišuje bezpečné adresy některých systémových funkcí jejich trasováním (snaží se tak vyhnout některým kontrolním programùm).

Každá 32 generace viru v neděli mezi 12 a 13 hodinou zablokuje klávesnici, představí se:

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

a pak začne přepisovat obsah náhodně vybraných sektorů pevných disků.

Virus Socha

Rezidentní virus napadající spouštěcí soubory typu COM. Šíří se pouze, pokud je nastaven rok 1981. Nenapadá programy, které jsou součástí Norton Commanderu. Vyhne se také programům (nepodařilo se nám je identifikovat), které používají soubor `me$.ovl`.

Virus obsahuje tyto texty:

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

kteří slouží k identifikaci nenapadaných programů.

Virus StarDot

Nerezidentní viry, které hledají a napadají soubory typu COM a EXE.
Obsahují krátký nezakódovaný text:

[AMZ](#)

Občas přepisují začátek disků.

Varianta StarDot.600

Destrukční činnost je spouštěna náhodně.

Varianta StarDot.789.A

Obsah disků přepisuje 24.9. po sedmé hodině.

Varianta StarDot.801

Destrukční akce je načasována na 13. února po jedné hodině odpoledne.

Virus Susan

Jeden z mála zajímavých přepisujících virů. Je rezidentní (!) a používá nedokumentovaných služeb operačního systému k převzetí kontroly nad příkazem DIR. Při jeho použití pak napadá soubory a jestliže jich napadne alespoň šestnáct začne také mazat obsah aktuálního adresáře.

Spuštění napadeného programu končí simulací chybového hlášení interpretru příkazů MS-DOSu (COMMAND.COM):

```
Bad command or file name
```

V těle viru jsou dále čitelné tyto texty:

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


Virus Tack

Rodina jednoduchých nerezidentních virů, které napadají COM soubory. Jednotlivé varianty se příliš neliší a obsahují chybu, která znemožňuje jejich léčení. (Na začátku souboru mají šest bajtů, ale schovávají si původní hodnoty pěti bajtů)

Varianta Tack.411

Při spuštění napadeného souboru píše text:

```
Infected file.
```

Varianta Tack.449

Při spuštění napadeného souboru píše text:

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

Varianta Tack.460

Při spuštění napadeného souboru píše text:

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

Varianta Tack.477

Při spuštění napadeného souboru píše text:

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

Varianta Tack.635

Tato varianta je doplněna o kódovací smyčku a na začátku souboru poškodí jenom pět bajtů, takže je možné virus odstranit.

Napadené soubory prodlužuje o svou délku a až o 255 bajtů s náhodným obsahem.

Při napadení souboru napíše:

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

Virus Ten_Bytes

Rezidentní viry, které napadají spouštěcí soubory typu COM a EXE. Instalují se do paměti poněkud bezstarostně na absolutní adresu, takže lze očekávat časté havárie operačního systému.

Od září do prosince Ten_Bytes sleduje zápisy na disk a nyní je takovým způsobem, že posune ukazatel na zapisovaná data o deset bajtů dopředu.

Virus Tequila

Rezidentní virus napadající EXE soubory a MBR pevného disku. Patří mezi nejlépe napsané viry a dodnes je jeho výskyt hlášen z mnoha míst. Při prvním spuštění na počítači se Tequila pokusí zjistit původní adresu obsluhy diskových operací (a obejít tak kontrolní programy) a napadne MBR, ale nezačne se šířit. Teprve po novém startu počítače napadá spuštěné EXE soubory. Vyhýbá se souborům jejichž název obsahuje 'SC' nebo 'V' a poškozují validaci kódy připojované SCANem k chráněným programům.

Pokud je virus v paměti, upravuje délku napadených souborů tak, aby se zdálo, že je vše v pořádku.

Tělo viru je složité kódováno a dekodovací část je proměnná. Má čtyři základní typy a celkem může vytvořit asi 25 000 různých tvarů.

Tequila občas při ukončení běhu nějakého programu namaluje na obrazovku fraktál a napíše text:

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

Jestliž je spuštěn program obsahující více uvedené instrukce, virus se zdvojnásobí představí:

```
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

Jeden z prvních multipartitních virů. Napadá spouštěcí soubory typu COM, tabulku rozdělení pevného disku a boot sektor diskety.

Obsahuje čitelný text `V-1L` podle kterého poznává již napadené objekty. Dále je v těle viru zakódovaný text:

```
Disk error
```

Ten zobrazí pokud se mu nepodaří přečíst svá data.

Po 24.12.1990 přepisuje obsah disku.

Virus Tiny

Skupina rezidentních virů, které obvykle napadají spouštěcí soubory typu COM.

Jsou zřejmě pokusem o vytvoření nejmenšího, plně funkčního, viru.

Virus Tiny-GM

Jednoduché viry, které vyhledávají a napadají soubory typu COM.
Nekontrolují jestli už oběť nebyla napadena a mohou tak stejný soubor infikovat několikrát.
Patří zřejmě k pokusům o napsání nejmenšího, plně funkčního, viru.

Virus Tiso

Varianta Tiso.846

Rezidentní virus, který napadá spouštěcí COM soubory a tabulku rozdělení pevného disku. Pokud je připojen k souboru, je jeho tělo jednoduchým způsobem zakódováno. Občas napíše bílé na modrém:

`Nech zije Jozef Tiso, prvý slovensky prezident !`

Virus Uruguay

Rodina polymorfních rezidentních virù, které napadají COM a EXE soubory při jejich spuštění nebo otevírání. Snaží se zjistit původní adresy důležitých služeb operačního systému jejich protrasováním a vyhnout se tak některým antivirovým programům. Se stejnými úmysly nemění tabulku obsluhy přerušování, ale raději přímo přepisují začátek příslušného kódu instrukcí skoku do těla viru.

Uruguay nenapadá `COMMAND.COM` a některé varianty se také raději vyhnou programům F-PROT, SCAN a takovým jejichž jméno začíná AI a vyskytuje se v něm znak V.

Další vlastnosti, které se vyskytují v některých variantách (a zaslouží si připomenout) jsou:

- Sledování stisku Ctrl-Alt-Del a následný pokus o "přežití" restartu počítače.
- Udržování viru v paměti v zakódovaném tvaru.
- Odvození konstanty pro jednoduchou identifikaci napadených souborů z kontrolního součtu ROM počítače.
- Oznámení o úspěšné instalaci do paměti. Například ve tvaru:

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

Při spuštění napadeného programu se Uruguay s pravděpodobností cca 0.4% představí, 5 sekund počká a pak teprve pokračuje. Text, kterým oznamuje svou přítomnost je v každé verzi viru jiný.

Varianta 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.  
ABBAY 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.
```

Varianta Uruguay.2

```
I love ROXETTE !!!
```

```
Virus 'Uruguay-#2'  
Programmed in Montevideo (URUGUAY) by F3161. 04/92.
```


This is a research virus - DO NOT DISTRIBUTE.

Varianta Uruguay.3

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

Varianta Uruguay.4

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

Varianta Uruguay.5

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

Varianta Uruguay.6

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

Varianta Uruguay.7

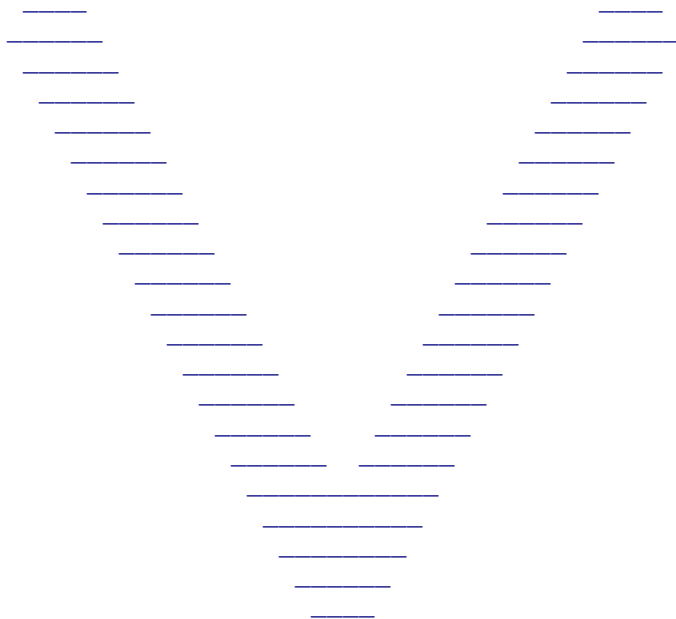
Uruguay-#7 Virus
Programmed in Montevideo (URUGUAY). 02/93.
This is a research virus - DO NOT DISTRIBUTE.

Varianta Uruguay.8

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

Virus V-Sign

Tento virus napadá BOOT sektor disket a MBR pevného disku. Na počest napadení každé třicáté druhé diskety pomalu zobrazí velké V a skončí v nekonečné smyčce.



Virus Vic

Rezidentní virus českého původu, který napadá spouštěné a otevírané soubory typu COM a EXE. Tělo je zakódováno a dekryptovací smyčkou virus modifikuje.

Aktivní virus v paměti způsobuje, že systémové hodiny počítače jdou pozpátku. To jistě ocení všichni uživatelé různých systémů zálohování a správy dat.

Vic obsahuje (ale nepoužívá) tento text:

VZDY MAS O JEDEN VIRUS VIC, NEZ SI MYSLIS.

Virus Vienna

Rodina jednoduchých nerezidentních virů, které napadají COM soubory. Tomu že zdrojový kód tohoto viru byl mnohokrát publikován vděčíme za obrovské množství nejružnějších mutací, které se většinou liší jen v úplných maličkostech. Některé mutace občas neopravitelným způsobem poškodí napadený program.

Virus Vietnam

Varianta Vietnam

Virus napadající BOOT sektor disket a MBR disku. Jeho zdrojový text byl distribuován v elektronických časopisech, vydávaných hackerskými skupinami. Jako autor byl uveden Vu Minh Phuong.

Mezi 17. a 30. červnem Vietnam přepisuje obsah pevného disku.

Virus Voronezh

Rodina rezidentních virů ruského původu, které většinou napadají pouze COM soubory.

Varianta Voronezh.1600

Tato varianta neobsahuje žádný text a neprovádí žádnou akci. Útočí na soubory nejen při jejich spouštění, ale i při otevírání a napadá i EXE soubory. Snaží se vynechat COMMAND.COM.

Varianta Voronezh.650

Pokud je napadený program spuštěn ve třetí minutě, virus přepne obrazovku do režimu 40x25 znaků a napíše:

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

Také obsahuje nezakódovaný text:

```
16.01.91, v1.00, ÓšÈšà & žÀ«°
```

Virus Yale

Jeden z nejstarších virů. Šíří se tak, že při stisku Ctrl-Alt-Del, napadne BOOT diskety v mechanice A:.

Existuje několik variant, ale většina z nich se na současných počítačích nedokáže šířit.

Virus Yog-Sothoth

Hloupouèký rezidentní virus domácí produkce. Při spuštění programu napadne všechny soubory typu COM v aktuálním adresáři.

Přesně v deset hodin na sebe upozorní:

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

A pak provede reset počítače.

Neobsahuje žádnou přímo destruktivní akci, ale způsob jakým zachází s operačním systémem a s pamětí lze považovat za žádost o pravidelné hroucení operačního systému.

Tělo viru je zakódováno a Yog-Sothoth dokonce obsahuje jakýsi zárodek polymorfismu - má dvě různé (leč velmi podobné) dekryptovací smyčky a pravidelně je stěídá.

Virus ZP

Malý rezidentní virus, který napadá otevírané a spouštěné soubory typu EXE. Třináctý den v měsíci po několika hodinách od své instalace do paměti provede restart počítače.

Virus 10_Past_3

Rodina rezidentních virů napadajících spouštěcí COM soubory. Neobsahují vysloveně destruktivní akce, ale vlnují značnou péči obtěžování uživatele. Obsahují kód, který má zabránit jejich trasování.

Varianta 10_Past_3.748

Tato varianta neobsahuje žádný text. Pokud se instaluje do paměti dvacátého druhého, provede RESET počítače. V některé další dny vypíná některé životně důležité funkce operačního systému. Po patnácti hodinách a deseti minutách od startu počítače převezme kontrolu klávesnice a občas "stiskne" klávesy Ctrl a Shift.

Virus Seventh_son

Rodina jednoduchých nerezidentních virů napadajících COM soubory.
Obsahují nezakódovaný text:

`Seventh son of a seventh son`

Tento text virus vypíše při spuštění sedmé kopie pocházející ze sedmé kopie původního viru. (Sedmý syn sedmého syna)

Virus Eight_Tunes

Rezidentní virus, který napadá EXE a COM soubory. Občas zahraje jednu z osmi melodií. Obsahuje nezkódovaný text [COMMAND.COM](#).

Pokud zjistí přítomnost programu FLUSHOT, přestane se šířit. Zdá se, že umí v paměti zjistit a deaktivovat ještě jeden obdobný antivirový program, ale nepodařilo se nám zjistit, který by to mohl být.

Virus Armagedon

Rodina rezidentních virů českého původu. Napadají pouze COM soubory a jsou zajímavé pouze tím, že se snaží vytáčet pomocí modemu nějaká telefonní čísla.

Varianta Armagedon.1079

Mezi pátou a šestou hodinou ráno se pokouší vytočit telefonní číslo 081-141 (prý přesný čas v Česku). Obsahuje nezakódovaný text:

```
Armagedon the GREEK
```

Také je v něm vidět příkaz pro vytočení telefonního čísla, určený pro modemy kompatibilní se standardem Hayes:

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

Varianty Armagedon.1079.B a Armagedon.1079.C se snaží vytočit číslo 911 (tísňové volání v USA) a obsahují jiný text:

```
Support Your Police
```

Virus Arusiek

Rezidentní virus, který napadá soubory typu COM i EXE. V těle viru je nezakódovaná tabulka jmen souborů, kterým se raději vyhne

```
MKS  
NAV  
CLEAN  
COMMAND
```

Také obsahuje text Arusiek R., který je v souboru viditelný v tomto tvaru:

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

Virus Better_World

Rezidentní virus napadající spouštěcí EXE soubory. Obsahuje nezakódovaný text, kterým se pochlubí pokud je spuštěn v zázdí:

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

Virus Bomber

Tento virus napadá velmi zvláštním způsobem COM soubory. Vloží se na náhodné místo v oběti a po jejím zbytku rozmístí náhodně vytvořené "ostrůvky" instrukcí, které si navzájem předávají řízení. Poslední pak spustí vlastní kód v těle viru.

Tělo viru není nijak kódováno a obsahuje tyto texty:

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


Virus Explosion

Rezidentní virus, který napadá soubory COM a EXE. Nenapadá soubory, které se jmenují SCAN, CLEAN, FINDVIRU nebo GUARD.

Sedmý den v měsíci (za splnění dalších, složitějších, podmínek) napíše:

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

Začne pípat a počítá od devatenácti do nuly. Pak napíše:

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

Po skončení této show sice zůstane v paměti, ale přestane napadat soubory.

Virus Frodo

Rodina rezidentních virů, které napadají soubory typu COM i EXE. Zcela jistě patří k technicky nejdokonalejším virům. Zejména komplexnost jejich stealth techniky stojí za zmínku. Kromě toho, že se maskují i při volání zastaralých funkcí DOSu (což zdaleka není běžné), tak se ze souboru zcela odstraní, pokud zjistí pokus o zápis do něj, nebo o jeho prohlížení nějakým debuggerem.

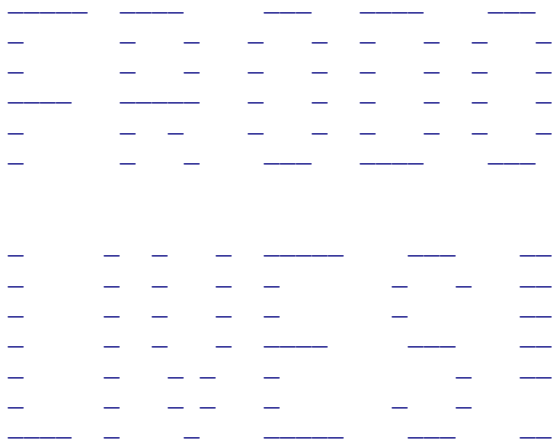
Snaží se trasováním zjistit původní adresy obsluhy nejdůležitějších funkcí systému a jejich přímým použitím obejít různé kontrolní programy.

Viry z rodiny Frodo nekontrolují přímou své oběti přímo, ale pomocí kontrolního souětu. Vedlejším efektem toho je, že také mohou "napadnout" datové soubory (z běžnějších přímou například BMP, CDX, DIR, FAX nebo PIF). Změna těchto souborů se díky stealth technice projeví až po odstranění viru z paměti.

Varianta Frodo.Frodo.A

Frodo.Frodo testuje obsazení paměti a pokud se uvolní místo, které mu lépe vyhovuje, tak se klidně přestěhuje.

Od 22.září virus volá destrukční akci (v tento den slaví narozeniny Frodo Pytlík, postava z knih J.R.R. Tolkiena). Tato funkce je bohužel ve všech vzorcích, které máme k dispozici, poškozena. Zdá se, že má za úkol přepsat BOOT sektor diskety nebo disku tak, že po novém startu počítače bude v rámečku tvořeném "světelným hadem" vypsán text:



Varianta Frodo.Fish_6.A

Frodo.Fish je odvozen z viru Frodo.Frodo. Na rozdíl od svého předka je zakódován (nejen v napadených souborech, ale i v paměti) a obsahuje značné množství triků, které mají ztížit jeho analýzu.

Po roce 1991 se při spuštění napadeného programu představí:

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

V zakódovaném tile viru jsou rozmístiny tyto texty:

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

Tisni pøed koncem viru je tento nezakódovaný text:

FISH FI

Virus Geld_wasch

Rezidentní virus napadající spouštěcí soubory typu EXE. Po roce 1991 se vždy dvacátého pátého dne v sudém měsíci představí:

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

Pak zněí obsah pevných disků.

Virus Hydra_II

Rezidentní viry, které napadají spouštěné EXE soubory.
Od roku 1995 při spuštění 1.1., 5.5. nebo 9.9. demonstruje svou přítomnost. V tyto dny se také nešíří.

Varianta Hydra_II.A

Představuje se tímto textem:

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

Varianta Hydra_II.B

Představuje se tak, že zajímavým způsobem zaručuje s obsahem obrazovky a napíše:

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

Virus KWZ

Rezidentní virus, který napadá spouštěcí soubory typu COM.

Od 25. do konce měsíce zpomaluje počítač a při pokusu o vytvoření adresáře provede reset.

Autor viru si pravděpodobně nepřejí být svým výtvořem obtěžován a tak se KWZ nešíří, jestliže identifikuje počítač pomocí tohoto čísla BIOSu:

[01/15/8808/30/9006/06/9207/07/91](#)

Na konci obiti je tento nezakódovaný text, podle kterého virus rozlišuje již napadené soubory:

K WZ

Virus Monika

Rezidentní virus českého původu, který napadá COM soubory. Připojuje se sice klasickým způsobem na konec své oběti, ale poškodí také dva bajty v jejím těle. Zřejmě se tak snaží zabránit svému odstranění některým z programů pro kontrolu integrity souborů.

Osmého řádku přepíše textem `Monika` obrazovku a bohužel také začátek pevného disku.

Virus Nina

Jednoduchý rezidentní virus napadající COM soubory.
V jeho těle je nezakódovaný text `Nina`, který nikdy nevypisuje.

Varianta Nina.D

Text `Nina` je v této variantě nahrazen textem:

`RIOT!`

Virus One_Half

Rezidentní polymorfní multipartitní virus slovenského původu. Pokud je aktivní v paměti tak používá stealth techniku na zamaskování změny MBR a "zkracuje" napadené soubory. Trasuje si obsluhu systémových služeb a snaží se tak vyhnout některým kontrolním programům. Také nenapadá některé antivirové programy.

One_Half obsahuje velmi nepříjemnou a zákeřnou destrukci. Při každém spuštění počítá a zakóduje na disku dvě stopy. Jakmile je takto poškozeno víc jak 50% kapacity disku, tak na sebe virus začne upozorňovat. Napíše:

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

Pak pípne a počká na stisk klávesy.

Za normálních okolností není nic poznat. One_Half sedí v paměti, kontroluje přístup k disku a data podle potřeby zase dekóduje. Amatérský pokus o odstranění tohoto viru (např. pomocí FDISK /MBR) sice zničí virus, ale s ním také informace potřebné k zpětnému dekódování obsahu disku.

Varianta One_Half.3544

Obsahuje text:

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

Nenapadá tyto programy:

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

Jestliže je spuštěn `CHKDSK`, tak si raději odpustí stealth velikosti napadených souborů.

Varianta One_Half.3570

Obsahuje text:

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

Nenapadá tyto programy:

```
SCAN  
AIDS
```

FINDVIRU
WEB
NOD
VSAFE
MSAV

Jestliže je spuštěn [CHKDSK](#), tak si raději odpustí stealth velikosti napadených souborů.

Varianta One_Half.3577

Obsahuje text:

[DidYouLeaveTheRoom?](#)

Nenapadá tyto programy:

SCAN
CLEAN
FINDVIRU
GUARD
EMM

Jestliže je spuštěn [CHKDSK](#), tak si raději odpustí stealth velikosti napadených souborů.

Virus Pivr nec

Jednoduchý virus, který napadá spouštiné soubory typu COM.

Desátého øíjna znièí tabulku rozdílení pevného disku (MBR),
pøedstaví se:

```
Mé jméno je Pivr nec a chtíl bych  
Vám podíkovat za poskytnutí  
podmínek potøebných pro moji  
inkubaci a zdárný vývoj mé  
osobnosti ...!?!...
```

Pivr nec `95

PS: Doufám, že Vás nepøešla ŽãZÈÒ !?

a skonèí v nekoneènèé smyèce.

Virus CLI

Jednoduchý rezidentní virus, který napadá spouštěné a otevírané soubory typu COM. Nenapadá COMMAND.COM.

Druhého února 1997 poškodí kontrolní součet paměti CMOS, počká na stisk klávesy a přepíše tabulku rozdělení pevného disku (MBR).

