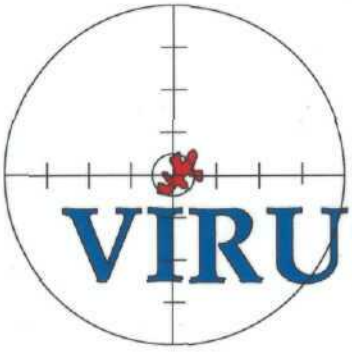
KIS JÁNOS — SZEGEDI IMRE



VÍRUSHATÁROZÓ

ALAPLAP KÖNYVEK 4

Kis János – Szegedi Imre

VÍRUSHATÁROZÓ

Kis János – Szegedi Imre

VÍRUSHATÁROZÓ

CÉDRUS KIADÓ

Szerkesztette: Faklen Pál
Sorozatszerkesztés és borítóterv: Faklen Pál

Felelős kiadó: Sebestyén Ilona
Cédrus Kiadó Kft

ISSN 963 7429 00x
ISBN 963 7429 026

Nyomdai előkészítés: **PRINTSELF** Kft
Felelős vezető: Kassay Árpád
Nyomtatás: Sprint[R] – Fónix Kft.
Felelős vezető: Tóth Éva
Készült a Stoffel & Tsai. gondozásában

Előszó

Eredetileg szerettük volna az Új víruslélektan megjelenését követően minél hamarabb kiadni ezt a tulajdonképpen szorosan hozzá tartozó Vírushatározó kötetet is, de éppen akkoriban a vírusfront alaposan megváltozott, s szinte követhetetlenné vált. Egyre csak csúsztunk a végleges kézirat leadásával, hogy lépést tartsunk a fejleményekkel, azok pedig folyton lekörözték bennünket.

Vírusgyűjteményünk már 1991 június elején elérte az ötszázat, év végére pedig a vírusváltozatokkal is számolva átléptük a bűvös ezres határt. A gyarapodáshoz jelentősen hozzájárult, hogy egyes programozók „cserealapként" szorgalmasan gyártják egy-egy ismert vírus éppen csak egy kicsit átírt variációit, hogy cserével újabbakhoz jussanak hozzá. Jelenleg vírustörzsekből mintegy 1100-at tart nyilván a szakirodalom, s a változatokkal együtt számuk már több ezerre rúg. Az Amiga világában az „összkészlet" mintegy százötven vírustörzs.

Ugyanakkor a tapasztalat szerint a vírusirtó programok nem képesek — vagy nem is akarnak — lépést tartani a növekvő vírusáradattal. Talán azért, mert tartogatnak valamit a következő verzióra is, vagy nem jutnak hozzá idejében a legfrissebb vírusokhoz, s anélkül nem nagyon lehet víruskeresőt és vírusirtót írni.

Újabb fejleményként forgalomba került az (ál)multitaszk üzemmódra képes MS-DOS 5.0 és a PC-DOS 5.0, ami alaposan megkeveri a vírusok működését és az ellenük küzdő szakemberek lelkivilágát is. Ha ugyanis az egyik taszkon fut a vírus, a másikon pedig a kereső vagy az irtó program, akkor azok soha nem találkoznak!

A növekvő vírusáradat láttán többen is elindultak a hardveres vírusvédelem irányába. Megszületett a Virus Guardian és a Thunderbyte antivíruskártya, amelyekben az alapötlet jó volt, de egyes vírusok nem tisztelték a konstruktőr szándékait. „Élő" vírusok nélkül nem lehet antivírus kártyát sem készíteni. A hazai programozói tudást „dicséri", hogy éppen egy eredeti magyar vírus, a Polimer alkalmas a hardvervédelmi eljárások tesztelésére. (Eddig minden általunk tesztelt antivírus-kártyán átment.) Az NSZK-ban viszont a Metalthunder vírust kifejezetten a Thunderbyte forgalmazóinak bosszantására szánták, a vírus ugyanis a kártya egyik gyenge pontját kihasználva megy át rajta. További gondot okoz, hogy az új elveken működő vírusok megjelenésekor a legjobb esetben is csak a BIOS frissítését (upgrade) tudják nyújtani a felhasználóknak, egyébként meg kell venni a modernebb víruskártyát.

Az elv, hogy a hardvert tegyük immunissá a vírusok ellen, például egy AVP (antivírus-processzor) segítségével, nem rossz, csak más úton kell elindulni. Elkészült — saját fejlesztésünkben — a magyar vírusvédő kártya is, a Top Guard

(TG). A vírusok elemzése során rájöttünk arra, hogy nagyon nehéz általánosan meghatározni a vírusok működési módját, és arra alapozni az észlelési algoritmust. A TG éppen ezért olyan általános vírusvédelmi rendszer, amelynek hardveres megoldása állandó, míg a vírusspecifikus rész szoftveresen, lemezről kapcsolódik hozzá. A „névjegyzék" frissítésére és az új elven működő vírusok ellen is mindig csak a lemezt kell cserélni.

Egyre inkább szükség van folyamatos (on-line) védelemre, mert az új típusú vírusok az adatokat már nem mentik el sehova, hanem azonnal pusztítanak, s egyszerűen nem adnak rá módot, hogy közbeavatkozásunkkal mérsékeljük a kárt. Ráadásul sem az időközönkénti vírusellenőrzés, sem a tárrezidens ellenőrző program nem nyújt védelmet.

Sajnos a „fejlődés" nem áll meg. E sorok írásakor jutottunk hozzá a vírusokat generáló, első nyilvánosan is terjesztett program, a Virus Construction Set német programrendszer első verziójához. A vírusháború tovább eszkalálódik...

Annak tudatában bocsátjuk közre Vírushatározónkat, hogy e „pokoli panoptikum" idővel sajnos akár lexikon méretűvé is duzzadhat.

Budapest, 1992. március

Kis János *Dr. Szegedi Imre*

Hogyan használjuk a Vírushatározót?

A Víruslélektan első kiadása után olvasóink közül sokan kifogásolták, hogy nagyon merev, mechanikus volt a vírusok bemutatása, ezért amennyire csak tudtunk, igyekeztünk elszakadni a korábbi tárgyalási módtól. A vírusokról több érdekességet, történeti hátteret is közlünk, ugyanakkor mellőzzük az olvasók túlnyomó részének nem sokat mondó információkat — például a kód típusa adatmező sokszor egyébként is vitatott azonosítóit, rövidítéseit. Hasonlóképpen a detektálási eljárásnál is inkább csak arra koncentráltunk, hogy a legelterjedteb McAfee-féle antivírus programokból melyik Scan verzió ismeri fel, illetve annak párjaként melyik Clean távolítja el a vírust. Képtelenség lenne a világban elterjedt több mint 300-féle antivírus programot és hardveres megoldást mind bemutatni. Ahol a korábbi kiadásban hivatkoztunk több antivírus programra, ott azokat mégis meghagytuk, de az újabbakat más csak a Scan és a Clean programra vonatkozóan vettük fel. A könyv végén található vírusazonosító táblázat és hosszmutató is a McAfee Scan/Clean készlet 89-es verziója alapján készült.

Újítás, hogy a vírusokat valamilyen közös tulajdonságuk szerint csoportosítottuk fejezetenként. Ez lehet felhasználásbeli, programozástechnikai, származási vagy más rokonság. E mesterséges rendezőelvek között az eligazodást segíti a kötet végén a vírusokról található számos táblázat.

A rendszerezés ötletét Jim Goodwin hasonló munkájából merítettük, aki 1989 áprilisában állt elő a BBS-eken keresztül terjesztett ALLVIRUS.LST című, akkor teljesnek tartott listájával. Az úttörő szerep az övé, s mi csak annyit tettünk, hogy az eredeti anyagokat a legújabb fejleményekkel és a hazai vonatkozásokkal „megpatkoltuk".

A vírusok készítésének fő helyszíne az utóbbi időben megváltozott. Az USA-ban a szigorú adatvédelmi törvények miatt már elég nagy kockázattal jár a vírusírás. Inkább Bulgária, a (volt) Szovjetunió, Németország, Olaszország, a Közel-Kelet és sajnos Magyarország lett a víruskészítés melegágya. Intelligenciájuk és meglepő számítástechnikai ötleteik miatt különösen rettegi a világ a bolgár és az orosz eredetű vírusokat.

A szakirodalmat és a BBS rendszerek üzeneteit tanulmányozva sajnálattal láttuk, hogy a vírusok elnevezése még nem egységes. Arra a következtetésre jutottunk, hogy az eligazodás elősegítésére a John McAfee-féle Virscan programrendszer által használt elnevezéseket célszerű alkalmaznunk. Ezeket a neve-

ket a program is felismeri, az egyébként még használatos többi elnevezést pedig — akárcsak más természettudományokban — szinonimaként kezeljük.

Ami az egyes vírusok leírásait illeti, a biológiából vettük módszerünket, és azokat a tipikus vírusokat igyekeztünk leírni, amelyeket már töviről hegyire áttanulmányoztak a víruskutató és adatvédelmi központokban, és általában hozzánk is eljutottak. Egységes szempontok alapján próbálunk rámutatni az azonosított vírusok kódjának a felismerés szempontjából fontos részleteire. A jelenlegi lista az 1992. márciusi állapotot tükrözi.

Vírusrendszertan

Először ismerkedjünk meg a felhasznált űrlap egyes mezőivel. Figyelmesen olvassuk el tartalmukat, hogy azután a fogalmakat egységesen értelmezzük, kezeljük.

A vírus neve: Ebben a rovatban a vírust a bevezetőben említett, nemzetközileg elfogadott neve alapján regisztráltuk.

Egyéb elnevezése: Itt felsoroltuk azokat a neveket, amelyeken az angol nyelvű szakirodalmi közleményekben még előfordulnak. A magyar elnevezések is ide kerültek.

Hossza: Az a bájtokban megadott hosszúság kerül ebbe a rovatba, amellyel a vírus a fertőzés során megnöveli az egyes programok vagy rendszerkomponensek — mint például a COMMAND.COM — hosszát. Egyes esetekben, így a bootszektorba beépülő vírusok esetében, nincs értelme ennek az adatnak, mert a boot hossza adott, és a kód egy része máshol is előfordulhat, a vírusíró leleményétől függően. Más esetekben — az önmagukat titkosító vírusoknál — a hosszúság változó lehet, ezért ilyenkor ennek az adatnak minimális a jelentősége. Végül az is előfordul, hogy egyszerűen nincs ilyen mérhető adat, mert a vírus szétszórja magát a lemez különböző részein. Ilyenkor ebben a rovatban n/a (nincs adat) jelzés szerepel. Egy-két esetben előfordul a ??? megjelölés is, amikor a vírus olyan gyorsan okoz rendszerösszeomlást, hogy visszafejtésére nincs mód, s nem lehet eldönteni, hogy trójai programmal vagy vírussal állunk-e szemben.

Kódtípusa: Ebben a pontban megkíséreljük röviden megadni a kód főbb jellemzőit. Az első Víruslélektan könyvben alkalmazott meghatározások és rövidítések nem voltak egyértelműek, ezért döntöttünk a szöveges jellemzés mellett.

Megjegyzés: A rövidség kedvéért gyakran alkalmazzuk a parazita vírus kifejezést, ami a magyar szakirodalomban szokatlan. Az általunk korábban használt „appendelő" (az állományokhoz hozzáépülő és azok hosszát megnövelő) szó — azon túl, hogy a magyar nyelvben idegen — csak akkor találó, ha a vírus

az állomány végéhez kapcsolódik. Önmagát az állomány elé másoló vírusra (lásd Péntek 13), vagy arra, amelyik az állomány belsejébe épül be, jobb az angol szakirodalomban használt „parasitic" megfelelője, a parazita, azaz élősködő jelző.

Azonosítása: Ebben a pontban kíséreljük meg összefoglalni, miként lehetséges az egyes programvírusokat azonosítani. Mi itt csak az MS-DOS™, illetve az IBM-DOS™ világának programvírusaival foglalkozunk. Segédprogramként amerikai szabadszoftvereket ajánlunk szakirodalmi adatok alapján, tekintet nélkül arra, hogy azokat ismerik-e Magyarországon vagy Európában. A szakirodalom ezeket a programokat tekinti etalonnak. Az utóbbi időben több mint háromszáz ilyen termék jelent meg a piacon. Ezek nagy része csak néhány vírust ismer fel, sokszor mégis horribilis az áruk. Másoknál a felismerés megbízhatatlan. Meghagyva a korábbi kiadás adatait, az újabbaknál már csak azt vizsgáltuk, milyen sorszám feletti (+) Scan program deríti fel a vírust. A Szegedi Imre féle PC-Scan detektor az e könyv írásakor analizált vírusokból nyert információk alapján a hazai vírusokra koncentrál.

A hivatkozásainkban szereplő programok:

- F-Prot — Fridrik Skulason's F-Prot vírusdetektor és fertőtlenítő.
- IBM Scan — IBM Virus Scanning Program. Kereskedelmi szoftver, bár magas ára és a forgalmazó hiánya miatt Magyarországon és Európa legtöbb országában szabadszoftverként használják. Vírusszekvenciákat keres.
- Scan, NETScan, ScanRes, VShield, FShield — A McAfee Associates víruskereső programjai.
- Pro-Scan — A McAfee Associates professzionális vírusfelismerő és detektor programja.
- NAV Norton Antivirus — Vírusvédelmi programcsomag, állandóan felújítva.
- PC-Scan — Szegedi Imre vírusdetektora.

Eltávolítása: Ebben a pontban igyekszünk tanácsot adni arra, hogyan szabadulhatunk meg a kellemetlen betolakodóktól. A nemzetközi standard programok a legtöbb esetben a fertőzött állomány törlését ajánlják. Ez érthető is, hiszen egy vírust felismerni viszonylag könnyebb, mint úgy eltávolítani, hogy a megtámadott programállományok sértetlenül megmaradjanak, ezért erre csak egyes kereskedelmi szoftverek képesek. Sajnos az utóbbi időben elterjedt felülíró vírusok esetén ennek a módszernek már semmi értelme, mert az új vírusok többnyire nem mentik el a helyreállításhoz szükséges alapvető információkat. A vírusok eltávolítására használatos programok közül könyvünkben az alábbiakra hivatkozunk.

ANTICRIM — Jan Terpstra's AntiCrime Program (Hollandia).

BOOTKILL — Szegedi Imre és Farmosi István programja Ping Pong, Ping Pong-B, Ogre/Disk Killer, Ogre/Disk Killer-B magyar átírás, Töltögető, Stoned, Stoned-B, valamint Stoned-C bootvírusok ellen.

CHKVIR — Leitold Ferenc és Tábor Csaba programsorozata. Korábbi változatai detektálták a Cascade és a rebootvírusokat. Újabb és már kereskedelmi

szoftverként forgalmazott változatai a dokumentáció szerint a vírusváltozatokkal együtt mintegy 80 vírust irtanak.

CHKSEQ — Leitold Ferenc és Tábor Csaba szekvenciális víruskereső programja. Szabadszoftver. A szerzők igyekeztek a szakirodalomban fellelhető minden keresési szekvenciát, illetve vírusazonosítót beleépíteni. Előzetes detektálásra igen jó, viszont ha jelez is, nincs mindig vírus. Sok vakriasztás fordulhat elő olyankor, amikor a keresés a szakirodalomban található és onnan kiemelt rövid szekvenciára támaszkodik, mint például a Brain vírus esetében.

CLEAN — John McAfee's Clean, általános vírusirtó program. Nem képes felderíteni a vírust, meg kell neki mondani, milyen vírus eltávolítására kérjük, és csak azokat fogja kitakarítani — az esetek nagy részében úgy, hogy törli a vírust tartalmazó állományokat is. Másik ismert neve: CleanUp. A magyar vírusátírásokat irtva nem elég korrekt, a fertőzött állomány sok esetben tönkremegy. Ezekre csak akkor alkalmazzuk, ha nincs jobb megoldás.

DOS COPY — A DOS operációs rendszer COPY parancsát nyugodtan használhatjuk arra, hogy a bootvírussal fertőzött lemezről állományainkat lementsük. Ez a megoldás akkor hatásos, ha a bootvírus rezidensen nem aktív. Ne használjuk azonban a DISKCOPY, illetve az XCOPY parancsokat erre a célra, mert a fertőzött bootszektort is átvisszük az új floppylemezre!

DOS SYS — Ezt a DOS parancsot használjuk arra, hogy felülírjuk a fertőzött bootszektor tartalmát a lemezen. Ebben az esetben egy írásvédővel leragasztott, a winchesteren lévő rendszerrel azonos rendszert tartalmazó floppylemezről kell a rendszert újraindítani, majd kiadni a megfelelő lemezre vonatkozó SYS parancsot.

DXU2 — A Műszertechnikának a Potyogós vírustól (Cascade) mentesítő programja.

EDDIKILL — A Dark Avenger vírusfertőzésekor hasznos „takarító" program. Szegedi Imre és Farmosi István fejlesztői példánya. Széles körben elterjedt.

F-PROT — Fridrik Skulason's F-Prot detektor és vírusmentesítő programcsomagja.

KILLVAC — Vacsina-B vírust eltávolító program. Szegedi Imre és Farmosi István fejlesztői példánya.

TNTVIRUS — A Carmel Software antivírus programja. Jelenleg érvényes verziója a 7.06A, amely DOS 5.0 alatt is működik. Ennek része a rezidens Defender védelmi program. Az immunizálás funkciójának használata sok programra veszélyes, és megtévesztő MSDOS szignatúrával látja el azokat.

M-1704 — Cascade/Cascade-B vírust eltávolító program.

M-1704C — Cascade-C vírusfertőzést megszüntető program.

M-3066 — Traceback vírusfertőzést megszüntető program.

M-DAV — Dark Avenger vírusfertőzést megszüntető program, valamint a fertőzés megelőzését is szolgálja azzal, hogy a lemez bootszektorába felteszi a Dark Avenger azonosítóját.

M-JRUSLM — Jerusalem-B vírusfertőzést megszüntető program.

M-VIENNA — Vienna, Vienna-B vírusfertőzést megszüntető program. (A rebootvírusok ellen hatásos.)

MDISK — MD bootvírusfertőzést megszüntető program. Természetesen a felhasználó DOS verziójának megfelelő típusú bootszektort kell helyreállítania.

PRGDOKI — Szegedi Imre és Farmosi István programja a Magyarországon honos vírusok ellen. A 2.11E verzióig szabadszoftver, onnan kezdve kereskedelmi termék. (A szabad verziónak több trójai jellegű illetéktelen átírása ismert.) A program újabb változata 1701/Cascade, 1704/Cascade, 1701-Y/Cascade, 1704-Y/Cascade, Vienna/DOS62, Vienna-B/DOS62, Iván/Victor v1.0, Dark Avenger, Yankee Doodle, Yankee Doodle-B, Jerusalem, Jerusalem-B, Jerusalem Mutant, valamint Vacsina-B vírusok hatásos ellenszere.

SATURDAY — Az Európában előforduló Jerusalem vírusváltozatok ellen általánosan hatásos fertőtlenítő.

SCAN /D /A — A Scan futtatása a /D és /A opcióval. Ilyenkor töröl is.

SCAN /D — A Scan futtatása a /D opcióval. Ilyenkor szintén töröl.

SYSDOKI — Szegedi Imre és Farmosi István újgenerációs vírusölő és fertőzésmegelőző programja. Szegedi Imre 1991 áprilisától annak fejlesztésében már nem vett részt. A korábbi verziók kibővültek az izraeli és az amerikai vírusellenes együttműködés keretében kapott standard vírusok detektálásának és irtásának képességével.

UNVIRUS — Yuval Rakavy (Izrael) vírusfertőzést gyógyító programja, Brain, Jerusalem, Ping Pong, Ping Pong-B, Typo Boot, Suriv 1.01, Suriv 2.01, Suriv 3.00 vírusok ellen.

SPS — Buruzs Tamás immunizáló vírusvédő szabadszoftvere.

VIRUS BUSTER — Yuval Tal's Virus Buster, detektor és vírusölő program.

VIR05 — A Yankee Doodle vírusfertőzést megszüntető program. Szegedi Imre és Farmosi István fejlesztői példánya, gyorssegélyként terjesztették.

VIR05MEM — A Yankee Doodle vírust a memóriából kiölő program. Szegedi Imre és Farmosi István fejlesztői példánya, gyorssegélyként terjesztették.

Leírása: Ebben a részben igyekszünk elmondani minden rendelkezésünkre álló részletes információt a vírusok eredetéről, történetéről, „munkamódszereiről", üzeneteiről, aktivizálódásának feltételeiről stb.

Utolsókból elsők

Mini-45, Tequila, Patricia, 1381, Iraqui Warrior, Finger, Arf, Mirror, V516, Exterminator, BadGuy, Demon, Label, Metal Thunder, FellowShip, Vírusölő, Taunt, Michelangelo, Dir2/FAT.

Ez a fejezet a többitől eltérő módon, rendszertelenebbül, és más fejezeteket is átfedve ismerteti a vírusokat, részben azért, mert így beszámolhatunk a legújabb fejleményekről, részben pedig, mert jó részüket adatok hiányában még nem tudtuk a részletes ismertetésbe felvenni. A könyv végén lévő vírusazonosító táblázat azonban már majdnem mindegyiküket tartalmazza.

Mi jellemzi az újdonságokat? A vírusok névtelen szerzői felfigyeltek a vírusellenes szoftverekre, és részben ellenük irányítják a vírusokat, részben olyanná teszik őket, hogy azok elmentés nélkül felülírják az állomány egy részét. A terjedési és pusztítási fázis között egyre kisebb az időintervallum. A vírusok másik része viszont trójai programokká válik, bár ez valószínűleg nem lesz tartós irányzat, mert szerzőiket könnyebb tettenérni és megbüntetni.

Mini-45

Az elektronikában a miniatürizálás a divat. A vírusírók között is folyik valami vetélkedő, hogy ki tudja megírni a legrövidebb működő vírust. Az Alaplap egyik régebbi számában ismertettük a 144 bájt hosszú vírust, ami annak idején a csúcs volt. Azóta sikerült őt közelebbről is megszemlélni. Kiderült, hogy orosz eredetű. Az 1991 nyarán megjelent Mini-45 pedig már csak 45 bájtos. A vírus nem rezidens, és a COM állományokat fertőzi. A jelenlegi rekorder már csak 26 bájtnyi, szintén orosz eredetű, és e sorok írásakor még nem kaptuk kézhez.

Tequila

Nagy vihart kavart a Tequila vírus megjelenése és terjedése. E fájlvírus a fájlból a winchester nullás pályájára installálja magát. Ennek nyomán történt Európában az első letartóztatás vírusírás miatt.

A Tequila vírus elemzése folyamatban van, már megkaptuk karakteres azonosítóját. A vírusban a következő szöveg található:

```
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 !
```

(Köszöntjük a T.Tequila legújabb termékével. Vegye fel a kapcsolatot T. Tequila

P.O.Box 543/6312 St'Hausen/Switzerland. Szerelmes gondolataim L.I.N.D.A.-nak. Sör és Tequila mindörökké!)

Patricia

A vírusok dedikálásának divatját annak idején a holland Sylvia vírus írója kezdte el. Legutóbb ilyen „ajándék" címzettje lett Patricia Hoffman, a Virsum nevű vírusadatbázis kiadója. A vírust Olaszországból indították el az ismét aktivizálódó IVRL olasz vírusfejlesztő csoport tagjai. A vírus rezidens résszel rendelkezik és a memória felső szegmensébe épül be. Az aktivizálódás során „legyalulja" a lemez FAT tábláját. A vírusban lévő szöveg a következő:

```
Is today Friday? (Y/N)
Sorry but on Friday I wish not to work!!
You are untruthful!!
For punishment I'll format your HD Fat!!
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!
```

(Ma péntek van? (I/N) Sajnálom, de pénteken nem kívánok dolgozni. Ön most valótlant állít! Büntetésül formattálom merevlemezének FAT tábláját. Ezt a vírust Programtörő Jack írta Olaszországban, 1991-ben. IVRL. Minden jog fenntartva, kérem, ne törje fel a vírust. Speciális üzenet Patricia Hoffmannak: Szeretlek!!!! Puszi... puszi! Megadná a telefonszámát? Szia, szépségem!)

Ezek után más már nem segít, csak a DOS format parancsa. Tapasztalataink szerint most az ilyen romboló vírusok és trójai programok kerültek előtérbe, melyek ellen az időszakos vírusellenőrző szoftveres megoldások nem segítenek. A vírusírók arra törekszenek, hogy „munkájuknak" alapos és egyértelmű nyoma maradjon.

1381

Elindítása után a vírus szétrobbantja a képernyőn lévő szöveget. A kép tényleg úgy néz ki, mintha a monitoron az alsó sorban egy bomba robbant volna. A jelenség után a vírus kéri a felhasználót, hogy okvetlenül vegye fel a kapcsolatot a hardver szállítójával.

Iraqui Warrior

Az iraki háború nemcsak a katonák, hanem a számítógépvírusok háborúja is volt. Sorra jelentek meg a háborúval kapcsolatos, egyik vagy másik fél nézeteit propagáló számítógépvírusok. Magyarországon először a Szaddam sorozat tagjainak előfordulását jelezték, majd felbukkant az Iraqui Warrior is, melynek elindítása után a következő szöveg jelenik meg:

```
I come to You from The Ayatollah!
(c) 1990, VirusMasters
An Iraqui Warrior is in your computer…
```

(Az Ayatollahtól jöttem Önhöz!. (c) 1990, VirusMasters. Az iraki harcos itt van az ön számítógépében...)

Finger

A vírus egyik célpontja a ZIP állomány, amelynek egyes részeit felülírja. Ezzel hihetelen károkat tud okozni, mert sok esetben az automatikus mentés csak annyi, hogy egy korábbi verziót „becipzárazunk" ugyanazon a merevlemezen. A vírus elindítása után a következő üzenetet írja ki:

```
Cannot remember what I was dooing!!
Insert fingers is ears and reboot please
```

(Nem emlékszem rá, hogy mit csináltam! Fogd be füledet, és indítsd újra a rendszert!)

Arf

Ez a vírus BIOS szintű sávformázását végez. Az egyszerű szoftveres védelemnek ebben az esetben már nincs mit tennie. Eltűnik a pusztítás maradék eleganciája is, kizárólag a rombolás hatékonysága játszik szerepet. A durva vírusok egyik legelső darabja. Ha elvégezte a közvetlen sávformázást, akkor már csak konstatálni tudjuk a kárt. Ez is arra figyelmeztet, hogy inkább a vírusok bejutását kell megakadályozni, nem pedig utólagos gyógykezelésre berendezkedni. Ha a vírus a merevlemez egyik sávját már formázta, a következő üzenetet jeleníti meg:

```
Arf Arf Got you!
-- RABID '90
```

(Uff! Uff! Elkaptalak! RABID '90)

Az aláírás persze még nem azonosítja íróját, aki valószínűleg az olasz vírusgyártó műhelyekben nevelkedett. Ha a fenti felirat megjelenik, már késő bármilyen víruskereső és vírusölő programot futtatni.

Mirror

A vírus nem hosszú, de gyilkos. Aktivizálódása során a képernyő betűinek tükörképét állítja elő — innen a neve is. A Norton Commander ablakait látványosan cserélgeti. Több felhasználó arról számolt be, hogy valami nagyon gyorsan (5 mp alatt) legyalulta a merevlemezt. Azt nem tudták megmondani, hogy mi volt az, mert a vírus is a merevlemezen volt... (Az 1991. évi IFABO és BNV alatt ezt a vírust használtuk a TG vírusvédelmi rendszer éles tesztelésére.)

V516

Szokásos COM fertőző rezidens vírus. Érdekessége, hogy a programok által lekérdezett DOS verziószámot állítgatja. A legszélsőségesebb esetben 0-s DOS verziószámot ad vissza és a DOS programok sem futnak a hibás DOS verziószám miatt. A Sysdoki 4.xx vírusölő program sem tudja irtani, mivel az a floppyról csak keres, a memóriából pedig nem irt, csak fájlból. Hatékony ötlet, mert a legelemibb DOS programok is „Incorrect DOS version" hibaüzenettel szállnak el.

Exterminator

Az Amiga, az Atari és az Apple gépek használói már régóta ismerték a Lamer Exterminator nevű vírust, amelynek PC verziója is megjelent 1991 májusában. Új generációs, felülíró, nem rezidens típusú. Fertőzése során az aktuális könyvtárban lévő COM programok első 451 bájtját írja felül, beleértve a COMMAND.COM-ot is. Nevét a vírusban lévő szöveg alapján kapta.

```
Exterminator 1.0 - (c) by Cracker Jack 1991 (IVRL)
Italian Virus Research Laboratory (C) 1990,1991
```

(Ez az üzenet azonban csak a szakembereknek, a vírus visszafejtése során válik láthatóvá.)

```
Non rompetemi le palle o mi arrabbio...
non so se sono stato abbastanza chiaro.....
```

A vírus a csak olvasható (read only), a rejtett (hidden) operációs rendszerállományokat, a normál programokat és a lemez címkéjét is megfertőzi. A fertőzött állomány dátuma nem kerül átállításra és mérete sem változik meg, csak akkor, ha a fertőzött program rövidebb volt, mint a vírus hossza. Ha a vírus fertőzése során hiba lép fel és a rendszerdátum hétfőt mutat, akkor a C: winchester első 160 szektorát tönkreteszi, a „legyalulást" egymás után 160-szor ismételve meg. Ha a vírus végzett munkájával, akkor a következő üzenetet jeleníti meg:

```
Exterminator Virus 1.0 (c) by Cracker Jack 1991 (IVRL)
No panic_this is a Harmless Virus_
```

A vírus ismert mutánsának hossza 256 bájt, viselkedésében csak annyi a különbség, hogy hétfőn nem törli le a merevlemezt, hanem a CGA/EGA monitor vízszintes szinkronjelét tologatja jobbra-balra. A vírusban a következő szöveg található:

```
BadGuy Virus (c) by Cracker Jack 1991 (IVRL)'
Italian Virus Research Laboratory (C) 1990,1991
IVRL Head Quarter, Milan Italy
```

Demon

A Demon vírus is az IVRL olasz műhelyben készül. A víruscsalád többi tagjával azonos víruskódoló rutint tartalmaz, és a copyright jelet használja. Üzenete:

```
"Demonhyak Viri X.X (c) by Cracker Jack 1991 (IVRL)"
"Error eating drive C:"
```

Label

Az újabb vírusok egy része kivétel nélkül minden attribútumú állományt megfertőz, beleértve a lemez címkéjét is. Az Exterminatorhoz hasonlóan a Label is ilyen. A lemez címkéje ugyanis gyakorlatilag fájlként kezelhető, és némi furfanggal írni lehet bele, illetve olvasni lehet belőle. Ez ad lehetőséget a lemezcímkék megfertőzésére. A Sysdoki installálási folyamata során szintén a harddiszk címkéjének paramétereit tárolja el, és ennek megfelelően működik demó vagy teljes verzióként. Ez az oka annak is, hogy ha a szoftvert lemásolják a merevlemezről és átviszik egy másik gépre, ott az csak demóként működik.

Az Exterminator és a Label vírus a Sysdoki jogos felhasználóinak teljes értékű példányából demó verziót készít. Ilyen típusú vírusok jelenléte is okozhatja tehát, ha a Sysdoki egyszer csak demó programmá vedlik át. A Sysdoki floppyról csak megkeresi a vírust, kiirtani pedig a merevlemezről, fájlból tudja, s nem a memóriából. Ha a felhasználó ilyen vírussal találkozik, akkor az irtást floppyról emiatt nem tudja elvégezni, a merevlemezről pedig azért nem, mert a vírus demóprogrammá varázsolta a Sysdokit. A kör bezárult. S ezzel elérkeztünk kifejezetten az antivírus eszközök ellen írt vírusok terebélyesedő családjához.

Metal Thunder

A Thunderbyte vírusvédelmi kártyán áthatoló vírust nem nehéz írni, csak ki kell használni annak gyenge pontjait. (A Polimer is ezt teszi.) Ennek a vírusnak a szerzője valószínűleg az olasz vírusírók iskolájának neveltje, és a Plague vírust vette alapul, azt barkácsolta át úgy, hogy a Thunderbyte kártya mellett átmenjen és ezen ténykedését még jelezze is a felhasználónak. A vírusban lévő szöveg:

```
Metal Thunder Virus - Ver. 1.X
(C) by Metal Thunder
-* IVRL *- All rights reserved
```

Ez a vírus is igen kártékony, BIOS szintű sávformázást végez, és ez végleges adatvesztést jelent.

Fellowship

Viszonylag régen, egy nyugatnémet szoftverszállítmánnyal együtt érkezett Magyarországra. Akkor az importőr megkereste Szegedi Imrét ezzel a vírusproblémával, de a telefonbeszélgetés után — félve a következményektől és az esetleges perektől — nem volt hajlandó a köz érdekében a vírust átadni. Később egy felhasználótól kaptuk azt meg. Érdekességképpen a vírusban lévő képmutató szöveget tesszük közzé:

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

(Ezt az üzenetet ajánlom a Földön minden PC-felhasználó társamnak. Egy jobb holnap felé. Amelyben jobb lesz élni.)

Vírusölő

Nem megerősített információk alapján Magyarországon már olyan vírus is kering, amely először a víruskereső és vírusölő programokat támadja meg. A hír szerint a vírus a rendszerbe jutva megkeresi a SCAN, PCSCAN, CLEAN, TNTVIR, SYSDOKI programokat, majd törli azokat a lemezről, bejelenti, hogy átvette a vezérlést és a gép az övé. A híreket Szeged és Debrecen térségéből kaptuk, s ha azok igazak, az egyik vírusíró egyetemi programozópalánta termékéről lehet szó.

Tömör gyönyör

Nemrégiben kaptuk kézhez az első tömörített vírust. Az ilyen típusú vírusos állományok létrehozásának lehetőségét több mint másfél éve ismerjük, de szerencsére csak most jutott el hozzánk. A recept nagyon egyszerűnek látszik. Vegyél egy nem fertőzött programot. Fertőzd meg valamilyen vírussal, majd nyomd össze olyan állománytömörítő programmal, amely futtatás közben csomagolja ki magát (Pklite, LzExe, SCRNCH stb.). Az így összezsugorított vírust a normál víruskereső programok nem ismerik fel, mert ahhoz ismerniük kellene a tömörítő algoritmust, amit a szoftvergyártó cégek nem adnak ki. Egy két algoritmust azért beépítenek a víruskeresőkbe. Például a SCAN felismeri az LZEXE algoritmusát, a CHKVIR az LZEXE-vel és az EXEPACK-kal tömörített állományt. A PKLITE teljes, antidebug verziója, amit egyre többen használnak, jó lehetőséget nyújt a vírusok eldugására.

Ha ezt a megoldást több vírussal megismétlik és mindig más tömörítő algoritmust használnak, akkor elkészíthető egy szinte tökéletes „vírus-szendvics". A víruskereső programok soha nem fogják tudni, melyik program a hordozó, csak a másodlagosan fertőzött állományokból tudják kiölni a vírust, amennyiben nem az új generációhoz tartozó, felülíró vírusokkal van dolgunk. Az így elkészített vírusos állományt csak rezidens víruskereső programmal vagy valós idejű vírusellenőrző programmal lehet detektálni.

CRC-ellenőrzés, fájl-immunizálás

A jelenlegi vírusírási trendeket látva a későbbiekben a vírusirtás fő módja a fertőzött fájlok törlése lesz. Az antivírus programok már most is nagyon sok vírus esetén írják ki az alábbi üzenetet:

```
Removal method: Delete infected file
```

A TG vírustesztje során Norton Commandert használva teszteltük az egyes vírusokat. Meglepő, hogy a „forgalomban lévő" vírusok közül milyen sok támadja meg a COMMAND.COM programot. Másik érdekes tapasztalat az, hogy először általában a Norton Commander NCMAIN.EXE programját akarják megfertőzni. Nyilvánvalóan azért, mert a rezidens Commander (NC.EXE) ezt hívogatja. Ilyen felhasználói környezetben a fenti fájlokra külön figyelmet kell fordítani. Tapasztalataink szerint az NC.EXE tűri a Buruzs Tamás-féle SPS rendszer ráültetett önvédelmi rutinját, s így legalább az vísít, ha vírus került a rendszerbe.

Sokan felteszik a kérdést, hogy mennyire hatékonyak a CRC ellenőrző programok és a fájl-immunizáló (SPS, SYSDOKI) kis rutinok. A konkrét vírusoktól független, CRC változásellenőrző eljáráson alapuló programozástechnikai megoldások kezdetben még hatásosak voltak, a későbbi vírusok ellen azonban alig használhatók. A CRC ellenőrzés menete viszonylag lassú, és csak annyit tudnak megállapítani, hogy a fájl tartalma megváltozott, feltehetően vírusos lett. Ezt is csak akkor, ha a vírus megengedi nekik, hogy az eredeti fájltartalmat lássák, mert a 4096-os és a hasonló programozástechnikát alkalmazó többi vírus bizony nem teszi meg ezt a szívességet.

A CRC megoldásnak egyéb hátrányai is vannak. Ilyen ellenőrző programokkal csak a nem nagyon változó fájlokat célszerű ellenőrizni, mert a gyakran változó tartalmúak (adatbázisok, táblázatok) állandóan visongatnának.

Piszkos trükkök

A vírusírás piszkos trükkjeiből is egyre több lesz. Már találkozhattak olyan vírussal, amelyik egy hasonnevű .COM állományt hoz létre az .EXE mellett, így programindításkor az fut le elsőként, és az startolja az .EXE programot. Ezt a technológiai megoldást teljesen legálisan és jó célokra is fel lehet használni. Az MS-DOS és a PC-DOS 5.0 verziójában ilyen típusú betöltő rutinokkal tudjuk futtatni például a Codeview programot.

Vannak azonban más ötletek is! A DOS-ban nincs korlátozva az állomány és a kiterjesztés neve, az lehet akár yyyyyyyy.xxx is. Ez természetesen nem futtatható név, a vírus működéséhez pedig futtatható állomány kell. Azt azonban a vírus ráér majd akkor létrehozni, amikor aktivizálni akarja magát (pl: yyyyyyyy.com).

Néhány vírusellenőrző módszert igen primitív és ezért hatásos ötlettel döntöttek meg. A sebesség növelése és a hamis vírusriasztások minimalizálása érdekében néhány víruskereső program COM vírusokat csak COM programokban, EXE vírusokat pedig EXE programokban keres. Meg kell őszintén vallanunk, mi is ezt az elvet követtük, és lenéztük azt, aki nem így cselekedett. Az elv egy ideig biztonságosan működött is.

Azután valaki úgy gondolta, hogy az .EXE programot átnevezi .COM-ra, és a víruskereső nem fogja megtalálni. Az ötlet nem igazán eredeti. A 3.0-nál régebbi GEM rendszerek installálásakor nem fogadták el az újabb DOS verziók FORMAT.EXE-jét, ha viszont .COM-má neveztük át, vígan futott. A DOS ugyanis az egyes programokat nem a fájlnév alapján futtatja. Ez adhatta a vírusírónak az „isteni szikrát". Én a Fellowship vírushoz .COM néven jutottam hozzá, de a program valójában EXE volt, vagyis „MZ" volt az első két bájtja. A McAfee-féle SCAN víruskereső nem is találta meg, de amint átneveztem az állományt .EXE kiterjesztésűre, rögtön lefülelte a vírust.

A másik trükk is elég egyszerű, de egy kicsit jobban kell hozzá ismerni a DOS-t. Feltehetnénk a kérdést: Hogyan lehet az .EXE programban lévő vírust sok víruskereső számára felismerhetetlenné tenni úgy, hogy nem írjuk át, az állomány hosszán sem változtatunk, de nem is csinálunk belőle mutánst? A recept: *Cseréljük fel az .EXE program elején lévő „MZ"-t „ZM"-re.* Ezt az akadályt csak a SCAN, a HTSCAN és a PCSCAN vette, a SYSDOKI nem. Az alábbiakban egy eredeti vírus fájlnévellenőrző részeletét mutatjuk be:

```
NoComFile:
  CMP       ES:[DI+18],4558  ; Check for ?XE file
  JZ        CheckForEXE      ; If so - infect it
  JMP       SkipFile         ; Else skip file
```

```
CheckForEXE:
  CMP       ES:[DI+17],45     ; Check if file is realy
                              ; an EXE-named
  JZ        CheckEXEsign      ; If so -> check for MZ,ZM
  JMP       SkipFile          ; Else skip file
CheckEXEsign:
  CMP       [SI],5A4Dh        ; Check for MZ
  JZ        InfectEXE         ; If so -> infect file
  CMP       [SI],4D5Ah        ; Check for ZM
  JZ        InfectEXE         ; If so -> infect file
  JMP       SkipFile          ; Otherwise -> skip file
```

Vírusok az Ablakban?

Lehet-e vírust írni a Windows grafikus felhasználói felületre? Ez a kérdés már hosszabb ideje foglalkoztatja a szakembereket, akik rettegve gondolnak arra az időszakra, amikor ez be fog következni. A Windows grafikus interfésszel rendelkező, multitaszkos operációs rendszerű program. Bár a DOS fejlesztése nem a multitaszk irányában indult el, most már az 5.0-s DOS verzió a DOSSHELL segítségével képes erre az üzemmódra is. Több program egyidejű futtatását megvalósító Windows-t nagy teljesítményű, legalább 386-os processzorú számítógépekre ajánlják. A processzornak egyidejűleg egymástól függetlenül kell több feladaton (taszkon) dolgoznia. Ha az egyik elakad, számítógépünk akkor sem merevedik le, mert az adott program a processzornak csak egy szeletét használta. Sajnos a multitaszkos rendszerek alá könnyen lehet vírust írni és nagyon nehéz ellene védekezni. Ilyen technológiát alkalmaznak a Windows alá írt másolásvédelmek is. Nyitnak egy taszkot, amelynek sem képernyőkimenete, sem billentyűzet-interfésze nincs. Ekkor nem lehet látni, be sem lehet kívülről szállni, és mégis ott fut. Ki sem tudjuk a Task Managerrel irtani.

A multitaszkos rendszer az elindított programnak processzoridőt és memóriát biztosít, amelyet a a többi program felülírása elől megvéd. A rendszernek így kell működnie, nehogy az egyik program beleírjon a másikba, ezzel megsemmisítve azt. Ebből a tulajdonságból kiindulva nagyon könnyen lehet olyan vírust írni, ami processzor időszeletet és saját védett RAM területet kap. Tételezzük fel azt, hogy két programot indítunk el Windows alatt. Az egyik egy víruskereső program, a másik pedig egy vírus. A víruskereső megtalálja a vírust és kiöli a programból. Amikor pedig a vírusra kerül az időosztás, az ismét megfertőzi a tiszta programot. Ezt a játékot végtelen ciklusban lehet ismételni és nem tudjuk elérni a vírusmentes állapotot.

A vírust nem lehet kiirtani az multitaszkos operációs rendszerből (Windowsból), mivel az operációs rendszer védi őt. A dolgot az is nehezítheti, hogy a vírusnak nincs képernyő-megjelenítési funkciója, csak időt és egy kis RAM-ot kér a gépben. Van-e hát értelme víruskereső és vírusölő programokat írni Windows

alá? Amíg nincs Windows vírus – csak DOS vírus –, talán igen, mert szép a grafikus megjelenítés, de Windows alatt valamivel lassabban futnak a jelenlegi vírusellenőrző programok, mint DOS alatt. Nem sok értelme van ennek a megoldásnak. Talán hatékonyabb a real-time vírusellenőrzés, amikor minden taszkot figyelni lehet a háttérből.

A vírusok és a DOS

Az 5.0 MS-DOS és a PC-DOS újdonságai csak igen rövid ideig fogják visszavetni a vírusok működését. Mindenesetre az már biztosnak látszik, hogy új bootvírus-írási technológiákat fognak keresni. Most már ugyanis — miként a DR DOS esetén is — a rejtett állományok fizikai helye nem kötött. Ugyanakkor a DOS az alsó sávot maszkolja. Erről mindenki meggyőződhet, ha 6.0-ig bezárólag a PC Tools Compress programjával próbálja helyrerakni a merevlemezt. Az első sávot üresnek látja a lemeztérképen, és amikor a program oda akar írni, „Sector not found" hibaüzenettel kiakad. Ugyanezt idézik elő egyes vírusok is.

Tovább bonyolítja a vírusok életét a multitaszk lehetősége, amelyről már szóltunk egypár szót. Most még két 5.0 DOS sajátosságról érdemes szólni, a SETVER parancsról és az XMS memóriakezelésről.

A SETVER paranccsal állíthatjuk be, hogy egy program milyen DOS-verzió környezetet lásson maga körül. Ha a vírus a programkód része, akkor ez rá is vonatkozik. De mi van akkor, ha belép egy másik DOS verziójú programba? Amikor kilép a memóriába, akkor egy másik DOS verziójú környezetbe került. Ilyenkor legtöbbször kiakad. Gondoljunk csak bele. Hasonló okok miatt nem működik az új DOS alatt a korábbi verziójú Matawindow, s jó pár, a memóriában real-time üzemmódban kipakoló program sem.

A vírusok másik akadálya a multitaszk mellett az XMS kezelése. Lehetőségünk van a DEVICE helyett DEVICEHIGH parancsot írni a CONFIG.SYS-ben, s akkor a 640 K fölé töltődik be a meghajtóprogram, illetve a DOS. Hasonló lehetőségünk van, ha az LH segítségével töltünk be egy programot, akkor a ráakaszkodott vírus is felmegy a 640 K fölé. Mit tesznek ilyenkor a vírusok? Némelyik változatlanul fut tovább — csak éppen nem látják a víruskereső programok. Más esetben totális rendszerlemerevedés a vírusfertőzés következménye, olyannyira, hogy a DOS be sem tud töltődni.

Új fejezet kedődött tehát a vírusok és az ellenük védekezők harcában. Egy furcsa dolog is tapasztalható. Van néhány igen fejlett „hadibaci", amelyet mintha felkészítettek volna ezzel az operációs rendszerrel való találkozásra. Honnan ismerték előre a vírusírók, hogy mit is tud az új operációs rendszer?...

Hogyan lett kommunista Michelangelo?

Itt vált azzá, Magyarországon! Származási helye kétes, vannak, akik szerint Svédország vagy Hollandia is lehet (mert onnan jelezték először, 1991 áprilisában), míg mások egyértelműen az olasz Virussoft csapatot gyanúsítják. Magyarországon legelterjedtebb a Kommunista Michelangelo. Nevét onnan kapta, hogy a vírus eredeti aktivizálódási dátumát március 6-ról — Michelangelo születésnapjáról — valaki átírta október 23-ra.

A Michelangelo a Stoned alapján készült, de különbözik tőle. Memóriarezidens, a floppylemez katalógusterületét írja felül, a merevlemezt formázza, a rendszermemóriát csökkenti. Vírusos floppylemezről történő betöltéssel válik rezidenssé és fertőzi meg a bootszektort. Ha a vírus a memóriában rezidens, akkor a DOS CHKDSK programja 2048 bájttal kisebb memóriaméretet mutat, mint amennyi a rendszerben installálva van: 640 K – 2 K = 655360 bájt – 2048 bájt = 653312 bájt. A 12-es megszakítás (INT 12 — usable memory size) a memória végében ülő Michelangelo vírusra mutat és ez megakadályozza a vírus által lefoglalt terület felülírását. Ez az egyik detektálási lehetőség is.

Ha a Michelangelo vírus rezidens, akkor minden floppylemezt azonnal megfertőz, amelyikhez a gép hozzáfordul. (Az írásvédett, leragasztott floppyt azonban nem tudja megfertőzni.) A 360 K-s, 5.25"-es floppy-lemeznél a vírus az eredeti bootszektort a logikai 11-es szektorra helyezi át (a katalógusterület utolsó szektora). 1,2 megás floppy esetén az eredeti bootszektor a logikai 28-as szektorra kerül át (oldal=1, sáv=0, szektor=14). A vírus által felülírt katalógusbejegyzésnek megfelelő fájlok, programok a floppy-lemezről elvesznek, pontosabban elérhetetlenekké válnak. Ez a fogás hasonlít a Stone víruséhoz.

A merevlemezen a partíciós táblába épül be. A merevlemez eredeti partíciós tábláját a 0. oldal, 0. sáv, 7. szektorra (side 0, cylinder 0, sector 7) teszi át.

Felismerő program: ViruScan V80, F-Prot 1.16 és természetesen a későbbi verziók. A Clean 80 a teszt során a floppyt tönkretette, a későbbi Clean verziókban ezt a hibát kijavították.

Az eddigi legintelligensebb vírus, a DIR2/FAT

A vírusírók fantáziája ismét megmozdult. 1991 őszén megjelent egy vírus, amelyre elmondható, hogy szinte ideális — mármint a vírus nézőpontjából. Felismerése, irtása eléggé szokatlan.

A vírus olasz eredetű, egy „Virussoft" nevű társaság szüleménye. A magyar számítástechnikusok a találó Cluster Buster nevet adták neki (lásd Alaplap 1992/1.), s csak a szakirodalom szorgos olvasói, no meg az antivírus programok HELP szövegének lelkiismeretes tanulmányozói jöhettek rá arra, hogy ez azonos a McAfee program által D2-ként azonosított vírussal. A helyzetet bonyolítja, hogy külföldön, főleg egyes nyugati publikációkban szintén több nevet adtak e vírusnak, melyek közül legismertebb a DD (disk directory) és a Creeping Death. A magyarul „lopakodó halál"-nak fordítható elnevezés a vírus teljesen új működési elvével függ össze. Az eddig elterjedt szoftveres vírusfigyelő és vírusvédelmi rendszereket ugyanis kijátszotta.

Mielőtt rátérnénk a vírus működésének konkrét leírására, érdemes felelevenníteni a vírusok kritériumait. Mi különbözteti meg őket egyéb programoktól? Richard B. Lewis monográfiája (The Computer Virus Handbook) a következő 3 vírusismérvet tartja meghatározónak:

1. Végrehajtható, vagyis működőképes legyen (executable).
2. Önmagát másolva tudjon terjedni (cloning itself).
3. Képes legyen hozzáépülni más végrehajtható állományokhoz.

Ha egy program a fenti feltételeket teljesíti, akkor az vírusprogramnak minősül.

A D2 vírus működési elvét tekintve parancssorból betölthető lemezmeghajtóként (disk device driver) működik. Ennek következtében az eddig „megszokott" fájlvírusokhoz képest nem növeli meg a fertőzött állomány hosszát (azaz nem ír bele az állományba, nem írja elé-mögé magát), így nem is változik meg annak ellenőrző összege (CRC). Ha a program immunizáló önvédelmi (farok)programmal volt ellátva, az sem jelez semmit, hiszen az összes paraméter megegyezik, csak — egy kivétellel — a kezdő szektorok mások. Ha elindítjuk a vírusos programot, a vírus a lemez utolsó szektorcsoportját (clusterét) lefoglalja és oda egy példányban befészkeli magát. Ezt követően minden COM és EXE program elindításakor az adott program kezdő szektorait (clusterét) a katalógus bejegyzésben (directory) magára irányítja, a további FAT láncolást pedig a vírusban elhelyezett kód szerint kódolja. A vírus futásképes, hiszen ha egy programot elindítunk, akkor a DOS a katalógus bejegyzésének megfelelően lefuttatja a programot... vagyis magát a vírust.

Ez a megoldás egyúttal sok megnyilvánulásra is magyarázatot ad. Ha tiszta operációs rendszerről töltjük be a DOS-t, akkor a vírus nem tud beépülni, és nem tudja dekódolni magát, ezért csak a directory bejegyzésnek megfelelő egy clusternyi szektort lehet fájlként kimásolni (DD floppy esetén 1 cluster = 2 szektor = 1024 bájt, HD lemezeknél általában 4 szektor, vagyis 2048 bájt). Ha ilyenkor adjuk ki a CHKDSK parancsot, akkor az összes fertőzött COM és EXE programra „Cross linked" üzenetet kapunk. Ha ebben az állapotban ki akarjuk másolni COM és EXE programjainkat, akkor csak tisztán a vírust másoljuk ki és minden programunk egyforma hosszú és tartalmú lesz. Ráadásul a vírus a továbbfertőzés során a FAT kódolását változtatja!

Néhány szakember ezt a D2 vírust azért nem tekinti vírusnak, mert az általa ismert és az eddigiekben hatásosnak bizonyult mintavételezési algoritmussal nem tudja azt detektálni. Az észleléshez ugyanis feltételeznie kell, hogy a mintavételezés pillanatában a program nem vírusos, ha pedig vírusos lesz, akkor a vírusnak a program elé vagy mögé kell beépülnie; a vírus nem írhatja felül a programot; a vírus nem lehet tömörített (LZEXE, PKLITE, DIET, EXEPACK); a vírus nem rejtheti el magát és nem mutathatja meg a program eredeti állapotát; a vírus nem lehet a memóriában aktív... és még lehetne tovább sorolni a kizáró feltételeket.

Érdekes, hogy a szoftveres antivírus programok fejlesztői közül ennek az új vírusnak a megjelenésekor először McAfee és csapata, valamint az F-Prot programcsomag írója, Fridrik Skulason volt hajlandó addigi detektálási elveit teljesen felülbírálni. Sokan azonban inkább kitartottak a „nem vírus" felfogás mellett, mert nem tudták beilleszteni az új jelenséget eddigi védelmi rendszerükbe.

Ha egy vírus terjed, akkor kicsit furcsa azt mondani róla, hogy „nem önreprodukáló". Sajnos a vírusok egyik alapvető tulajdonsága az is, hogy elszabadulnak. A D2 pedig egy új elven működő vírus ügyes megvalósítása, ami (a visszafejtett saját kódverzió és a szakmai körökben közkézen forgó — szeren-

csére még csak ott ismert — eredeti kód alapján bizton állíthatjuk) a maga kategóriájában programozástechnikai remekmű. Viszont az ilyen vírusok elleni küzdelemre is fel kell készülni. Ne reménykedjünk abban, hogy ezt a vírust kivételesen nem írják át, illetve nem írnak ilyen elven működő újabb vírusokat. Az elsők most a bolgárok voltak, onnan valószínűleg 4 átírt verzió indult útnak, s jutott el többek között Magyarországra is, elindítva a Potyogós óta a legnagyobb hazai vírusjárványt.

Magyarországon a fertőzés első áldozata valószínűleg egyik vidéki városunk gyára volt. A vezetők sokáig titkolni igyekeztek a vírust, s régi szokás szerint végül azt a programozót bocsátották el állásából, aki felfedezte a szokatlan bajt, és tenni szeretett volna valamit ellene. Amikor külső segítségért folyamodott, egyenesen üzemi titoksértőnek minősítették.

Az első terjesztők akaratukon kívül az államigazgatás (különösen a bankok és pénzügyi szervek) számítógepes rendszerei voltak, ahol az adatokat önkicsomagoló állományokkal továbbítják, mégpedig elég sűrű időközönként.

Amikor a D2 első észlelője jelentkezett nálunk, magunk is tanácstalanok voltunk, hogyan távolítsuk el a rendszerből a furcsa betolakodót — ami esetleg nem is vírus. A felhasználók a vírussal történő együttélés során megtanulhatták, hogy a vírus csak COM és EXE programokhoz láncolja hozzá magát. A vírusnak ezt a tulajdonságát felismerve a .COM programokat néhányan átmásolták mondjuk .CO kiterjesztésűre az .EXE programokat pedig .EX-re. Mások az összes .COM és .EXE programot betömörítették, mivel a vírus a ZIP-be nem tud belemenni. Utána letörölték az eredeti programokat és tiszta rendszert hívtak, megszabadulva a vírustól is.

A vírus következtében a Novell hálózaton is furcsa dolgok történtek, a végeredmény pedig rendszerösszeomlás lett. Nem baj, ez nem is vírus, csak egy hardverre írt rossz adatvédelmi rendszer! Ezen az alapon néhány fejlesztő tudatosan fertőzte meg vele gépeit, mondván, akkor nem lopják el a programjait.

McAfee Scan sorozatának 84-es változata volt az első, amely a D2 vírust detektálta, a Clean 84 pedig le is szedte. A vírus azonban a Scan 84 megjelenése előtt két hónappal, amikor még a korábbi verziókat használták, már javában dühöngött. A Scan a lemezen lévő összes .COM és .EXE állományhoz hozzáfordul, így az történt, hogy még olyan állomány is vírusos lett, amelyik előtte nem volt az. (Hasonló eset történt két évvel előtte a V2000 vírus megjelenésekor, de az tudatos manipuláció volt.)

Bekerült azonban a Scan/Clean rendszerbe egy érdekes hiba. A Scan 84 és 85 a D-2 azonosítót adta meg, míg a Clean megfelelő verziói a D2 azonosítót, kötőjel nélkül. Ez a kis programhiba sok ember életét keserítette meg. A VIRSCAN.DAT hazai vírusokat ismerő átiratában (TOPSCAN.ZIP, illetve TOPSCAN2.ZIP, majd egy új változata TOPSC2U.ZIP, TOPSU9101.ZIP néven vált ismertté) az első publikációk alapján a Creeping Death, azaz a Lopakodó Halál nevet kapta.

* * *

Körülbelül két évvel ezelőtt még azt hittük, hogy a fájlimmunizáló programok hatásos általános vírusvédelmet tudnak nyújtani. A jelenlegi vírushelyzetben ezt már nem lehet kijelenteni. Ha a vírus formázza a merevlemezt (vírussal kísérletezőknél többször is előfordult már ez a baleset), akkor mindegy, hogy az állományok immunizálva voltak-e vagy sem. Ha a vírus felülírja (tönkreteszi) az állományokat, akkor rá sem fut az immunizáló rutinra, de nem is lenne mit helyreállítani (1, 2, 8 kilobájtos programrészlet). Sajnos le kell tenni az ilyen jellegű fejlesztésről is. Borzasztó dolog belátni, hogy az út, amelyen járunk, már nem vezet sehova. Újra vissza kell térni a kiindulási pontra, és elindulni a cél felé, egy eddig még járhatatlannak bizonyult úton. Ha azonban már jártunk arra, talán könnyebben sikerül haladni.

Víruskirajzás a (néhai) SZU-ból

Anti-Pascal, AP-529, Anti-Pascal II, AP-440, AP-480, Kemerovo, Kemerovo-B, USSR 311, Attention!, F-Word, USSR 492, USSR 516, USSR 576, USSR 707, USSR 711, Akuku, USSR 948, Bebe, Lozinsky, USSR 1049. Voronezh, Voronezh-B, Voronezh Related, USSR 1689, USSR 2144, Dir, Hymn, MGTU, Crash, Sverdlov, Victor.

A szovjet (orosz) vírusirodalom sokáig ismeretlen volt számunkra. Az információcsere bővülésével sajnos kiderült, hogy a PC-k rejtelmeit alaposan ismerik. 1990 végén robbanásszerűen megjelentek vírusprogramozóik remekei. Az ottani vírusok közül az általunk ismertek (és e fejezetben ismertetettek) úgy tűnnek, mintha egy-két vírusgyártóműhely tesztvírusai lennének. Ennek ellenére ezek életképesek, átírásukkal, a bennük lévő ötletek felhasználásával számolni kell. A bemutatott vírusok között olyan is van, amelyik orosz programozók ötlete alapján az USA-ban született. Az összatartozó, rendszertanilag egy egységet képező vírusok leírását igyekeztünk egy bokorba tömöríteni, ezért itt csak az Anti-Pascal és az USSR család tagjait mutatjuk be, a többi orosz eredetűt más fejezetekben.

A vírus neve: **Anti-Pascal**

Egyéb elnevezése: Anti-Pascal 605, AP-605, C-605, V605.

Hossza: 605 bájt.

Kódtípusa: Nem rezidens, parazita, a .COM állományokat fertőzi meg.

Azonosítása: Scan /X V67+, Pro-Scan 2.01+.

Eltávolítása: Pro-Scan 2.01+, Scan /D /X, vagy minden .COM programot törölni kell.

Leírása: Az programnyelvek elleni első vírus. Szülőhazája szinte biztosan a Szovjetunió, így került könyvünk ezen fejezetébe. Keletkezési helye valamelyik moszkvai egyetem lehet. A vírus Bulgáriában bukkant fel 1990 júniusában, ahonnan Veszelin Boncsev jelezte előfordulását.

A vírus a .COM állományokat támadja meg, de nem memóriarezidens. Az INT 24 segítségével fertőz, azt irányítja magára, amikor egy fertőzött program kerül végrehajtásra. A fertőzés vagy az aktuális meghajtón, vagy pedig a D: meghajtón történik. (Írójának legalább két partíciója volt a merevlemezén.)

Fertőzéskor másik két .COM állományba teszi bele magát. Ezek hossza 605 és 64930 bájt közötti lehet, amit a vírus ellenőriz is. A megfertőzött állományoknak nem lehet READ ONLY attribútuma. Ha a vírus a feltételeknek megfelelő programra lelt, akkor az első 605 bájtot felülírja, de ezt a felülírt 605 bájtot hozzákapcsolja a program végéhez. Ennek alapján lehet később helyreállítani az állományt. Bár felülírással épül be, a program hossza így mégis növekszik a vírus hosszával.

A fertőzött programban található a következő szöveg:

PQVWS

valamint egy második, amely egyben meghatározza, milyen állományokat tekint céljának. Ez utóbbit a offset 0X17 helyen találjuk meg az állományban:

combakpas???exe

A fertőzött állomány dátuma az eredeti marad, de az azt tartalmazó könyvtár dátumát átállítja a fertőzés időpontjára. A vírus telítődéskor kapcsol át rombolásra, vagyis akkor rombol, ha már nem talál a fent említett feltételnek megfelelő .COM állományokat a meghajtón. Ilyenkor az aktuális meghajtó aktuális könyvtárában .BAK és .PAS állományokat keres. Ha talál ilyet, saját kódjával gondosan felülírja. Ha azt megtette, akkor őket átnevezi .COM állománnyá. Ha már létezik azonos nevű .COM állomány, akkor .EXE kiterjesztésűvé kereszteli, de ez a funkció a vírus egyik programhibája miatt nem minden esetben hajlandó működni.

AP-529: Az Anti-Pascal egyik ismert, de a szakirodalom szerint ritka változata. Alapvető eltérés, hogy csak olyan .COM állományokat fertőz meg, amelyek hosszúsága meghaladja a 2048 bájtot. A .BAK és .PAS állományok felülírásakor egyet-egyet töröl is a 2048 bájtnál rövidebb fertőzetlen .COM állományok közül. Abban is különbözik, hogy csak akkor fertőz, ha a fertőzött .COM programot a C: meghajtó főkönyvtárából, illetve az A: vagy a B: meghajtóról, floppyról indítják. (Ebből gyanítható, hogy ez volt az ősibb, a kísérleti példány.)

A vírus neve: Anti-Pascal II

Egyéb elnevezése: Anti-Pascal 400, AP-400.

Hossza: 400 bájt.

Kódtípusa: Parazita, nincs rezidens része, a .COM programokat támadja meg.

Azonosítása: Scan /X V67+, Pro-Scan 2.01+

Eltávolítása: Pro-Scan 2.01+, Scan /D /X vagy a fertőzött programok törlése.

Leírása: Egy ötlet vándorötletté vált. Az orosz vírus gegjét mások is megkísérelték megvalósítani. Ez a vírus az orosz Pascal mintájára született, de eredeti bolgár konstrukció. Programkódjában, megoldásaiban fejletlenebb, mint az előzőkben ismertetett Anti-Pascal vírus. Egyes szakírók az orosz vírus bolgár előképének tekintik, mások, közöttük mi is, egy párhuzamos fejlesztés első eredményének. Jelenlétét Bulgáriából jelezte Veszelin Boncsev 1990 júniusában.

A vírus hossza 605 és 529 bájt között változik! Minden .COM állományt megfertőz, belelértve a COMMAND.COM-ot is, így igen gyorsan felfedezhető a je-

lenléte. Nem memóriarezidens, s szintén a fertőzött állomány végrehajtásakor, az INT 21-gyel manipulálva tud fertőzni.

Amikor a fertőzött program végrehajtódik, a vírus a hozzáférhető meghajtó főkönyvtárában egyetlen .COM állományt fertőz meg, de a fájl hosszának legalább 2048 bájtnak kell lennie, míg a fertőzött állomány hossza legfeljebb 64 K lehet. Ez a vírus nem esett a korai szovjet vírusok azon hibájába, hogy fertőzés után túllépik a DOS által fogadható 64 K-s határt. Más a fertőzési mechanizmusa is, mert nem felülír, hanem a kód végére épül be. Először ő hajtódik végre, majd a vezérlés átugrik az eredeti programra.

Elődjéhez hasonlóan csak a könyvtár dátumát írja át a fertőzés adataira, aktivizálódási feltételei azonban eltérnek tőle. Ha nem talál megfertőzhető .COM állományt, vagy pedig már két .COM programot megfertőzött, elkezdi keresgélni a .BAK, .PAS és .BAT állományokat. Ha talál ilyeneket, akkor törli őket, de csakis az aktuális meghajtó aktuális könyvtárában és a főkönyvtárban. Ha viszont ezeken a helyeken egyet sem lel a megadott kiterjesztésű állományokból, olyankor máshol töröl. A fertőzésről árulkodik az állományok 400 bájtos hossznövekménye, és az, hogy kezdenek eltünedezni a .BAK, .PAS és .BAT állományok.

Lényeges különbség még, hogy a bootszektor eltérést mutat, ezért az annak CRC-jét ellenőrző programok vísítanak. Miközben pedig a felhasználó a bootszektor eltéréseinek okait kutatja, a vírus egész máshol és más módon fertőz. Az egyik legkorábbi és szinte mindenki által „megevett" álcázási metódus.

Az Anti-Pascal II sikeres vírus, többen megpróbálkoztak már további átírásával, de ezek a vírusváltozatok szerencsére igen ritkák. ìme közülük néhány:

AP-440: Hosszabb, mint a 400 bájtos alapverzió: 440 bájt. A bootszektor eltérései is nagyobbak. Különben aktivizálódásának feltételei ugyanazok, mint az alapváltozaté.

AP-480: A hosszeltérés itt is alapvető. Ennek a változatnak a hossza 480 bájt. Nem törli viszont a .BAT állományokat, csak a .BAK és a .PAS állományokra vadászik. Szakirodalom szerint ennek a sorozatnak ez a legkésőbb felbukkant tagja.

A vírus neve: Wisconsin

Egyéb elnevezése: Death To Pascal

Hossza: 825 bájt.

Kódtípusa: Parazita, nem rezidens, .COM fertőző.

Azonosítása: Scan V67+, Pro-Scan 2.01+.

Eltávolítása: Scan /D vagy törölni a fertőzött állományokat.

Leírása: Az orosz vírus ötlete új életre kelt az USA Wisconsin államában, 1990 szeptemberében. Szerzője ismeretlen. A kód csak algoritmusaiban mutat hasonlóságot az eredeti vírussal. Nem rezidens, a .COM állományokra vadászik, de a fertőzés elkerülésére intelligensen kihagyja a COMMAND.COM-ot.

Amikor a fertőzött programkód lefut, a vírus az állomány dátumát megváltoztatja a futás idején aktuális rendszeridőre. A Wisconsin vírus egy másik .COM állományt fertőz meg az aktuális könyvtárban. A hossznövekedés ekkor 825 bájt lesz, és a kód a megfertőzött állomány elején található.

A vírusban van egy leleplező súlyos programozási hiba: ha a vírust írásvédett floppyról indítjuk el, akkor a rendszer „write protect error" jelzést ad. A vírus nem ismeri fel és nem tudja kezelni ezt az alapvető hibát.

A fertőzött program a következő hibaüzenettel „örvendezteti meg" a gép használóját:

```
Death to Pascal.
```

Amikor ezt az üzenetet látjuk akkor már késő. Az aktuális könyvtárban minden .PAS kiterjesztésű állományunk elveszett. Ezt a szöveget nem látjuk a vírusban, mert azt a vírus írója kódolta.

A vírus neve: Kemerovo

Egyéb elnevezése: USSR 257, Kemerovo-B.

Hossza: 257 bájt.

Kódtípusa: Parazita, nem rezidens, a .COM programokat támadja meg.

Azonosítása: Scan V74+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: A Kemerovo vírus is az 1990. decemberi víruskirajzás tagja. Nem rezidens, a .COM programokat fertőzi meg — a COMMAND.COM-ot is beleértve.

A víruskód lefutása során az aktuális meghajtó aktuális könyvtárában keres megfertőzhető .COM programot. Ha talál ilyet, akkor megfertőzi, és az eredeti program végére épül be. A hossznövekedés 257 bájt. Fertőzéskor a dátumbejegyzést kicseréli a fertőzéskor aktuális rendszeridőre. Ha nem lel fertőzhető állományra, családjának jó pár tagjához hasonlóan a következő hibaüzenettel lep meg bennünket:

```
????????COM Path not found
```

Majd a program végrahajtása nélkül kilép a DOS-ba. Ismert átirata:

Kemerovo-B: Megirigyelték a Kemerovo ötletét az USA-ban, onnan származik ez az átirat. Először is annyira átírták a programot, hogy az ismert keresési szekvenciák alapján ne legyen megtalálható. Másodszor pedig az aktuális meghajtó aktuális könyvtárában csak öt programot fertőz meg. Minden egyéb jellemzője azonos az orosz eredetiével.

A vírus neve: USSR 311

Egyéb elnevezése: V-311.

Hossza: 311 bájt.

Kódtípusa: A COMMAND.COM-ot COMMAND.CON-ra átnevező, nem rezidens, a .COM állományokat megfertőző parazita program.

Azonosítása: Scan V74+.

Eltávolítása: Scan /D vagy a fertőzött programok törlése.

Leírása: A vírus a szovjet vírusfejlesztési irányzat egyik „örömprogramozott" darabja. Írója beletette mindazt az ötletet, amivel tanulmányai során találkozott. A cél látható volt, minél kisebb méretben, minél több funkciót bepakolni. A vírus 1991 januárjában bukkant fel Nyugat-Európában, majd rövid idő múlva az USA-ban.

A program csak a .COM állományokat fertőzi meg, nincsen rezidens része. A COMMAND.COM-ot is megfertőzi, illetve manipulál vele. Ugyanis a fertőzött program kódjának lefutása után a programvírus kinéz a rendszerórára. A vírusban 16 előre meghatározott időérték van, s ha az óra ezek valamelyikét mutatja, akkor a COMMAND.COM-ot átnevezi COMMAND.CON-ra. A névváltozás hatására a gép az ilyenkor szokásos „Cannot load COMMAND.COM. System halted" rendszerüzenettel lefagy, illetve ha rendszer akarunk indítani, az istennek se indul el. Ha az óra nem egyezik egyik előre beprogramozott lehetőséggel sem, akkor az aktuális könyvtárban megfertőz egyetlen .COM állományt, és nem nevez át semmit.

A megfertőzött program 311 bájttal lesz hosszabb, a víruskód az állomány végére épül be. Amelyik alkönyvtárban már fertőzött, ott ugyan az állományok eredeti dátumait megtartja, de megváltoztatja az alkönyvtár létrehozásának a dátumát a következőre:

11:19:32

Ez a vírus számára a fertőzés jele. Ez azonban nem minden! Átállítja az egyes állományok attribútumbitjét az alkönyvtáron belül, mégpedig ha az 8-15 között van, akkor reseteli. Ezzel néhány ezt alkalmazó program (így például a backup) meglepetésszerű dolgokat művel.

A vírus neve: Attention!

Egyéb elnevezése: USSR 394.

Hossza: 394 bájt.

Kódtípusa: Parazita, rezidens, .COM fertőző.

Azonosítása: Scan80+.

Eltávolítása: Clean80+ vagy a fertőzött állományok törlése.

Leírása: A vírus nevét arról a szövegről kapta, amellyel felülírja a megfertőzött állományokat. Az 1990. decemberi víruskibocsátás tagja, és része az USSR sorozatnak. Memóriarezidens, a .COM állományokat fertőzi, beleértve a COMMAND.COM-ot is.

Amikor rezidenssé válik, a hagyományos DOS memória felső szegmensében 416 bájtnyi helyet foglal le magának. Az INT 21 vezérlését magára veszi. A CHKDSK csak a 416 bájtos csökkenést jelzi a memóriában.

Amikor a vírus rezidens, nevéhez méltóan minden billentyűlenyomáskor csengőimitációt hallunk a gép hangszórójából. Írója tiszta szívből utálhatta a DOS Edlin segédprogramját (mely érzéseivel nincs egyedül), mert amikor az Edlint akarja valaki behívni és a vírus a memóriában van, a program nem jön, csak helyette a szemtelen hibaüzenet:

```
Invalid drive or file name
```

Az Attention! a .COM állományokat és a COMMAND.COM-ot akkor fertőzi meg, amikor végrehajtatjuk a DOS-szal. A hossznövekedés 394 bájt, a víruskód az állomány végén található. A fertőzött program kódjának elején található a névadó karaktersorozat:

```
ATTENTION !
```

A vírus neve: F-Word

Egyéb elnevezése: Fuck You.

Hossza: 417 bájt.

Kódtípusa: Rezidens, a .COM állományokat fertőzi, beleértve a COMMAND.COM-ot.

Azonosítása: ScanV80+.

Eltávolítása: A fertőzött állományok törlése.

Leírása: Az ukrán lövészhadtest szakszókincse volt az első gazdag káromkodásgyűjtemény, amely az oroszhon népei között nyomdafestéket kapott. Most már vírusban is káromkodnak, igaz, viszonylag enyhén. Az angolul szemérmesen F-Word-nak titulált vírus is az 1990. decemberi orosz víruskirajzás tagja.

A kód végrehajtása során a normál DOS memória „RAMTOP" részén foglal helyet magának. Az INT 12 vezérlését magára veszi, hasonlóan az INT 08-hoz és az INT 21-hez. A rendszer által használható memóriaterületet 1024 bájttal csökkenti. Nevét a fertőzött állományok elejét felülíró (magyar nyelvű változatában kötőszóként is használatos) angol trágárkodásról kapta:

```
Fuck You!
```

A fertőzött állományok mintegy 2 K-val több helyet kérnek, amikor végrehajtjuk őket. A 417 bájt hosszú víruskód a programkód után épül be, csak a szöveg kerül az állomány elejére. A fertőzés során a könyvtár létrehozásának dátumát átírja a fertőzés rendszeridejére.

Szerzője azonos lehet az Attention! orosz vírusával, mert a programkód hasonló stílusú, és mert az Edlin DOS editor indítását ez is megakadályozza, helyette az „Invalid drive or file name" üzenetet küldve.

A vírus neve: USSR 492

Egyéb elnevezése: Még nem ismeretes.

Hossza: 495–508 bájt

Kódtípusa: Rezidens, a .COM állományokat megfertőző parazita program.

Azonosítása: Scan V74+.

Eltávolítása: Scan /D vagy a fertőzött programok törlése.

Leírása: A vírus 1990 decemberében jutott ki a Szovjetunió határain túlra. A víruskód memóriarezidens, a .COM állományokat fertőzi, beleértve a COMMAND.COM-ot is. Az állományok dátumjelzését a fertőzés során átírja.

A vírus az INT 21 átirányításával kezdi beépülését a memória tetejére (a 640 kilobájton belül!), de nem tudja kihasználni a HIMEM lehetőségeit. Az állományleíró blokkban (FCB) nem foglalja le magának azt a részt, ahová beépült, ezért más program ezt a területet felülírhatja. A vírus installálódása után azt nézi meg, hogy a C: meghajtón fertőzött-e a COMMAND.COM. Ha nem, akkor sürgősen pótolja ezt a hiányosságot. Miután ezzel végzett, megfertőz minden .COM állományt, amit végrehajtunk. Ha nincs merevlemez és az A: meghajtóról indítunk rendszert, az ott lévő COMMAND.COM-ot is képes megfertőzni.

Ha a programvírus megfertőz egy állományt, akkor annak hossza 495–508 bájttal növekszik. A vírus a programkód végére épül be. Amikor fertőz, kicse-

réli a lemez alkönyvtárában az állományok dátumát arra a rendszeridőre, amikor a fertőzés megtörtént.

Más cselekedeteiről eddig még nem tudunk. Úgy tűnik, hogy egy terjedési algoritmus kipróbálására hozták forgalomba.

A vírus neve: USSR 516

Egyéb elnevezése: Leapfrog.

Hossza: 516 bájt.

Kódtípusa: Parazita, rezidens résszel rendelkezik, a .COM állományokat fertőzi meg.

Azonosítása: Scan V74+.

Eltávolítása: Scan /D vagy törölni a fertőzött állományokat.

Leírása: Az 1990. decemberi első nagy orosz víruskirajzással került külföldre. A vírus minden .COM állományt megfertőz, beleértve a COMMAND.COM-ot is.

A fertőzött program lefutásával együtt a víruskód is lefut. Ekkor épül be a memóriába, mégpedig egy DOS definíciók által üresen hagyott lyukba, amelyet az MS-DOS rendszerállományai és a DOS stack között találunk. A trükk ebben az, hogy a memória ezen része adatterületként van címezve. Amikori ide beépül a vírus, magára veszi a 21-es interrupt vezérlését, így jelenléte nem látható, hiszen sem a rendszer memóriája, sem pedig a DOS által jelzett szabad memória nem változott meg.

Rezidenssé válva akkor kezdi el a fertőzést, ha elindítunk egy fertőzetlen .COM programot. Arra viszont a lebukás elkerülése érdekében ügyel, hogy a fertőzendő állomány legalább 512 bájt hosszú legyen. A vírus a programkód végére épül be, 516 bájt hossznövekedést okozva.

A szakirodalom egyetért abban, hogy ez a vírus is egy demonstrációs célú program, vagy valamilyen terjedési algoritmus, illetve eljárás tesztelésére szolgál. A memórialyuk kihasználása még meglehetősen ritka a vírusprogramok között.

A vírus neve: USSR 576

Egyéb elnevezése: Még nem ismeretes.

Hossza: 576 bájt.

Kódtípusa: Nem rezidens, .EXE fertőző, a bootszektort és a partíciós táblát károsítja, rendszerkiakadást, illetve a töltési idő jelentős növekedését okozza.

Azonosítása: Scan V71+, Pro-Scan 2.01+.

Eltávolítása: A fertőzött programok törlése.

Leírása: Az 1990. évi nagy víruskirajzás során került ki a Szovjetunióból, és októberre már eljutott az amerikai kontinensre. Saját magát jelentősen átkódolja, megnehezítve a felismerést. Rendszerkiakadást, a bootszektor és a partíciós tábla károsítását tekinti céljának. A programok csigalassúsággal, több tízszeres idő alatt töltődnek be. Nincs rezidens része, az .EXE állományokra specializálta magát.

Amikor a vírusprogram a kód lefutása után elfoglalta helyét a memóriában, megkeresi az aktuális könyvtárban található első olyan .EXE állományt, ame-

lyet még nem fertőzött meg. Ha megleli, akkor megfertőzi. Néhány esetben a fertőzés során a meghajtó lámpácskája égve marad, és a rendszer kiakad. Ennek ellenére a fertőzés sikeres volt. A víruskód minden esetben az eredeti állomány végéhez épül be, mégpedig úgy, hogy a hosszúsága a paragrafushatártól függően 576 és 586 közötti értékkel nő meg.

Ha a rendszerben jelen van a vírus, akkor az megkeresi a merevlemez bootszektorát. Ezt, valamint a partíciós táblát károsítja úgy, hogy a McAfee-féle M-DISK segédprogram /P opciójával vagy Norton Utility-vel barkácsolva lehet csak helyreállítani. Különben a károsított meghajtó a DOS számára nem elérhető.

A vírus akkor kezdi pusztítását, amikor elfogynak a megfertőzhető állományok a merevlemezen. Ugyanis addig, amíg ilyenek vannak, a betöltési idő is normális, és a merevlemez boot és partíciós tábla állományait sem károsítja. Ez a megoldás nagyon emlékeztet a bolgár Eddie, valamint az orosz Viktor vírus működésére, annak ellenére, hogy ezek nincsenek rokonságban egymással.

Ez a vírus is az 1990. decemberi nagy víruskirajzás során került ki az akkori Szovjetunióból. Magyarországon szórványos előfordulására utaló nyomok vannak. A vírus a .COM állományokat fertőzi meg, beleértve a COMMAND.COM-ot is.

A CHKDSK 2048 bájtos főmemória-csökkenést jelez. A vírus a szokástól eltérően nem vonja ellenőrzése alá a 12-es megszakítást, de a 21-est és a 24-est magára veszi.

A vírus rezidenssé válva lesz alkalmas a fertőzésre. A megtámadott állományok 600 bájttal lesznek hosszabbak. Ugyanakkor a régebbi .COM vírusokhoz hasonlóan a víruskód a fertőzött program elejére épül be! Károkozása és aktivizálódási feltételei még nem ismeretesek.

A vírus neve: USSR 707

Egyéb elnevezése: Még nem ismeretes.
Hossza: 707 bájt.
Kódtípusa: Rezidens, .COM fertőző, parazita.
Azonosítása: Scan V74+.
Eltávolítása: A fertőzött programok törlése.
Leírása: A vírus szintén az 1990. decemberi víruskirajzás során került ki a Szovjetunióból. Valószínű, hogy a terjedési algoritmusok kipróbálására irányuló tudatos akcióról volt szó, mert ezek a rövid orosz vírusok egyazon műhelyre utalnak.

Amikor a vírus rezidenssé válik, a DOS 640 kilobájtnyi konvencionális memóriájának a tetejére ül be. Néhány korábbi ötlettel ellentében a vírus a megszakításokat önmagán keresztül vezetve meg tudja akadályozni, hogy felülíródjon az a terület, ahova beült, annak ellenére, hogy az állományleíró blokkban (az FCB-ben) nem könyvelte el. Új trükk, hogy a 21-es interrupt manipulálásával képes a HIMEM használatára is. Normál esetben a rendszermemóriát 720 bájttal csökkenti.

Amikor a vírus a memóriában van, már minden lefutott .COM program fertőzötté vált, beleértve a COMMAND.COM-ot is, a hosszakat 707 bájttal megnövelve. A víruskód az állományok végére épül be.

A vírus neve: USSR 711

Egyéb elnevezése: Még nem ismeretes.

Hossza: 711 bájt.

Kódtípusa: Rezidens, .COM fertőző, parazita, a rendszer lemerevedését okozza.

Azonosítása: Scan V74+.

Eltávolítása: A fertőzött programok törlése.

Leírása: Az 1990. decemberi szovjet víruskirajzás tagja. A COMMAND.COM kivételével a .COM programokat fertőzi meg, memóriarezidens részén keresztül.

Az orosz vírushagyományoknak megfelelően a 640 KB konvencionális memória tetejére ül be. Ezt a rész viszont — többi orosz társától eltérően — szabályosan lefoglalja, magára irányítja a 08-as, 13-as, valamint a 21-es rendszermegszakítókat, és a CHKDSK a vírus jelenlétében 704 bájttal csökkentett memóriát jelez. Nem tér el viszont családtagjaitól a 12-es interruptvektor kezelésében.

Amikor a program már rezidens, alkalmas arra, hogy fertőzzön. Minden fertőzés előtt elvégez egy feltételvizsgálatot. Ha a kiszemelt .COM állomány hosszabb, mint 1600 bájt, akkor fertőz, különben nem. Az állományok végére épül be a víruskód, és a hossznövekedés a paragrafushatárok miatt 705–717 bájt közötti lehet.

A vírus egyetlen ismert károkozása: időnként kiakasztja a rendszert, ha fertőzött programot indítunk el. Ez azonban valószínűleg programozási hiba. Itt egyértelmű, hogy csak egy terjedési algoritmus tesztjéről van szó.

A vírus neve: Akuku

Egyéb elnevezése: USSR 891.

Hossza: 891 bájt.

Kódtípusa: Parazita, nem rezidens. .COM és .EXE fertőző.

Azonosítása: Scan V74+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: 1991 januárjában valamelyik orosz vírusműhely újabb szellemességgel lepte meg a világot. A programvírus a benne lévő szövegről kapta az Akuku nevet. A fertőzés a .COM és az .EXE állományokra egyformán kiterjed, s ami a vírusvilágban hibának számít: a COMMAND.COM-ot is megtámadja. Alkotója arra még figyelt, hogy a vírus ne támadjon meg 1 kilobájtnál rövidebb programokat, de valószínűleg nem volt tisztában az .EXE állományok normális szerkezetével, mert a vírus az .EXE állományoknál sok esetben a fertőzés után nem működik, és csak az „Error in EXE file" rendszerüzenet érkezik.

A fertőzés során az Akuku meglepetésszerűen keresi áldozatait az egyes meghajtókon. Amikor a víruskóddal fertőzött program lefut, akkor az aktuális meghajtó aktuális könyvtárában három programot megfertőz. Ha már nem talál fertőzetlen programot, akkor kezd el keresgélni egyéb helyeken, például a C: meghajtó gyökérkönyvtárában. A fertőzés hossza 891–907 bájt között válto-

zik, a kód a fertőzött program végére épül be. Az eredeti állománydátumot és időpontot nem bántja, azok a fertőzés után is megmaradnak eredetinek.

Minden fertőzött programban megtalálhatjuk a következő épületes lengyel nyelvű üzenetet:

```
A kuku, Nastepny komornik !!!
```

Ez a szöveg sohasem jelenik meg, csak az .EXE állományokra vonatkozó üzenet.

A vírus neve: USSR 948

Egyéb elnevezése: Még nem ismeretes.
Hossza: 948 bájt.
Kódtípusa: Parazita, rezidens. .COM és .EXE fertőző.
Azonosítása: Scan V74+.
Eltávolítása: Törölni a fertőzött állományokat.
Leírása: Ez is az 1990. decemberi nagy víruskirajzással érkezett. Rezidens résszel rendelkezik, a .COM és .EXE állományokat egyaránt megtámadja, beleértve a COMMAND.COM-ot is.

A vírus a többihez hasonlóan a konvencionális memória tetejére ül be, amit le is foglal. Nem veszi el az INT 12-t, viszont céljait tökéletesen eléri az 1C és a 21-es interrupt átvariálásával.

Amikor a memóriában van, akkor a megnyitott .COM és .EXE állományokat megfertőzi, kivéve a COMMAND.COM-ot. A parancsprocesszor esetében viszont korszakalkotó, bár már nagyon várt trükkel élt. Itt a stack részére fenntartott üres helyre, az állomány belsejébe építi be magát, annak végén, a stack helyének felülírásával. Ennek következtésben hossznövekedés nincs, s a legtöbb esetben a rendszer is látszólag zavartalanul üzemel. A normál fertőzés folyamán a hossznövekedés, minden ilyen vírushoz illően, a paragrafushatárok miatt 950–963 bájt lesz, a vírus a kód végére épül be.

A vírus neve: Bebe

Egyéb elnevezése: Még nem ismeretes.
Hossza: 1004 bájt.
Kódtípusa: .COM fertőző.
Azonosítása: F-Prot 1.14+.
Eltávolítása: F-Prot 1.14+.
Leírása: Az orosz vírusiskolának meglehetősen drasztikus kifejezéseket tartalmazó frissen felbukkant darabja, amelynek létéről Skulason vírusriasztásából értesültünk. A vírus a következő belső üzenetet tartalmazza, amely kimutatására is alkalmas:

```
VIRUS! Skagi "bebe" Fig Tebe !
```

(Lefordíthatatlan, meglehetősen drasztikus orosz szójáték)

Ez az 1004 bájt hosszú vírus csak a .COM állományokat fertőzi meg, belelértve a COMMAND.COM-ot is.

A vírus neve: Lozinsky

Egyéb elnevezése: Még nem ismeretes.

Hossza: 1023 bájt.

Kódtípusa: Parazita, .COM fertőző, beleértve a COMMAND.COM-ot is. Rezidens része van.

Azonosítása: Scan V80+.

Eltávolítása: Törölni a fertőzött programokat.

Leírása: Az 1990. decemberi orosz vírusinvázió tagja. Magyarországon még nem bukkant fel. Rezidens résszel rendelkező általános .COM fertőző vírus, amelyik a COMMAND.COM-ot is megtámadja.

A normál DOS memória „RAMTOP"-ján válik rezidenssé, a DOS által használható területet 2048 K-val csökkenti. Az INT 13 és INT 21 vezérlését és az INT 12 visszatérésének figyelését magára veszi. Ilyenkor fertőzi meg a COMMAND.COM-ot, ha esetleg még nem lenne vírusos. Megnyitáskor és végrehajtáskor fertőz! A fertőzés során a program végére épül be. A könyvtári bejegyzés dátumát kicseréli a fertőzés aktuális időpontjára.

A vírus neve: USSR 1049

Egyéb elnevezése: Még nem ismeretes.

Hossza: 1049 bájt.

Kódtípusa: Parazita, rezidens. .COM és .EXE fertőző.

Azonosítása: Scan V74+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: Az 1990. decemberi vírusraj tagja. Itt is terjedési tesztelésről van szó. Nem fertőzi meg a COMMAND.COM-ot, és mint a hasonló többi orosz eredetű vírus, ez is a rendszermemória tetejére épül be.

A memória tetején 1056 bájtnyi területet lefoglal magának. Békén hagyja a 12-es interruptot, de a 21-es megszakítóval állandóan manipulálva mégis eléri célját. A végrehajtás során megfertőzi a .COM és .EXE állományokat, és a kód a fertőzött program végére épül be. A hossznövekedés itt 1051-től 1064 bájtig terjedhet.

A fertőzés a tapasztalatok szerint az .EXE állományok futtatásánál történik. Ilyenkor a rendszer sok esetben lemerevedik, de csak miután a fertőzés már megtörtént. Más esetekben a lefagyás akkor következik be, ha a megfertőzendő programba a víruskód korábban egyszer már beépült. Elképzelhető, hogy a telítődés, azaz a fertőzésre alkalmas programok hiánya okozza az aktivizálódást, ami egyszerűen csak a rendszerek kimerevítését jelenti. Más hatásait eddig még nem ismerjük.

A vírus neve: Voronezh

Egyéb elnevezése: Voronyezs.

Hossza: 1600 bájt.

Kódtípusa: .COM és .EXE fertőző.

Azonosítása: Az állományok szemrevételezése.

Eltávolítása: Törölni a fertőzött programokat.

Leírása: A vírus az 1990. decemberi víruskirajzás tagja. Általános .COM és .EXE fertőző, de nem támadja meg a COMMAND.COM-ot. Elnevezését a benne lévő, angol helyesírású orosz helységnévről kapta.

A programkód lefutása után válik memóriarezidenssé. Mint az orosz vírusok túlnyomó része, ez is a 640 K-s konvencionális DOS memóriának a tetején épül be. Ott a CHKDSK tanúsága szerint 3744 bájtnyi helyet lefoglal, ennyivel csökkentve a DOS számára rendelkezésre álló memóriát. Nem birizgálja a 12-es interruptot de a 21-es vektort magára irányítja. Érdekessége, hogy 24 bájtnyi helyet még a videomemóriában, a grafikus kártyán is lefoglal.

A memóriarezidens vírus a végrehajtás után megfertőzi a .COM és .EXE programokat. A vírus által okozott hossznövekedés 1600 bájt, amit a programkód végére épít be. A programvírus belsejében a következő „névadó" szöveget találjuk:

`Voronezh,1990 2.01`

Fridrik Skulason említi, hogy ez a vírus sok esetben felülírással károsítja az állományokat. A .COM állományok elejét felülírja, és magát tikosítva, azaz átkódolva helyezi el a fertőzött állomány végén. Az .EXE programoknál az eredeti CS:PC értékét nem változtatja meg, de az első 5 bájtot felülírja egy asszembler FAR CALL hívás kódjával, ami a vírusra mutat. Így sok esetben a víruskód lefutása után a végrehajtás nem tud magára a főprogramra visszaugrani, és a gép megdermed.

Mutációi:

Voronezh-B: Hasonló, mint az alapverzió, de tökéletesítették terjedési algoritmusát. Az eredeti vírus csak akkor fertőz, ha a fertőzés céljára szolgáló programkód lefut. Ez a verzió viszont minden állománymegnyitásra fertőz. Ezáltal nagyobb a fertőzés hatásfoka. Például elegendő egy CHKDS-t vagy egy SCAN programot lefuttatni, és merevlemezünkön garantáltan minden (fertőzhető) állomány fertőzött lesz. Néhány mutáció esetében pedig csak a belső rendszerüzenetet írták át.

Voronezh Related: 2200 bájt hosszú, tehát hatszáz bájttal hosszabb, mint az alaptípus. Viszont csak .COM állományokat képes megfertőzni. Valószínűleg ez volt a legelső verzió.

A vírus neve: USSR 1689

Egyéb elnevezése: SVC V4.00, Russian Stealth.

Hossza: 1689 bájt.

Kódtípusa: Parazita, rezidens. .COM és .EXE fertőző.

Azonosítása: Scan V74+, F-Prot 1.14+.

Eltávolítása: F-Prot 1.14+ vagy törölni a fertőzött állományokat.

Leírása: Az 1990. decemberi nagy orosz víruskirajzás tagja. Magyarországon a jelek szerint még nem bukkant fel. A .COM és az .EXE állományokat támadja meg, időnként rendszerkiakadásokat okozva. Meglehetősen furcsán válik rezidenssé, mert ugyanazt a memóriaterületet használja, ahová a parancsértelmező, azaz a COMMAND.COM költözik. Ennek a területnek „társbérlet-

ben" történő használata meglehetősen nehézkes, és itt általában nem számítunk a vírus megjelenésére. Első leírója Fridrik Skulason izlandi antivírus-program-író szakember.

Rezidenssé válása után akkor fertőz, amikor a fertőzetlen programkód lefut, de egy korábbi fertőzött programmal a vírus már bejutott a memóriába. A rendszert a fertőzött program futtatása során tudja kiakasztani. Ez azonban nem minden esetben következik be, aminek oka valószínűleg olyan programozási hiba, hogy a vírus másodszor is rezidens szeretne lenni ugyanazon a területen, és így belepancsol a memóriában a COMMAND.COM állandó részébe.

A vírusban a következő karakteres rendszerüzenet található:

`(c) 1990 by SVC,Vers. 4.0`

A fertőzés során az állomány 1689 bájttal növekszik, viszont a vírus beépül, ha a fertőzendő program hossza ezt meghaladja. A hossznövekedés egészen addig rejtve marad a DOS DIR parancsa előtt, amíg a vírus a memóriában aktív. Ilyenkor a DOS a fertőzés előtti hosszat mutatja. A vírus a programkód végére épül be. Más károkozásról, mint a rendszer kiakadása, nincs tudomásunk.

A vírus neve: USSR 2144

Egyéb elnevezése: Még nem ismeretes.

Hossza: 2144 bájt.

Kódtípusa: Parazita, rezidens. .COM és .EXE fertőző.

Azonosítása: Scan V74+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: Az USSR 2144 vírus is az 1990 végi víruskirajzás során jutott el külföldre. Jelentősen csökkenti a rendszer rendelkezésére álló szabad memóriát, ugyanakkor a .COM és az .EXE állományokat is megfertőzi, a COMMAND.COM-ot is beleértve. Rezidens része van.

A vírus a 640 K-nyi DOS memória felső végére épül be. A CHKDSK programmal megnézve 4608 bájt memóriacsökkenést tapasztalhatunk. A vírus nem piszkálja az INT 12-t, de a víruskód lefutása során számos más interruptot meghív.

A 2 K-nál hosszabb .COM és .EXE állományokba épül be, ha egy fertőzött program lefuttatása után már rezidenssé vált. A .COM programoknál 2144 bájtnyi hossznövekedést tapasztalhatunk. Az .EXE programoknál a növekedés a 2144 és a 2159 bájt között ingadozhat a paragrafushatárok miatt. Nem változtatja meg az egyes állományok dátumát és időjelzését, de a vírus által okozott hossznövekedést sem rejti el a DOS elől. A víruskód a programok végére épül be.

A vírus neve: Dir

Egyéb elnevezése: Még nem ismeretes.

Hossza: 691 bájt.

Kódtípusa: .COM fertőző, rezidens résszel rendelkezik, parazita, ráül a DIR parancsra.

Azonosítása: Scan V74+.

Eltávolítása: Scan /D.

Leírása: 1991 januárjában került külföldre ez a „Ki ír minél rövidebb vírust?" vetélkedő jegyében született orosz programvírus. Memóriarezidens, megfertőzi a .COM állományokat, bebeértve a COMMAND.COM-ot is.

Amikor a vírussal fertőzött program lefut, a vírus rezidenssé válik, és az alapmemória alsó részén 1008 bájt helyet foglal le magának. Magára veszi az INT 21 vezérlését. Ha a COMMAND.COM még nem fertőzött, sürgősen pótolja mulasztását.

Akkor fertőz, ha a DIR parancsot kiadjuk. A fertőzés feltételeinek megfelelő minden olyan állományba belelül, amelyiket a DIR érinti. Ugyanakkor nem fertőz sem a program végrehajtásakor, sem pedig a .COM állomány más céllal történő megnyitásakor. Ha a DIR parancs kiadásakor nem fertőzött .COM állománnyal találkozik, akkor a gép egy pillanatra lemerevedik, megtörténik a fertőzés, majd a lista tovább fut a monitoron.

Az egyes állományok hosszát 691 bájttal növeli meg,. De amíg a program a memóriában van, addig a könyvtárlistázás során ezt a növekedést elmaszkolja, miként a hagyományos ellenőrző programok előtt is. A vírus a fertőzés során a megtámadott programok végére ül be és a dátumot nem változtatja meg.

Ha a vírus a memóriában ül, akkor a CHKDSK program igen sok keresztkapcsolt szektort jelez. Ilyenkor az /F paraméterrel futtatva tönkre is tesszük a merevlemezt. Ha viszont a vírus nincs jelen a memóriában, akkor a CHKDSK futtatásakor sincsenek ilyen hibás szektorok. Aktivizálódási mechanizmusáról, határidőiről többet nem tudunk.

A vírus neve: Hymn

Egyéb elnevezése: Még nem ismeretes.

Hossza: 1865 bájt.

Kódtípusa: Rezidens résszel rendelkező, parazita .COM és .EXE fertőző.

Azonosítása: Scan V76+

Eltávolítása: Clean 76+

Leírása: A Hymn vírust is 1990 november végén eresztették el. Nagyon gyorsan elterjedt, Magyarországon is szinte mindennapos. A vírus .COM és .EXE fertőző, de a COMMAND.COM-ot is megtámadja. Csökkenti a DOS által igénybe vehető memóriaterületet és időnként zenél.

Lefutása után a fertőzött kód a memória tetejére épül be, de a normál 640 KB-os DOS területen belül. Helyfoglalását a CHKDSK 3712 bájtos memóriacsökkenéssel jelzi. (A várakozással ellentében nem nyúl az INT 12 megszakítóhoz.) Ha a COMMAND.COM még nem fertőzött, ekkor azzá válik. Minden fertőzött program végrehajtása mintegy 2 K többletmemóriát igényel. A memóriába „cipőkanállal" bepréselt programok nem hajlandók elindulni, és az elégtelen memóriáról hibaüzenetet adnak. A vírus a fertőzések során az állomány végére mászik be, a .COM fájlok méretét 1685 bájttal, az .EXE állományokét pedig a paragrafushatártól függően 1698-1883 bájt hosszal növeli meg. A program a következő két karakteres azonosítót tartalmazza:

```
ibm@SNS
```

A vírusnak eddig három mutánsát tudtuk összegyűjteni. Közülük az egyik rövidebb, a másik kettő valamivel hosszabb, mert önkódoló, illetve antidebug funkciókat tartalmaznak.

A vírus elindítása után semmilyen feltűnő jelenséget nem produkál. A Magnitogorsk 2048 vírussal együtt elindítva az operációs rendszer lefagyott, majd a reset gomb megnyomása után a számítógép belső modemének hangszórója elkezdett zenélni, az operációs rendszer pedig bejött. A zene és a DOS betöltése egymástól független volt, mivel a számítógép hangszórója a rendszerindításnál sípolt. Ezt követően zenei aláfestéssel lehetett használni a számítógépet. Az egész úgy tűnt, hogy a vírus kibírta a rendszerindítást és a modemben bújt meg.

A vírus neve: MGTU

Egyéb elnevezése: Még nem ismeretes.
Hossza: 273 bájt.
Kódtípusa: .COM fertőző, beleértve a COMMAND.COM-ot is. Nem rezidens.
Azonosítása: Scan V80+.
Eltávolítása: A fertőzött programok törlése.
Leírása: Az MGTU vírus a Kemerovo édestestvére, valószínűleg annak korábbi verziója. Egyszerre indultak terjedésnek is, 1990 végén. Miként a Kemerovo, közvetlenül fertőz, nincsen rezidens része.

Teljes egészében illik rá az előző vírus leírása, mind a fertőzés feltételeire, mind annak módjára vonatkozóan. A vírus a program végére épül be.

Feltűnő az igen erős lemezhozzáférés, amikor a vírus ellenőrzi, hogy hogy hová épülhet be. Ha már csak fertőzött programot talál, akkor a következő üzenetet jeleníti meg:

```
????????COM Path not found.
```

Aktivitásának egyéb paraméterei még nem ismertek, Magyarországon előfordulását szerencsére még nem jelezték.

A vírus neve: Crash

Egyéb elnevezése: 1075
Hossza: 1075 bájt.
Kódtípusa: Nem ismeretes.
Azonosítása: Scan V76+.
Eltávolítása: A fertőzött állományokat csak törölni lehet.
Leírása: Egészen furcsa program. Kérdés, hogy vírus-e vagy trójai. Mindenesetre a Szovjetunióból származó BBS programok egy részénél fordul elő, hogy beléjük van ültetve egy kódészlet, ami a program elindításakor rendszerösszeomlást okoz.

Szaporodásáról még nincs hír, mert a vele fertőzött program egyszerűen nem fut. Néhány AT gépen a program elindítható, de megleheteősen kaotikus körülmények között képes önmagát reprodukálni. Valószínűsíthető, hogy közbenső fejlesztési fázissal vagy valamilyen programvírus „petéjével" állunk szemben.

A kód mindenesetre a batch-vírusok, illetve az ANSI-bomba típusú vírusok

felé mutat. A batch-vírusoknál bináris kódot indítanak el némi furfanggal egy .BAT állományból. Például a bináris kódot ráirányítva meghívják a Debug programot, ami a DOS könyvtárban lévén amúgy is az elérési útvonalon van. A másik esetben a bináris állományt ANSI escape vezérlőszekvenciával indítják el. Ilyenkor egy szövegállomány, ha TYPE paranccsal íratják ki, „felrobban", és elindul a vírus. E fejlesztések a hadi célú számítógépes vírusok irányába mutatnak. Néhány példaprogram már van a birtokunkban, de szerencsére ez a technológia Magyarországon még nem terjedt el.

A vírus neve: Sverdlov

Egyéb elnevezése: Szverdlov.

Hossza: 1962 bájt.

Kódtípusa: Parazita, rezidens résszel rendelkező, .COM és .EXE fertőző.

Azonosítása: Scan V80+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: A Sverdlov vírussal is az 1990. decemberi víruskirajzás során ismerkedett meg a világ. Memóriarezidens, megfertőzi a .COM és az .EXE állományokat, belelértve a COMMAND.COM-ot is. Önmagát titkosítja.

A víruskód lefutása után a normál DOS terület felső részén 4080 bájtnyi területet lefoglal magának. Az INT 12 visszatérését úgy manipulálja, hogy nem észlelünk eltérést az eredeti állapothoz képest. Az installálás során először a COMMAND.COM-ot fertőzi meg, utána egy ideig más programokat megkímél.

A fertőzött állományok futásához 2 K-val több hely kell mint különben. A fertőzés az állományok megnyitásakor történik. A bekövetkező hossznövekedés a .COM állományok esetében 1962 bájt, míg az .EXE programok esetében 1962 és1977 között ingadozik a paragrafushatár függvényében. A vírus a programok végére másolódik be. Feltételezik, hogy a Voronyezs vírus rokonságába tartozik és esetleg szerzője is azonos.

A vírus neve: Victor.

Egyéb elnevezése: Rettenetes Iván, Victor V.1.0.

Hossza: 2442 bájt.

Kódtípusa: Parazita, rezidens része van, a .COM és az .EXE állományokat fertőzi meg.

Azonosítása: CHKSeq v.1.0, Prgdoki 3.02., Scan V63+, Pro-Scan 1.4+, VirexPC, F-Prot 1.12+.

Eltávolítása: CHKVir v.4.01, Prgdoki 3.02, Sysdoki, Pro-Scan 1.4+, F-Prot 1.12+ vagy a fertőzött állományok törlése.

Leírása: A vírus Magyarországon 1990 januárjában bukkant fel először, szinte egyidejűleg két helyen, a Kandó Kálmán Villamosműszaki Főiskolán, valamint tőle több mint száz kilométerre, egy Novell alatt futó rendszerben. Azóta Nyugat-Európában és az USA-ban is elterjedt.

Önmagát a vírusmag is Victor-nak, azaz Győzőnek nevezi. Származásának kiderítése eddig nem járt sikerrel, valószínűsíthető mind a lengyel, mind a bolgár, mind pedig az orosz eredet.

A vírusnak van rezidens része, de nem minden programindításkor fertőz, ezért elég nehéz felfedezni. Lassan terjedő, de hatásában annál veszedelmesebb! Teljes elszaporodása esetén a főkönyvtár és az aktuális könyvtár állományait támadva kíméletlenül tönkretesz minden programot.

A vírus a normál DOS memória tetején installálja magát. Ekkor 3072 bájt szabad területet foglal le magának. Miután memóriarezidenssé válik, megkeresi és megfertőzi a COMMAND.COM-ot. Igen gyors fájlfertőző vírus. A fertőzés után 1-10 programvégrehajtás közül egy esetben és véletlenszerűen fertőz. A fertőzés által okozott hossznövekedés 2443-2458 bájt között van, a paragrafushatártól függően. A hossznövekvést nem rejti el a DIR parancs elől.

A fertőzött állomány végrehajtásakor rendszerleállást, illetve adatkárosodást okoz. Ha overlay állományba mászott be, akkor „File linkage error" hibaüzenettel akad ki a rendszer.

Felkészítették a Novell hálózattal való találkozásra is, s ott a rendszer teljes összeomlását idézi elő. A Novell védelmi rendszere sem akadály számára. A vírusban egy kicsit bőbeszédű rendszerüzenetet találunk, de azt soha nem írja ki a képernyőre:

```
VICTOR V:1.0
The incredible high performance VIRUS.
Enchanced versions available soon
This program was imported from USSR.
Thanks to Ivan.
```

(A hihetetlenül nagy teljesítményű vírus. Hamarosan fejlettebb verziók is megjelennek. A Szovjetunióból importált program. Köszönet Ivánnak.)

Magyarországon 1990. június közepén felbukkant egy másik változata is. Ennek kódja teljesen azonos az eredetiével, csak ismeretlen kezek a rendszerüzenetet cserélték ki:

```
Victor V1.0 The Incredible High Performance Virus
This is computermind killer.
For every user:WARNING!!!
Virus in BOX!
```

(A hihetetlenül nagy teljesítményű vírus. A komputeragyú gyilkos. Figyelmeztetés minden felhasználónak! Vírus van a dobozban!)

Hadibacik

4096, 4096-B, 4096-C, Fish, Whale, Guppy, Stupid, Saddam, Iraqui Warrior, ZeroHunt, 834/Arab, 834-B/Arab, Grither, Holocaust.

Az előző kötet külön fejezete ismertette a számítástechnikában immár nyíltan emlegetett vírus-hadviselés jelenlegi helyzetét. Több olyan programvírus van, amelyek alkalmazási körülményeiket vagy programozástechnikájukat figyelembe véve nem lehetnek magányos zsenik elmeszüleményei. A csoportosítás ugyanakkor kicsit önkényes, mert első felhasználását tekintve a közismert Péntek 13 is hadibaci, hiszen az izraeli számítógépes hálózatok ellen vetették be a terroristák. A vírust — és kiterjedt rokonságát — eltérő jellege alapján mégis másik fejezetben ismertetjük.

A vírus neve: 4096

Hossza: 4096 bájt.

Egyéb elnevezése: 100 Year, 4K, Century, Frodo, FroDo, IDF, Stealth.

Kódtípusa: Parazita, rezidens része van, a .COM és az .EXE állományokat fertőzi meg.

Azonosítása: Scan V53+, CHKSeq v.1.0, F-Prot, Sysdoki, IBM Scan, Pro-Scan, VirexPC 1.1+, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: Scan /D, F-Prot, Sysdoki, Clean V62+, Pro-Scan 1.4+, F-Prot, VirHunt 2.0+, TNT, NAV 1.0.

Leírása: A 4096-os vírust először 1990 januárjában észlelték. A tipikus programférgek családjába tartozik, lassú munkával okoz helyreállíthatatlan károkat az adatállományokban. Izraeli eredetű. A tudományos fantasztikus irodalomból vett hasonlattal ez a vírus a „második fázisban" él. Ez azt jelenti, hogy a hagyományos eszközökkel láthatatlan a számítástechnikai rendszer felhasználói számára. Az eddigi információk szerint a vírus a .COM és az .EXE állományokat fertőzi meg, amelyek hossza ezáltal 4096 bájttal nő meg. A „százéves" elnevezést onnan kapta, hogy az évszámnak a DOS DIR által nem mutatott első két számjegyéhez 100-at hozzáad.

A vírus rezidensen beül a memóriába. A „lopakodó" technikát alkalmazza, azaz ha aktívan jelen van a memóriában, akkor a DOS operációs rendszeren keresztül (például a DIR paranccsal lekérdezve) az eredeti hosszat mutatja, ezért az állományok hosszának megnövekedését csak külön eljárással lehet kimutatni. Ilyenkor a CRC ellenőrzés is használhatalan! Az állományok megnyi-

tásakor már fertőz, beleértve ebbe a másolást is a DOS COPY, illetve XCOPY parancsával.

Ez a vírus egyaránt pusztítja az adatállományokat és a végrehajtható programállományokat, igen sok keresztkapcsolt szektorcsoportot (clustert) hozva létre a lemezen, amelyek azután sorra okozzák a hardverproblémákat. Maga a vírus pedig közben eltűnik a káoszban. Ezt a hatást még azzal is fokozza, hogy manipulálja a FAT-tábla bejegyzéseit, cserélgeti a szabad szektorok számának adatait. A DOS pedig csendesen megzavarodik — a tulajdonossal egyetemben.

Az egész cirkusz másik jelenete szinte hihetetlenül hangzik: ha másolatot készítünk egy fertőzött állományról — miközben a vírus ott ül a memóriában —, a fertőzött állomány másolata fertőzésmentes lesz! Ez azután felkínálja a mentesítés abszurdnak tűnő alábbi eljárását is. Amikor a vírus a memóriában van, minden futtatható állományról készítünk floppyra egy másolatot a COPY parancs segítségével, úgy hogy a másolat nevében ne szerepeljen a programfájl szokásos .EXE, .COM, .SYS, .OVL stb. kiterjesztése. Amikor ezzel elkészültünk, kapcsoljuk ki a gépet a főkapcsolóval, majd utána újra bekapcsolva egy tiszta, írásvédett floppyról indítsuk a rendszert, így a vírus nem kerül be a memóriába. A rendszer bejelentkezése után a DOS DEL parancsával töröljük ki az összes futtatható állományt, majd az átkeresztelten lemásolt állományokat visszanevezhetjük eredeti nevükre és kiterjesztésükre.

Amikor kitakarítottuk a fertőzött állományokat, utána még elég sokat kell kínlódnunk a nagyon sok keresztkapcsolt cluster miatt, mert ha azokat nem szüntetjük meg, az ott lévő állományok nagyon gyorsan károsodni fognak. A vírus néhány adatállományban is pusztít. A 4096 vírus a lopakodó („stealth") programozási technikával készült vírusok családjának legelső tagja. Sajnos a benne alkalmazott eljárások terjedésével az új vírusok felfedezése és a fertőzött állományok megtisztítása egyre nehezebb lesz.

A vírus minden évben szeptember 22-én, valamint utána az év végéig terjedő napokon — de csakis azokon — lemereviti az operációs rendszert. Ezen időszakban egy érthetetlen „programhiba" vagy rendszerlefagyás esetén erre a vírusra kell gyanakodnunk. (A fantasztikus irodalom kedvelői számára talán ismerős, hogy szeptember 22-e Tolkien-nek A gyűrűk ura című trilógiájában Zsáklaki Bilbó születésnapja.)

Van a vírusnak egy érdekes trükkje: egy komplett bootszektor minden információját tartalmazza, holott ismereteink szerint soha sem ír a bootrekordba. Ha valakinek az az ötlete támad, hogy ezt az egyedi bootrekordot közvetlenül a helyére másolja, akkor érdekes meglepetésben lesz része. Amikor ugyanis erről a lemezről indítja a rendszert, akkor megjelenik a monitoron az alábbi szöveg:

FRODO LIVES

Ha viszont várunk a szeptember 22-i dátumig, akkor a vírus maga másolja fel a bootrekordot a megfelelő helyre és létrejön a fenti jelenség. Érdekessége, hogy bizonyos esetekben a gép órája látszólag visszafelé jár.

Ismert vírusváltozatok:

4096-B: A vírus viselkedése teljesen azonos az eredeti verzióéval. Az eltérés

annyi, hogy a kódolási algoritmust a nehezebb felderítés érdekében megváltoztatták. Ez a vírusverzió Mgayrországon Pécs környékén jelent meg. Egyik ottani tudományos intézet Németországból kapott tervezőrendszerrel együtt szerezte be.

4096-C: 1991 januárjában bukkant fel. Valószínűleg az eredeti kód birtokában vagy az eredeti írónál született újjá. Kiküszöbölte a korábbi változatok azon hibáját, hogy a CHKDSK DOS parancs leleplezte a keresztkapcsolt szektorokat. Egy hiba azért még maradt benne: a DOS DIR parancsa kevesebb szabad helyet mutat, mint a CHKDSK.

A vírus neve: Fish

Egyéb elnevezése: Fish 6, European Fish.

Hossza: 3584 bájt.

Kódtípusa: Parazita, rezidens része van. Titkosítja, azaz elkódolja magát. A .COM és az .EXE állományokat fertőzi meg.

Azonosítása: ViruScan V63+, Pro-Scan 1.4+, VirexPC, F-Prot 1.12+, VirHunt 2.0+.

Eltávolítása: Scan /D, CleanUp V66+, Pro-Scan 1.4+, VirHunt 2.0+, vagy a fertőzött állományok törlése.

Leírása: A virus a .COM és az .EXE állományokba épül be. A monitor képének remegését okozza — legalábbis a grafikus kártyák többségénél. Alaposan lelassítja a videoműveleteket is.

A vírusok programozástechnikájában úttörő jelentőségű. Talán ez volt az első olyan vírus, amelyet igen nagy valószínűséggel hadviselési célra fejlesztettek ki. Később a 4096 vírusprogram bázisán jött létre két igen veszélyes, önmagát folyamatosan változtató, mutáló vírus: a Whale (azaz Bálna) valamint az 1992 elején még csak létében jelzett izraeli eredetű „Israeli Defence Force" nevű szörnyszülött.

Amikor a Fish vírust 1990 májusában feltételezett szülőhelyén, az NSZK-ban azonosították, már alaposan elterjedt Európában. Aktivizálódásának eddig ismert feltétele: a rendszerórának 1991-et kell mutatnia. Kódja szövevényes, a megfejtés ellen tudatosan védett. Teljesen visszafejteni nem is sikerült, így romboló hatásának csak néhány megnyilvánulását ismerjük.

A vírus általános .COM és .EXE fertőző, beleértve a COMMAND.COM-ot is. Rezidens része van, a memóriában igen stabil. Ha meleg rendszerindítást (warm reboot), vagy Ctrl-Alt-Del újraindítást hajtatunk végre, akkor is a memóriában marad. A programvírus önmagát titkosítja. A fertőzés egyetlen, árulkodó jele, hogy a megtámadott programokban ott találhatjuk a vírusazonosító szöveget:

```
FISH FI
```

Még ez is tartogat azonban meglepetést: az azonosító szövegrészlet egy meg nem határozható idő eltelte után eltűnik a programból, a vírus azonban bennmarad.

Amikor egy Fish vírussal fertőzött program lefut, akkor a vírus igen gyorsan installálja magát a szabad memória alsó tartományában. Ha még semmi nem

foglalta le a 13h interruptot, sürgősen magára irányítja ezt a megszakítást. Miután megtörtént a megszakításvektor átvétele, elfoglal a memóriából 8192 bájtnyi területet, azon a részen, ahol ő maga is ül. Viszont az a helyzet is előfordul, hogy egy másik vírus vagy pedig egy alkalmazói program már használja ezt a megszakítástvektort. Ő ilyenkor is beépül, de a tárban maradó része csak 4096 bájtnyi helyet foglal el a memóriából. A vírus feltehetően csak azokat a részeit csomagolja ki tömörített kódjából, amelyekre ott és akkor szüksége van. Ha pedig más már használja a 13h megszakítást, akkor ő nem épül rá.

Ha a 13h interrupt nincs láncolva, és a vírus rezidensen ül a memóriában, akkor véletlenszerű időközönként meleg rendszerindítást csinál. Ez utóbbira azért van szüksége, hogy bentmaradhasson a memóriában, és megfertőzhesse a COMMAND.COM-ot is. Nincs viszont rendszerindítás akkor, ha már más üldögél a 13h megszakításban. Már ennek a hatása is elég kellemetlen: a felhasználó véletlenszerűen fellépő alaplaphibára gyanakszik. DBase alapú programrendszert használva a lezáratlanul maradt állományok adatai eltűnnek.

Ha a vírus a memóriában van, akkor — ugyanúgy mint a V2000 és az Eddie — az állomány megnyitásakor beépül a többi .EXE és .COM programba. Elég a Viruscan program lefuttatása, és minden programunk fertőzött lesz. A fertőzés során a program 3584 bájttal nő meg, de ezt a lopakodó (stealth) programozástechnika miatt nem lehet észrevenni, ha a vírus a memóriában van. Így a DOS DIR parancsa is az eredeti állapotot mutatja. A CRC ellenőrzés vagy hosszellenőrzés is „lepereg" róla.

Árulkodó jel, hogy ha a fertőzött rendszerben kiadjuk a CHKDSK parancsot, akkor minden fertőzött állományra „File allocation error" hibaüzenetet kapunk. Persze ilyenkor — mivel a vírus állománymegnyitásra fertőz — garantáltan minden fertőzött lesz, ha valami esetleg még nem lett volna az. A CHKDSK /F parancs hatására pedig szinte az egész merevlemez egyetlen elveszett clusterhalmazzá válik.

A vírus alaposan lelassítja a videomemória írását és olvasását. Ez a monitor villogásában is megnyilvánuló egyik fertőzési jel lehet. Hardverhibát szimulál. A vírus írásvédetté tett merevlemezre is tud írni, de írásvédett floppyra már nem!

A „Halat" a 4096 vírus alapján, valószínűleg annak teljes forráskódját ismerve írhatták meg. Elődjénél is mesteribb módon kódolja azonban át magát a rendszer memóriájában. Ha akkor nézi meg valaki a rendszer memóriáját, amikor a vírus ott ücsörög, akkor jó pár hal nevét láthatja karakteresen az egyes memóriacímeken.

A vírus neve: Whale

Egyéb elnevezése: European Whale, Mother Fish, Z The Whale.

Hossza: 9216 bájt.

Kódtípusa: Parazita, rezidens része van. Titkosítja, azaz elkódolja magát. A .COM és az .EXE állományokat fertőzi meg.

Azonosítása: ViruScan V67+, NAV 1.0 (de csak akkor ha a melléadott WHALE.DEF 4654 bájtnyi állományt is hozzátöltjük a definíciós alapállományhoz!).

Eltávolítása: Scan /D, Clean V67+, vagy a fertőzött állományok törlése.

Leírása: A vírus 9216 bájt hosszú, ennyivel növeli a fertőzött állományok méretét, de a hossznövekedést elrejti előlünk. Folyamatosan készít saját magából véletlenszerű mutációkat — eddig több mint 30 változata ismert —, s ezek viszonylag rövid idő alatt keletkeznek a számítógépben. A mutánsok továbbfertőzéskor eltérő méretűek is lehetnek. A vírus 1990 augusztus végén bukkant fel Hamburgban, majd négy hónappal később jelent meg a Fish 6 vírus, valószínűleg ugyanazon fejlesztőktől.

Amikor a vírus installálódik, a DOS memória tetején, közvetlenül a 640 K-s határ alatt helyezkedik el. A rendelkezésre álló memóriát általában 9984 bájttal csökkenti. Egy szerző XT-szerű gépén úgy találta, hogy a vírus munkáját a 9D90h memóriacímen kezdi. A fertőzés jele, hogy a memóriában megtalálható a következő karaktersorozat:

```
Z THE WHALE
```

Amikor a Bálna a memóriában dolozik, a memóriaműveletek, különösen a videoműveletek jelentősen lelassulnak. Villog a monitor, lassan frissíti fel a képet. Jó pár program használata esetén a rendszer egyszerűen lefagy.

Ha a DOS CHKDSK programját futtatjuk, akkor az nagyon sok „File allocation error" hibaüzenetet ad. Erre természetes reakcióként a felhasználó a CHKDSK /F parancsot adja ki, aminek hatására — a Whale jelenlétében — minden állomány tönkremegy.

Időnként a Whale vírus a rendszer újraindítását szimulálja, máskor megakadályozza, hogy a felhasznló az AUTOEXEC.BAT futását a Break gombbal leállítsa. Eddig nem tisztázott körülmények között többször létrehoz, majd eltüntet egy hidden állományt a C: meghajtó gyökérkönyvtárában, de nincs rá magyarázat, hogy miért teszi. Ennek az állománynak a neve FISH-#9.TBL, az alábbi tartalommal:

```
Fish Virus #9
A Whale is no Fish!
Mind her Mutant Fish
and the hidden Fish Eggs
for they are damaging.
The sixth Fish mutates
only if the Whale is in
her Cave.
```

(Kilences számú Hal vírus. A bálna nem hal! Figyelj mutáns halaira és a rejtett haltojásokra, mert azok pusztítóak. A hatodik Hal csak akkor szül új változatokat, ha a Bálna a barlangjában van.)

Miután a szerencsétlen polgár megtalálta ezt az állományt, azt hiszi, hogy a Fish vírus valamelyik mutánsa dolgozik a rendszerében, holott a valószínűsíthetően azonos szerzőkön kívül a Whale vírusnak nem sok köze van a Fish 6-hoz. Ha pedig a felhasználó rosszul határozza meg a fertőzés okát és jellegét, a vírusnak nagyobb az esélye a garázdálkodásra.

A Whale figyeli az eltérést a program dátuma és a programot tartalmazó alkönyvtár létrehozási dátuma között, ügyelve arra, hogy ezeket a fertőzés során ne állítsa el, amint azt sok más vírus teszi. Néhány esetben a fertőzéskor el-

maszkolja azt az alkönyvtári belépési pontot, ahol előbb az immár fertőzötté vált programot futtattuk. Így azt sok segédpgrogram a továbbiakban nem képes elérni, és „Invalid directory entry" vagy annak megfelelő más rendszerüzenettel állományunk látszólagosan elvész.

A Whale gyakran változtatja memóriarezidens viselkedését. Bizonyos időszakokban csak akkor fertőz, ha a programot végrehajtják, máskor ezt minden állománymegnyitásra megteszi. Van, amikor a vírust eltávolítja abból az állományból, amelyet a DOS COPY parancsával másolunk. A viselkedésmódok változásában még nem találtak szabályszerűséget. Érdekes a röptében való fertőzés (infect on the fly) és a hasonló eltűnés (disinfect on the fly) véletlenszerű változtatása is, ami szintén megnehezíti a felfedezést és az azonosítást.

Várható volt előbb-utóbb annak a félrevezető fogásnak az alkalmazása is, hogy a vírus egy másik ismert vírussal összetéveszthető legyen. A szimuláns, megtévesztési technikák az élővilágban és a hadiiparban mindennaposak. A Bálnával ez a módszer a víruskészítésbe is bevonult. Ezt jelzi teljesen véletlenszerűen megjelenő másik rendszerüzenete is, amit a monitorra ír ki:

```
The Whale in Search of the 8 Fish I Am in Hamburg
```

(A Bálna keresi a nyolc halat. Én Hamburgban vagyok)

Találkozni lehet egy feltehetően korábbi verzió programhibájával is, amikor a fenti üzenet eképpen módosul:

```
THE WHALE IN SEARCH OF THE 8 FISH
I AM '~knzyvo}' IN HAMBURG addr error D9EB,02
```

A szakirodalomból nyert információk alapján valódi, éspedig igen fejlett hadi-programvírussal állunk szemben. A kód igen nehezen megfejthető, az is lehet, hogy elektronikus programgenerátor terméke, amely a végletekig optimalizált.

Jim Bates, az ismert angol számítógép-virológus Virus Bulletin című kiadványában arról számolt be, hogy 1990 végén egy angol antivírus konferencia küldöttei névtelen táviratot kaptak. Ebben az ismeretlen feladó az alábbiakat közölte: „A Bálna nem egyszerű vírus, hanem olyan lény, amely képes megtanulni az őt üldözők összes technikáját. Folyamatosan növeli saját kódjának bonyolultságát, annak függvényében, hogy mindenkori környezete mennyira támadóan lép fel vele szemben." Az üzenet azzal a figyelmeztetéssel zárul, hogy a vírust még nem kezdték el széles körben terjeszteni.

A sci-fi ízű hír ellenére szakmai körökben nagy a vele kapcsolatos bizonytalanság. Ahhoz a Trojan AIDS Information — jelenleg már megoldott — rejtélyhez hasonlít, amelyről Új víruslélektan című kötetünkben már beszámoltunk. Mindenesetre ha valaki véletlenül hozzájut a Bálna vírushoz, legyen vele nagyon óvatos!

Eddig azonosított és hexa kódban számozott mutációi a Norton Antivírus programcsomagból kinyerhető információk alapján 27-nél tartanak (Whale 01 ... Whale 1B).

A Whale nagyon nem szereti, ha programkódját piszkálják és nyomkövetéssel rá akarnak jönni a program titkosítási mechanizmusára. A visszafejtés ellen úgy védekezik, hogy az első néhány lépés után leblokkolja a billenytűzetet, elegánsan lehetetlenné téve a debugger használatát.

A vírus neve: Guppy

Egyéb elnevezése: Még nem ismeretes.

Hossza: 152 bájt.

Kódtípusa: Rezidens, parazita, COM és .EXE fertőző

Azonosítása: Pro-Scan 2.01+.

Eltávolítása: Pro-Scan 2.01+, vagy minden fertőzött állomány törlése.

Leírása: A Guppy vírust 1990 október végén találta meg az USA Washington államában Paul Ferguson. A vírusnak valami köze lehet a Fish és a Whale vírusokhoz, mert neve előfordul azok halnevei között. Igen szapora, minden .COM állományt megfertőz, belelértve a COMMAND.COM-ot is.

A vírussal fertőzött kód lefutása közben a vírus rezidenssé válik a normál DOS memóriaterületen, és magára veszi az INT 21 ellenőrzését. Mindössze 720 bájttal csökkenti a DOS rendelkezésére álló szabad területet. A fertőzött .COM program hossza 152 bájttal nő meg, ebből 150 bájt a fájl végére kerül, az elejére pedig csak a 2-bájtos ugrókódot teszi, amely megmutatja, hogy hol kezdődik a vírus. A fertőzés során a könyvtári dátumot átállítja a fertőzéskor érvényes rendszeridőre.

Amikor a Guppy ott evickél a memóriában, az éppen futtatott COMMAND.COM megfertőződik. De itt valami belső programhiba lehet, mert ha újra rendszert hívunk, akkor a gép nem hajlandó beindulni és a következő rendszerüzenetet adja:

```
Bad or missing command interpreter
```

A Guppy kidolgozói is ellenszenvvel viseltettek a neopromitív DOS editor, az Edlin iránt, mert ha azt hívja be valaki, akkor rögtön kilép a DOS-ba a következő rendszerüzenettel:

```
Invalid drive or file name
```

Tekintve, hogy néhány orosz vírus hasonlóképpen viselkedik, fel kell tételezni, hogy valamelyikük ötlete nem eredeti, hanem csak koppintás. A fertőzött állományok azonosítója a következő hexa karaktersorozat:

```
3ECD211F5A5B58EA
```

Ismert változata a Guppy-B, ami hasonló mint az alap Guppy, de jó pár bájtja eltér, viszont nem írták át az azonosítót. Talán ez lenne az eredeti orosz változat?

A vírus neve: Do-Nothing

Egyéb elnevezése: Stupid, 640K.

Hossza: 583 vagy 608 bájt.

Kódtípusa: Parazita, rezidens része van, .COM-ot fertőz.

Azonosítása: Scan /X V67+, F-Prot, CHKSeq v.1.0., Pro-Scan, VirexPC, AVTK 3.5+.

Eltávolítása: Scan /D, F-Prot, vagy törölni a fertőzött állományt.

Leírása: Ennek a vírusnak első előfordulását Izraelből jelezte Yuval Tal, 1989 októberében. A vírus a számítógépes terrorizmus jegyében fogant. A .COM állományokat fertőzi meg, de mindig csak az aktuális könyvtár első bejegyzését, s a többit békén hagyja. A vírus a memóriában a 9800:100h címre

építi be magát, és az egész 640 kbájt memóriára kiterjeszti működését. Megszünteti az egyes programok által lefoglalt memóriaterület védelmét, így azokat egy másik program szabadon felülírhatja. Végül a rendszer összeomlik, működésképtelenné válik.

A vírus a Do-Nothing nevet azért kapta, mert a számítógépet megfosztja cselekvőképességétől. Nagyon nehezen vehető észre, mert más kárt nem okoz, és a felhasználó sokáig géphibára gyanakszik. Az egyszerűbb hadivírus-írók ezt a vírust tekintik nyersanyagnak saját átírásaikhoz. Forráskódja is közkézen forog.

A vírus neve: Saddam

Egyéb elnevezése: Még nem ismeretes.

Hossza: 919 bájt.

Kódtípusa: Rezidens, parazita, COM fertőző.

Azonosítása: Scan V74+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: A rádióamatőr világban létezik egy AX25 jelzésű csomagkapcsolt adatátviteli hálózat, amely a postai vonalaktól függetlenül köti össze sok ország számítógépes szakembereit. Ezen a félprofesszinális hálózaton keresztül elérhető szinte az egész világ. Újabban a vírusriasztások egy része is ezen a rendszeren keresztül történik. Magyar rádióamatőr kollégák segítségével jutottunk hozzá az izraeli Baruch Even által 1989. október 5-én izolált vírus, a Szaddam leírásához, illetve az ezzel kapcsolatos, és azóta többször megismételt felhíváshoz.

A vírust akkor fogták meg, amikor azt egy BBS-re telepítették, hogy járványt indítsanak el vele. A kód stílusából bizonyosra vehető, hogy írója a Stupid (Do-Nothing) néven ismert vírus teljes, kommentált forráskódjának ismeretében írta meg az ugyanabba a víruscsaládba tartozó programot. Terjesztésére a Scan program 68-as verzióját választotta. Ismertetőjele: ez az ál-Scan nem a szokásos .EXE, hanem .COM kiterjesztésű. Tömörített formája a SCANV68.ZIP. Az izraeliek felkértek minden BBS tulajdonost, hogy ezt a programot távolítsák el a BBS-ből.

A Saddam vírus fellépését először 1990 szeptemberében, Franciaországban jelezték, s csak utána következett be az izraeli fertőzés. A fejlesztés tehát valószínűleg Franciországban vagy az NSZK-ban történt.

A vírus memóriarezidens .COM fertőző, beleértve a COMMAND.COM-ot is. Nem hagyományos módon válik rezidensé, a memória alsó területét választja ki erre a célra. Innen ered több I/O hibája, illetve a nem elegendő memóriára utaló kiakadása. Először az INT 21 és az INT 22 megszakítókat láncolja magára, azután megfertőzi a COMMAND.COM-ot.

A fertőzés és állomány megnyitásakor történik. A megfertőzött .COM programok hossza 919 bájttal nő, s a vírus az állomány végéhez kapcsolódik. Nem állítja át a fájl eredeti időpont- és dátumjelzését.

A vírusfertőzés után a rendszernek számos baja lesz. Nem elegendő a memóriája, elfelejti a floppyt vagy a merevlemezt, időnként nem tud írni vagy olvasni

a lemezegységekről... Néha az iraki államelnökre, Szaddam Husszeinre vonatkozó, zagyva angolságú alábbi üzenet olvasható a monitoron:

```
HEY SADAM
LEAVE QUEIT BEFORE I COME
```

Ez a szöveg azonban az nem látható közvetlenül a vírusban, mert kódolva van. A vírustól a gép néhány esetben meghülyül és nem indítja el a .BAT állományokat, a fertőzött COMMAND.COM kiakad, a DOS DIR parancsa rapszódikusan működik.

A vírus neve: Iraqui Warrior

Egyéb elnevezése: Iraqui.
Hossza: 777 bájt.
Kódtípusa: Parazita, nem rezidens, .COM fertőző.
Azonosítása: Scan V74+
Eltávolítása: Törölni a fertőzött állományokat.
Leírása: Az iraki háború kirobbanásakor, 1991 január 17-én propaganda diverzáns akcióként megjelent az USA-ban az Iraqui Warrior vírus. Minden .COM állományt megfertőz, de nem memóriarezidens. A COMMAND.COM-ot is megtámadja. A vírust sietősen írták, a Vienna vírus forráskódjának bázisán.

Amikor a vírus megfertőzi a gépet, kikeresi az első négy .COM állományt az aktuális meghajtó aktuális könyvtárából, és ezek közül egyet megfertőz. A vírus az egyes állományokat 777 bájttal megnöveli. Ennek rejtett utalása is van: a Bibliában a végítélet apokaliptikus leírásánál szerepel a 777 (valamint a 666 és a 999) mint mágikus szám.

A vírusban a következő üzenet egyszer a vírus elején, egyszer pedig a megfertőzött állomány végén jelenik meg:

```
I come to you from The Ayatollah!
(c)1990, VirusMasters
An Iraqui Warrior is in your computer…
```

(Az Ajatollahtól jövök önhöz. (c)1990 VirusMaters. Az Iraki Harcos az ön számítógépében van.)

Az üzenetet a vírus a monitoron sohasem jeleníti meg. Ha ezzel a vírussal fertőzött COMMAND.COM-os floppyról indítunk rendszert, akkor a következő rendszerüzenettel akad ki a gép:

```
Memory allocation error, Cannot start COMMAND, exiting
```

A fertőzött program futtatása során a hangszóró sorozatosan sipákol, amikor a szóköz billentyűt lenyomjuk. Időnként a rendszert újraindítja, utána pedig „boot hiba" rendszerüzenetet kapunk. Ha a rendszer mégis újraindul, akkor a gép folyamatosan fütyül.

A vírus neve: ZeroHunt

Egyéb elnevezése: Minnow.
Hossza: 416 bájt.
Kódtípusa: Parazita, felülíró, .COM fertőző.
Azonosítása: Scan V72+, Pro-Scan 2.01+.

Eltávolítása: Pro-Scan 2.01+, vagy (ami gyakorlatilag ugyanaz) kitakarítani a fertőzött állományokat.

Leírása: Méretéhez képest meglehetősen sokat tud ez a vírus, amely a lopakodó programozástechnika lehetőségeit igen jól kiaknázza. 1990 decemberében lelt rá Washingtonban Paul Ferguson vírustalanító szakember. Kódjának visszfejtése éppen tömörsége miatt nem egyszerű.

A program a .COM állományokat, közte a COMMAND.COM-ot is megfertőzi, egyes részeit felülírja. Lefutása után a víruskód a memória meglehetősen szokatlan helyére, a parancskörnyezet területére épül be. Számos megszakítást ellop, természetesen az INT 21-est is.

Miután alig 200 bájtnyi helyet lefoglalva beül a memóriába, arra vár, hogy olyan programot indítsanak el, amely tartalmazza az állományban a verem (stack) helyét jelző karaktereket. Ha .EXE állománnyal találkozik, azt sürgősen .COM állománnyá konvertálja. Ha a .COM állományban van 00h karakter, akkor a Zerohunt a víruskóddal felülírja az első 416 bájtot, a 00h karaktertől kezdődően. Az első négy bájt azonban eltér, egészen a víruskód első végrehajtásáig, amikor azokat átírja.

Mint általában a lopakodó technikát alkalmazó vírusok, minden állományhozzáférésre (nyitásra, zárásra, futtatásra) fertőz. Amikor a memóriában van, az állományok hosszának és CRC-jének változása nem detektálható. Hasonló ötlet, hogy az állomány belsejébe, a verem területre írja be magát. Így hagyományos körülmények között fel sem tűnik a hosszváltozás.

A vírus neve: 834

Egyéb elnevezése: Arab.

Hossza: 834 bájt.

Kódtípusa: Rezidens résszel rendelkező, parazita, .COM fertőző.

Azonosítása: Scan V76+.

Eltávolítása: Fertőzött állományok törlése.

Leírása: A vírus az USA-ban, 1991 februárjában bukkant fel. Nincs benne ugyan utalás eredetére, de az időpont miatt összefüggésbe hozzák a közel-keleti konfliktussal. Sok érdekes programozástechnikai ötlet található benne. Némi rokonságot mutat a Guppy családdal is. Minden .COM állományt megfertőz, de intelligensen kihagyja a COMMAND.COM-ot.

Amikor a víruskód végrehajtódik, 1808 bájtot foglal le önmagának a 640 K-s DOS memóriaterület alsó részén. Rezidenssé válása hasonlít a ZeroHunt-éhoz, az INT 21-et magára veszi. A merevlemez partíciós táblájába bejegyzést tesz.

A fertőzés során a fertőzött program 4 K többletmemóriát kér. Az állományok 834 bájttal növekednek meg, a víruskód az állomány végére épül be. A fertőzés során a dátum- és időpontbejegyések nem változnak meg.

A vírus bizonytalanná teszi a winchester használatát (unexpected access), amikor lemezről futtatjuk a fertőzött programot. Ekkor kissé átírja a partíciós tábla programját, ami arra tökéletesen elegendő, hogy a gép rendszerindításkor alaposan kiakadjon.

Ismert átirata:

834-B/Arab: Teljesen hasonló az eredeti vírushoz de ez megfertőzi a már fertőzött programokat is, ha azok a fertőzés után 1 K-nál nagyobbak. Fertőzi a második COMMAND.COM-ot is, ami 1 K-val növekszik meg. A vírusban két szövegtöredék található, két eltérő változatban:

```
nsed Materi
```

illetve

```
COMMAND.COM
```

A rendszer alsó tartományába épül be, 1792 bájtot lefoglalva.

A vírus neve: Grither

Egyéb elnevezése: Még nem ismeretes.

Hossza: 774 bájt.

Kódtípusa: Parazita, nincs rezidens része, .COM és .EXE fertőző.

Azonosítása: Scan V72+.

Eltávolítása: Törölni a fertőzött állományokat (ha van egyáltalán még hol és mit törölni).

Leírása: Ha versenyt írna ki valaki, hogyan lehet a legrövidebb víruskóddal a lehető legnagyobb kár okozni, akkor jelenleg ez a vírus biztosan dobogós helyre kerülne. Jelenlétére Paul Ferguson hívta fel a figyelmet 1991 januárjában, az USA-ban.

Ha a Grither víruskód lefut, nem lesz rezidens, de közvetlenül megkeres és megfertőz az aktuális könyvtárban egy .COM állományt. Ha van ott COMMAND.COM, akkor azt is. A kód a programállomány végére épül be, hossznövekedést okozva. A dátumot és az időpontbejegyzést a fertőzéskor békén hagyja. Károkozása abban nyilvánul meg, hogy nyolc futása közül egy esetben alaposan felülírja a merevlemez C:, és ha van akkor D: partíciójának elejét. Ekkor helyreállíthatalanul tönkreteszi a bootszektor, a FAT és a partíciós tábla, valamint a rendszerállományok területét. Már csak a lemez újraformázásával érdemes foglalkoznunk.

A program nem eredeti alkotás. A Violator és a Vienna forráskódjának az ismeretében barkácsolta valaki. A Scan72 és néhány más szoftver tévesen Vienna-B-nek ismeri fel.

A vírus neve: Holocaust

Egyéb elnevezése: Holo, Spanish Telecom.

Hossza: 3784 bájt.

Kódtípusa: Parazita, általános .COM fertőző, beleértve a COMMAD.COM-ot is.

Azonosítása: Scan V74+.

Eltávolítása: Törölni a fertőzött programokat.

Leírása: A vírus s lopakodó programozástechnikát kiválóan alkalmazó, önmagát titkosító vírus. Megjelenését 1990-ben Barcelonából jelentette David Llamas antivírus szakember. Amikor a vírus aktív a memóriában, jelenléte

nem látszik. Állományok megnyitásakor és programvégrehajtáskor fertőz, enyniben rokonságot mutat a kalsszikusnak számító 4096-tal.

A vírusos program lefutása után a vírus beépül a hagyományos 640 K-s DOS memória felső részébe, mégpedig a Command Data Area részbe, azaz a parancsok számára fenntartott területre. Az INT 21 vezérlését átveszi. 4080 bájt területet foglal el a memóriában. Sok memóriamutató program ezt a parancsértelmező származékának mutatja, így nem tűnik fel.

Memóriarezidens vírus. A .COM állományokat megnyitásukkor, illetve futtatásukkor fertőzi. A hossznövekedés 3784 bájt, ami nem látszik, ha a vírus éppen a memóriában van. A víruskód az állomány végére épül be. Az 1 K-nál kisebb .COM programokat is megfertőzi. Amikor a tárban van, a CHKDSK sok állományról „File allocation error" üzenetet ad. Ha az ilyenkor szokásos /F paraméterrel lefuttatjuk, akkor tönkreteszi a fájlokat. Módosítgatja az egyes állományok és könyvtárak FAT bejegyzéseit is.

A vírus változó algoritmusokkal titkosítja önmagát. Néhány esetben a fertőzött állomány végére kódolás nélküli, olvasható formában a következő szöveget teszi:

```
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 -
```

Ez a szöveg más esetekben kódoltan van jelen, és csak az állomány teljes visszafejtése után válik láthatóvá. A nyílt és a titkosított szöveg a kódolási algoritmusok rotálásával változik. A vírust a spanyol telefontársaság bosszantására írhatták, s a szövegben is „alacsonyabb tarifákat és jobb szolgáltatást" követelnek. Jim Bates Virus Bulletinje Spanish Telecom néven regisztrálja ezt az igen fejlett programozástechnikával megírt vírust.

A vírus lassan terjedt el, első felbukkanásától majdnem fél évnek kellett eltelnie, míg eljutott Londonba. Az üzenet végén látható 666-os szám szintén utalás a Biblia apokaliptikus látomására (lásd Saddam vírus). A vírusírók saját névválasztása (Holocaust Csoport), szintén utalás az égő áldozatra, az Apokalipszis lovasaival előrejelzett eseményekre.

Eddie — a zenekedvelő zseni

Dark Avenger, Dark Avenger-B, V651, V800, V800M, V1024, V2000, V2000-B/Die Young, V2100, Anthrax, Red Diavolyata.

Valahol Szófiában él egy középkorú úr, a vírusírás professzora. Életműve, az Eddie sorozat jól jellemzi felfogását. Szereti az Iron Maiden együttest, olyannyira, hogy annak jellegzetes csontvázfiguráját, Eddie-t választotta példaképül. Munkáiban is ez a felfogás tükröződik, meg akarja örökíteni a halál szimbólumát a programok művészi halálának eszközével, a vírusprogrammal. Van egy barátnője — vagy talán felesége —, Diana P., aki az egyik vírus ajánlásában szintén bevonult a Pokoli Panoptikumba.

Eddie vírusíró professzora mindent tud a gépről, amit tudni kell. Víruskódjainak visszefejtése során igen sokat tanultunk az operációs rendszer belső, nyilvánosságot előzőleg soha nem kapott dolgairól. Az ő munkássága döbbentett rá bennünket arra — no meg egy ismeretlen debreceni diák, a Polimer vírus írója —, hogy a legjobb vírusellenes program se ér semmit, ha az operációs rendszer és a hardver védtelenül átadja magát a támadásoknak.

A vírus neve: Dark Avenger

Egyéb elnevezése: Black Avenger, Eddie.

Hossza: 1800 bájt.

Kódtípusa: Parazita, rezidens része van, a .COM, az .EXE és az átfedő (*overlay*) állományokat, valamint a COMMAND.COM-ot fertőzi.

Azonosítása: ViruScan V36+, F-Prot, IBM Scan, Pro-Scan, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: M-DAV, Clean36+, F-Prot, Prgdoki, Sysdoki.

Leírása: A Dark Avenger vírust az USA-ban izolálták először, a Davis támaszponton. Származási forrása Bulgária. Magyarországon először 1989 augusztusában jelentkezett, tömeges járványt okozva. Utána robbanásszerűen terjedt el a többi kelet-európai országban. Mongóliában például az erősen centralizált számítástechnikai rendszerek miatt igen nagy pusztítást végzett.

A vírus egyformán fertőz .COM, .EXE, valamint átfedő (overlay) állományokat, a COMMAND.COM-ot is beleértve. A vírus rezidens része installálja magát a rendszer memóriájában, magára irányítja az állomány- és könyvtárkezeléssel kapcsolatos összes DOS megszakítást és DOS funkciót. Így bármilyen célra nyitunk is meg egy állományt — tehát akár egy DIR utasítás erejéig is —, a „timer interrupt" segítségével elveszi a vezérlést és bemásolja magát. Ha-

gát. Hasonló meglepetésben lehet része annak, aki a COPY vagy az XCOPY utasításokkal másol fertőzetlen állományokat: Eddie ott fog majd ülni minden másolati példányban. Mintegy 20 perc alatt képes egy teljes merevlemez minden futtatható állományát megfertőzni. A fertőzött állomány 1800 bájttal növekszik meg.

Dark Avenger fertőzés esetén egy írásvédett (leragasztott) vírusmentes floppy rendszerlemezről kell elindítani a rendszert, majd ráereszteni a megfelelő mentesítő programot. Másképpen esetleg maguk a mentesítő programok lehetnek a fertőzés továbbhurcolói, az integritásvédelemmel ellátottak pedig nem is működnek.

A vírus aktivizálódásának feltétele, hogy a lemezen minden megfertőzhető állomány fertőzött legyen. Amikor ez bekövetkezik, akkor részben azzal teszi tönkre az állományokat, hogy azokba véletlenszerűen bemásolja saját darabjait és szöveges részét. Később a főkönyvtárt tartalmazó rész kivételével a merevlemezen egyes sávokat alacsony szintű formázással tönkretesz. Ez okozza a rossz, illetve íráshibás szektorok felszaporodását, majd végül a rendszer összeomlását. 1989. november-decemberben Budapesten és Győrben kiadós járványt okozott. A vírus még csak részleteiben sem azonos a Jerusalem vírussal, bár hosszuk közel ugyanannyi.

A Dark Avenger vírus a következő szöveges üzenetet tartalmazza:

```
The Dark Avenger, copyright 1988, 1989
This program was written in the city of Sofia
Eddie lives.... Somewhere in Time!
```

(A Sötét Bosszúálló, copyright 1988, 1989. Ezt a programot Szófia városában írták. Eddie él.... Valahol az időben!)

A vírus aktivizálódása során először a COMMAND.COM-ot támadja meg. A DOS-tól gyakorlatilag a teljes vezérlést elveszi (óra, billentyűzet, videojelek, lemezírás és -olvasás, memóriában maradás). Terjedésének gyorsasága miatt csak a vírusmegelőző programok bizonyulnak vele szemben hatásosnak. Ha a Dark Avenger minden állományt megfertőzött, akkor szektoronként, azaz 512 bájtonként beépül az állományok közepébe, ezzel gyakorlatilag tönkretéve azokat. A vírus jelenléte gyakran okoz rendszerleállást, megmagyarázhatatlan géplefagyást.

E vírus zseniális programkódjával vált népszerűvé a vírusok átírói között, de mi is, akik a barikád másik oldalán foglalkoztunk vele, tiszteltük tudását. Amit csak ismerni lehet a gépről, a merevlemez-kontrollerek „lelki életéről", azt ő valóban felkutatta. Létezik a vírusnak egy 2000 bájt hosszú verziója is, amely egy korábbi kísérleti darab lehet és Fridrik Skulason tájékoztatása szerint a skandináv országokban felbukkant.

Egy harmadik változat szintén az eredeti vírus szerzőjének kezenyomát viseli, ráadásul két eltérő szövegrésszel:

„A" szövegrészlet:

```
Copy me - I want to travel
```

(Másolj le, utazni akarok)

„B" szövegrészlet:

```
Only the Good die young…
```

(Csak a jók halnak meg fiatalon...)

A vírusban szerepel egy női név is:

```
Diana P
```

De a szöveg legérdekesebb részlete a következő:

```
Copyright (C) 1989 by Vesselin Bontchev
```

Veszelin Boncsev ismert vírusszakértő, de a vírust nem ő írta. Ez volt az első eset, hogy egy antivírus-szakember lejáratására a vírust úgy dedikálták, mintha az illető írta volna. Azóta ezt a „kitüntetést" majdnem minden ilyen szakember megkapta. Dr. Solomon éppúgy (Adolf Hitler baci), mint Patricia M. Hoffman (Patricia), Ralph Burger (Burger), vagy egykori kollégánk, Farmosi István (Phantom). Sajnos nagyon kevesen hiszik el, hogy valóban semmi közük a vírusgyártáshoz. Az Eddie vírust kommentált forráskódban is terjesztik, ami az átiratok melegágya.

Ismert átirata:

Dark Avenger-B: Teljesen hasonló az A variánshoz, de benne a fertőzés-ellenőrző rutin hibás, a .COM állományokat többször is megfertőzi. Hossza 1800 bájt. A rendszermemória felső részébe épül be, de később áttelepül az alsó részbe. Valamelyest különbözik a víruskód szöveges része is:

```
Eddie lives...somewhere in time!
Diana P.
This program was written in the city of Sofia
(C)1988-1989 Dark Avenger
```

Az alkalmazott megoldások alapján a vírus leszármazási kapcsolatban állhat a V2000, V1024, V651 vírusokkal.

A vírus neve: V651

Egyéb elnevezése: Eddie 3.

Hossza: 651 bájt.

Kódtípusa: Parazita .COM és .EXE fertőző, rezidens része van.

Azonosítása: Scan V66+, VirHunt 2.0+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: A Dark Avenger nagytudású professzorának ujjgyakorlata a V-sorozat. Biztosan bolgár eredetű. Az ismeretlen szerző időközben forráskódot is piacra dobott. A hivatalosan V651-nek, de sok helyen Eddie 3-nak nevezett vírust ugyanaz a Veszelin Boncsev izolálta 1990 áprilisában, akinek bosszantására a kasszikus Eddie-t dedikálták. A vírus rokonságban van a V1024 és a V2000 vírusokkal is.

A .COM és az .EXE állományokat fertőzi meg. Rezidens része van, amelyik a memória méretét 688 bájttal csökkenti. A program növekedése a fertőzés után 651 bájt, vagy .EXE esetén a paragrafushatárok miatt ennél valamivel több. A hossznövekedést azonban a vírus elrejti a DIR parancs elől, s ha a memóriában van, akkor az eredeti hosszat és CRC-t láthatjuk. A hecc kedvéért ennek megfelelően mutatja a lemez üres helyét is, így a vírus munkálkodását nem

lehet észrevenni. Lebuktatásának módja: a rendszerindítást garantáltan vírusmentes floppyról végezzük, majd a kiadott DIR parancs hatására láthatóvá válik a 651 bájtos hossznövekedés, ilyenkor ugyanis nincs a memóriában, és nem tudja elfedni a méretváltozást. Emellett minden fertőzött állomány végén olvasható a következő (ismerős!) szöveg:

`Eddie Lives.`

Amikor a vírus jelen van a memóriában, igen sok keresztkapcsolt szektort jelez. Ha azonban elindítjuk a CHKDSK /F utasítást, akkor garantáltan összekuszáljuk merevlemezünket. (Végül tehát a kárt nem is a vírus, hanem a felhasználó okozza?!)

A V651 nagyon hasonlít másik két vírushoz: a V2000-hez és a Dark Avengerhez, de ez a vírus kizárólag futtatáskor fertőz, míg a többiek állománymegnyitáskor is. Valószínűleg ez volt a fejlesztés első stádiuma.

A vírus neve: V800

Egyéb elnevezése: Live After Death.

Hossza: 800 bájt.

Kódtípusa: Parazita .COM fertőző. Rezidens résszel rendelkezik.

Azonosítása: Scan V63+, Pro-Scan 1.4+, F-Prot 1.12+.

Eltávolítása: Clean V64+, Scan /D, F-Prot 1.12+ vagy törölni a fertőzött állományokat.

Leírása: Ennek az önmagát titkosító vírusnak a megjelenését szintén Veszelin Boncsev jelezte, 1990 májusában, Bulgáriából. A vírus memóriarezidens, a COM állományokat fertőzi, de kihagyja a COMMAND.COM-ot a fertőzendők listájáról. Bár látszólag nem tartozik az Eddie családba, a kód több részlete mégis azonos szerzőre utal. A vírus onnan kapta másik elnevezését, hogy a vírusban kódolva a következő üzenet található:

`Live after Death`

(Elevenen a halál után)

A víruskód az első fertőzött állomány futtatásakor épül be a memóriába. Elkapja az INT 2A megszakítót és 16 K-val csökkenti a memória méretét, miközben a DOS memória tetején 8192 bájtnyi helyet foglal magának.

Amikor elindítunk egy nem fertőzött .COM programot, akkor a vírus gondolkodni kezd. Megnézi, hogy a program hossza meghaladja-e az 1024 bájtot. Ha nem, akkor lemond a fertőzésről, ha meghaladja, akkor megfertőzi. Ha újrafertőzi az állományt, akkor minden új fertőzéskor 800 bájtot ad hozzá az eredeti hosszhoz, így a hossznövekmény 800-zal osztható!

Ismert átirata:

V800M: Teljesen hasonló az eredetihez. Az eltérés a fertőzés módjában van. Ugyanis ez a változat állománymegnyitásra és futtatásra egyaránt fertőz, a lopakodó technika alkalmazásának mezsgyéjén van. Amikor memóriarezindessé válik, a rendszermemóriát 8192 bájttal csökkenti. Az eredeti változattal ellentétben ebben a verzióban nincs kódolt szöveg, hanem annak a helyére van elrejtve a hosszabb terjedési rutin.

A vírus neve: V1024

Egyéb elnevezése: Dark Avenger III.

Hossza: 1024 bájt.

Kódtípusa: Rezidens résszel rendelkező parazita vírus. A .COM és az .EXE programokat egyaránt fertőzi.

Azonosítása: Scan V64+.

Eltávolítása: Törölni a fertőzött programokat.

Leírása: Danile Kalcsev bolgár antivírus-szakember jelentette 1990 áprilisában Bulgáriából ezt a vírust, amely az Eddie család tagja. Amerikai szakértők fel is vetették: a Dark Avenger sorozat nem egy személy, hanem a forráskód birtokában dolgozó több szerző vagy csoport munkája. Saját információnk szerint azonban egyetlen személy írta e programokat. A forráskódok elemzése ugyanezt támasztja alá.

A vírus .COM és .EXE állományokat is megtámad, a COMMAND.COM kivételével. Rezidens része is van. Valószínűleg az Eddie korai verziója. Nem fertőz meg minden megnyitott állományt. Amikor a kód lefut, elhelyezi magát a memóriában. Itt ellenőrzése alá von több megszakítót is. Érdekes az anti-debugger megoldása. Azt tételezi fel, hogy a debug az INT 1 és az INT 3 interruptok közül legalább az egyiket használni fogja. Ha azután ilyet tapasztal, akkor a vírus ráugrik egy olyan — különben soha nem aktivizálódó — szubrutinjára, amelytől a rendszer kimerevedik. Ilyenkor a vírusnak természetesen esze ágában sincs szaporodni!

A rendszer rendelkezésére álló memória méretét 1072 bájttal csökkenti, ugyanakkor az interrupt-bűvészet eredményeként a DOS változatlan memóriaméretet közöl velünk. Több megszakítót is magára irányít, ezáltal a gépet maximális mértékben ellenőrzése alatt tartja. Ha memóriatérképet nézünk egy erre a célra szolgáló szoftverrel — például a közkedvelt SMAP-pal —, akkor a vírust nem ott látjuk a memóriában, ahol valójában ül. Ha jelen van a memóriában, akkor a DIR parancs elől elmaszkolja a méretnövekedést és az eredeti méretet láttatja. A fertőzött program végén található számsor (7106286813) hexadecimális karakterkódokból álló értelmetlen zagyvaléknak tűnik.

A vírus neve: V2000

Egyéb elnevezése: Dark Avenger II, Travel.

Hossza: 2000 bájt.

Kódtípusa: Parazita, rezidens, a .COM és az .EXE állományokat fertőzi, beleértve a COMMAND.COM-ot is.

Azonosítása: Scan V59+, Pro-Scan 1.4+, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: Scan /D , Sysdoki vagy törölni minden fertőzött állományt.

Leírása: A vírust 1989-ben jelezte Bulgáriából Niki Szpahiev, valamint Daniel Kalcsev. Magyarországon egy vírushordozó trójaivá átbarkácsolt Scan programba beültetve terjedt el, a jelek szerint a Budapesti Műszaki Egyetemről. Akkor a Scan programoknak még nem volt változásjelző önvédelmük, így mind a sorszám átvakarását, mind a vírus betelepítését kockázat és szinte munka nélkül meg lehetett tenni. Szerencsére az akkor lezajlott járvány óta

nincs tömeges előfordulása. A vírust utazásra felszólító belső szövegrészlete miatt Travel néven is ismerik.

A vírus a fertőzött program elindítása után rezidensen beköltözik a memóriába. Ezt követően megkeresi a COMMAND.COM-ot és megfertőzi azt. Utána már minden elindított vagy bármilyen hozzáfordulás céljából (másolás stb.) megnyitott .COM és .EXE állományt meg fog fertőzni. A vírus 2000 bájttal növeli meg az állományokat, de ezt a felhasználó a DOS DIR parancsával nem látja, *mert* a vírus a katalógusba az eredeti fájlhosszt írja vissza. A vírus nagyon agresszív, rendszerösszeomlást, adatvesztést okoz, és az operációs rendszer újbóli betöltését teszi lehetetlenné. Az operációs rendszer akkor válik betölthetetlenné — nem minden operációs rendszerverzió esetén! —, ha a vírus beépült a rejtett állományokba és a COMMAND.COM-ba.

A vírus az állományok végére fűzi be magát. Benne szöveges azonosítók találhatók.

A vírus elején:

```
Only the Good die young.....
```

(Csak a jók halnak meg fiatalon.....)

A vírus végén:

```
(c) 1989 by Vesselin Bontchev
```

Veszelin Boncsev kiváló virológus programozó szakembert vírusíró ellenségei azzal a módszerrel akarták lejáratni, hogy több vírust is — a V2000-et is — az ő művének igyekeztek feltüntetni. Ez a manőver azonban nem bizonyult elég hihetőnek.

A vírus floppyról kerülhet be a gépbe. Akkor fertőz, ha valamelyik másik program olvasásra nyitott meg egy futtatható állományt. Ez volt az értelme a Scan programra való ráépítésének is. Először a merevlemezen fertőz, a floppyn csak akkor, ha a merevlemezen már nem talál több fertőzhető állományt. Rendszerlefagyást okoz. Amennyiben többszörösen épült be, akkor olyannyira felülírja az egyes állományokat, hogy azokat már nem lehet helyreállítani. Ha a memóriában aktív, akkor minden olyan állomány hosszából, amelyikbe beépült, a kimutatásnál levon 2000 bájtot, így azokat a tartalomjegyzékben eredeti hosszúságúaknak látjuk.

Ha a vírus jelen van a memóriában, a CHKDSK hihetetlen mennyiségű keresztkapcsolt szektort lát. Lefuttatva a szokásos CHKDSK/F-et, a sok alkönyvtár belépési pontja összekeveredik vagy eltűnik a FAT-tábla bejegyzésein.

A vírusban lévő „utazási" bejegyzésnek két szövegváltozata van, nyilvánvalóan a billentyűzet kétféle kiosztása miatt nálunk is gyakori tévesztésből, elgépelésből fakadóan:

```
Zopy me - I want to travel
Copy me - I want to travel
```

(Másolj le, utazni szeretnék)

Ismert átiratai:

V2000-B/Die Young: Teljesen hasonló, mint az alapváltozat. Csak az utaztatási felszólítást cserélte ki (először ugyancsak elgépelve) egy másik vírusban

már kipróbált szállóigére, amely az Iron Maiden együttes egyik nótájából vett idézet:

```
Mnly the Good die young...
Only the Good die young...
```

(Csak a jók halnak meg fiatalon...)

Ide kívánkozik a görög legendárium egyik története. Az anya elmegy a jóshelyre, és megkérdezi, mi a legnagyobb jó, amit egy ember jutalomként kaphat az istenektől. A jósok erre azt felelik: Fiatalon, a halál tudata nélkül, fájdalommentesen meghalni. Erre az anya hazatért és megmérgezte szeretett fiát...

Talán Eddie alkotója is így szereti a számítástechnikát?

A vírus neve: V2100

Egyéb elnevezése: 2100, UScan.

Hossza: 2100 bájt.

Kódtípusa: Rezidens résszel rendelkező .COM és .EXE fertőző vírus.

Azonosítása: Scan V66+.

Eltávolítása: Törölni a fertőzött programokat.

Leírása: Ha egy ötlet beindul... Ezt a vírust is vírustalanító programmal, a nyugat-európai BBS-eken terjesztett UScan antibacival szórták szét a világban. Bulgáriában 1990 júliusában izolálta Veszelin Boncsev. A kód és a közben kikerült eredeti forráskód alapján bizonyos, hogy szerzője azonos az Eddie zenekedvelő víruskészítőjével.

Amikor a vírus installálja magát a hagyományos DOS memória felső részébe, elkapja az INT 12 megszakítót, és 4288 bájtnyi helyet foglal magának. Ezután számos esetben magtámadja a COMMAND.COM-ot és természetesen elrejti annak hossznövekedését a DOS elől. A fájlok megnyitására és futtatására egyaránt fertőz, a támadás célpontjai pedig .COM, .EXE és .OVL állományok — abban az esetben, ha hosszuk eléri vagy meghaladja a vírus hosszát. Nemcsak eltitkolja a hosszövekedést, hanem néhány esetben a fertőzött állományok hosszából többet von le, mint amennyit kellene, és azok 2100 bájttal rövidebbnek mutatkoznak eredeti hosszuknál, ha a vírus jelen van a memóriában. Emellett ilyenkor hihetetlen ötletességel szimulál hibákat. Szinte egymásba érve jelentkeznek a FAT tábla hibájára, a keresztkapcsolt szektorokra és a DOS által produkált egyéb jelenségekre vonatkozó hibaüzenetek. Mindezek a vírus jelenléte nélkül egy csapásra megszűnnek. Ha azután ráeresztjük a CHKDSK /F-et, akkor alapos irtást rendezünk a merevlemez programkészletében..

A vírus „beszélget" és maximális mértékben együttműködik a szintén bolgár eredetű Athrax partíciós tábla vírussal. Amikor a V2100 bekerül a memóriába, megnézi, hogy az Anthrax vírus jelen van-e a partíciós táblában. Ha nincs is ott, lehet, hogy a maga másodpéldányát a merevlemez utolsó szektorában tárolja, ezért a V2100 végigbogarássza a winchester utolsó 16 szektorát az Anthrax nyomai után. Ha megtalálta annak rejtettt másik kópiáját, akkor azt sürgősen bemásolja a partíciós táblába, hogy ott feléledjen.

A vírus neve: Anthrax

Egyéb elnevezése: Még nem ismeretes.

Hossza: 1040–1279 bájt.

Kódtípusa: A .COM és az .EXE állományokat, valamint a partíciós táblát fertőzi, rezidens résszel rendelkezik.

Azonosítása: Scan V66+, Pro-Scan 2.01+.

Eltávolítása: Törölni a fertőzött állományokat, MDisk/P, Pro-Scan 2.01+, valamint Clean V80+.

Leírása: A bulgáriai „Eddie professzor" sok régi ötlettel fűszerezett újabb leleménye. 1990 júliusában holland BBS-ben találták egy friss verziójelzést viselő UScan víruskereső trójai programba építve, az USCAN.ZIP állományba csomagolva.

A memóriarezidens vírus a partíciós táblát, továbbá a .COM és .EXE állományokat fertőzi meg, belelértve a COMMAND.COM-ot is. Túlélési esélyeinek növelésére biztonsági másolatot helyez el magáról a merevlemez utolsó 16 szektorának valamelyikén, hogy alkalomadtán egy véletlenül arra járó V2100 majd felélessze. (Lásd a V2100 vírus leírását.) Amikor ezt a másolatot lerakta, a vírus tovább már nem lesz memóriarezidens. Ha a fészeknek használt 16 szektoron véletlenül adatunk volt, akkor az elveszett.

Amikor a merevlemez partíciós tábla programja az újabb induláskor betöltődik, akkor a vírus is betöltődik újra, s mindaddig memóriarezidens marad, amíg el nem indítjuk az első programot. Ekkor eltávolítja magát a memóriából, de mielőtt ezt megtenné, egy .COM vagy .EXE állományt megfertőz, lehetőleg nem a saját alkönyvtárából, mert oda csak végső esetben teszi be magát, amikor már nem talál másutt megfertőzhető állományt. Folyamatosan halad a könyvtári fa ágain felfelé, a fertőzést a legalsó szinteken kezdve.

Az Anthrax vírus programkódja 1024 bájt, de ez a paragrafushatárok miatt változhat, az .EXE programoknál 1040–1279 bájt között mozog. A fertőzött állományok hossza minden esetben osztható 16-tal. Az Anthrax vírusban a következő szöveges azonosítót találhatjuk:

```
(c)Damage, Inc.
ANTHRAX
```

Az állományban lévő harmadik szöveg (cirill betűkkel): Szofia 1990.

Az Anthrax vírusfertőzés megszüntetését a merevlemez partíciós táblájának takarításával kell kezdeni. Utána az MDISK/P opciójával helyre kell állítani a korrekt PC-DOS vagy MS-DOS bootszektort. (Ezt most már a Clean újabb verziói is meg tudják tenni.) Utána írásvédett DOS lemezről rendszert kell hívni, és az Anthrax vírussal fertőzött összes programot törölni, vagy — ha lehet — valamilyen hatékony antivírus programmal fertőtleníteni. Végül meg kell keresni a legutolsó pályán elrejtett kópiáját és azt felül kell írni.

A vírus neve: Red Diavolyata

Egyéb elnevezése: Még nem ismeretes.

Hossza: 830 bájt.

Kódtípusa: Parazita, rezidens résszel rendelkezik, .COM fertőző.

Azonosítása: Scan V80+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: A sikeres embereket rendszerint igyekeznek másolni, utánozni. Ezt „Eddie professzor" sem kerülhette el. *Műve* 1990 decemberében egy orosz számítástechnikai gimnázium (MLTI) diákjainak jóvoltából kelt új életre. (MLTI = Matematyicseszkij Liceum Tehnyicseszkij Insztitut = Matematikai Líceum Technikai Intézete.)

A Red Diavolyata (Vörös Ördög) a memória tetejére épül be a hagyományos 640 K-s tartományban. Nem manipulálja az INT 12-t, így jelenléte ennek az megszakítónak a figyelésével nem észlelhető, de az INT 21-et magára láncolja. 960 bájttal csökkenti a rendszermemória méretét. Memóriarezidens, a .COM állományokba azok futtatásakor ül bele. (A COMMAND.COM-ot sem mellőzve.)

A fertőzött program 830 bájttal lesz nagyobb. A fertőzés során az aktuális rendszeridőre és dátumra írja át a megfertőzött állomány időadatait. A vírus a fertőzött program végére épül be. A *megfertőzött* állományok belsejében a következő szöveges vírusazonosító látható, de csak véletlenszerűen:

```
MLTI!COMMAND
```

Mivel ez felülír, megakadályozza az állomány helyreállítását. A vírusban, a fertőzött program végén a következő szöveg olvasható:

```
Eddie die somewhere in time
This programm was written in the city of Prostokwashino
(C) 1990 RED DIAVOLYATA
Hello! MLTI!
```

(Az értelemzavaró angol helyesírási hibákkal terhelt szöveg feltételezhető jelentése: Eddie meghalt valahol az időben. Ezt a programot Prosztokvascsino városában írták. (C) 1990 Vörös Ördögök. Helló! MLTI!)

A bolgár iskola

1226, 1226D, 1126M, 512, 512-B, 512-C, 512-D, 512-E, 512-F, Destructor, Kamikazi, Murphy, Murphy-2, AntiChrist, HIV, Migram, Kamasya, Nina, Happy New Year, Happy New Year B, Nomenklatura, MG, MG-2, MG-3.

Az orosz mellett talán a bolgár vírusok váltak leghírhedtebbé a számítástechnikai szakmában, különösen azután, hogy a rendszerváltozáskor szabotázs céljára kifejlesztett vírusokat eresztettek el. A minimális jogi szabályozás hiánya kifejezetten bátorította a programozási tudásukat ily módon fitogtatni akarókat. Innen sarjadt a vírusírás és forgalmazás néhány új tendenciája, például az, hogy mások nevében írjanak vírust, hogy minimális vírusmérettel maximális kárt okozzanak, hogy víruscserével gyűjtsenek be minél több vírust, hogy minden programozó palánta megírja a maga vírusát... És ne feledkezzünk meg róla, hogy Bulgáriában alkot „Eddie professzor", s feltehetően tanítványai is bőven akadnak.

A vírus neve: 1226
Egyéb elnevezése: V1226.
Hossza: 1226 bájt.
Kódtípusa: Parazita, rezidens része van, .COM fertőző.
Azonosítása: Scan V66+, Pro-Scan 2.01+.
Eltávolítása: A fertőzött állományok törlése.
Leírása: A vírus a .COM állományok hosszának növekedését okozza, s közben jelentősen csökkenti a rendszer szabad memóriáját. A floppy is folyton forog, a programok futása közben zagyva karakterek jelennek meg, oda nem illő helyeken. Időnként a rendszer „kiakad" vagy lemerevedik. A vírus minden .COM állományt megtámad, de a COMMAND.COM-ot a lebukás elkerülése érdekében nem bántja.

E vírus a bolgár műhelyek egyik prominens darabja, szerencsére viszonylag ritkán bukkan fel. 1990 júliusában izolálta a vírusírással alaptalanul gyanúsított bolgár vírusszakértő Veszelin Boncsev.

A vírus önmagát titkosítja, így a hagyományos keresési módszerek hatástalanok vele szemben. Amikor a víruskód lefut, az a memória felső részén (a „RAMTOP"-on) lefoglal magának 8192 bájt szabad helyet és a 2A megszakító vektort magára irányítva használja.

Amikor a 1226-os vírus memóriarezidenssé válik, akkor megfertőz minden

olyan .COM állományt, amely hosszabb, mint 1226 bájt. A vírus kissé „bugaras", ugyanis a fertőzés nem mindig sikerül neki úgy, hogy utána még fusson is a program. Ha mégis összejön, akkor a megfertőzött állomány hossza 1226 bájttal lesz nagyobb. Többször is beépülhet ugyanabba az állományba. Ilyenkor a hosszövekedés az 1226 többszöröse. Annyira nem figyel a többszörös beépülésre, hogy emiatt áldozatai könnyen túllépik a .COM állományok 64 K-s méretahatárát, és nem férnek be a memóriába.

Ha a rendszerállomány fertőződik, elképzelhető, hogy a rendszer kiakad, miközben egy programot hajt végre. A vírus jelenlétének másik ismertetőjele a felesleges soremelés vagy két hamis karakter megjelenése a monitoron a parancssorban.

A későbbi átiratokat, az 1226D és az 1226M vírusokat alkotójuk egy kicsit kipoloskázta, ezért azok nem döglenek meg szaporodás közben.

A vírus neve: 1226D
Egyéb elnevezése: V1226D.
Hossza: 1226 bájt.
Kódtípusa: Parazita, .COM fertőző, rezidens része van.
Azonosítása: Scan V66+, Pro-Scan 2.01+.
Eltávolítása: Törölni a fertőzött programokat.
Leírása: Veszelin Boncsev fedezte fel ezt a vírust Bulgáriában, 1990 júliusában. A víruscsere csatornáitól eltekintve eddig szerencsére nem nagyon bukkant fel. Általános .COM fertőző, de mellőzi a COMMAND.COM-ot. Önmagát titkosítja, így egyszerű keresési algoritmussal nem észleljük.

Az 1226D vírus a nem kódolt 1226-nak kódolt és kijavított átirata. Jó a terjedési algoritmusa, nem pusztul el fertőzés közben. Állományok megnyitásakor és a .COM állományok futtatása során fertőz. A rendszer memóriájában 8192 bájtot foglal le magának a szabad memória felső részén. Az INT 2A vektort magára irányítja. Amikor memóriarezidenssé válik, utána minden futtatott .COM állományt megfertőz, hosszukat 1226 bájttal növelve. Az eredeti 1226-os többször is képes megfertőzni ugyanazt az állományt, míg a „javított és bővített" második kiadás, az 1226D már figyeli a fertőzést és csak egyszer épül be. Rendelkezik azzal az ötletes megoldással, hogy a .COM állományok megnyitásakor is fertőz. Így egy sima DOS COPY parancs kiadásakor az eredeti és a másolat egyaránt fertőzött lesz.

Az 1226D átirata, a 1226M/V1226M azonos az 1226D-vel, azzal az egyetlen különbséggel, hogy állományok megnyitásakor nem fertőz, csakis futtatáskor.

A vírus neve: 512
Egyéb elnevezése: 512-A, Number of the Beast.
Hossza: 512 bájt.
Kódtípusa: Rezidens résszel rendelkező, parazita, .COM fertőző.
Azonosítása: Scan V58+, VirexPC 1.1+.
Eltávolítása: Clean V58+.
Leírása: „Fogjunk ki az új vírusdetektorok íróin!" — valószínűleg ez a szán-

dék vezette ennek a bolgár vírusnak a szerzőjét. E vírus megszületéséig a gyors víruskeresés logikája az volt, hogy meg kell nézni, hova mutat az első ugrócím. Ha az állomány végére, akkor valószínűleg vírussal van dolgunk. Nos, ebben az esetben az első ugrócímet a vírus békén hagyja, és a másodikat írja át önmagára mutatóan, majd a kilépő ugrását arra a címre, ahova ez a második JMP mutatott. Jó szórakozás!

E vírus nyomán egyre több olyan .COM fertőző baci készül el, ahol a vírus az állomány végére épül be, és nem sokat ér az a detektálás, amelyik az ugrásokat vizsgálja.

Hasonlóságai ellenére semmi köze a közismert Péntek 13 vírushoz. Bolgár eredetű, 1989 novemberében izolálta Veszelin Boncsev. Maga a vírus általános .COM állomány fertőző, beleértve a COMMAND.COM-ot is. Az első fertőzött program futtatásánál épül be a memóriába, majd a megnyitáskor megfertőz minden olyan .COM állományt, amelynek hossza eléri az 512 bájtot.

Programelszállást és rendszerlemerevedést okoz. A CHKDSK/F paraméterrel futtatva tönkreteszi az állományokat. Elrejti a DOS elől a méretnövekedéseket, amikor a memóriában van.

A vírus a 666-os bibliai utalású számot alkalmazza annak megjelölésére, hogy az állomány már fertőzött. Ezt az állomány végén találhatjuk meg.

Az 512-es vírus eddig ismert átiratai:

512-B: Hasonló, mint az eredeti, csak a DOS verziószám-ellenőrző rutint hagyta el a szerző, hogy a 3.30-nál alacsonyabb DOS verziók alatt is fusson. Kitörölte a 666-os vírusazonosítót is.

512-C: Némi poloskairtás és kódrövidítés az 512-B vírus átiratán, különben azzal azonos.

512-D: Hasonló az 512-C változathoz, azzal az eltéréssel, hogy a vírus ellenőrzi a SYSTEM attribútumot, s ha az be van kapcsolva, akkor nem végez hosszellenőrzést, hanem fertőz.

512-E: Hasonló az eredeti 512-es vírushoz, azzal az eltéréssel, hogy számos videokártya esetében képes a DOS fölé, annak memóriájába beépülni. A rendszermemóriát 55 104 bájttal csökkenti, legalábbis ennyit jelez a CHKDSK program. Nem alkalmazza a 666-os stringet a fertőzés jelzésére.

512-F: Amikor a vírus rezidens, a CHKDSK semmilyen memóriacsökkenést nem mutat. Minden másban azonos a C változattal. A vírusfertőzés megtörténtének felismerésére alkalmazza a 666-os stringet, amely az állományon belül az 1FD offset címen található meg.

A vírus neve: Destructor

Egyéb elnevezése: Destructor V4.00.
Hossza: 1150 bájt.
Kódtípusa: Parazita, rezidens, .COM és .EXE állományokat fertőz meg.
Azonosítása: Scan V74+.
Eltávolítása: Törölni a fertőzött állományokat.
Leírása: Eddig még elég ritkán fordult elő. 1990 decemberétől terjed Bulgá-

riából kiindulva. Memóriarezidens, .EXE és .COM fertőző, beleértve a COMMAND.COM-ot is. Skulason vírusriasztásából szerezhettünk róla tudomást.

Egy vírussal fertőzött program lefutása során installálódik a memóriába a 640 K-s hagyományos DOS memória felső részébe. Magára irányítja az INT 12 megszakítót, és azon keresztül vezérli a rendszert. A DOS számára látható memória méretét 1216 bájttal csökkenti. Ha megfertőzte a COMMAND.COM-ot, akkor a rendszer újraindításáig mást nem fertőz meg.

Ha a vírus a memóriában ül, akkor állományok megnyitásakor és programvégrehajtáskor is fertőz. A megfertőzött állomány hossza .COM esetén 1150 bájttal lesz nagyobb, az .EXE programok növekedése 1154–1162 bájt. Fertőzéskor nem állítja át az állomány dátumát és nem rejti el a hossznövekedéseket sem.

A vírusban a következő rendszerüzenet található, amely a képernyőn sohasem jelenik meg:

```
DESTRUCTOR V4.00 (c) 1990 by ATA
```

Félelmetes neve ellenére eddig csak a vírusscsere csatornáin bukkant fel. A Skulason által valószínűsített skandináv eredet nem állja meg a helyét. Bulgária mellett még egy származási ország jöhet szóba: Olaszország.

A vírus neve: Kamikazi

Egyéb elnevezése: Még nem ismeretes.
Hossza: 4031 bájt.
Kódtípusa: Felülíró, nem rendelkezik rezidens résszel, .EXE fertőző.
Azonosítása: Scan V80+.
Eltávolítása: Törölni a fertőzött állományokat.
Leírása: Rengeteg felesleges izgalomnak volt az oka, pedig Magyarországon eddig még elő sem fordult. A Scan V79 és néhány amatőr program a rossz szekvenciakiválasztás miatt teljesen tévesen a Turbo Pascal 6.0 „run time" részében jelezte a vírus jelenlétét. Veszelin Boncsev jelezte Bulgáriából, 1990 augusztusában.

A vírus a fertőzés során felülírja az .EXE állományokat. Nem rendelkezik rezidens résszel. Mivel elpusztítja a felülírt információt, a helyreállítással nem lehet kísérletezni. Amikor a kód lefut, a vírus az aktuális könyvtárban keres egy olyan .EXE állományt, ami hosszabb, mint 4031 bájt, s annak egy részét a vírus hosszával megegyező felületen teketória nélkül felülírja. Így a hossz sem változik. Tönkreteszi az EXE fejlécet is. Azzal tudatja ugyanis, hogy ő van egy adott állomány helyén, hogy az első nyolc bájtra ráírja a saját nevét:

```
KAMIKAZI
```

Innentől kezdve a gépnek számos baja támad. Kiakad, újra indul, a fertőzött program pedig természetesen nem fut le. Sőt ha a gyanútlan felhasználó ismételt futtatással kísérletezik, akkor a vírus mindig újabbakat fertőz meg. Néha karakteresen, „csillag, halálfej..." üzenettel tölti meg a képernyőt, azaz kiírja a memóriatartalmat.

A vírus neve: Murphy
Egyéb elnevezése: Murphy-1, V1277.
Hossza: 1277 bájt.
Kódtípusa: Parazita, rezidens, .COM fertőző.
Azonosítása: Scan V63+, Pro-Scan 1.4+, F-Prot 1.12+.
Eltávolítása: Törölni a fertőzött állományokat.
Leírása: Ami elromolhat, az el is romlik. Különösen igaz Muprhy alaptörvénye a számítástechnikában. Akkor pedig különösen, ha valaki tudatosan elő is segíti a programok elromlását. Ilyen a bolgár eredetű Murphy vírus, amely párjával, az Antikrisztussal együtt alaposan megkeseríti a felhasználók életét.

A Murphy vírust 1990-ben áprlis elején fogták meg Bulgáriában. A vírus a lopakodó technikát alkalmazza. Általános .COM és .EXE fertőző, beleértve a COMMAND.COM-ot is. A kód lefutása után a vírus beül a memóriába. Ezután a .COM és .EXE állományokat megnyitáskor és futtatáskor egyaránt fertőzi. Amikor bekerül a gépbe, az első nem fertőzött program futásakor megkeresi a COMMAND.COM-ot és azt fertőzi meg. Utána már „normálisan" dolgozik. Az állományok hosszúnövekedése 1277 bájt. Amelyik program ennél rövidebb, azt nem fertőzi meg.

A vírus figyeli a rendszerórát. Ha az délelőtt 10 vagy 11 órát mutat, akkor bekapcsolja a hangszórót és sorozatban kiküldi rá a 61h kódot. Magyarán sípol. Máskor néma marad.

A vírusban a következő, a képernyőn soha meg nem jelenített szöveg található, amelyben a vírus bemutatkozik:

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

(Hello, Murphy vagyok. Örülök, hogy találkoztunk, barátom. Engem november/december óta írtak.)

Ha a rendszerállományok Murphy vírussal fertőzöttek, a rendszer kiakadhat, amikor a vírus .EXE állományt akar megfertőzni.

Ismert átirata:

Murphy-2: Hasonlóan viselkedik, mint a Murphy alapvírus, csak a hossza 1521 bájt. Más a vírus belső üzenete is, csak annyit közöl, hogy ő a Murphy:

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

A Murphy-2 minden .COM és .EXE állományt megfertőz, amelynek hossza nagyobb, mint 900 bájt. Délelőtt 10 és 11 órakor ő is bekapcsolja a hangszórót. Ez a változat a rendszeridő perceit 00-ra állítja át. Ugyanakkor a pingpongozó karakter látható a képernyőn, miként jó pár másik vírus hatására is. Más esetekben kiakasztja a rendszert.

A vírus neve: AntiChrist
Egyéb elnevezése: Antikrisztus.
Hossza: 1008 bájt.
Kódtípusa: Parazita, rezidens, .EXE fertőző.
Azonosítása: Scan V76+.
Eltávolítása: Törölni a fertőzött állományokat.
Leírása: A vírust az USA-ban írták, David Grant izolálta 1991 márciusában, azonban programozástechnikailag teljes egészében a Murphy családjába tartozik, ezért került könyvünk bolgár fejezetébe. (Az nem valószínű, hogy szerzőjük azonos.)

Ha kultúrtörténetileg nézzük (lásd a hadibacikról szóló fejezet néhány vírusleírását), akkor ez is az apokaliptikus vírusokhoz tartozik. A Biblia szerint az Antikrisztus eljövetele a Gonosz időleges győzelmét és a Végítélet kezdetét jelzi.

A vírus memóriarezidens. Miután egy fertőzött állomány első futtatása megtörtént, a vírus installálja magát a hagyományos 640 K-s DOS memória tetejére. Nem variálja át az INT 12 megszakító visszatérését, az INT 21-et viszont manipulálja. A rendszer rendelkezésére álló szabad memóriaterületet, amit a CHKDSK program lát, 1040 bájttal csökkenti.

Miután a vírus rezidenssé válik, programfuttatáskor vagy állományok megnyitásakor megfertőzi azokat az .EXE programokat, amelyek 1 K-nál nagyobbak. A vírust a fertőzött állományok végén találjuk meg, a fertőzés dátuma nem jelentkezik a könyvtári bejegyzések módosulásában.

A vírus neve: HIV
Egyéb elnevezése: Még nem ismeretes.
Hossza: 1614 bájt.
Kódtípusa: A .COM és az .EXE állományokat fertőzi meg. Parazita.
Azonosítása: Scan V76+.
Eltávolítása: Törölni a fertőzött állományokat.
Leírása: Hogyan kerül egy eredeti olasz vírus a bolgár fejezetbe? — tehetik fel a kérdést, miután ez a vírus valóban talján. Gyökerei azonban Bulgáriáig érnek és a Murphy igen közeli leszármazottjának tekinthető, amelyet 1991 márciusában az USA-ban csípett meg David Grant vírusszakértő. A vírus memóriarezidens, a .COM és az .EXE állományokat fertőzi, és a COMMAND.COM-ot sem hagyja ki.

Amikor a víruskód lefut, a vírus először azt vizsgálja meg, jelen van-e már a memóriában. Ha még nincsen, akkor beépül a hagyományos 640 K-s DOS memória tetejére. A memóriaméretet (amit a CHKDSK lát), 1632 bájttal csökkenti. Ugyanakkor az INT 21-et alaposan manipulálja. Mind programfuttatásra, mind pedig állományok megnyitására fertőzi a .COM és az .EXE állományokat. A hossznövekedés a fertőzés után 1614 bájt, a vírus az állományok végére épül be. Az állományok dátumát nem módosítja.

A fertőzött programban a következő szöveg található:

```
HIV Virus - Release 1.0
```

Created by Cracker Jack
(C) 1991 Italian Virus Laboratory

Egyéb aktivizálódási feltételeit még nem ismerjük. Az Olaszországból az ottani víruslaboratóriumok aktivizálódásával megindult vírushullám első darabja. Cracker Jack kirívó termelékenységével hasonlóan megkeseríti az életünket, mint bolgár barátai.

A vírus neve: Migram

Egyéb elnevezése: Még nem ismeretes.
Hossza: 1221 bájt.
Kódtípusa: Rezidens résszel rendelkező, parazita, .COM fertőző.
Azonosítása: Scan V76+.
Eltávolítása: Törölni a fertőzött állományokat.
Leírása: A művek akkor válnak klasszikussá, amikor eredeti vagy átdolgozott kiadásokban újra meg újra napvilágot látnak. Így van az a vírusokkal is. A Migram egy USA-ban megjelent Murphy átdolgozás. Ezt is David Grant fogta meg 1991 márciusában. A többivel azonos helyszínen való felbukkanás valószínűsíti, hogy a HIV vírussal együtt Olaszországban készített vírusátirat, bár ezt néhány szakértő kétségbe vonja.

Igen hasonlít a bolgár Murphyhez. Rezidenssé válása előtt szintén ellenőrzi, hogy ott van-e már a memóriában. Ha nincs, akkor beépül a 640 K-s hagyományos DOS memória felső részére. Az INT 12 visszatérését nem bántja, de az INT 21-et magára irányítja. A CHKDSK a szabad memóriaméret 1248 bájtos csökkenést jelzi. A vírus az 1 K-nál hosszabb .EXE állományokat fertőzi meg, a hossznövekedés 1221 bájt. A fertőzés során a vírus az állomány végére épül be. A könyvtári bejegyzések dátumát fertőzéskor nem módosítja. Üzenete:

MIGRAM VIRUS 1.0
(C) 1991 IVL

Aktivizálódásának feltételei eddig nem ismertek. A Murphy vírus kódjának ismeretében készült.

A vírus neve: Kamasya

Egyéb elnevezése: Még nem ismeretes.
Hossza: 1098 bájt.
Kódtípusa: Rezidens résszel rendelkező, parazita, .EXE fertőző.
Azonosítása: Scan V76+.
Eltávolítása: Törölni a fertőzött állományokat.
Leírása: Ismét egy Murphy utánzó. 1991 márciusában bukkant fel az USA-ban David Grant „számítógép-bakterológus" praxisában. A vírusban lévő szöveg alapján nem amerikai eredetű, talán valami skandináv nyelvű üzenet lehet benne.

A vírus .EXE fertőző, rezidens résszel rendelkezik. A kód lefutása után megnézi, nem ül-e már a memóriában. Ha nem, akkor beköltözik a DOS memória tetejére. Egy részét azonban eldugja a rendszermemória aljára, hogy nehezebben legyen megtalálható. Az INT 21-et a rendszer tetején leselkedő része irá-

nyítja magára, míg az INT 00-át az alsó részen lévő rész fogja magára irányítani. A CHKDSK 1120 bájt memóriacsökkenést jelez. A vírus az állományok hosszát 1098 bájttal növeli meg, és az állományok végére épül be. A fertőzés után a könyvtári bejegyzések dátuma nem tér el az eredetitől.

A vírusban található szöveg:

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

Miután nekünk még nem sikerült megfejteni, aki tudja, hogy milyen nyelvű és milyen tartalmú a fenti (esetleg sifrírozott) szöveg, szívesen vesszük, ha közli a könyv szerzőivel.

A vírus neve: Nina

Egyéb elnevezése: Még nem ismeretes.

Hossza: 256 bájt.

Kódtípusa: A .COM állományokat fertőzi meg. Parazita, rezidens résszel rendelkezik.

Azonosítása: F-Prot 1.14+, Scan V74+.

Eltávolítása: F-Prot 1.14+.

Leírása: A vírusról igen kevés adat áll rendelkezésre. Skulason vírusriasztásából értesültünk felbukkanásáról 1991 közepén, de az USA-ban már 1990 decemberében észlelték. 256 bájt hosszú. Rendszerüzenetében található a névadó Nina szó. (Akárcsak a Happy New Year vírusában, ami bizony alapul szolgál a kettő összekeverésére!)

Bulgáriai eredetű, igen rövid vírus. Nem a Tiny család tagja. A .COM állományokat fertőzi, beleértve a COMMAND.COM-ot is. A hagyományos DOS memória tetejére fészkeli be magát. A CHKDSK 1024 bájt helyfoglalást jelez vissza. Az INT 21-et magára irányítja. A COM programok hosszát 256 bájttal növeli, a vírus a fertőzött állományok elejére épül be.

A vírus neve: Happy New Year

Egyéb elnevezése: Happy N.Y., 1600, V1600.

Hossza: 1600 bájt.

Kódtípusa: A .COM és .EXE állományokat fertőzi meg, felülíró.

Azonosítása: F-Prot 1.14+, Scan V74+.

Eltávolítása: F-Prot 1.14+.

Leírása: A bolgár vírusgyártók terméke, valószínűleg középiskolások írták ezt a programvírust. Az 1600 bájt hosszú vírusban a következő belső rendszerüzenetet találjuk:

```
Dear Nina, you make me write this virus; Happy new year!
1989
```

(Kedves Nina! Te késztetsz ennek a vírusnak a megírására. Boldog új évet! 1989)

Az üzenet sohasem jelenik meg a monitoron.

A program meglehetősen primitív, bár a célnak igencsak megfelel. Terjedé-

sét korlátozza, hogy felülírva tönkreteszi az állományokat, többek között a COMMAND.COM-ot is, ami meglehetősen gyerekes vírusprogramozási hiba. A károsodott programokat csak a fertőzetlen állományokkal lehet felülírni. Hex 00-val írja felül a víruskódnál hosszabb állományok maradékait. Csak detektálható. A rendszermemóriából 2432 bájtnyi helyet foglal el a rendszer alsó részén. Az INT 21-et magára láncolja, mint minden rendes TSR program. Az állományok végére épül be, 1600 bájt hosszan.

A vírus belepancsol a floppy bootszektorába, de ott nincs futtatható víruskód. Az eredmény a hibás betöltési folyamat és a következő épületes rendszerüzenet, ha már a COMMAND.COM fertőzött lett:

```
Bad or missing command interpreter
```

Ismert átirata:

Happy New Year B: Hasonló, mint az eredeti. Az eltérés öt bájt, aminek következtében néha a fertőzött COMMAND.COM is végrehajtódik, mert nem írja felül.

A vírus neve: Nomenklatura

Egyéb elnevezése: Nomenclature, 1024-B.

Hossza: 1024 bájt.

Kódtípusa: A .COM és az .EXE állományokat fertőző, rezidens résszel rendelkező parazita vírus.

Azonosítása: Scan V67+, Pro-Scan 2.01+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: A vírust először 1990 augusztusában észlelték Hollandiában. Valószínűleg bolgár eredetű, mert Skulason a benne található szöveget bolgár szövegként azonosítja. Ebben szerepel a vírus nevét adó Nomenklatura szó is. Bár hossza azonos, mint a V1024-é, semmi köze hozzá!

A vírus a .COM és az .EXE állományokat egyformán megfertőzi, beleértve a COMMAND.COM-ot is. A fertőzött programkód futása során a vírus a hagyományos 640 K-s DOS memória tetejére épül be, a szabad területet 1024 bájttal csökkentve. Az INT 21-et magára irányítja. Amikor a .COM és .EXE állományokat felülírja, azok 1023 bájttal lesznek hosszabbak. A különbség a felülírt szakasz, ami miatt nem helyreállítható az állomány. A vírus szerencsére ritka, ténykedéséről csak szakirodalmi adatokkal rendelkezünk. Egyes esetekben nem rombol, ilyenkor a hosszövekedés szabályos, 1024 bájt. Állománynyitáskor és végrehajtáskor egyaránt fertőz. A hossznövekedést nem rejti el a DOS DIR parancsa elől.

Ha fertőzetlen programot akarunk futtatni írásvédett lemezről, akkor azt nem hajtja végre, hanem az alábbi üzenetet produkálja:

```
Sector not found error
```

A vírus igen romboló, talán ezért is nem volt képes jobban elterjedni. A károsítás véletlenszerűen történik, adat- vagy programállományt egyaránt érhet. Időnként a szektor puffer területén egymásra írja a szavakat, vagy a hecc kedvéért tönkretesz néhány clustert a FAT területen és a bootrekordban. A tönkretett clusterekre kerülő állományrészletek természetesen olvashatatlanok lesznek.

A vírus neve: MG

Egyéb elnevezése: Még nem ismeretes.

Hossza: 500 bájt.

Kódtípusa: Parazita, rezidens résszel, .COM fertőző.

Azonosítása: Scan V74+.

Eltávolítása: Törölni a fertőzött programokat.

Leírása: Ilyen vírusról már olvashattunk az orosz bacikról szóló fejezetben. Két matematikai iskola párbeszéde zajlik a vírusok közvetítésével. (Miként a szerelmi levelezés a bolgár Nina kisasszonnyal.)

Az MG vírusra 1991 januárjában leltek rá. Forrása a Várnában található matematikai gomnázium. Ott bizonyíthatóan az iskolaév kezdete alkalmából írták, 1990 szeptember elején.

A vírus memóriarezidens, a memóriában lévő interrupt táblába rejti el magát. (Nagy ötlet, hiszen ki keresné ott?) Az INT 21-et és más időleges megszakító vektorokat is magára irányít. A fertőzés akkor történik, ha kiadjuk a DOS DIR parancsát vagy pedig elindítunk egy programot. Ha abban a könyvtárban, ahonnan egy programot elindítottunk, már van fertőzött, akkor nem fertőz. Amikor a DIR parancsot adjuk ki, akkor az adott könyvtárban csak egyetlen programot fertőz meg.

A COM programok hossza 500 bájttal növekszik csak meg, de a vírus (amíg a memóriában van) ezt a növekedést elrejti. A könyvtárbejegyzések időadatait nem módosítja. A fertőzés során a programállomány végére épül be. Ha a vírus jelen van a memóriában és kiadjuk a CHKDSK parancsot, akkor a DOS

```
File allocation errors
```

hibaüzenetet ad, és az összes .COM programot megfertőzi! Ilyenkor a DIR parancs sem működik többé. Ha kiadjuk a meghajtóra a DIR parancsot, akkor — bár jó pár .COM program van rajta — az állományok hiányára utaló DOS rendszerüzenetet kapunk. Mivel a memória megszakító (interrupt) táblájában ücsörög, néha előfordul, hogy egy-egy speciális rendszerhívást nem tud lekezelni. Ilyenkor a rendszer kiakad.

Rokona az MG-2 és az orosz vírusokról szóló fejezetben található MGTU vírus.

A vírus neve: MG-2

Egyéb elnevezése: Még nem ismeretes.

Hossza: 500 bájt.

Kódtípusa: A .COM állományokat fertőző parazita program, rezidens résszel.

Azonosítása: Scan V74+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: A várnai gimnazisták ezt a változatot egyszerre engedték el az előzővel. Valószínűleg egy fejlesztési stádiumban lévő vírus különböző készültségi szintjén készített fordításokról van szó. Memóriarezidens, COM fertőző program. A COMMAND.COM-ot is fertőzi. A fertőzés során az állománynövekedés 500 bájt, és a vírus a programok végére épül be.

Lefutása után a fertőzött programkód beépül a memóriába. Időlegesen számos megszakítót elvesz, főképpen azonban az INT 24-et irányítja magára. A CHKDSK a rendszerről a vírus jelenlétében 55 104 bájt memóriacsökkenést jelez vissza. A memóriában a 640 K-s hagyományos DOS memória fölé is képes beülni!

A memóriarezidens vírus egyszerre csak egy .COM állományt fertőz meg egy könyvtárban. Amikor a vírus a memóriában aktív, a hossznövekedést a DOS DIR parancsa nem mutatja. A CHKDSK minden fertőzött állományra „File allocation error" hibaüzenetet ad. Hasonlóan a DIR parancs esetéhez a fertőzött állományokat nem látja, és „File not found" üzenettel jön vissza.

Ismert változatai:

MG-3: Teljes funkcionális kópiája az MG-2-nek. Eltérés, hogy más eljárást kell alkalmazni a felismerésre, mert más a szekvenciája. Szintén 500 bájt hosszú.

Oktatni veszélyes!

Amstrad, Pixel/V-345, V-277, V-299, V-847, V-847B, V852, Tester, Number One, Virus-90, Virus101, 405, VirDem, Proud.

A vírusírás elég bonyolult programozási technika. Ezért egyesek úgy gondolták, hogy a módszerek oktatásából is hasznot lehet húzni. Számos vírusváz, kereskedelemben is megvásárolható fejlesztő egységcsomag készült, amelyek eszközzé váltak újabb vírusok készítéséhez.

Meg kell azonban különböztetni tőlük a valóban oktatási célú vírust, amely „éles bevetésre" azért alkalmatlan, mert azonnal lebukik. Ilyen például az a potyogós, amelyet egy pesti gyerek írt Turbo Pascalban. Mindössze 550 K méretű. Hasonló jellegű volt Ralph Burger könyveiben a Basic nyelven publikált oktató vírus. (Ugyanakkor van Burger elnevezésű valódi vírus is, amihez Ralph Burgernek semmi köze.)

Előfordult már — külföldön és Magyarországon is —, hogy egy korábbi vírusíró „átállt", és addigi tevékenységét feladva az antivírus kutatásnak szentelte tudását. Ilyenkor egy a lényeg: az illető valóban hagyjon fel a vírusírással és csak a vírusvédelemmel és -irtással foglalkozzék. A szakma nagy nyereségei ők, mert ugyebár, rablóból lesz a legjobb pandúr...

A vírus neve: Amstrad

Egyéb elnevezése: Még nem ismeretes.

Hossza: 847 bájt. (Valójában 850, mert a vírus végén 3 bájt nulla van.)

Kódtípusa: Parazita, rezidens része nincs, a .COM állományokat fertőzi meg.

Azonosítása: Scan/X V67+, F-Prot, IBM Scan, Pro-Scan, VirexPC 1.1+, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: Scan /D, F-Prot, valamint a fertőzött állományok törlése.

Leírása: Az Amstrad vírusra a vírusszakértők közül először Jean Luz figyelt fel 1989 novemberében, Portugáliában, de az valószínűleg már korábban megjelent Spanyolországban is. Maga a vírus általános .COM fertőző, és bár nem memóriarezidens, nem fertőzi meg a COMMAND.COM-ot sem, nehogy idő előtt észrevegyék.

A vírus az Amstrad számítógép-hamisítványokat jelzi. Nem okoz más kárt a rendszerben, mint azt, hogy megfertőzi az állományokat és kimutatja jelenlétét. Kódját Portugáliában, a Pixel számítástechnikai magazinban írták le, ez-

által mintegy megalapítva a Pixel családot. (Nem éppen etikus magatartás egy számítástechnikai lap részéről.)

Az Amstrad vírus „iskolát" teremtett, oktatási célra hihetetlenül sokan átírták. Bulgáriában is népszerű nyersanyag lett. Leszármazottainak követésére érdemes megnézni a könyv végén található családfát.

Az Amstrad vírus átiratai:

Pixel/V-345: Ez az átirat Görögországban készült 1990-ben. Hasonló az alapvírushoz. Eltér a hosszában (345 bájt), és abban, hogy megfertőzi a COMMAND.COM-ot, továbbá szöveges üzenetet is tartalmaz:

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

(Programbetegség hiba: Hívjon orvost vagy vásároljon Pixel magazint, ahol megtalálja a gyógymód leírását)

V-277: Hasonló a Pixel/V-345 vírushoz azzal az eltéréssel, hogy csak 277 bájt hosszú, és nem tartalmaz üzenetet. A szöveg helyére applikáltak egy gépi kódú rutint, amely a fertőzött programoknak mintegy felénél paritáshibát okoz, és elküldi a rendszert „vadászni". Ezt a verziót Bulgáriában stoppolták össze, alapos szaktudással.

V-299: Bolgár remekmű, teljesen hasonló az eredeti Pixelhez, csak a kód hossza tér el: 299 bájt.

V-847: Szintén hasonló az eredeti Pixelhez, de a kódot újrafordították, s ezúttal 847 bájt hosszúra sikeredett. Az akciót Bulgáriában hajtották végre.

A Pixel magazinban a V-847 vírusnak is publikálták a (Basic) forráskódját. Nem csoda tehát, hogy hamarosan víruscsalád kerekedett belőle. A lefordítás után keletkező .COM program igazi „élő" vírus, melynek működése ugyan nagy hülyeség, de mint sok más értelmetlen őrület, ez is népszerűvé vált, és a vírus az egyik legelterjedtebb átírási nyersanyag.

A V-847 vírus az aktuális lemezen az aktuális könyvtárban lévő .COM programokat fertőzi meg, és a fertőzést mindaddig ismétli, amig névjegyét az adott könyvtár összes programjára rá nem teszi. Nem memóriarezidens, tehát csak akkor aktivizálódik és fertőz, ha egy vírussal már megfertőzött programot elindítunk. A vírus a .COM programok elejére épül be, 847 bájttal. Minden fertőzött fájl tartalmazza a vírus úgynevezett generációs számát, amelynek az 5. generációig nincs jelentősége. Az 5. generáció után a generációs bájt alsó részét (1/2 bájt) megváltoztatja a rendszerórával történő véletlenszám-generálással. Ha ezt a műveletet másodszor is megismétli, akkor megjelenik a képernyőn a már ismert üzenet:

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

Ezt követően a vírus kilép, a vírushordozó programot nem engedi lefutni.

Az új vírusok kódját optimalizálták, kisebbre vették. A Bulgáriában átírt és onnan elterjedt két ismert verzió hossza 299 és 345 bájt. (A részletekről bővebben a többi leírásban.)

V-847B: Az előző bolgár átirat spanyol honosítása. Mindössze annyiban különbözik, hogy a szaporodás ötödik generációjában a következő spanyol nyelvű üzenetet jeleníti meg:

```
=!= En tu PC hay un virus RV1, y esta es su quinta
generacion
```

(Az ön PC-jében egy RV1 vírus van, amely már az ötödik generáció)

A vírust egy spanyol számítástechnikai magazin mellékletének lemezén lévő NOCARGAR.COM programállományba építették be.

V-852: A V-857 átirata, de nem tartalmazza annak teljes szövegét. Az aktuális könyvtárban minden .COM állományt megfertőz, ha ott van a COMMAND.COM, akkor azt is. Ez a változat ellenőrzi a .COM állományok 4. és 5. bájtját, s ha az SS, akkor az állományban a vírus már benne ül!

A fertőzött programok a hexadecimálisan megadott következő karaktersorozattal indulnak, amelyben az nn a vírusgenerációk száma:

EB14905353nn2A2E434F4D004F040000

A vírus neve: Tester

Egyéb elnevezése: TestVir.

Hossza: 1000 bájt.

Kódtípusa: Nem rezidens, parazita, a .COM programokat fertőzi meg.

Azonosítása: Scan V76+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: A Tester vírus eredete ismeretlen. Valószínűleg valamilyen intézmény készítette tesztelési vagy oktatási célból. 1991 április elején bukkant fel az USA-ban, majd Európára is átterjedt. A vírus nem rendelkezik rezidens részszel, minden .COM programot megfertőz, belelértve a COMMAND.COM-ot is. Az első menüvezérlésű vírus!

Amikor elindítunk egy Testerrel fertőzött programot, rögtön láthatóvá válik a vírus menüje, amire a felhasználónak kell válaszolnia:

```
This is TESTVIRUS B V1.4 !
1 = infect COM-files of this directory + run orig. prog.
5 = run only orig. program
9 = abort
```

(Ez a Tesztvírus B V1.4! 1 = Ebben a könyvtárban megfertőzöm a .COM állományokat, majd lefuttatom az eredeti programokat. 5 = Csak az eredeti programot futtatom. 9 = Kilépek.)

A továbbiakban a kapott válaszoknak megfelelően cselekszik. Az 1-es alternatíva esetén fertőzés közben annak előrehaladásáról is tájékoztat a képernyőn. Ha az adott könyvtárban még nem volt fertőzött program, akkor a következő üzenetet küldi:

```
INFECTED: - - - - - - - >  xxxxxxxx.COM
```

(Megfertőzve: állománynév.COM)

Ha már volt fertőzött program, akkor a következő kiírást kapjuk:

```
Already infected:  xxxxxxxx.COM
```

(Már fertőzött: állománynév.COM)

Az 5-ös menüpont választása esetén csak az eredeti programkód fut le, fertőzés nélkül, míg 9-esre a program fertőzés és végrehajtás nélkül kilép a DOS-ba. Egy nagyobb vírus viszonylag ártalmatlanná tett változatának tűnik, amire a menüpontok foghíjas számozása is utal. Vajon ki és mire készítette az eredetit?

A fertőzött programok 1000 bájttal lesznek hosszabbak. A vírus a .COM állomány elejére épül be. A könyvtári bejegyzést átállítja a fertőzéskor érvényes rendszeridőre és dátumra.

A vírus neve: Number One

Egyéb elnevezése: Number 1.

Hossza: 12 032 bájt.

Kódtípusa: *Nem rezidens, .COM fertőző.*

Azonosítása: SCAN V76+.

Eltávolítása: Törölni a fertőzött állományt.

Leírása: A vírust új vírusként 1990 szeptemberétől jegyzi a szakirodalom, pedig valójában egy ősi darab. M. Vallane 1987 októberében írta Turbo Pascal V3.01A programnyelven. (Ezért ilyen hosszú.) A kódot Ralph Burger egyik könyvében teljes egészében közölte. Valaki itt fedezte fel, újra lefordította és 1990 nyarán útnak indította.

A vírus nem rezidens, fertőzés közben felülírja és ezzel tönkreteszi a .COM állományokat. Egy terjedési tesztvírusról van szó. A víruskódot az állomány elejétől kezdve *ráírja a fertőzendő állományra. Ha az rövidebb volt, akkor* 12032 bájt lesz, ha hosszabb, akkor a hossza nem változik. A könyvtári bejegyzés dátumát kicseréli a fertőzéskor aktuális rendszerdátumra és időre.

A fertőzés végén a következő rendszerüzenetet küldi a monitorra:

```
This File Has Been Infected by Number One!
XXXXXXXX.COM infected.
```

(Ezt az állományt a Number One fertőzte meg! A programnév.COM fertőzött.)

Ha valamelyik állományban már benne van, akkor azt nem fertőzi meg újra, hanem a következő üzenettel boldogít bennünket:

```
This File Has Been Infected by Number One!
<Smile>
```

(Ezt az állományt a Number One fertőzte meg! <Mosolyogni>)

Nem fertőzi meg a csak-olvasható attribútumú állományokat. Sajnos egyedül a fertőzött állomány kitörlése segít, mert amit felülír, azt nem menti el sehová.

A vírus neve: Virus-90

Egyéb elnevezése: Még nem ismeretes.

Hossza: 857 bájt.

Kódtípusa: Parazita, rezidens része van, a .COM állományokat fertőzi meg.

Azonosítása: ViruScan/X V67+, F-Prot, IBM Scan, Pro-Scan 1.4+, VirexPC, AVTK 3.5+.

Eltávolítása: Scan /D, F-Prot vagy a fertőzött állományok törlése.

Leírása: A Virus-90 Patrick Toulme által oktatási célzattal készített és forráskódban is árusított program volt. Forgalmazása 1989 decemberében kezdő-

dött az USA-ban. Akkor 20 dollárért bárki hozzájuthatott. 1990 januárjában már széles körben elterjedt, a szellem kiszabadult palackjából. Csak terjed, mást nem csinál. Sajnos azonban más vírusszerzők hordozórutinként kezdik használni saját, már kártékony programjaikhoz. 1990 novemberében a szakemberek tiltakozására Patrick Toulme a következő nyilatkozatot adta ki:

„Ez egy oktatási és kutatási céllal készült vírus, amelyet Patrick Toulme a vírustevékenység közvetlen tanulmányozására és a vírusoknak ellenálló szoftverek kifejlesztéséhez segédeszközként fejlesztett ki. A vírus egy egyszerű .COM fertőző program, a merevlemezen nem is képes rátelepedni az állományokra, csak a floppyn. A megfertőzött állományokat nem károsítja, de feltételezhető, hogy a vírust és a fertőzött állományokat a felhasználó ennek ellenére kitörli. Biztonsági okokból, hogy a szerző megelőzze a véletlen fertőzéseket és a visszafejtést, a vírus kódja igen bonyolult. A Virus-90 csak a vírusellenes szövetségek és a víruskutató szakemberek számára hozzáférhető."

A szellemet azonban a nyilatkozatban foglalt állítás ellenére nem sikerült a palackban tartani. A Virus-90-ből, lelkiismeretlen vírusgyártók jóvoltából, új ötletekkel megspékelt — és már romboló — vírusvariációk születtek.

A vírus neve: Virus-101

Egyéb elnevezése: Még nem ismeretes.

Hossza: 2560 bájt.

Kódtípusa: Parazita, rezidens része van. Minden végrehajtható programállományt megfertőz, beleértve a COMMAND.COM-ot is.

Azonosítása: Scan/X V67+, Pro-Scan 1.4+, F-Prot 1.12+, VirHunt 2.0+.

Eltávolítása: Scan /D vagy törölni minden fertőzött állományt.

Leírása: A Virus-101 a „big brother", azaz a Virus-90 programvírusnak orwelli értelemben vett „mindent figyelő nagy testvére". Szintén Patrick Toulme írta, oktatási segédeszközként, 1990 januárjában. A vírusnak van memóriarezidens része, a fertőzött állományokat figyeli, hogy hol vannak. Amennyiben megfertőzött minden fertőzhetőt, akkor a boot-rekordba is beépül. A jelenleg ismert verzió kizárólag floppylemezt képes megfertőzni!

A vírus első elindítása után nagy piros ablakban megjelenít egy szöveget, majd folyamatosan pörgeti a floppy meghajtó motorját. Ha a floppymeghajtóba nem teszünk lemezt, akkor a rendszer újraindításáig folyamatosan így fog működni. A meghajtóba floppyt téve a vírus azonnal meg akarja fertőzni a COMMAND.COM programot. Megjelenített rendszerüzenete a következő:

```
VIRUS 101
Copyright 1990
Patrik A. Toulme
Suite #104
2007 N. 15th Street
Arlington, VA 22201
(703) 836-9340 Ext. 225
This file has been safely infected by
VIRUS101 - the safe, education virus utility.
This copy furnished to XY.....
```

(Ez az állomány szerencsésen megfertőződött a VIRUS 101-gyel, a megbízható oktatási vírus-segédprogrammal. Ez a példány X.Y. rendelkezésére bocsátva.)

Ha egy állományt megfertőzött, akkor a rendszert összeomló képernyővel újraindítja. A betöltés hangeffektusokkal is jár.

Az X.Y. helyén minden példányon egy-egy ismert nyugati antivírus szakember neve szerepel, meglehetősen bonyolult algoritmussal kódolva.

Patrick Toulme ez esetben is magyarázkodni kényszerült:

„A Virus-101 egy kifinomult, önmagát folyamatosan titkosító vírus, amelyet a Virus-90 szerzője, Patrick Toulme írt. A vírus a .COM és az .EXE állományokat fertőzi meg, és lehetővé teszi az antivírus szoftverek és a víruskeresők számára a nem algoritmikus keresés tesztelését egy önmagát folyamatosan módosító víruson. A vírushoz csak állami ügynökségek és szervezetek biztonságtechnikai csoportjai férhetnek hozzá az antivírus programok és hardvereszközök tesztelésére."

A vírus neve: 405

Egyéb elnevezése: VirDem.

Hossza: 405 bájt.

Kódtípusa: Felülír, nincs rezidens része, a .COM állományokat fertőzi.

Azonosítása: Scan, F-Prot, IBM Scan, CHKSeq v.1.0.

Eltávolítása: Scan /D, F-Prot vagy törölni a fertőzött állományokat.

Leírása: 1987-ben bukkant fel. Korát tekintve tehát már öregnek számít a vírusok világában. A 405-ös nevet viselő, felülíró típusú vírust kiveszettnek vélték, mert alig jelent meg róla publikáció. Ausztriából, Salzburg környékéről származik, többen tévesen hiszik NSZK eredetűnek.

Csak a .COM állományokat fertőzi meg az aktuális könyvtárban. Az eredeti állomány 405 bájtnál kisebb mérettel nő, az eredeti vírushossz azonban mindig 405 bájt. A saját hosszúsága és a növekedés hossza közötti különbség az a szakasz, amelyet helyrehozhatatlanul felülír. A vírus folyamatosan felismeri a már fertőzött állományokat, de azért újra meg újra megfertőzi őket. A szakirodalomban nincsenek részletesebb adatok ennek a sajátos vírusnak a működéséről.

A vírus neve: VirDem

Egyéb elnevezése: VirDem 2.

Hossza: 1236 bájt.

Kódtípusa: Nem rezidens, .COM fertőző, parazita vírus.

Azonosítása: VirexPC, AVTK 3.5+, F-Prot 1.12+, ViruScan V71+, VirHunt 2.0+, Pro-Scan 2.01+.

Eltávolítása: F-Prot 1.12+ vagy törölni a fertőzött állományokat.

Leírása: VirDem elnevezéssel egymástól lényegesen eltérő két vírus is forog közkézen. A 405 bájtos destruktív, felülíró VirDem előző leírásunkban szerepelt. A másikat demonstrációs anyagnak, írásos programpéldaként készítette Ralph Burger német vírusszakértő. A szerző ezt gépi formában soha nem is terjesztette, hanem a könyv alapján gépelték be mások, és nyersanyagnak hasz-

nálták saját víruskódjuk terjesztésére. A vírusforráslista a „Computer Viruses: A High-Tech Disease" című könyvében annak illusztrálására jelent meg, hogyan dolgozik egy közvetlenül fertőző, nem rezidens vírus. A könyvet a Német Alkotmányvédő Hivatal egyik szakértőjének javaslatára „elsüllyesztették", nem szerezhető be sem angol, sem német nyelvű kiadása, de még könyvtárakból is csak igen nehezen. Olaszul kalózkiadásban jelent meg.

A VirDem ezen változata a felülírt szakasz kódját korrektül elmenti az állomány végére. A számos létező verzió főleg a vírusban lévő szöveg nyelvében tér el, attól függően, hogy a könyv angol vagy német kiadásából írták-e le a kódot.

A vírus nem memóriarezidens, és csak az A: meghajtó .COM állományait fertőzi meg. Kihagyja a katalógusban első helyen bejegyzett állományt, de a COMMAND.COM-ot is békén hagyja. Nem fertőzi meg a második szint alatti alkönyvtárak állományait sem. Ha a .COM állomány nagyobb mint 1500 bájt, akkor a hossznövekedés 1236 bájt.

A vírus nem titkosítja magát, és szinte játszik a felhasználóval. A vírus elindulásakor az angol verzióban a következő üzenet jelenik meg:

```
VirDem Ver.: 1.06 (Generation %%) aktive.
Copyright by R.Burger 1986,1987
Phone.: D - xxxxx/xxxx
This is a demoprogram for
computerviruses. Please put in a
number now.
If you're right, you'll be
able to continue.
The number is between
0 and #
```

(Ez számítógépvírusok demóprogramja. Kérem, írjon be egy számot. Ha eltalálta, akkor folytathatja. Ez a szám 0 és # között lehet.)

A % jel helyén a vírus elindítása óta lefutott generációk száma, az x-ek helyén pedig Burger telefonszáma szerepel, arra az esetre, ha a vírus elszabadulna. Amikor a felhasználó jó számot ír be, akkor tovább fut a program, ellenkező esetben viszont nem, s helyette a következő üzenetet kapja:

```
Sorry, you're wrong
More luck at next try ....
```

(Sajnos tévedett. Több szerencsét, és próbálja meg újra.)

Amikor valaki eltalálja a generációs számot, akkor a fertőzött programkód lefut, és a következő üzenet jelenik meg:

```
Famous. You're right.
You'll be able to continue.
```

(Pompás. Eltalálta. Most folytathatja.)

Végezetül, ha az A: meghajtón fertőzhető állományokat talál, megfertőzi azokat, és a következő üzenetet küldi:

```
All your programs are
struck by VIRDEM.COM now.
```

(A VIRDEM.COM most már az ön összes programját eltalálta.)

A VIRDEM.COM az a trójai program, amellyel a VirDem vírust terjesztik.

Mellette általában ott található a VIRDEM.DOC állomány is, amely elmondja a fentieket. A program nem destruktív és szerencsére igen ritkán fordul elő.

Ismert változata:

VirDem 2: Az angol verziónál korábban készült. Egyetlen eltérése, hogy a VIRDEM.COM dokumentációs állomány és a vírusszöveg német nyelvű.

A vírus neve: Proud

Egyéb elnevezése: V1302, P1 Related.

Hossza: 1302 bájt.

Kódtípusa: Önmagát titkosító, .COM állományokat fertőző, parazita vírus, tárban maradó része van.

Azonosítása: Scan V71+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: Veszelin Bocsev regisztrálta 1990 augusztusában Bulgáriában. Kész csoda, hogy az oktatásban való használata ellenére (az önmagukat titkosító vírusok tanulmányozására alkalmas) nem terjedt el nagyon széles körben. Ennek talán az is az oka, hogy nem produkál szellemes szövegeket, látványos effektusokat.

A vírus a COMMAND.COM-ot is beleértve az összes .COM állományt fertőzi. A tárban való installálódás után figyeli, hogy az INT 13-at használja-e másik program. Ha igen, akkor a rendszert lemerevíti, nehogy hibaszűrést (debugging) lehessen végezni. Ezt a trükköt alkalmazza számos másolásvédelem is. Ha az INT 13-on nem ül semmi, akkor a 640 K-s hagyományos DOS memória felső részében rezidenssé válik. A szabad memória méretét 8192 bájttal csökkenti és az INT 2A vezérlését magára irányítja.

Amikor a vírus rezidens, elkezd vadászni fertőzhető .COM állományokra, amelyeknek a következő hossz-tartományokba kell esniük:

2 048 — 14 335 bájt
16 384 — 30 719 bájt
32 768 — 47 103 bájt
49 152 — 63 487 bájt

A vírus önmagát nemcsak titkosítja, hanem szét is tördeli. Az állományban két helyen van a kód két különböző titkosított részlete. Nem is tudja felismerni, hogy már benne van-e az állományban, ezért többször is megfertőzi azt. Talán az ebből adódó túlszaladás megakadályozására szolgál a fenti hosszkritérium-korlátozás? Érdekessége még, hogy 256 fertőzés közül egy esetben a FAT táblában eltünteti az egyes állományok, könyvtárak belépési pontját.

A fertőzött programok 1302 bájttal lesznek hosszabbak, kivéve a COMMAND.COM-ot, amely ugyanakkora marad, mert a vírus beépül, és részleteit a 00h részekre írja felül. Ezt a trükköt később tökéletesítve alkalmazták a Zerohunt vírusban.

Három szapora család

Vacsina, TP Worm, Vacsina-B, TP4, TP5, TP6, TP16, TP23, TP24, TP25 TP33, TP34, TP38. TP41, TP42, TP44, TP45. Yankee-2, 1624, Tiny Family, Tiny-133, Tiny-134, Tiny-138, Tiny-143, Tiny-154, Tiny-156, Tiny-158, Tiny-159, Tiny-160, Tiny-167, Tiny-198, Tiny Virus, Enigma, Alameda, Golden Gate, Golden Gate-B, Golden Gate-C, SF, Devil's Dance, Joker.

A vírusirodalomban talán ezzel a három vírucsaláddal foglalkoztak eddig a legtöbbet. A Tiny, a Yankee Doodle és a Vacsina olyannyira jól sikerült, hogy kódjukat állandóan átbarkácsolják, így változataik mindig újraélednek.

Fejezetünket kissé rendhagyóan egy bizonyos bolgár „úr" (T. P.) viselt dolgainak ismertetésével kezdjük. T. P. ugyanis egy gyenge pillanatában megírta élményeit és szétterítette azokat a számítógépes alvilág csatornáin. Innen tudjuk, hogy ő a Vacsina és a Yankee Doodle programok szerzője. Angol nyelvű vallomása annyi programozástechnikai részletet tartalmaz ezekről a vírusokról, hogy nagy valószínűséggel a többi információ is igaz.

Ezeket a víruscsaládokat azért tárjuk közös fejezetben olvasóink elé, mert mindegyik egy-egy érdekes új ötlettel vagy kihívással jelentkezett. A Tiny provokálta a „ki tudja a legrövidebb és a legnagyobb kárt okozó vírust írni" nemtelen programozói versenyt. A Vacsina vezette be az .EXE és a .COM állományok közötti konverziót, és azt, hogy előbb ráteszi az EXE-COM konvertert az EXE állományra, majd a második lépcsőben fertőz. A Yankee Doodle terjesztette el a felhasználó egyetértése nélkül történő zenélés szokását. A munka végére és az ötórai teára figyelmeztető dal azért lett éppen a Yankee Doodle, mert a programozó véletlenül ennek a forráskódjához jutott hozzá.

A Vacsina/Yankee Doodle víruscsalád

A számítógépvírusok fogalomkörében célszerűnek látszik bevezetni a „víruscsalád" fogalmát. Egy családba sorolhatjuk azokat a vírusokat, amelyek (feltehetően vagy bizonyosan) ugyanattól a szerzőtől származnak, illetve mások által, de a forráskód ismeretében íródtak. Ugyancsak családtagnak számítanak

a vírusátiratok, a családfőn végzett kisebb-nagyobb módosítás alapján készült változatok.

Hogyan lehet megállapítani, hogy egy vírus ugyanattól a szerzőtől származik? Többféleképpen is. Például igen kicsi a valószínűsége, hogy egy adott feladatot két programozó egymástól függetlenül dolgozva ugyanúgy oldjon meg. Mindegyiküknek más a programozási stílusa is. Ha egy vírust vagy bármely más programot visszafejtünk és megnézzük programozási megoldásait, abból a szerző elég jól azonosítható, feltéve, hogy egyéb programjait ismerjük. A személyes kapcsolatokon keresztül szintén elég pontos információkat lehet szerezni. Könyvünk anyagának összegyűjtésekor mi is felhasználtunk ilyen forrásokat, de természetesen nem hivatkozhatunk rájuk, nehogy veszélyeztessük őket. Végül a kutatómunkában igen hasznosak a „bűnbánó", vagyis átállt vírusprogramozók információi.

Hogyan keletkezett a TP víruscsalád? A TP vírusokat Bulgáriában fejlesztették ki. A víruscsalád nevét a szerző nevének kezdőbetűiből kapta. T. P. Emlékirataiból kiderül, hogy mint sok más programozót, őt is érdekelték a számítógépvírusok. Kellő előképzettség megszerzése után egyszer csak úgy döntött, hogy megírja saját vírusát. Alkotása sajnos sikeresen működött. Ezt követően vírusmegelőzéssel kezdett el foglalkozni. Újabb vírusokat fejlesztett ki, és azokhoz igazítva tökéletesítette vírusvédelmi programját is. Végül is több mint 50 vírust készített. Az egyes vírusverziók számát hexadecimálisan feltüntette a fertőzött program utolsó előtti bájtján.

T. P. „device driver"-nek tervezte vírusmegelőző rendszerét. Későbbi vírusai képesek is voltak kommunikálni ezzel az eszközmeghajtóval. A vírusmegelőző device driver a „VACSINA" nevet írta ki, ha meghívták. A „VACSINA" elnevezés megfelel a francia vaccine vagy a magyar vakcina szónak. A vírusmegelőző program a későbbiek során nem ellenőrizte a „VACSINA" név cirill betűs megfelelőjét.

Az általa kifejlesztett összes vírus felülről kompatibilis. Magasabb verziószámú vírusai úgy fertőzik meg a fájlokat, hogy az alacsonyabb verziószámúakat eltávolítják onnan. Ez fordítva nem igaz. Ha egy fájlt először Vacsina vírussal fertőzünk meg, majd ezt követően a Yankee Doodle vírussal, a Yankee Doodle először eltávolítja a Vacsina vírust (a vírus egy kis darabja ott maradhat — EXE-COM converter) és csak ezt követően fertőzi meg a fájlt. Fordított sorrendben, tehát a Yankee Doodle vírussal történt fertőzés után a fájlt Vacsina vírussal már nem tudjuk megfertőzni.

A T.P. által készített vírusok nem tartalmaztak pusztító (destruktív) rutint. Ugyanakkor a víruscsalád kifejlesztése során egyre több trükköt használt fel, és egyre jobban kihasználta a DOS operációs rendszer működését. Egyik vírusverzióját a DOS I/O kihasználatlan pufferében rejtette el, egy másik vírusa az .EXE programok fejlécében található üres helyre telepedett be. Később olyan vírusok kifejlesztésével foglalkozott, amelyeket az INT 13 és INT 21 megszakítók változását figyelő vírusellenes programok sem vesznek észre.

Sajnos a teljes TP víruskollekció tudomásunk szerint senkinek nincs meg, az alacsonyabb vírusverziókat még a szerző sem tartotta meg magának. A „fenn-

maradt" összes TP memóriarezidens .COM és .EXE állományokat fertőz, de rezidenssé válásuk (memóriába történő beépülésük) és az .EXE programok megfertőzésének módja különböző.

Az alábbi táblázat a birtokunkban lévő TP vírusok verzióját, a fertőzhető programok minimális hosszát és a fertőzési vírusméretet tartalmazza, a méretadatokat bájtban megadva.

Vírusnév	Verziószám	Minimális fájlméret	Vírusméret
Vacsina	4	1213	1215
Vacsina	5	1207	1215
Vacsina	6	1270	1279
Vacsina	16	1340	1343
Vacsina	23	64	1753
Vacsina	24	64	1760
Vacsina	25	64	1805
Yankee Doodle	33	64	2680
Yankee Doodle	34	64	2568
Yankee Doodle	38	64	2756
Yankee Doodle	41	64	2932
Yankee Doodle	42	64	2997
Yankee Doodle	44	64	2885
Yankee Doodle	45	64	2901
Yankee Doodle	46	64	2981

A TP sorozat

TP04: Az első sikeres TP vírusok egyike. Elég gyakori Bulgáriában. Ha a vírussal megfertőzött programot elindítjuk, vagy amikor a vírus éppen fertőz, egyszerű hangeffektust ad (ASCII 7).

A DOS az .EXE programokat nem a nevük, hanem a programban lévő első két bájt alapján („MZ") ismeri fel. A TP víruscsalád is mindig ellenőrzi a programok első két bájtját. Még nem találkoztunk olyan hagyományos .EXE programmal, amelyben elöl a felcserélt „ZM" szignatúra lenne, de a TP víruscsalád tagjai ilyenkor is működőképesek. Ezt arra használják ki, hogy álcázzák vele magukat: megváltoztatják az .EXE MZ jelét ZM-re.

A 37. vírusverzióig T. P. még nem dolgozta ki, hogyan kell az .EXE programokat megfertőzni. Ennek megfelelően az .EXE programokat a DOS EXE2BIN konverteréhez hasonló módon átkonvertálta COM programokká. Természetesen az átalakított .COM programok mérete maximálisan 64 Kbájt lehet, így a TP vírusok is csak ennél kisebb EXE programokat fertőznek meg. A konverzió hatására viszont az addig .EXE-ként működött programokat a csak

.COM programok megfertőzésére képes más vírusok (1701/Cascade, Vienna) szintén megfertőzhetik.

TP05: Hasonló mint a TP04, csak a fertőzött programok nem pittyegnek (beep).

TP25: Ez a vírus már nem tartalmazza a „VACSINA" karaktersorozatot és hangeffektusa is más: ha Ctrl-Alt-Del-lel melegindítást kérünk, előbb eljátssza a Yankee Doodle zenéjét, és csak utána engedi betölteni az operációs rendszert.

A TP25 vírus néhány új trükköt is rejtegetett magában. A vírus új funkciója az INT 21 — 0C5 opció. A vírus ezt az opcióját memóriarezidenssé válásához, a memóriában az installáltság vizsgálatához, a fertőzés KI/BE kapcsolásához, valamint a memóriából és a fájlból történő eltávolításához (önpusztítás) használja. A későbbi vírusverziókban ezt a funkciót a szerző áthelyezte a 0C6 funkcióhívásra.

TP33: E vírus készítésekor értesült T. P. arról, hogy valaki romboló jellegűvé írta át az ő vírusait. Ezért új vírusába önkorrekciós rutint épített be, ami azt jelenti, hogy a vírus ellenőrzi a fertőzési műveleteket, és ha más vírusverziót (átírt vírust) talál, kijavítja azt. A vírus önkorrekciós rutinja azonban nem mindig működött tökéletesen, néha rendszerösszeomlást okozott.

Az önkorrekciós vírustípusokra az jellemző, hogy saját kódjukat többször is (redundánsan) tartalmazzák, általában tömörített formában. Ha valaki megváltoztatja a kódot, akkor a benne lévő információ alapján az eredeti állapotot állítja vissza.

Ez a vírus volt a sorozat első olyan darabja, amely anti-debug (visszafejtésellenes) rutint is tartalmazott. Alkalmazott továbbá másolásvédelmi programok által használt trükköket is (debugger kikapcsolása, az INT 13 és INT 1 tartalmának megváltoztatása). Ez a vírus játszotta először a Yankee Doodle zenét délután 5 órakor, nem pedig a Ctrl-Alt-Del billentyűkombináció lenyomásakor. Így lett egyik elnevezése angol nyelvterületen: Ötórai tea.

TP38: Ez látszólag már teljesen más (új) vírus. Közvetlenül megfertőzi a tetszőleges hosszúságú .EXE programokat, és nem kell hozzá az EXE-COM konverzió. Másik lényeges változtatás a vírus rezidenssé válása és a vírusfigyelő programok kijátszására írt új rutingyűjtemény. A vírus anti-debug funkciója is módosult. Ha a vírus aktív a memóriában és debuggert töltünk be a fertőzött program (vírus) visszafordítására, akkor a rezidens vírus figyeli az INT 21-4B-00h funkciót és a vírust eltávolítja a fertőzött programból. (Ezzel a módszerrel magunk is kitakaríthatjuk a vírust a fertőzött programból.) Ha a vírus nem aktív a memóriában és „egyszerű" debuggereket (Debug, AFD) használunk a fertőzött program vizsgálatához, akkor a vírusprogramnak csak néhány első bájtja hajtódik végre, majd a vírus kikapcsolja a hibakeresőt és beülteti önmagát a memóriába. Ha a debugger visszatér, az eredeti program első utasítására lép, mintha a vírus ott sem lenne. Hasonló trükköket alkalmaz a DiskEye és a Fast hardlock a visszafordítás megakadályozására.

TP42: Ez a verzió tartalmazza a sorozat előző vírusainak összes trükkjét, emellett alkalmas az olasz pingpongozó vírus kiirtására is: a 255. rendszerindítás után hatástalanítja őt, s utána már csak az Italian vírus „halott" (dead body) része található meg a lemezen a hibás szektorokban.

TP44: Ez a vírus 1/8 valószínűséggel játssza el 5 órakor a Yankee Doodle-t. A „ritkított zenélés" a vírus felderítésének megnehezítését szolgálja.

TP48: A vírus hasonló elődjeihez, de fertőzés előtt az 1701 elnevezésű vírust eltávolítja.

TP Worm (Kukac): Még nincs belőle példányunk, csupán a szakirodalomból és T.P. emlékirataiból értesültünk legújabb gyermekéről a TP Worm azaz TP Kukac nevű szüleményéről. Semmi köze a hasonló nevű magyar csodához! Szerencsére eddig csak néhány víruskutató laboratóriumban lehetett vele találkozni.

A Kukac névválasztás nem éppen logikus, de nem mi neveztük el. Az eredeti vírust Microsoft C v5.0-ban írták. Ez a vírus a megszokott elvektől eltérően működik. Kihasználja, hogy a DOS COMMAND.COM-ja (parancsértelmezője) a programok végrehajtása során azonos név esetén először a .COM kiterjesztésűeket, azt követően az .EXE programokat és végül a .BAT programokat keresi meg és hajtja végre.

A vírus működési elve roppant ötletes. Nem épül be semmilyen programba. Ha belekerül a rendszerbe, akkor először a DOS által megadott elérési utakat fertőzi végig. A vírus keres egy .EXE programot. Ha az adott könyvtárban nincs ezzel az .EXE programmal azonos nevű .COM program, akkor a vírus ugyanezzel a névvel, de .COM kiterjesztéssel legenerálja önmagát. Ezt a műveletet mindaddig folytatja, amíg el nem készül az összes .EXE fájlnévvel a .COM kiterjesztésű víruspéldány. A felhasználó mindebből csak annyit lát, hogy a merevlemezen rohamosan fogy a hely, és egyes programok végrehajtása lelassul.

Nézzünk egy példát: A \PROBA könyvtárban van egy PRG1.EXE nevű programunk. Ha a vírus a PRG1.EXE programot nem találja fertőzöttnek, akkor legenerál egy PRG1.COM programot. Ezek után a PRG1 programindításra a DOS előbb a .COM programot (vagyis a vírust) futtatja le, és csak ez a vírusprogram indítja el az eredeti PRG1.EXE programot. Ezek után következzenek a vírusok tételes leírásai.

A vírus neve: Vacsina

Egyéb elnevezése: Még nem ismeretes.

Hossza: 1206 bájt.

Kódtípusa: Parazita, rezidens része van, a .COM, az .EXE, a .SYS, valamint a .BIN állományokat is fertőzi.

Azonosítása: Scan, F-Prot, Pro-Scan 1.4+, VirexPC, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: Clean V64+, Scan /D /A, F-Prot, VirHunt 2.0+, vagy pedig a fertőzött állományok törlése.

Leírása: A Vacsina vírus rezidenssé válását a memória-ellenőrző blokk (MCB) közvetlen manipulálásával éri el, így a hagyományos detektorok és fertőzést megakadályozó programok nem sokat érnek ellene, mert nem látják. Melegindítás után is a tárban marad. Amikor fertőzéskor beépül egy másik programba, azt „beep" hanggal jelzi.

Valószínűsíthető, hogy „pandúrból lett rabló": egy vírusellenes programnak,

a francia Vaccine-nak vírussá átírt változata. A Vaccine ugyanis a vírustechnológiát felhasználva úgy védte a programokat, hogy maga épült be vírusként az egyes szoftverekbe, elmentette a beépüléskori helyzetet, majd figyelte és jelezte, ha az állomány valamilyen okból megváltozott.

A víruscsalád tagjainak hossza 1200 bájt körül van. Ismert változataik száma — a későbbi Yankee Doodle sorozattal együtt — mintegy negyvenöt.

A Vacsina a „.COM to .EXE" konverzióval fertőz. Azaz ha .EXE állományt talál és annak hossza a fertőzés után is belefér a 64 Kb-os limitbe, akkor az .EXE fájl MZ, illetve ZM jelét és fejrészét lecseréli a .COM állományokban szokásos JMP utasításkódra és a relokátor kódra, ami a memóriában való elhelyezkedését szabályozza. Utána már .COM állományként kezelhető, s a fertőzés is eképpen megy végbe.

A Vacsina egy csipogás (beep) jellel közli, ha fertőzött. A fertőzés során a könyvtári bejegyzést átváltoztatja a fertőzéskor aktuális rendszerdátumra és időre. (Egyéb tulajdonságairól fejezetünk első részében részletesen szóltunk.)

Az ismert változatok:

TP04VIR: Az .EXE állományokat fertőzés előtt .COM-má konvertálja. Mielőtt végrehajtódik, a memóriában keresi a VACSINA stringet. Ha megleli, nem fertőz. A verziószám a fertőzött állomány végétől visszafelé a második bájton van, itt 04h. A .COM to .EXE konverter mintegy 132 bájt hosszú, s azt sokszor fertőzés nélkül is felteszi az állományokra, ami hamis riasztással reagál, ha csak erre keresünk.

TP05VIR: Hasonló a TP04VIR-hez. A verzió jelzése 05h. Rendszerkiakadásokat is okoz. Hibákkal terhelt köztes fejlesztési változat.

TP06VIR: Hasonló mint a TP05VIR. Verziószáma 06h.

TP16VIR: Hasonló mint a TP06VIR. Verziószáma 10h.

TP23VIR: Hasonló mint a TP16VIR. Verziószáma 17h, de a Vacsina szöveg már nem jelenik meg a vírusban.

TP24VIR: Hasonló mint a TP23VIR. Verziószáma 18h.

TP25VIR: Hasonló mint a TP24VIR. Verziószáma 19h.

A vírus neve: Vacsina-B

Egyéb elnevezése: Zenélő, Forgószínpad, Yankee Doodle.

Hossza: 1765 bájt.

Kódtípusa: Parazita, rezidens része van, a .COM, az .EXE, a .SYS, valamint a .BIN állományokat is fertőzi.

Azonosítása: Scan.

Eltávolítása: Scan /D /A, Sysdoki, KillVac, vagy a fertőzött állományok törlése.

Leírása: Magyarországon az eredeti Vacsina sajátos átirata van terjedőben, amely valószínűleg „közvetlen import" az Egyesült Államokból, mert eddigi tömeges hazai előfordulásai szoros amerikai kapcsolatokkal rendelkező műszaki-tudományos számítóközpontjainkban voltak.

A vírus a 64 Kbájtnál rövidebb .EXE állományokba épül be, de a .COM állományokat is fertőzi. A memória-ellenőrző blokk (MCB) közvetlen manipulálá-

sával telepszik be a memóriába. Ha .EXE állományokat fertőz, akkor azokból .COM-ként futó, de változatlan nevű állományokat csinál. Ez megnehezíti a kitakarítását. Van viszont benne egy programozási hiba. Nem veszi észre, ha a vírussal együtt az .EXE mérete meghaladja a .COM állomány lehetséges maximális méretét. A fertőzés ilyenkor csak részben sikerül neki, a .COM állományt pedig azonnal tönkreteszi.

A már említett átírás annyiból állt, hogy az eredeti vírus „beep" hangjelzését valaki kicserélte a Yankee Doodle vírus által fújt nótát tartalmazó rutinra. Így a tárban maradó vírus ezt játssza maximális hangerővel a Ctrl-Alt-Del melegstart után. Egyes esetekben ilyenkor megrongál állományokat is, és a rendszer újratöltése után aktív marad.

A Vacsina vírus első magyarországi megjelenése után hamarosan felbukkantak a nemzetközileg ismert Vacsina-átiratok is: **Vacsina v05** — 1217 bájt. **Vacsina v16** — 1350 bájt. **Vacsina v24** — 1760 bájt.

Mindegyik egyaránt fertőzi a .COM és az .EXE fájlokat. Az egyes változatok a vírus utolsó előtti bájtjának decimális értéke alapján kapták a nevüket (5, 16, 24).

A vírus neve: Yankee Doodle

Egyéb elnevezése: Music, 5pm Tee, TP44VIR, Five O'clock.

Hossza: 2885-2900 bájt (a paragrafushatártól függően).

Kódtípusa: Parazita, rezidens része van, a .COM és .EXE állományokat fertőzi.

Azonosítása: Scan V42+, F-Prot, IBM Scan, Pro-Scan, VirexPC, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: Scan /D, VirClean, CHKVir v.4.01, F-Prot, Prgdoki, Sysdoki, vagy pedig törölni a fertőzött állományt.

Leírása: A bolgár eredetű Yankee Doodle vírust először 1989. szeptember 30-án, Bécsben, a North Atlantic Project számítógéprendszerében találta meg Alexander Holy. A vírus a .COM és .EXE állományokba ül be. A fertőzött programok a vírus beépülése után általában 2899 bájttal lesznek hosszabbak. Az .EXE állományok állománynövekedése a paragrafushatárok miatt eltérő.

Miután a vírus önmagát memóriarezidensként installálta, figyeli az órát. Amikor az eléri a 17:00 p.m. értéket, akkor a Yankee Doodle című, az amerikaiak által kedvelt dal melódiáját játssza, maximális hangerővel. Logikus tehát másik elnevezése is, hiszen 17 órakor, a munkaidő végét jelezve zenélésével mintegy „ötórai teára" invitál. (Ezt a kicsiny zeneművet valamelyik programozó honfitársunk beültette a Vacsina-B jelű vírustermékbe is.)

Az eredeti Yankee Doodle csak zenél, és azon kívül, hogy ezen képességgel felruházza a többi állományt is, nem tesz semmi ártalmasat. A vírus átírt változatai azonban már sokoldalúbbak. Van, amelyik például megkeresi és alaposan átírja a Ping Pong vírust, mégpedig úgy, hogy az 100 fertőzés után öngyilkosságot kövessen el. Csak találgatni lehet, vajon a szerző milyen kapcsolatban van a másik vírus írójával.

Más változatai a Potyogós vírushoz hasonlóan karaktereket potyogtatnak le

a színes monitorokról, néha pedig a főkönyvtárban található és „A" betűvel kezdődő állományokat törlik (AUTOEXEC.BAT, ANSI.SYS stb.). Részleges vagy teljes átírásokkal van dolgunk, ezeket azonban az ismert detektorok felismerik és a killerek gond nélkül kitakarítják. E lista elkészülte után, de még a könyv kinyomtatása előtt jelent meg ennek a vírusnak egy jóval hosszabb magyar átirata, amelyet a hagyományos standard szoftverek nem irtanak ki. Szerencsére azonnal elkészültek rá az ideiglenes killerek, és felismeri a Sysdoki is.

A Yankee Doodle a vírusátiratokat készítő „kollégák" körében népszerű alapanyag. Eddig három átírt változat terjedt el Magyarországon. Az egyik hosszúsága megegyezik a McAfee által regisztrált eredeti 2885 bájttal, a másik 2932, a harmadik 2941 bájt.

A nemzetközi vírusszakértők által még jegyzett egyéb külföldi átírások 2890, 2940 és 2772 bájt hosszúak. A külföldi vírusölő programok többnyire felismerik a Magyarországon elterjedt Yankee Doodle vírusváltozatokat, de az eltérő vírushossz miatt a kiirtásakor tönkreteszik a fertőzött programot. (A helyi vírusváltozatok ellen a helyben készült vírustalanítók mindig hatásosabbak és biztonságosabbak.)

Ismert változatai:

TP33VIR: Az INT 1 és INT 3 használatát tiltja le a nyomkövetés megakadályozására. Délután 17 órakor zenél. A végétől visszafelé számított második bájt a verziószám: 21h = decimális 33.

TP34VIR: Hasonló az előzőhöz, de másképpen válik rezidenssé. A végétől visszafelé a második bájton lévő verziószáma: 22h.

TP38VIR: Hasonló az előzőhöz, de eltünteti magát, ha a Codeview debugger aktív. A fertőzött állomány végétől számított második bájton lévő verziójelzése 26h. 1988 júliusától terjed Bulgáriából kiindulva.

TP41VIR: Hasonló a TP38VIR-hez, kivétel a verziószáma a végétől számított második bájton: 29h.

TP42VIR: A Ping Pong vírust teszteli. Ha ott van, akkor kitakarítja, Verziószám az utolsó előtti bájton: 2Ah.

TP44VIR: Verziószáma 2Ch, hasonló, mint a TP42VIR.

TP45VIR: Hasonló, mint a TP44VIR, de verziójelzése a végétől visszaszámolt második bájton 2Dh.

TP46VIR: Hasonló a TP45VIR-hez, de jelzi és kiirtja a Cascade (1701) vírust. Verziószáma 2Eh.

Yankee Doodle-B: A Yankee Doodle-B magyar eredetű, a visszafejtett kód újrafordítása. Hossza 2272 bájt.

A vírus neve: Yankee 2

Egyéb elnevezése: Yankee, Yankee-go-Home, 1961.
Hossza: 1961 bájt.
Kódtípusa: Parazita, nem rezidens, .EXE fertőző.
Azonosítása: Scan V62+, Virex PC, AVTK 3.5+, VirHunt 2.0+.
Eltávolítása: Törölni a fertőzött állományokat.
Leírása: A Yankee 2 vírus 1989-ben indult el útjára Bulgáriából. Nem való-

színű, hogy T. P. úrnak köze lenne hozzá, mert őt műveiből egy szolid, zseniális programozó őrültnek ismertük meg, aki választékosan fejezi ki magát, nem pedig közönségesen trágárkodik.

Vita van a szakirodalomban arról, hogy ez a vírus valóban új-e vagy csak változat. Néhány forrásmunkában találkozunk egy Yankee Doodle (2) elnevezéssel. Melyik vírus melyik? Sajnos nagyon nehéz eligazodni a Kelet-, illetve Nyugat-Európában honos és az amerikai víruselnevezések között, és megállapítani, hogy ugyanarról a vírusról beszélünk-e vagy sem. Az eligazodáshoz gyakran csak a fertőzési hossz ad támpontot. Az amerikai szakirodalomban Patricia Hoffman, a Virus Summary készítője a TP víruscsalád Yankee Doodle tagjait Yankee Doodle néven tartja nyilván és a vírusleírás végén említi meg a különböző TP vírusvariánsokat. A szakma Yankee Doodle–2 néven ismer még egy vírust, amely hosszában, működésében szintén eltér a fent leírt TP–Yankee Doodle vírustól.

A Yankee 2 nem rezidens, ami azt jelenti, hogy csak akkor fertőz, ha egy általa megfertőzött programot elindítunk. Ekkor megkeres egy még nem fertőzött másik programot, és beépül abba is. Közben lejátssza a Yankee Doodle zenét, majd végül engedi futtatni az eredeti programot. A vírusnak semmilyen más hatása nincs, de az alábbi szöveget tartalmazza:

```
motherfucker
6D6F7468657266756368657 2
```

A durván trágár szöveg (kb. anyabaszó) érdekessége, hogy Patricia Hoffman a Virus Summary dokumentációjában a fenti hexa kódot közli. (Hátha úgy nem hangzik olyan csúnyán?) Később minden egyéb vírushatározóban, például Fridrik Skulason F-Prot programjának ismertetésében és leírásában már szövegesen szerepel ez az azonosító. A vírus nem fertőzi meg a CodeView programot.

Ismert átirata:

1624: Funkcionálisan azonos az eredeti vírussal, a hossza azonban 1624 bájt.

A Tiny család

Úgy tűnik, szerzőjük folyamatosan eresztette el termékeit. 1990 júliusában jelent meg a Tiny-158, Tiny-159, Tiny-160, Tiny-167 és a Tiny-198. 1990 októberében pedig a Tiny-134, Tiny-138, Tiny-143, Tiny-154 és a Tiny-156. Végül 1990 decemberében a Tiny-133 okozott sok bosszúságot.

A Tiny víruscsalád „származási" sorrendje:

```
Tiny-198 → Tiny-167 → Tiny-160 → Tiny-159 →
Tiny-158 → Tiny-156 → Tiny-154 → Tiny-143 →
Tiny-138 → Tiny-13
```

1990. december 18-án Veszelin Boncsev, a közismert bolgár vírustalanító szakember felhívásban figyelmeztette a szakma képviselőit, hogy megjelent egy új, az akkori legkisebb, 128 bájtos vírus. Sokan a Tiny vírusok szerzőjének Boncsevet tartották, s ezért is igyekezett a Tiny veszélyeire felhívni a figyelmet. A számítógépvírusok egyik fő szülőhazájában Boncsev vette fel a harcot a

vírusok ellen. Ez a vírusírókat felbőszítette és a V2000 vírust az ő nevére dedikálták, mintha ő lenne a szerző.

A Tiny család többi tagjától a Tiny-128 több szempontból is elkülönül. Memóriarezidens, a .COM állományokat az elindítás pillanatában megfertőző vírus. A fertőzött állományok könyvtári bejegyzésének dátumát és idejét átállítja, megjelölve az egyes állományokat a későbbi felismerés céljából. (A Vienna/Dos 62, a V2000, a 4096 stb. vírusok is hasonló fájlmegjelölési elvet alkalmaznak.) Ha a fertőzés során a vírus nem tudja megváltoztatni a program dátumát és időpontját, akkor több esetben is megfertőzhet egy állományt. A vírus a csak-olvasható attribútumot viselő (read only) állományokat nem tudja megfertőzni.

Ezt a vírust a megszakításokat figyelő antibaci programok (Flushot+, AntivirPlus) észreveszik. A vírus a 3 bájtnál rövidebb és a 64 K-nál nagyobb programokat a fertőzés során tönkreteszi. Rezidenssé válása után megkeveri a memóriában a megszakításokat nyilvántartó és könyvelő interrupt vektortáblát. A INT C0h megszakítót az INT E0h-ra, az INT 21h-t pedig az INT E0h-ra helyezi át. Az áthelyezett megszakítók új helyükön az eredeti megszakítókat tartalmazzák. A Tiny-128 vírus szerzője szűk szakmai körben ismert, hivatásos programozó. Az bizonyos, hogy e vírus írója nem azonos a többi Tiny vírus szerzőjével.

A vírus neve: Tiny Family

Egyéb elnevezése: Tiny család.

Hossza: 133-198 bájt.

Kódtípusa: A .COM állományokat fertőzi meg.

Azonosítása: Scan V80+ (mindegyik verzióra), Pro-Scan 2.01+ (csak a hosszabbakra).

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: Ennek 11 tagú víruscsaládnak az eredetéről annyit tudunk, hogy azonos bulgáriai szerzőtől származnak, de nem a TP család készítőjétől.

A Tiny sorozat tagjai a vírusfertőzött program lefuttatásakor a memória 60h szegmensébe installálják magukat. Ezt a szegmenst a DOS csak akkor használja, amikor a rendszert betölti, utána már nem fordul ehhez a részhez.

A vírus az INT 21-et szintén magára irányítja. Rezidenssé válása után a futtatott .COM állományokat fertőzi meg, és a fertőzés időpontjára változtatja át a könyvtári bejegyzés dátumát és idejét. Az alábbi ismertetésben a verziószám mindig a bájtban megadott vírushosszt jelöli.

A Tiny család tagjai:

Tiny-133: Úgy készült, hogy a szerző kipoloskázta a Tiny-134 hibáit, ezért a program kiválóan szaporodik. Az elterjedt rezidens antivírus programok nem detektálják, míg a többi családtagot észreveszik. A legjobban sikerült „kislány".

Tiny-134: Meglehetősen sok poloskával terhelt. Nem éppen aktív, és rendszeresen kiakasztja a rendszert, amikor .COM fertőzés történik. Ezt a rutinját ugyanis hibásan írták meg.

Tiny-138: Hasonló a Tiny-134-hez, csak a mérete más.

Tiny-143: Hasonló a Tiny-134-hez, csak a mérete más.
Tiny-154: Hasonló a Tiny-134-hez, csak a mérete más.
Tiny-156: Hasonló a Tiny-134-hez, csak a mérete más.
Tiny-158: Hasonló a Tiny-134-hez, csak a mérete más.
Tiny-159: Hasonló a Tiny-134-hez, csak a mérete más.
Tiny-160: Hasonló a Tiny-134-hez, csak a mérete más.
Tiny-167: Hasonló a Tiny-134-hez, csak a mérete más.
Tiny-198: Hasonló a Tiny-134-hez, csak a mérete más.

A vírus neve: Tiny-163

Egyéb elnevezése: 163 COM.
Hossza: 163 bájt.
Kódtípusa: Nem rezidens, parazita, .COM fertőző vírus.
Azonosítása: Scan V64+, VirexPC, F-Prot 1.12+.
Eltávolítása: Scan/D, F-Prot 1.12+, vagy törölni a fertőzött állományokat.
Leírása: Fridrik Skulason izolálta Grönland szigetén, az egyetemi számítóközpontban 1990 júniusában. A vírus nem rezidens, általános .COM fertőző, de a COMMAND.COM-ot is megtámadja.

Amikor a fertőzött programmal együtt a víruskód is végrehajtódik, megfertőzi az első .COM állományt az aktuális könyvtárban. Rendszerlemezeknél ez természetesen a COMMAND.COM. Újabb víruslefutáskor újabb program válik fertőzötté. Nem támadja meg azokat a .COM állományokat, amelyek hossza nem éri el az 1 kilobájtot.

A megfertőzött .COM állományok hossza 163 bájttal nő. A fertőzés során az állomány könyvtári bejegyzésének dátumát és időpontját a fertőzéskori adatokra cseréli le. A fertőzött állomány végén a következő hexadecimális karaktersorozat található: 2A2E434F4D00, illetve ennek karakteres képe: *.COM

A minél kisebb DOS vírusok írására való törekvés jegyében készült egyik darab, a fertőzésen túl egyéb károkozása nem ismeretes.

A vírus neve: Enigma

Egyéb elnevezése: Cracker Jack.
Hossza: 1755 bájt.
Kódtípusa: Nem rezidens, parazita, .COM fertőző.
Azonosítása: Scan V76+.
Eltávolítása: Törölni a fertőzött állományokat.
Leírása: Az olasz vírusfejlesztő csoport terméke. 1991 februárjában jelentette fellépését Alberto Colusa, Olaszországból. A vírus nem rezidens, .EXE fertőző, de feltételezhető, hogy bizonyos körülmények között képes .COM fertőzést is végezni, csak annak feltételeit még nem ismerjük.

Az Enigma vírussal (neve rejtélyt jelent) a víruskód lefutása után az aktuális könyvtárban lehet egy másik .EXE állományt megfertőzni. A sikeres fertőzés után az állomány hossznövekedése 1755 bájt. A vírus a program végére épül be, s az alább bemutatott szöveget tartalmazza karakteres formában.

Egyik helyen:

```
This is the voice of the Enigma virus.....
the spirits of the hell are coming back!
```
(Ez az Enigma vírus hangja... A pokol szellemei visszatérnek!)

Később:

```
(C) 1991 by Cracker Jack * Italy * *.exe
newenigmavir
```

Eredetéről annyit tudunk, hogy egy főleg fiatalokból álló vírusíró számítógépes csoport terméke. Ők készítették az olasz pingpongozó vírust is, és azóta programozástechnikailag sokat fejlődtek. 1991 második felében igen aktívan működtek. Vírusaik szaporasága és veszélyessége kezdi elérni a bolgár vírusokét.

A víruskód a Yankee 2 kódjának ismeretében, annak alapos átbarkácsolásával készült.

A vírus neve: Alameda

Egyéb elnevezése: Merritt, Peking, Seoul, Yale.

Hossza: Nem értelmezhető.

Kódtípusa: Bootvírus, rezidens része van, csak a floppy bootszektorát fertőzi.

Azonosítása: Scan, F-Prot, IBM Scan, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: MDisk, Clean, F-Prot, CHKVir v.4.01, Sysdoki, vagy a DOS SYS parancsának kiadása.

Leírása: Maradvány az „őskorból". Először Kalifornia állam Alameda nevű városában bukkant fel, 1987-ben. Eredeti változata még nem okozott nagy károkkal járó nemzetközi járványt. Jelenleg a vírusnak létezik olyan átírt verziója, amely lemezindítás után lehetetlenné teszi a rendszerhívást a floppyról és a merevlemezről egyaránt. Ennek nemzetközi lajstromneve: Alameda-C.

Az Alameda vírus a Ctrl-Alt-Del melegindításkor teszi rá magát az 5 1/4"-os, 360 Kbájtos floppyra — de csakis arra —, oly módon, hogy a memóriában maradó rész megfertőzi a bootszektort a rendszerlemezen és a többi floppyn. Programozástechnikailag érdekes feladat volt úgy megírni, hogy melegindításkor aktívan a tárban maradjon és a DOS is üzemképesen betöltődhessen. (Az utóbbi időben Magyarországon is felbukkant a Vacsina-B vírus, amely hasonló elven működik.)

A vírus elmenti a valódi bootszektort a 39-es sáv, 8-as szektorának, 0. fejpozíciójára. Az Alameda vírus eredeti verziója csak a 8086/8088-as processzorú gépeken futott, mert a kódhossz csökkentése érdekében a korántsem tehetségtelen szerző direkt processzorkódot alkalmazott. Az újonnan felbukkanó változatok már felismerik a 80286-os processzort is.

A vírus neve: Golden Gate

Egyéb elnevezése: Mazatlan, 500.

Hossza: Nem értelmezhető.

Kódtípusa: Rezidens része van, a bootszektort fertőzi meg.

Azonosítása: Scan (Alameda vírusnak ismeri fel, de nem azonos azzal, csak az azonosítója!), CHKSeq v.1.0.

Eltávolítása: MDisk, F-Prot, vagy a DOS SYS parancsa.

Leírása: A Golden Gate vírus az Alameda vírus módosított változata. Akkor lép működésbe, ha belső számlálója jelzi, hogy már 500 floppyt megfertőzött. A vírus osztódását és terjedését a Ctrl-Alt-Del melegindítás váltja ki. Amikor új floppyt vagy merevlemezt fertőzött meg, a számlálót nullázza, de a nullázás csak az új példány számlálójára terjed ki, a sajátja tovább fut. Aktivizálódása katasztrofális: újraformázza a C: lemezegységet.

Eddig felfedezett változatai a következők:

Golden Gate-B: Ugyanaz, mint az eredeti Golden Gate, azzal az eltéréssel, hogy csak floppykat fertőz, és számlálója 30–500 közötti fertőzésre van beállítva.

Golden Gate-C: Hasonló, mint a Golden Gate-B, kivéve hogy merevlemezt is meg tud fertőzni. Ezt a változatot ismerik sok helyen Mazatlan vírusnak. Igen veszélyes, jól sikerült átírása az eredeti Golden Gate-nek!

A vírus neve: SF

Egyéb elnevezése: Még nem ismeretes.

Hossza: Nem ismeretes.

Kódtípusa: Rezidens része is van, a floppy bootszektorát fertőzi meg.

Azonosítása: Scan. (Alameda vírusként ismeri fel.)

Eltávolítása: MDisk, Clean, F-Prot, vagy a DOS SYS parancsának kiadása.

Leírása: Az SF Virus az Alameda vírusnak alaposan átírt verziója. Kicserélték az aktivizálódást irányító számláló beállítását, ezért már 100 reprodukció után formázza a floppylemezt. A fertőzés a Ctrl-Alt-Del melegstart hatására történik, és csak az 5 1/4"-os, 360 kbájtos floppykat fertőzi és formázza.

A vírus neve: Devil's Dance

Egyéb elnevezése: Mexican.

Hossza: 941 bájt.

Kódtípusa: Parazita, rezidens része van, a .COM állományokat fertőzi, és manipulálja a FAT-ot.

Azonosítása: Scan V52+, CHKSeq v.1.0.

Eltávolítása: Scan /D, vagy törölni a fertőzött állományokat.

Leírása: A vírus neve ördögtáncot jelent. Mexico Cityben fedezte fel egy Mao Fragosso nevű programozó. A vírus a fertőzés során a .COM állományok hosszát 941 bájttal megnöveli. Egy állományba akárhányszor beépülhet, így hamar elérkezik az az állapot, amikor a .COM program már nem tud betöltődni, lévén több mint 64 kbájt hosszú. Amikor pedig egy fertőzött programot futtatunk és melegindítást csinálunk, akkor a tárban visszamaradó programszegmens a következő üzenetet írja ki a képernyőre:

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

(Táncoltál már az ördöggel sápadt holdfényben? Imádkozz a lemezeidért!! A Joker)

Az üzenetből látható, hogy a Batman sorozat ördögi, de humorérzékkel rendelkező gonosz figuráját használták fel. (Lásd a Joker vírus leírását is.)

Ez a vírus romboló hatású. Aktivizálódásának feltétele a billentyűleütések meghatározott száma. Az első 2000 leütés után a vírus elkezdi csereberélni a monitoron megjelenített szövegek színét. Ez a fertőzés első, kívülről is észrevehető jele. A következő, már törlési fokozatba 5000 leütés után lép. Ekkor a vírus jóízűen elfogyasztja, azaz törli a FAT-tábla első másolatát. Ha újraindítjuk a rendszert, akkor ismét az első másolatot törli, és így tovább. Végül nem marad semmi, és még rendszert indítani (bootolni) sem tudunk.

A vírus neve: Joker

Egyéb elnevezése: Még nem ismeretes.

Hossza: 29 233 bájt.

Kódtípusa: Parazita, nem rezidens, az .COM és az.EXE állományokat fertőzi meg.

Azonosítása: Scan/X V67+, Pro-Scan, VirexPC.

Eltávolítása: Scan /D, vagy pedig törölni a fertőzött állományokat, ami egyremegy.

Leírása: A Joker vírust 1989 decemberében izolálták először Lengyelországban. A vírus általánosan fertőzi az .EXE állományokat, de ezt nagyon csendben teszi, mert nem minden lefutáskor fertőzi a többi állományt. Nevét az ismert Batman tévésorozat egyik alakjáról, Jokerről kapta, aki válogatott hülyeségekkel bosszantja Batham City békés polgárait. A hasonló hajlamú vírusszerző ugyanezt teszi a személyi számítógépek használóival. Először csak nevetünk rajta, s amikor sírnánk, akkor már késő...

Meglehetősen hosszú, ami azért van, mert a sok sületlenséget, amit tartalmaz, valahova el is kell tárolnia. Fertőzése teljesen a Vacsina algoritmusára történik. A .COM állományokat normálisan fertőzi még. Az .EXE programokhoz egy 139 bájtos konvertert ad, és azzal konvertálja át .COM-okká, hogy hasonlóképpen fertőzhesse meg őket. Vajon T. P. ujjgyakorlata lenne? Ebben sokan kételkednek. Mindenesetre szellemes! Ha mégis a bolgár T. P. írta, hogyan került Lengyelországba? Valószínűsíthető forrása ugyanis ott van.

A Joker vírus válogatott marhaságokat tartalmazó üzeneteit szöveg formájában elhelyezi a fertőzött állományokban a vírus programkódjának elején. Ha tehát ott ilyesmit olvashatunk, akkor a Joker tette tiszteletét gépünkben. Néhány üzenete kizárólag rá jellemző, ezért magát a szöveget is kereshetjük. Az üzenetek nagy részét kódolva tartja magában.

Néhány jellegzetes üzenete:

`Incorrect DOS version`
(Nem megfelelő DOS verzió)

`Invalid Volume ID Format failure`
(Érvénytelen lemezcímke-azonosító. A formázás nem sikerült)

`Please put a new disk into drive A:`
(Tegyen új lemezt az A: meghajtóba)

End of input file
(A bemeneti állomány vége)
END OF WORKTIME. TURN SYSTEM OFF!
(Vége a munkaidőnek. Kapcsolja ki a rendszert!)
Divide Overflow
(Túlcsordulás)
Water detect in Co-processor
(Vizet észleltem a koprocesszorban)
I am hungry! Insert HAMBURGER into drive A:
(Éhes vagyok! Tegyél egy hamburgert az A: meghajtóba)
NO SMOKING, PLEASE!
Thanks.
(Kérem, ne dohányozzon! Köszönöm!)
Don't beat me!!
(Ne püfölj ön !!)
Don't drink and drive
(Ne igyon, ha vezet)
Another cup of cofee?
(Kér még egy csésze kávét?)
Hard Disk head has been destroyed. Can you borrow me your one?
(A merevlemez feje megrongálódott. Kölcsönadná a sajátját?)
Missing light magenta ribbon in printer!
(Nincs halványlila szalag a nyomtatóban!)
In case mistake, call GHOST BUSTERS
(Ha eltévesztette, hívja a szellemvadászokat)
Insert tractor toilet paper into printer.
(Helyezzen WC-papírtekercset a nyomtatóba.)

Ha a vírus .DBF állományokkal találkozik, azokat is kiegészíti hasonló stílusú üzenetekkel.

A vírus analizálása során derült ki, hogy írója rosszul írta meg a vírus szaporodását biztosító rutint, mert az közvetlen gépi kódú lévén Intel 8088 processzorú gépeken nem működik, illetve néhány BIOS verziónál hibásan szaporodik. Így nem véletlen, hogy igen ritka vírus.

Péntek 13 és környéke

Jerusalem, Jerusalem B, Jerusalem C, Jerusalem B Mutant, Jerusalem D, Jerusalem E, Jerusalem B Destructive, A-204, Anarkia, Anarkia B, Mendoza, Park ESS, Puerto, Skism-1, Spanish JB, Jerusalem DC, Captain Trips, Swiss 1813, Frere Jacques, New Jerusalem, Payday, Sunday, Suriv 1.01, Suriv 2.01, Suriv 3.00, Westwood, 1605, Discom, 1720, Print Screen, Print Screen-2, 2930, Friday The 13th, Friday The 13th-B, Friday The 13th-C, Sunday, Sunday-B, Sunday-C, Alabama, Black Monday.

Péntek 13 szerencsétlen nap a babonásoknak. De az lett a számítógépet használók számára is, mióta megjelent a színen a péntek 13-án aktivizálódó, izraeli eredetű számítógépvírus. Azóta egyre több vírus aktivizálódását tették erre a napra. Ez ellen sokan úgy védekeznek, hogy ilyen napokon nem használják gépeiket. Ami persze csak ideglenes megoldás, az igazi cél a vírusmentes környezet biztosítása, a vírusok kitakarítása.

A Péntek 13 a leggyakrabban megpatkolt vírusok egyike. Annak idején e vírus forráskódjának közléséért titkosították Szegedi Imre hadtudományi doktori disszertációját. A vírus briliáns, még ma is helytálló programozástechnikai megoldásokat tartalmaz. Ez a vírus vagy legalábbis annak alapja valamelyik profi szoftveríró cég laboratóriumában született, és onnan került a Közel-Kelet terroristáihoz.

A vírus neve: Jerusalem

Egyéb elnevezése: PLO, Israeli, Friday 13th, Russian, 1813(COM), 1808(EXE), Péntek 13.

Hossza: 1813 bájt (.COM-fertőzés esetén), illetve 1808—1823 bájt között (.EXE-fertőzés esetén).

Kódtípusa: Parazita, rezidens része van, a .COM és az .EXE állományokba épül be.

Azonosítása: Scan, F-Prot, IBM Scan, CHKSeq v.1.0.

Eltávolítása: Scan /D /A, Saturday, CHKVir v.4.01, CleanUp, UnVirus, F-Prot, Prgdoki, Sysdoki.

Leírása: A Jerusalem vírus az úgynevezett terrorista víruscsoport oszlopos

tagja. Izraelben bukkant fel a Héber Egyetemen (Hebrew University) 1987 közepén. A vírusnak van memóriarezidens része. A .COM és az .EXE állományokat egyaránt fertőzi. A vírus utolsó 5 bájtja tartalmazza a fertőzést jelző szignatúrát. Az eredeti változatban itt egy érdekes programozási hiba van: egyes esetekben újrafertőzi a már megfertőzött .EXE állományt, mert „elfelejteti" kitenni a fertőzést jelző azonosítót.

A vírus elkapja az INT 8-as megszakítót, valamint fél órával a fertőzés után egy tízes faktorral, azaz tizedére lecsökkenti a gép sebességét. Néhány változat fekete ablakot vagy fekete keretet nyit a monitor képének bal felső részén, esetleg a képernyő görgetése közben összezavarodik, becsíkozódik a kép. GEM grafikus felületet használva az egér „odaszarik", azaz, amerre mozog, fekete szemetet hagy maga után. A magyar Ventura védelme ezt merényletnek veszi, és akkor mindenféle baja támad a rendszernek.

Ha elindítunk egy Péntek 13 vírussal fertőzött programot, először a vírus aktivizálódik. Bemásolja magát a gép memóriájába, és ott megbújik, átveszi néhány megszakítás (interrupt) kezelését az operációs rendszertől, de ebből még nem veszünk észre semmit. A memóriában elbújva minden meghívott programot megfertőz. A vírus mindaddig nem aktivizálja magát, amíg egy tizenharmadikai dátum nem esik péntekre. Ha péntekre esik és a vírus aktív, akkor az elindított programokat egyszerűen törli. Egyetlen vírusos program is elegendő teljes elszaporodásához! Külső, belső és helyi hálózatos adathordozókon lévő állományokra egyaránt veszélyes! A Péntek 13 vírus a Potyogós vírussal együttműködni is képes. Ebben az esetben a .COM állományokat mind a kettő megfertőzi, az .EXE állományokat viszont csak a Péntek 13.

A következő években az alábbi hónapok 13. napja esik péntekre: 1992 március, november. 1993 augusztus. 1994 május. 1995 január, október.

Vírusazonosító karaktersorozata: sUMsDos, de a különböző változatokban ezt is többféleképpen módosították. (Lásd ott: Jerusalem B, New Jerusalem, Payday, Suriv 3.00.) Az alapváltozat annyira jól sikerült, hogy különböző verzióit boldog-boldogtalan gyártja, sokan éppen csak annyit változtatva, hogy más legyen az aktivizálódás időpontja és a megszokott vírusdetektorok és killerek ne ismerjék fel. A Magyarországon Kedd 1-jére átírt változatának vírusazonosító sztringje: sUMsDns.

A Jerusalem vírus legismertebb változatai:

Jerusalem-B: A .COM és az .EXE állományokon kívül a .SYS állományokat is megfertőzi. Amennyiben a vírus a memóriában rezidensen párban van a Cascade/Poty vírussal, akkor komisz réteges fertőzés alakul ki, amelyet csak különleges technikákkal lehet jól eltávolítani. (Folytatását lásd a Jerusalem B-nél!)

Jerusalem-C: A Jerusalem B-vel azonos, de nem lassítja le a processzor működését. Magyarországon a Jerusalem B és C változata komoly pusztítást végzett a PC-k adatállományaiban. Folytatását lásd a Jerusalem B-nél!

Jerusalem-B Mutant (Kedd 1, Május 1): Eredeti magyar átírása a Jerusalem-B vírusnak. Mint az akkori sajtóközleményekből kitűnik, 1989 késő őszén készült, nagy valószínűséggel a Kandó Kálmán Villamosipari Műszaki

Főiskola hallgatói körében. A Péntek 13-i dátumot és a vírusazonosítót módosították. Így lett a neve Kedd 1, vagy az első aktivizálódási időpontra célozva: Május 1. Majdnem annyira elterjedt, mint az eredeti Jerusalem-B. Nyugat-Európában és az USA-ban is felbukkant.

A Péntek 13 vírus eredeti aktivizálódási dátuma 1987 utáni péntek 13-ára volt beállítva. A Kedd 1 vírusban a vírusazonosító kódot és dátumot 1980 utáni aktivizálódásra állították be. Az 1980-nak valószínűleg az volt az értelme, hogy dátumbeállítás nélkül is aktivizálódjon, mivel a PC-k dátuma alapértelmezésben 1980-tól indul. A program hatásában megegyezik az eredeti Péntek 13 (Jerusalem) vírussal.

A következő években az alábbi hónapok első napja esik keddre: 1992 szeptember, december. 1993 június. 1994 február, november. 1995 augusztus.

Jerusalem-D: Ugyanaz, mint a Jerusalem-C, azzal az eltéréssel, hogy 1990 után minden péntek 13-án törli a FAT-táblát.

Jerusalem-E: A Jerusalem-D-vel azonos, de aktivizálódásának kezdete 1992.

A vírus neve: Jerusalem-B Destructive

Egyéb elnevezése: Péntek 13, Jerusalem Mutant, Arab Star, Black Box, Black Window, Hebrew University.

Hossza: 1813 bájt (.COM fájlban) és 1808-1823 bájt között (.EXE fájlban).

Kódtípusa: Parazita, rezidens része van, a .COM és az .EXE állományokat fertőzi.

Azonosítása: Scan, F-Prot, IBM Scan, CHKSeq v.1.0.

Eltávolítása: F-Prot, Saturday, CHKVir v.4.01, CleanUp, M-JRUSLM, UnVirus, Prgdoki, Sysdoki.

Leírása: A Hebrew University rendszerében 1988 januárjában bukkant fel Izraelben. A károkozása a scroll lock gombhoz is kapcsolódik. Ha péntek 13-a van és a scroll lock aktív, akkor nem minden esetben töröl, károkozása nem tipikus.

A vírus a megadott hossznál +/– 256 bájttal rövidebben, illetve hosszabban épül be a programokba. Ha rövidebben, akkor felülírja az adott program utolsó 256 bájtját, ezzel lehetetlenné téve a program helyreállítását. A vírust Magyarországon először banki számítógépes rendszerben találták meg.

Átiratai és változatai:

A szokásostól eltérve fejezetünkben több vírusról két helyen is szólunk, ami nem véletlen. A változat főcsoporttá vált, és tagjait annyira keresztül-kasul átírták, hogy igen nehéz egyetlen fonalra felfűzni ezt a kavalkádot...

A-204: A Jerusalem-B azonosítóját (sUMsDos) cserélték ki az *A-204* karaktersorozatra, és változik a keresési algoritmus is. A memóriarezidenssé válás után 30 perccel a rendszer lelassul, és fekete doboz jelenik meg a monitoron. A vírus egy holland vállalatnál bukkant fel.

Anarkia: A fekete doboz sohasem jelenik meg, de az órajel drasztikusan lelassul. A vírusazonosító szöveget kicserélték a következőre: ANARKIA. A vírus

időpontját is átírták péntek 13-ról kedd 13-ra. A vírus eredete Spanyolországban valószínűsíthető.

Anarkia B: Hasonló az Anarkia vírushoz, csak aktivizálódási dátumát írták át minden év október 12-ére.

Mendoza: A Jerusalem-B vírus kódjának ismeretében íródott. Csak egyszer fertőzi az .EXE állományokat. A fekete doboz effektust EGA és VGA monitorokon idézi elő. Fél évig, azaz júliustól decemberig aktív. Amikor egy fertőzött program lefut, utána 10%-os valószínűséggel törlődik. Argentínában izolálták, nevét Mendoza városról kapta, ahol először megtalálták.

Park ESS: 1990 októberében Californiában, Happy Camp-ban került elő ez a Jerusalem-változat, amely megfertőzi a COMMAND.COM-ot is. A .COM állományok esetén a hossznövekedés 1813 bájt, az .EXE állományok első fertőzésénél a növekedés 1808—1822 bájt, a későbbi fertőzések esetén pedig már csak 1808 bájt.

A Jerusalem szokásos sUMsDos azonosító szövege hiányzik. Helyette található az, amiről ez a változat a nevét kapta: PARK ESS. Ez a változat alaposan a rendszer működését, mintegy 20 százalékkal. A vírus elindulása után 30 perccel kiteszi a fekete ablakot az EGA vagy VGA monitorokra.

Puerto: A Mendoza vírusverzió újabb átirata Puerto Ricoból, ahol 1990 júniusában került kézre. Tartalmazza a Jerusalem jellegzetes sUMsDos azonosítóját és az .EXE állományokat többszörösen is fertőzheti.

Skism-1: 1990 decemberében bukkant fel New York államban, az eredeti Jerusalem igen alaposan átírt változataként. Kicserélték az aktivizálódás feltételeit. Ez a változat 1991-ben és az azt követő években minden hónapban a 15-e utáni pénteki napokon lép működésbe. Nem törli az állományokat, hanem végrehajtás után 0 bájt méretűre csonkítja azokat.

A .COM állományok hossza a fertőzés után 1801 bájttal, az .EXE állományoké pedig 1808–1822 bájttal növekszik meg. Az .EXE fertőzés ugyanazon az állományon akárhányszor megtörténhet. A jellegzetes sUMsDos azonosítót kicserélték benne. Az új azonosító lett a vírus neve: SKISM-1. A fekete doboz effektus a vírus rezidenssé válása után itt is megtalálható, harmic perccel a memóriába való beépülés után. A rendszert ez is lelassítja.

Spanish JB: Teljesen hasonló, mint a normál Jerusalem, csak az .EXE állományokat többször is meg tudja fertőzni. A .COM állományok hossznövekedése 1808 bájt. Az .EXE állományok első fertőzési hossza 1808–1813 bájt, második, illetve későbbi fertőzések esetén 1808 bájt. Nem csinál fekete ablakot, ugyanakkor hiányzik az azonosító jelsorozata is. Ezt a spanyol eredetű változatot Jerusalem E2-ként lehet felismerni.

Jerusalem DC: Teljesen hasonló, mint a Jerusalem, csak az azonosítóját cserélték ki 00h karakterekre. Harminc perccel a memóriába való beépülése után a rendszer sebességét 30%-kal csökkenti. A fekete ablakot a monitor ernyőjének bal alsó részén generálja. Miként eredetije, ez is képes az .EXE állományok többszörös fertőzésére. Nem töröl, nincs aktivizálódási dátuma sem. Úgy tűnik, hogy ez a vírusnak egy „méregfog nélküli" oktató átirata. Az USA-ban, Washington kormányhivatalaiban tűnt fel először.

Captain Trips: 1991 márciusában az USA-ban került elő ez a Jerusalem-átirat. Nevét a benne lévő szövegről kapta. Captain Trips az USA-ban népszerű rajzfilm- és képregényhős, Superman-szerű figura. Azonosítója, a Captain Trips X. a vírus belsejében bukkan fel. Ez a verzió nem készít fekete dobozokat a monitorra, nem lassítja le a rendszer működését sem. Hasonlóképpen hiányzik azon képessége, hogy péntek 13-án töröljön, és hiába keressük benne a Jerusalem jellegzetes azonosítóját. Fertőzési hossza .COM állományok esetén 1808 bájt, az .EXE fájlok első fertőzésekor 1808–1822 bájt, a továbbiaknál pedig 1808 bájt.

Swiss 1813: 1991 februárjában Svájcban indították útjára ezt az átiratot, amely egy kedves bacivá szelídített Jerusalem vírus. Nem tesz ki fekete ablakot, nem lassítja le a rendszert, és nem is töröl péntek 13-án. Az sUMsDos azonosító sztringet bináris nullákra vakarták át: 00h. Szerepe valószínűleg egy vírus terjedésének követése volt.

A vírus neve: Frere Jacques

Egyéb elnevezése: Frere.

Hossza: 1808 bájt.

Kódtípusa: Rezidens résszel rendelkező, .COM és .EXE fertőző, parazita vírus.

Azonosítása: Scan V63+, Pro-Scan 1.4+, F-Prot 1.12+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: Az USA California szövetségi államában csípték el ezt a vírusátiratot 1990 májusában. A vírust a Jerusalem B kódjának felhasználásával kotyvasztották össze. Megfertőzi a .COM, az .EXE, valamint az overlay állományokat, de nem bántja a COMMAND.COM-ot.

A víruskód lefutása után a vírus beépül a memória alsó részébe, ahol 2064 bájt helyet foglal el magának, ugyanakkor magára veszi az INT 21 vezérlését. Utána minden olyan programot megfertőz, amelyet rezidenssé válása után indítottunk el. A .COM állományok növekedése 1808 bájt, míg az .EXE és overlay állományok 1808–1819 bájttal lesznek nagyobbak.

A vírus folyamatosan okoz rendszerkiakadásokat. Ennek kapcsán elrontja az adatállományok tartalmát is, azzal, hogy bemásolja magát például egy overlay állományba. Csökkenti a programok rendelkezésére álló szabad memóriaterületet.

A zenekedvelő vírusok családjába tartozik. Aktivizálódásakor, azaz minden pénteken a rendszer hangszórón keresztül nagy hangerővel eljátssza egy ismert francia gyermekdal dallamát: Frere Jacques, Frere Jacques, dormez vous, dormez vous, Sonne le matine, Sonne le matine, ding-deng-dong...

A vírus neve: New Jerusalem

Egyéb elnevezése: Még nem ismeretes.

Hossza: 1813 bájt (.COM fertőzéskor) és 1808 bájt (.EXE fájl esetén).

Kódtípusa: Parazita, rezidens része van, a .COM, az .EXE, a .SYS, valamint a Windows .PIF állományokat fertőzi meg.

Azonosítása: Scan V45+, F-Prot, CHKSeq v.1.0., Pro-Scan 1.4+.
Eltávolítása: Saturday, CleanUp, CHKVir v.4.01, F-Prot, Prgdoki, Sysdoki.
Leírása: Az eredeti Jerusalem vírus egyik változata. Az ismeretlen átírók igen nagy tudással éppen csak annyira változtatták meg az eredeti vírus kódját, hogy az IBM által 1989. október 20-án kibocsátott Virscan verzió ne ismerhesse fel V45 vírusként. A vírus 1989. október 14-én egyszerre jelent meg több nyilvános hozzáférésű elektronikus adatbankban (BBS) Hollandiában. A vírus pusztítását szintén mindig péntek 13-án fejti ki, ekkor törli az elindított programokat, függetlenül attól, hogy fertőzöttek voltak-e vagy sem. Más napokon csak terjed.

A vírus memóriarezidens, részben úgy viselkedik, mint az eredeti Jerusalem, de nemcsak azokat az állományokat képes megfertőzni, hanem a .SYS, a .BIN, és a .PIF állományokat is.

A vírus neve: Payday

Egyéb elnevezése: Még nem ismeretes.
Hossza: 1808 bájt az .EXE, és 1813 bájt a .COM állományok megfertőzésekor.
Kódtípusa: Parazita, rezidens része van, .COM és .EXE fertőző.
Azonosítása: Scan V51+, F-Prot, Pro-Scan 1.4+, AVTK 3.5+, VirHunt 2.0+.
Eltávolítása: M-JRUSLM, UnVirus, Saturday, Clean, F-Prot, Pro-Scan 1.4+.
Leírása: A Payday vírust az ismert holland vírusvadász, Jan Terpstra fogta meg 1989 novemberében. A vírus a Jerusalem B átirata. Az aktivizálódás feltételeit jelentősen átírták. Nemcsak péntek 13-án törli az állományokat, hanem minden pénteken. A neve — magyarul fizetésnap — szintén erre utal, lévén az angolszász területeken gyakori a heti munkabérfizetés, általában pénteken. A Jerusalem rokonságban szokásos fekete ablakot kiteszi a képernyőre és lassítja is a rendszer működését.

A vírus neve: Suriv 1.01

Egyéb elnevezése: April 1st, Israeli, Suriv01.
Hossza: 897 bájt.
Kódtípusa: Parazita, rezidens része van, csak a .COM állományokat fertőzi.
Azonosítása: Scan /X V67+, F-Prot, IBM Scan, Pro-Scan, VirexPC, AVTK 3.5+, VirHunt 2.0+.
Eltávolítása: Scan /D /X, F-Prot, UnVirus.
Leírása: A Suriv 1.01 memóriarezidens, az Izraelben felbukkant víruscsalád legelső tagja. Később sokszor átírták. Mintha arra készült volna, hogy felmérjék vele, hogyan terjed és milyen károkat tud okozni egy vírus, ha annak egy évnyi lappangási ideje van. Szerencsére könnyen lebukik, mert a fertőzés során a következő üzenetet írja ki a képernyőre:

```
YOU HAVE A VIRUS
```

(Önnek vírusa van)

Minden esztendőben egyszer, április elsején aktivizálódik, kissé bonyolult módon. Csak akkor lép ugyanis működésbe, ha egy fertőzött .COM állomány

után egy fertőzetlent is futtattunk. Ekkor a következő üzenetet küldi a monitorra:

APRIL 1ST HA HA HA YOU HAVE A VIRUS

(Április elseje, ha-ha-ha, önnek vírusa van)

Utána a rendszer lemerevedik, amin csak a főkapcsoló ki-, majd bekapcsolása segít. A vírus nevét az azonosító szövegről kapta, amely a víruskódban található: SURIV 1.01.

A vírus neve: Suriv 2.01

Egyéb elnevezése: April 1st-B, Israeli, Suriv02.

Hossza: 1488 bájt.

Kódtípusa: Parazita, rezidens része van, az .EXE állományokat fertőzi meg.

Azonosítása: Scan /X V67+, F-Prot, IBM Scan, VirexPC, Pro-Scan, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: Scan /D /X, F-Prot, UnVirus, VirHunt 2.0+.

Leírása: A Suriv 2.01 memóriarezidens résszel rendelkezik. Az .EXE állományokat fertőzi, ezzel mintegy kiegészíti korábbi változatát, amely a .COM-okat vette célba. Április elsején olyankor aktivizálódik, ha egy fertőzött állományt futtatunk. A rendszer itt is lemerevedik, és ugyanazt a szemtelen üzenetet kapjuk, mint a Suriv 1.01 vírus esetében. Szintén a főkapcsoló az egyetlen újraélesztési mód.

A korábbi változattól eltérően a fertőzés bekövetkezte után egy órával az április elsejei aktivizálódáshoz hasonló géplemerevedést okoz, de üzenetét ekkor nem jeleníti meg. Az .EXE állomány fertőzés esetén is baj nélkül lefut, abban az esetben, ha a rendszer az alapértelmezett dátumot (01-01-80) használja. Ilyenkor a kód lefutása után egy órával üzenet nélküli rendszerkiadást is okoz. A vírus ebben az esetben csak egy állományt fertőz meg. Vírusazonosítója a kódban található: SURIV 2.01.

A vírus neve: Suriv 3.00

Egyéb elnevezése: Israeli, Suriv03.

Hossza: 1813 bájt (.COM kiterjesztésű fájlok esetén) vagy pedig 1808 bájt (.EXE állományoknál).

Kódtípusa: Parazita, rezidens része van, .COM , .EXE, .SYS, .BIN, átfedő (overlay) állományokat fertőző programvírus.

Azonosítása: Scan /X V67+, F-Prot, Pro-Scan, VirexPC, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: CHKVir v.4.01, F-Prot, Prgdoki, Sysdoki, Clean, Scan /D /X, F-Prot, Unvirus, VirHunt 2.0+.

Leírása: A Suriv sorozat szerzője egy .COM és .EXE állományokat egyaránt fertőző vírus önálló elkészítése helyett barkácsoláshoz fogott. A kiindulást a Jerusalem vírus adta. Annak azonosító karaktersorozatát (sUMsDos) kicserélte saját verziójelzésére: sURIV 3.00. Még azt a fáradságot sem vette, hogy visszafejtse a kódot, ezért benne maradt az a programozási hiba, amelyik az ere-

detiben volt. Ugyanis az eredeti Jerusalem péntek 13-án aktivizálódik. Ekkor törölnie kell a fertőzött állományokat. Abban az esetben viszont, ha a vírus már jelen van a rendszer memóriájában, vagy ha ilyen kódot futtatunk, elmarad a törlés. Ha nincs péntek és 13-a, akkor a vírus 30 perccel a memóriába kerülése után a képernyőn egy „fekete ablakot" vagy egy elszíneződött ablakot nyit ki, ugyanakkor az időmérő-megszakítás manipulálásával lassítja is a gépet. Miként a Jerusalem-B vírus, ez is fertőz átfedő (overlay), .COM, .EXE, .SYS és .BIN állományokat, viszont COMMAND.COM-ot nem.

A vírus neve: Westwood

Egyéb elnevezése: Még nem ismeretes.

Hossza: 1819–1829 bájt.

Kódtípusa: Rezidens résszel rendelkező, .COM és .EXE fertőző.

Azonosítása: Scan V67+, F-Prot 1.12+, Pro-Scan 2.01+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: A vírus nevét a kaliforniai Westwood városról kapta, ahol a vírust először izolálták. Ez a vírus egy olyan Jerusalem átirat, amelyet 1990 augusztusában, az akkori antivírus programok még nem detektálnak.

Az eredeti vírushoz hasonlóan a .COM, az .EXE és az overlay állományokat fertőzi, de békén hagyja a COMMAND.COM-ot. Az eredeti Jerusalem vírustól eltérően nem tudja az .EXE állományokat ismételten megfertőzni. A kód lefutása után a memória alsó részében szabályos tárrezidens programként installálja magát, 1808 bájt hosszan. Ilyenkor az INT 8 és az INT 21 megszakító vektorokat magára irányítja. Ha péntek 13-a van, akkor az INT 22-t is elveszi.

A .COM programállományok elejére épül be, és az állomány 1829 bájttal lesz hosszabb. Az .EXE és az overlay állományoknak a végére épül be a vírus, és a hossznövekedés 1819–1829 bájt között van. Mint általában minden Jerusalem mutáns, a rezidenssé válás után 30 perccel alaposan lelassítja a rendszert. Ez idő tájt teszi ki a monitorra a fekete ablakot is, amely teljesen szétzilálja a monitorképet.

Ha rezidens a memóriában, péntek 13-án törli az elindított programokat. A Jerusalem-B közeli rokona.

A vírus neve: 1605

Egyéb elnevezése: Még nem ismeretes.

Hossza: 1605 bájt.

Kódtípusa: Rezidens résszel rendelkező, .COM és .EXE fertőző parazita vírus.

Azonosítása: Scan V67+, Pro-Scan 2.01+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: 1990 szeptemberében John McAfee Homebase BBS vírus szekciójába töltötte be egy ismeretlen felhasználó. A vírus azóta sem bukkant fel. Eredete ismeretlen. Nekünk sem sikerült belőle szerezni, így ismertetésénél csak a szakirodalomra hagyatkozhatunk.

A vírust a Jerusalem B alapján írták. Megfertőzi a .COM és .EXE állományo-

kat, de a COMMAND.COM-ot nem. Memóriarezidens. A memória alsó szegmensébe rezidens programként épül be, átirányítva magára az INT 13-at és az INT 21-et, a memóriában 1728 bájt területet foglal le magának. A rendszer működését 20 százalékkal lassítja le. Amikor már rezidens, minden végrehajtott .COM és .EXE állományt megfertőz. A hossznövekedés .COM állományok esetében 160 bájt, és a kód az állomány elejére épül be. Az .EXE állományok 1601–1610 bájttal nőnek, és ott a vírus az állomány végére telepszik be. Egyéb hatásai ismeretlenek. A vírus feladója valószínűleg csak saját vírusával akarta tesztelni McAfee rendszerét.

A vírus neve: Discom

Egyéb elnevezése: Még nem ismeretes.

Hossza: 2053 bájt.

Kódtípusa: Rezidens résszel rendelkező, a .COM és az .EXE állományokat megfertőző vírus.

Azonosítása: Scan80+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: 1990 novemberében izolálták a Discom vírust, amely jelenleg elég ritka. Jerusalem átirat, kevésbé bizonyult terjedőképesnek, mint többi társa. A COMMAND.COM kivételével a .COM és az .EXE állományokat fertőzi meg. A víruskód olyan mértékű hasonlóságot mutat a Sunday nevű vírusátirattal, hogy közös szerzőjük valószínűsíthető. Több vírusdetektor össze is keveri ezeket. Az általa okozott tünetek viszont már nem hasonlóak.

Lefutása után a víruskód átveszi az INT 08 és az INT 21 vezérlését, valamint a memóriában lefoglal magának 2304 bájtnyi helyet. Amikor már bent ül a memóriában, a futtatás során megfertőzi a .COM és az .EXE állományokat. A .COM programban az állomány elejére ül be, 2053 bájt növekedést okozva, az .EXE állományokban a végén foglal helyet és a növekedés 2059–2068 bájt. Minden fertőzött állomány végén a következő karaktersorozat található: 11121704D0h. (Hexadecimális formában írtuk, mert nem betűkarakterek.)

Nem lassítja le a rendszer működését, és nem teszi ki a fekete ablakot a monitorra. Kísérleti példánynak tűnik, kidolgozatlanságával és értelmetlen funkcióival.

A vírus neve: 1720

Egyéb elnevezése: PSQR, Spanish II.

Hossza: 1720 bájt.

Kódtípusa: Rezidens résszel rendelkező, .COM és .EXE állományok növekedését okozó vírus.

Azonosítása: Scan V61+, VirexPC 1.1+, F-Prot 1.12+, VirHunt 2.0+,

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: Az 1720 vírus másik neve PSQR vírus, nem tévesztendő össze a PRTSC bootvírussal. Ezt a 1720-ast először Barcelonában, Spanyolországban izolálták. A vírus a .COM és az .EXE állományokat fertőzi meg, de nem bántja az overlay állományokat és a COMMAND.COM-ot sem. Amikor rezidenssé vált, minden futtatott állományt megfertőz. Igen agresszív.

A vírus hossza 1720 bájt, amelynek utolsó 5 bájtja tartalmazza az =PSQR vírusazonosítót. Ha a vírus ezt a szignatúrát megtalálja a fájl végén, akkor az adott állományt már nem fertőzi meg. A vírus minden elindított .COM és .EXE állományt megfertőz, a COMMAND.COM kivételével. Az .EXE állományokban az utolsó 30 bájtot néha tönkreteszi.

Péntek 13-án a fertőzött program lefutása után a vírus beül a memóriába, és törli a forrásául szolgáló programot. Ekkor megnézi, van-e a gépben merevlemez. Ha lát ilyen eszközt, akkor helyreállíthatatlanul felülírja a bootszektort, valamint a partíciós táblát, hogy az adatok elvesszenek. Utána kimerevíti a rendszert. Agresszivitása miatt a vírusvédő hardverek tesztelésére alkalmas.

A vírus neve: Print Screen

Egyéb elnevezése: EB 21, 8290, PRTSC.

Hossza: Nem értelmezhető.

Kódtípusa: Bootvírus.

Azonosítása: Scan V64+, Pro-Scan 1.4+, VirexPC, F-Prot 1.12+, VirHunt 2.0+.

Eltávolítása: M-Disk, Pro-Scan 1.4+, Clean80+, vagy a DOS SYS parancsa.

Leírása: A vírus az indiai Bombayból származik, ahol élénk szoftverkészítő és -hamisító tevékenység is folyik. Egy ottani szakember, Neville Bulasara izolálta először. A vírus agresszív, a védekezés ellene nagyon sok fejtörést okoz. Igen sok változata van, amelyekben a korábbi programozási hibákat kijavították. Tudatos fejlesztés eredménye. Legalább két verziója terjedt el a világon.

Amikor a bootrekorddal együtt betöltődik, beépül a memória tetejére. Utána beállítja a memória új méretét, amely 2 K-val lesz kisebb. A floppyn az eredeti bootrekordot kiteszi a 11. szektorra. Amikor rezidens, alaposan lelassítja a lemezhozzáférést. Jó pár esetben összekeveri a főkönyvtári bejegyzéseket is. A néha itt látható „csillag-halálfej" jelsorozat a víruskód része.

A vírust a Ping Pong alapján írták, sok antibaci program annak ismeri fel. Az első változat nem fejezi be a képernyő kiprintelését, a javított kiadásban már igen.

Ismert változata:

Print Screen-2: Az első vírus javított és bővített kiadása. 255 I/O lemezművelet után kiprinteli a képernyőtartalmat.

A vírus neve: 2930

Egyéb elnevezése: Spanish.

Hossza: 2930 bájt.

Kódtípusa: Parazita, rezidens része van, a .COM (köztük COMMAND.COM) és az .EXE állományokat fertőzi meg.

Leírása: A DOS INT 21h megszakítás 31h funkcióján keresztül válik rezidenssé. A vírus minden elindított programot megfertőz. A hibakeresők (debuggerek) ellen néhány programozási trükköt használ.

A vírus neve: Friday The 13th

Egyéb elnevezése: COM Virus, Miami, Munich, South African, 512 Virus.

Hossza: 512 bájt.

Kódtípusa: Parazita, nincs rezidens része, a .COM állományokat fertőzi meg.

Azonosítása: Scan /X V67+, F-Prot, IBM Scan, Pro-Scan, AVTK 3.5+, VirHunt 2.0+

Eltávolítása: Scan /D, F-Prot, CHKVir v4.01, Prgdoki3+, Sysdoki, Pro-Scan 1.4+, VirHunt 2.0+ vagy az F-Prot.

Leírása: Az eredeti Péntek 13 vírust először a Dél-Afrikai Unióban lelték meg, 1987-ben. Készítője pusztító szándékkal alkotta művét. Hasonló, mint a Jerusalem sorozat darabjai, amelyek szintén péntek 13-ához kötődnek. Ez a vírus azonban nem memóriarezidens és a Jerusalemtől eltérően nem veszi valamennyi fontos megszakítás (interrupt) vezérlését magára. Csakis .COM állományokat fertőz, de egy időre kivételt tesz a COMMAND.COM-mal, hogy nehezebben fedezhessék fel.

Amikor végrehajtotta programját, azaz megfertőzte az állományokat, ránéz a C: és az A: meghajtóra, hogy talál-e ott COMMAND.COM-ot. Ha megleli, akkor megfertőzi, hogy teljes legyen a műve. A vírus éppen ezért nagyon gyorsan terjed. Azzal hívja fel jelenlétére a figyelmet, hogy az A: meghajtó jelzőfénye akkor is világít, amikor éppen a C: az aktuális meghajtó. A fertőzés után az állománynak 64 kilobájtnál kisebbnek kell lennie.

Elérkezvén péntek 13-a, ha ekkor a gazdaprogramot végrehajtatjuk a géppel, akkor az törli önmagát, mi pedig egy nemlétező állományra utaló üzenetet kapunk. Az ötlet vándortémává vált. Mielőtt még meríthettek volna belőle a Hebrew University számítástechnikai rendszerére vadászó terroristák, megszületett néhány kellemetlen átírása is.

A következő változatait ismerjük:

Friday The 13th-B: Hasonló az alaptípushoz, azzal a különbséggel, hogy az aktuális könyvtár minden állományát megfertőzi, de az egész rendszert is, ha a fertőzött program szerepel a rendszerre megadott hozzáférési útvonalban (path).

Friday The 13th-C: Hasonló, mint a Friday The 13th-B, azzal az eltéréssel, hogy amikor a vírus aktivizálódik, akkor a következő üzenettel „köszönti" szenvedő alanyait:

`We hope we haven't inconvenienced You`
(Reméljük, nem okoztunk kellemetlenséget Önnek)

Amikor ezt az üzenetet olvassuk, akkor már éppen elegendő kellemetlenségünk van...

A vírus neve: Sunday

Egyéb elnevezése: Még nem ismeretes.

Hossza: 1636 bájt.

Kódtípusa: Parazita, rezidens résszel rendelkezik, a .COM és az .EXE állományokat veszi célba.

Azonosítása: Scan V49+, F-Prot, IBM Scan, Pro-Scan, VirexPC 1.1+, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: CleanUp, Scan/D, F-Prot, Pro-Scan 1.4+, VirexPC, VirHunt 2.0+.

Leírása: 1989 novemberének végén bukkant fel Washington szövetségi állam Seattle városában ez a „szellemes" vírus, amely nevét a benne lévő szövegről kapta:

```
Today is Sunday! Why do you work so hard?
All work and no play make you a dull boy!
Come on! Let's go out and have some fun!
```

(Ma vasárnap van! Miért dolgozol ilyen keményen? Ha folyton dolgozol és soha nem játszol, unalmas srác lesz belőled! No, gyerünk! Menj el, és szórakozz egy kicsit!)

A vírus egy erősen megpatkolt Jerusalem vírus. Károsító hatása abban rejlik, hogy tönkreteszi a FAT-táblát. Mire azonban erre sor kerül, a felhasználók már jól feltöltik egymást a vírussal. A vírus fellobbanásszerű járványokat okoz. Sokan átírták, de valószínűleg mindegyik a hétvégéken aktivizálódik.

Eddig ismert verziói:

Sunday-B: Hasonló az eredeti vírushoz, azzal az eltéréssel, hogy ez nem minden hétvégén ünnepel üzemzavarral. A szöveget sokszor megjeleníti, de nem vasalja ki a FAT-táblát.

Sunday-C: Az eredeti vírus teljes funkcionális kópiája, azzal az eltéréssel, hogy az azonosítás elkerülésére a kódot átírták.

A vírus neve: Alabama

Egyéb elnevezése: Még nem ismeretes.

Hossza: 1560 bájt.

Kódtípusa: Parazita, rezidens része van, az .EXE állományokat fertőzi, manipulálja a FAT-ot.

Azonosítása: Scan /X V67+, F-Prot, IBM Scan, Pro-Scan, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: CleanUp, F-Prot, CHKVir v.4.01, Sysdoki, vagy pedig a fertőzött állományok törlése.

Leírása: Az Alabama vírusra 1989 októberében, a jeruzsálemi Héber Egyetemen bukkant rá Yasrael Radai. A vírus első aktivizálódása 1989 október 13-án volt. Magyarországon az eredeti változat 1990 augusztusában tűnt fel.

Az Alabama vírus az .EXE állományokat fertőzi meg, fertőzési hossza 1560 bájt. A fertőzést rezidens részén keresztül hajtja végre. Amikor a programkód lefut, a memóriába betelepszik a vírus rezidens része, s utána nem engedi használni a normál TSR funkciókat. (TSR = terminate but stay resident — programfutást befejezni és a memóriában maradni.) Ezek helyett a vírus az INT 9 megszakításra akaszkodik és kihasználja az IN és OUT utasításokat is.

Amikor a vírus Ctrl-Alt-Del billentyűkombinációt észlel, egy látszólagos betöltést hajt végre, hátrahagyva magát a RAM-ban. A vírus a memória végére építi be magát — mintegy 30 K hosszan — úgy, hogy a DOS és BIOS által meghatározott memória méretét nem csökkenti. (Ezt a módszert több vírus is al-

kalmazza rezidenssé válása esetén.) Ebben az esetben a vírus a memória-ellenőrző blokkon (MCB = memory control block) keresztül lesz rezidens. Amikor a vírus már egy órája rezidens módon a tárban tartózkodik, egy villogó keretben a következő üzenetet jeleníti meg a gép monitorán:

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

(A nemzetközi jog által tiltott szoftvermásolatok... Postafiók 1055 Tuscambia Alabama USA.)

Az Alabama vírusban igen komplex mechanizmus határozza meg, hogy megfertőzi-e vagy sem azt az állományt, amelyet futtatunk. Először is körülnéz az aktuális könyvtárban, hogy talál-e ott fertőzetlen állományokat. Szerinte legalább egynek fertőzöttnek kell lennie, ezért ha nem talál ilyet, akkor elvégzi a fertőzés műveletét, hogy neki legyen igaza.

Eddig még nem tisztázott néhány esetben azonban ahelyett, hogy a fertőzésre váró és a már fertőzött programokkal foglalkozna, elkezd manipulálni a FAT bejegyzéssel: felcseréli egy nem fertőzött másik állomány nevével. A szerencsétlen felhasználó pedig elgondolkodhat azon, hogy miért nem az a program fut le, amit ő elindított. Végül az egész rendszer szétzilálódik. A fertőzés lassan, alattomosan történik. Az állományok felülírásában nagyon pedáns, „rendes teendőjeként" elvégzi minden pénteken. (A Jerusalem vírus írójának feltehetően ez a vírus adta az alapötletet az aktivizálódás feltételének kiválasztásához.)

A vírus neve: Black Monday

Egyéb elnevezése: Még nem ismeretes.

Hossza: 1055 bájt.

Kódtípusa: Rezidens résszel rendelkező, .COM és .EXE állományokat fertőző.

Azonosítása: Scan V67+, Pro-Scan 2.01+.

Eltávolítása: A fertőzött állományok törlése.

Leírása: A távoli Malajzia fővárosa, Kuala Lumpur is bekerült a vírusgyártó helyszínek sorába. 1990 szeptemberében Fiji szigetén leltek először a Black Monday vírusra, amely nagyon gyorsan elterjedt a Közel-Keleten és Ázsia számos országában. Európában csak elvétve bukkant fel.

A vírus a COMMAND.COM is megtámadja, valamint megfertőzi a .COM és az .EXE állományokat. Memóriarezidens része a rendszermemória alsó részén foglal el magának 2048 bájt helyet, és ezzel egyidejűleg magára irányítja az INT 21-et. A vírus a programok futtatása során épül be azokba, ha előtte önmagát sikerült a memóriában installálni. A .COM állományok végéhez 1055 bájtot ad hozzá, és az .EXE állományoknak is a végére épül be. Nem képes többszörös fertőzésre. A fertőzés során kicseréli a könyvtárbejegyzés dátumát a fertőzéskori adatokra, és a hossznövekedést sem rejti el a DOS elől. Sajnos a fertőzött állomány helyreállíthatatlan, mert néhány bájtot felülír benne. A vírusban a következő szöveg található a víruskód elején:

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

Megfejthető értelmezése: Fekete Hétfő, 1990 március 2. (vagy február 3?) KV K(uala) L(umpur) Mal(ajzia).

Computer AIDS

AIDS, AIDS-B, AIDS-II, Frog's Alley, Violator, Violator B4, Vienna, 645, Vien6, Vienna B 646, Ghostballs, Ghost COM, Lisbon, VHP, VHP-348, VHP-353, VHP-367, VHP-435, VHP2, VHP-627, W13, W13-A, W13-B, Casper, 1260, V2P2, V2P6, V2P6Z, Adolph, Leprosy 1.00, Leprosy B, Leprosy C, Leprosy D.

Várható volt, hogy korunk rettegett betegsége a számítógépes vírusok szerzőinek fantáziáját is megmozgatja. Így születtek meg a Computer AIDS vírusok, amelyekben a programozók erkölcstelenségéhez nagy adag morbid humor is vegyült. Több számítógépvírus tartalmaz az AIDS-szel kapcsolatos belső üzenetet. Hatásukban is van valami hasonlóság: viszonylag sokáig lappanganak, alattomosan terjednek és a végső fázisban hirtelen fejtik ki romboló hatásukat. Más vírusokat azért soroltunk ebbe a csoportba, mert egy részük a fertőzés pillanatában gyógyíthatatlanul tönkreteszi a megtámadott állományokat, más részük pedig szinte kiirthatatlannak tűnik, és ez kelti a hasonlóság látszatát az AIDS kórokozójával. De általában is elmondható, hogy számítógépvírus lett korunk egyik átka, az információs kor pestise — akárcsak az AIDS.

A vírus neve: AIDS
Egyéb elnevezése: Hahaha, Taunt, VGA2CGA.
Hossza: Nincs rá adat.
Kódtípusa: Felülír, nem rezidens, a .COM állományokat fertőzi.
Azonosítása: Scan /X V67+, Pro-Scan, VirexPC 1.1+, AVTK 3.5+.
Eltávolítása: Scan /D, vagy pedig a fertőzött .COM állományok törlése.
Leírása: Az AIDS vírusról Hahaha vírus elnevezéssel Európában már korábban beszámolt a szakirodalom. Az IBM ugyanezt Taunt vírus néven tartja nyilván. A vírus kifejezetten rosszindulatú. Amikor aktivizálódik, megjeleníti a monitoron a következő üzenetet:

```
Your computer now has AIDS
```

(Az ön számítógépe most AIDS-es)

Ebből az AIDS betűi elfoglalják a fél képernyőt. Azután a rendszer leáll. Ha a tápfeszültséget ki- és bekapcsoljuk vagy a Reset gombot megnyomjuk, akkor lehetséges a rendszer újraindítása. Ha a vírus már aktivizálódott, semmilyen

eljárással nem állítható helyre a megrongálódott adatállomány, mivel a végrehajtható programok első 13 952 bájtját felülírja, de nem menti el sehova. A vírus ebben a 13 kilobájtban tárolja az AIDS felirat nagybetűit. Csak a fertőzésmentes eredeti állomány visszatöltésében reménykedhetünk — ha megvan!

Megjegyzés: Ez a vírus nem tévesztendő össze az AIDS Information Disk (PC Cyborg) trójai programjával. Az nem vírus, hanem programrendszer!

Ismert átirata:

AIDS-B: Megtévesztésig hasonlít az eredetihez, de csak funkcionálisan. Hossza szintén 13 952 bájt. Miként az eredeti vírus, ez is a .COM állományokat támadja meg, belelértve a COMMAND.COM-ot is. Aktivizálódási feltételei mások. Ez a változat a következő üzenettel szórakoztatja áldozatait.

```
I/O error 99, PC=2EFD
Program aborted
```

1991 januárjában jelezték felléptét, valószínűsíthető forrása Bulgária.

A vírus neve: AIDS-II

Egyéb elnevezése: Companion.

Hossza: 8064 bájt.

Kódtípusa: Nem rezidens, .COM és .EXE fertőző.

Azonosítása: Scan /X V67+, Pro-Scan 1.4+.

Eltávolítása: Csak törölni lehet a fertőzött állományokat.

Leírása: A vírust 1991 áprilisában izolálták. Hollandiában készült. Nem parazita. Arra az DOS szabályra építi taktikáját, hogy ha azonos néven, de eltérő kiterjesztéssel két program van, akkor az operációs rendszer először a .COM-ot futtatja le, és csak utána az .EXE állományt. Ennek alapján betöltő rutinnal startoltathatunk egy programot, mint a DOS 5.0 esetében, de vírusműveletekre is lehet alkalmazni, mint ez a vírus is teszi. Ezt a jelenséget megegyező állományok technikájaként tárgyalja a szakirodalom (corresponding file technique).

A vírus nem fertőzi meg közvetlenül az .EXE állományt. Előtte csinál egy kópiát a vírusból, de az .EXE állomány nevén és .COM kiterjesztéssel. Így elindítva a programot, először a vírusprogram indul el. Erről a szokásáról kapta a Companion, azaz Társas nevet. A .COM programokat hagyományosan kreálja, gyakorlatilag azok viszik tovább a fertőzést. A .COM állományok hossza mindig 8064 bájt, könyvtári bejegyzésük ideje és dátuma a fertőzéskor aktuális rendszeridő. Az .EXE állomány eközben sértetlen marad! Ugyanakkor az .COM állományok létrehozásához szokványos technikát alkalmaz, ezért azokat nem veszik észre a tárrezidens vírusellenes programok és víruskártyák.

Ha a „kakukkfióka" .COM állományokat felfedezzük, kitörlésükkel megszabadulhatunk a vírustól is. Amikor létrehozza az új .COM állományt, mellékesen muzsikával szórakoztat bennünket, közben a képernyőre a következő üzenetet írva ki:

```
Your computer is infected with . . .
♥ Aids Virus II ♥
- Signed WOP & PGT of DutchCrack -
```

(Az ön számítógépét az AIDS II vírus fertőzte meg.)

Ezután elindítja az .EXE programot, amelyik problémamentesen lefut. Utána a vírus ismét visszaveszi a vezérlést és zenél, majd a következő üzenetet teszi ki a monitorra:

```
Getting used to me?
Next time, use a Condom .....
```

(Hozzámszoktál? Legközelebb használj gumióvszert...)

A vírus neve: Frog's Alley

Egyéb elnevezése: Frog.

Hossza: 1500 bájt.

Kódtípusa: Parazita, .COM fertőző, rezidens résszel rendelkezik.

Azonosítása: Scan V76+.

Eltávolítása: Törölni a fertőzött programokat.

Leírása: A Békák fasora valahol az USA-ban lehet. Ezt a programvírust David Grant számítógép-virológus szakember ott fogta meg 1991 márciusában. Memóriarezidens, .COM fertőző, a COMMAND.COM-ot is megfertőzi.

A vírus a rendszermemória alsó részére épül be, de nem foglalja le a területet, hogy ne lehessen könnyen észrevenni. Átirányítja magára az INT 09, az INT 20, valamint az INT 21 és az INT 2F megszakítókat. A vírus az éppen aktuális könyvtárban fertőzi meg a .COM állományokat. Minden DIR parancs kiadása egy újabb állomány megfertőzését jelenti. Hasonlóképpen a futtatott .COM program is megfertőződik. A fertőzés hatására a programállomány hossza 1500 bájttal nő meg, és a vírus az állomány elejére épül be. Hatására a lemezműveletek igen lelassulnak (mintegy 55-60%-kal!).

A vírus minden hónap 5. napján akkor aktivizálódik, ha fertőzött programot indítunk el. Ilyenkor a monitoron a névjegyét nyújtja át egy üdvözlés kíséretében:

```
(V) AIDS R.2A - Welcome to Frog's Alley !, (c) STPII
Laboratory - Jan 1990
```

Utána ez a szöveg minden DIR parancs hatására megjelenik. Amikor először látjuk, eltünteti a rendszerállományokat és a COMMAND.COM-ot a lemezről. Később a többi elindított programot is tönkreteszi. A vírus nem tartózkodik hosszan a memóriában, de amikor onnan kilép, kicseréli a lemezcímkét a következőre:

```
s Alley !
```

Ekkor már a DIR parancsra sem látunk állományokat a lemezen. Végül pedig, ha sokszor próbálkozunk, alaposan felülírja a FAT táblát és a főkönyvtár területét ezzel az üzenettel.

Ha a vírus aktív, nemcsak a lemezműveletek lassulnak le szinte csigatempóra, hanem a B: meghajtóhoz sem lehet hozzáférni. A memóriát intenzíven használó számos program kimerevedik a vírus hatására, aminek az az oka, hogy az FCB-ben nem jelöli be az általa használt területeket.

A vírus neve: Violator

Egyéb elnevezése: Violator Strain B.

Hossza: 1055 bájt.

Kódtípusa: Parazita, nem rezidens, .COM fertőző.

Azonosítása: Scan V67+, Pro-Scan 2.01+

Eltávolítása: Clean V71+, vagy törölni a fertőzött állományokat.

Leírása: A Vienna alapokon kifejlesztett, Violator nevű vírust postás helyett alkalmazza egy olasz vírusíró csoport. Ki nem állhatják John McAfee munkásságát, s neki küldözgetik ily módon üzeneteiket. Az elsőt 1990 augusztusában juttatták el McAfee Homebase BBS-ére.

A Violator nem rezidens, .COM fertőző, belelértve a COMMAND.COM-ot is. Működése erősen a rendszer pillanatnyi állapotának függvénye. Amikor végrahajtódik, körülnéz a gépben, tájékozódik. Ha a dátum 1990. augusztus 15-e előtti, akkor a vírus az aktuális könyvtárban megfertőz egy .COM állományt és ahhoz 1055 bájtot ad hozzá. Ha a dátum 1990. augusztus 15-e utáni, akkor már nem fertőz! (Nyilván akkorra akarták, hogy McAfee kézhez kapja a küldeményt.)

A fertőzés jele, hogy a B: meghajtónak hirtelen mindenféle baja lesz. Váltogatva kapjuk a DOS-tól az írásvédelemre, a szektor hiányára vagy akár magára a floppy hiányára vonatkozó üzeneteket. A McAfee-nek szóló — inkább csak a vírus névjegyének tekinthető — szöveg a víruskódban található:

```
TransMogrified (TM) 1990 by
RABID N'tnl Development Corp
Copyright (c) 1990 RABID!
Activation Date: 08/15/90
- Violator Strain B -
! (Field Demo Test Version) !
! * NOT TO BE DISTRIBUTED * !
```

Átírási nyersanyagként sajnos egyre többen alkalmazzák frappáns programozási megoldásai miatt.

A vírus neve: Violator B4

Egyéb elnevezése: Christmas Violator, Violator Strain B4.

Hossza: 5302 bájt.

Kódtípusa: Nem rezidens, parazita, .COM fertőző.

Azonosítása: ViruScan V74+.

Eltávolítása: Törölni a fertőzött programokat.

Leírása: A szakirodalomban tévesen tartják ezeket a vírusokat amerikai eredetűnek. Forrásuk majdnem biztosan Olaszország, egy olasz vírusfejlesztő csoport. A „vidám fiúk" ezúton küldték el második levelüket McAfee-nek. A célnak megfelelően a vírus terjesztésére a DSZ (alias DSZ1203) közprogramot használták, ami ezáltal trójai program lett.

A vírus nem rezidens, a .COM állományokat fertőzi meg, beleértve a COMMAND.COM-ot is. Ez a változat is tartalmaz néhány programozási trükköt, ugyanis működése processzorfüggő. A vírusszerzők McAfee-n kívül Peter Nor-

tont sem szeretik. Ha ugyanis a gépben 80286-os processzor ketyeg, a vírus aktivizálódása után felülírja a merevlemez első szektorait, mindent úgy tönkretéve, hogy azt a Norton Disk Doctor sem tudja helyreállítani. Ekkor jeleníti meg a vírus karácsonyi üdvözletét is. Ha pedig az ANSI.SYS nincs bekötve, akkor a monitor ernyőjén mindenféle zagyvalék látható. Ha a gép processzora 8088-as, akkor a Violator B4 nem szaporodik!

Fertőzéskor a fertőzött program kódjának lefutása után egy másik .COM állományt fertőz meg az aktuális könyvtárban. Az állományok 5302 bájttal lesznek hosszabbak. A könyvtári bejegyzés dátuma és időpontadata nem változik. A vírus a fertőzött program végére épül be.

A Merry Christmas üdvözleten kívül a tényleges üzenet a vírus belsejében található, amely azonban sohasem jelenik meg a monitoron. Címzettje McAfee:

```
Violator Strain B4 - Written by RABID Nat'nl Development
Corp.
RABID would like to take this opportunity to extend it's
sincerest holiday wishes to all Pir8 lamers around the
world! If you are reading this, then you are lame!!!
Anyway, to John McAffe! Have a Merry Christmas and a
virus filled new year. Go ahead! Make our day!
Remember! In the festive season, Say No to drugs!!! They
suck shit! (Bah! We make a virus this large, might as
well have something positive!)
```

(Violator B4 fajta. Írta a RABID Nemzeti Fejlesztő Csoport. A RABID szeretné megragadni az alkalmat, hogy kifejezze őszinte ünnepi jókívánságait minden Kalóz-8 bénítónak szerte a világon. Ha ezt olvasod, akkor már te is béna vagy! Mindenesetre neked John McAfee, kellemes karácsonyt és vírusokkal teli új évet. Előre! Legyen ez a mi ünnepünk! Ne feledd! Ebben az ünnepi időszakban mondjál nemet a kábítószernek. Ők mocskosul beszívnak. (Jaj! Egy kicsit hosszú vírust csináltunk, de talán abban is lehet valami jó!))

A vírus december hónapban aktív. Az egyik legbőbeszédűbb vírus.

A vírus neve: Vienna

Egyéb elnevezése: Austrian, Unesco, DOS-62, DOS-68, 1-in-8, 648, Vienna A.

Hossza: 648 bájt.

Kódtípusa: Parazita, nincs rezidens része, a .COM állományokra specializálta magát.

Azonosítása: Scan, F-Prot, IBM Scan, Pro-Scan, VirexPC, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: Clean, F-Prot, VirHunt 2.0+, Pro-Scan 1.4+, VirexPC.

Leírása: A Vienna vírusra először 1988 áprilisában leltek rá Moszkvában, az UNESCO által a gyermekeknek tartott számítástechnikai szaktáborban. A fertőzött program futtatásakor megfertőzi az útjába eső első .COM állományt. Minden nyolcadik fertőzés után melegindítást (warm reboot) végez a rendszeren, mialatt a víruskódot is végrehajtja. A vírusban van egy programozástechnikai hiba is: bizonyos .COM állományok megfertőzése után nem hajlandó ismét elindulni.

A Vienna vírust a bécsi Technikai Főiskolán írták. Kódleírása megjelent könyvben is, ezért hihetetlen mennyiségű átirata ismert, de belőlük csak kevés terjedt el széles körben. A vírusírók „kötelező tananyaga" ennek a vírusnak a tanulmányozása.

Ismert és elterjedt mutánsai:

Vienna B 645: Ennek a változatnak a hossza 645 bájt. Nem töröl és nem ír felül programot, viszont megfertőzi a COMMAND.COM-ot is. Amerikai átirat, Európában igen ritka.

Vien6: Ez a Vienna változat lényegében azonos az eredetivel, csak a meleg indítást előidéző rutint kivették belőle. Hossza 648 bájt, és minden hetedik esetben fertőz az aktuális meghajtón. Legelőször a COMMAND.COM-ot támadja meg ott, ahonnan a rendszert indították.

A vírus neve: Vienna B

Egyéb elnevezése: 62-B, Reboot #2, Rendszerhívó.

Hossza: 648 bájt.

Kódtípusa: Parazita, rezidens része is van, a .COM állományokat fertőzi.

Azonosítása: Scan, F-Prot, CHKSeq v.1.0.

Eltávolítása: M-Vienna, CleanUp, VirClean, CHKVir v.4.01, F-Prot, Prgdoki, Sysdoki.

Leírása: A Vienna B vírus a Vienna egyik változata. Lényeges különbség a kettő között, hogy amikor saját maga melegindítást hajt végre, egyúttal törli azt a programállományt, amellyel elindították. A magyarországi tapasztalatok részben ellentmondanak a szakirodalomnak. Ez annak a következménye, hogy a kódot néhányan „átbarkácsolták". Hosszúsága ennek ellenére nem változott, és a vírus irtásához szükséges információk is megegyeznek az eredetiével. A fertőzéseknek csak kis hányadában lehetséges az állomány megmentése. (Amikor az első öt bájt felülírása már bekövetkezett, speciális programozástechnikai megoldásokkal még helyreállítható a program, ha előtte egy olyan vírus fertőzte meg, amely — jóindulatú lévén — elmentette az eredeti öt bájtot, mert szüksége volt rá...)

A reboot (rendszerhívó) vírusok kevésbé ügyesen megírt, néha mégis gonoszabb vírusrutinok, mint amilyen például a Potyogósé! A vírusfertőzött program indítását követően először itt is a vírus aktivizálódik. Nem másolja be magát a gép memóriájába, hanem rögtön terjeszkedik abban az alkönyvtárban, ahonnan a programot indítottuk. Amennyiben talál olyan kisebb programot, amelyet meg tud fertőzni, akkor két eltérő algoritmus alapján működhet:

1. A terjedési algoritmus működésbe lépésekor ráülteti magát az egyik programra, de nem feltétlenül arra, amelyikből hívták. A program futásán ezt gyakorlatilag nem is lehet észrevenni.

2. A rombolási algoritmus elindulásakor megsemmisíti (felülírja) a program első 5 bájtját, lecserélve az ott található információkat a ROM-BIOS belépési pontjára (JMP FFFF0000).

Ha az első módon fertőzi meg programunkat, akkor a vírusrutinokat ki lehet úgy irtani, hogy az állomány helyreállítható. A második módon megfertőzött

programokat nem lehet megmenteni, mert a vírus az eredeti program fontos információit hordozó első öt bájtot megsemmisítette. Sajnos ilyenkor programunkat törölni kell!

A vírus neve: 646

Egyéb elnevezése: Vienna C.
Hossza: 646 bájt.
Kódtípusa: A .COM állományokat fertőzi meg. Nem rezidens, parazita.
Azonosítása: Scan V71+, Pro-Scan 2.01+.
Eltávolítása: Pro-Scan 2.01+ vagy törölni a fertőzött állományokat.
Leírása: A vírus 1990 októbere óta ismert. Forrása valószínűleg ugyanaz a bécsi főiskola, ahol az eredeti Vienna vírus is készült. A víruson tudatos kísérletezés figyelhető meg, éspedig a kód bonyolítása és méretének csökkentése érdekében.

A vírus nem rendelkezik rezidens résszel. A COMMAND.COM-ot és az összes .COM állományt megtámadja. Amikor a kód lefut, beépül egy állományba az aktuális könyvtárban. A vírus a fertőzött állományok hosszát 646 bájttal növeli meg. A fertőzött állományok végén megtalálható az EAF0FFFFFF hexadecimális értékekkel leírható karaktersorozat.

A vírus neve: Ghostballs

Egyéb elnevezése: Ghost Boot.
Hossza: Nem értelmezhető.
Kódtípusa: Rezidens része nincs, a bootszektort fertőzi meg.
Azonosítása: Scan V46+, F-Prot, CHKSeq v.1.0.
Eltávolítása: MDisk, CleanUp, F-Prot, vagy a DOS SYS utasításának kiadása.
Leírása: Az egész kísérteties Ghost vírusházaspárt, azaz a bootszektort és a .COM állományokat fertőző változatot is Fridrik Skulason fedezte fel Grönlandon, az Icelandic University-n. A Ghost bootvírus egyaránt rámegy a floppy és a merevlemez bootszektorára, és egy kicsit hasonló a Ping Pong vírushoz. (Írója nyilván visszafejtette és ismerte annak működését.) A vírus véletlenszerűen választja ki azt az állományt, amelyet azután alaposan megrongál.

Figyelem: Ha megtaláltuk és eltávolítottuk a Ghost bootvírust, még ne örüljünk! A rendszert alaposan át kell vizsgálni a .COM verzió után is, mert azért család a család, hogy tagjai kitartsanak egymás mellett. A .COM verzió egyetlen feladata, hogy megszülje a boot verziót. Így ha nem távolítottuk el a rendszerből, a .COM változat mindig újra és újra kitermeli a bootvírust!

A vírus neve: Ghost COM

Egyéb elnevezése: Ghostballs.

Hossza: 2351 bájt.

Kódtípusa: Parazita, nincs rezidens része, a .COM állományokat fertőzi meg.

Azonosítása: Scan /X V67+, F-Prot, IBM Scan, Pro-Scan, VirexPC, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: MDisk, vagy a DOS SYS parancsának kiadása és az összes fertőzött .COM állomány törlése. A Clean és az F-Prot is kitakarítja.

Leírása: A Ghost kísértetcsalád női tagja, amely megszüli a fertőző bootvírust. (Bővebben lásd az előző leírásban.) A Ghost COM általános .COM állomány-fertőző. A folyamat során a megfertőzött állomány hossza 2351 bájttal megnő. A fertőzés tünetei hasonlóak a Ping Pong víruséhoz: véletlenszerűen károsítja a rendszert, vagy egyszerűen csak fertőz. A Ghost COM vírus volt az első olyan ismert vírus, amely kétféle funkcióban tud működni, fertőzve a .COM állományokat is, a lemez (a floppy és a merevlemez) bootszektorait is. Miután a boot fertőzése megtörtént, már hagyományos vírusként viselkedik.

A vírus eltávolítása során arra kell figyelemmel lenni, hogy bár nincsen tárban maradó része, mégis aktív fertőzőképes és bootvírus. A mentesítés következő lépése, hogy az írásvédett DOS rendszerlemezről — amelynek természetesen garantáltan vírusmentesnek kell lennie — újraindítjuk a rendszert, majd valamelyik segédprogrammal visszatöltjük a korábban elmentett bootszektort, vagy rendszerlemez esetén a SYS paranccsal visszatesszük az eredeti rendszert. Jelenlegi ismereteink szerint az összes fertőzött .COM állományt törölni kell.

A vírus neve: Lisbon

Egyéb elnevezése: DOS 62.

Hossza: 648 bájt.

Kódtípusa: Parazita, nincs rezidens része, a .COM állományokat fertőzi meg.

Azonosítása: Scan V49+, F-Prot, IBM Scan, Pro-Scan, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: Scan /D, Pro-Scan 1.4+, VirexPC, F-Prot, VirHunt 2.0+.

Leírása: A Lisbon vírus a Vienna vírustörzs hajtása. Ezt a változatot 1989 decemberében különítette el Lisszabonban Jean Luz adatbiztonsági szakember.

Maga a vírus igen egyszerű, a Vienna vírushoz nagyon hasonló, bár egy trükk azért van benne. Az eredeti víruséhoz képest minden kódszóban 1-2 bájttal el van tolva („shiftelve" van) a kód, így az a hagyományos vírusdetektorok számára rejtve marad. Ezért nehéz a régebbi detektorokkal észlelni. A vírus minden nyolcadik fertőzésnél pusztít. A megtámadott program 1-es szektorának első öt bájtját felülírja a következő szöveggel: @AIDS. Ezzel természetesen a program helyreállíthatatlanul tönkremegy!

A vírus neve: VHP

Egyéb elnevezése: VHP-348, VHP-353, VHP-367, VHP-435.

Hossza: 348–435 bájt.

Kódtípusa: Parazita, .COM fertőző, nem rezidens.

Azonosítása: Scan V64+, AVTK 3.5+, F-Prot 1.12+, Pro-Scan 2.01+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: A VHP vírusok önálló családot alkotnak. Bulgáriából kerültek forgalomba, s valószínűleg egy szerző művei. Jelenleg a 435 bájt hosszú verziónál tartanak. Igen szapora, a Vienna vírus bázisán íródott. Nagy járványokat okozott Nyugat-Európában és az USA-ban.

A VHP család tagjai:

VHP-348: A változat első variánsnak tekinthető, számos programhibával terhelt. Ha mégis szaporodik, akkor .COM állományokat fertőz. Az állománynövekedés 348 bájt.

VHP-353: A COMMAND.COM-ot is megfertőzi. Ha egy .COM állományt már megfertőzött, akkor másik .COM-ot ugyanott nem fertőz meg. A hossznövekedés 353 bájt. Az előző vírus programhibáit kijavították benne, az új terjedési algoritmussal viszont más hibák keletkeztek, aminek következtében a rendszert időnként kiakasztja. Ugyanabba az állományba nem épül be többször.

VHP-367: A korábbi programhibákat kijavították. A COMMAND.COM kivételével a .COM állományokat fertőzi. A hossznövekedés 367 bájt. Igen ritkán többször is beépül egy állományba. Néhány esetben a VHP-353 nem fertőz meg minden .COM állományt, amelyet a fertőzött program lefutásakor végrehajtunk. Ilyenkor ezek a programok védetté válnak a VHP-367 további fertőzésével szemben, ami programhiba következménye.

VHP-435: Ez a verzió az előző programvírusok tapasztalatai alapján 1989 júliusában került forgalomba. Nem destruktív, de hatalmas járványokat okozhat, mert nagyon jól terjed. Amikor a kód lefut, csak egy .COM állományt fertőz meg, és nem bántja sem a COMMAND.COM-ot, sem az .EXE állományokat. Nem árt tudni, hogy a VHP-435 és a VHP-367 vírusokat számosan átírták, hordozóként alkalmazzák más vírusrutinokhoz.

A vírus neve: VHP2

Egyéb elnevezése: 623, VHP-623.

Hossza: 623 bájt.

Kódtípusa: Parazita, nem rezidens, .COM fertőző.

Azonosítása: Scan V64+, Pro-Scan 1.4+, AVTK 3.5+, F-Prot 1.12+, VirHunt 2.0+.

Eltávolítása: Pro-Scan 1.4+, F-Prot 1.12+.

Leírása: 1990 márciusában jelentkezett ez a bolgár csoda a „víruspiacon". A Vienna vírus bázisán és a korábbi VHP vírusok alapján készült. Gyakorlatilag a VHP-435 változata. Alapvető differencia, hogy a vírus nyolc közül egy esetben nem magát építi be, hanem reboot paranccsal írja felül a megfertőzött programot. Így ha azt elindítjuk, akkor melegindítás történik. Fertőzési hossza

623 bájt. Csak a .COM állományokat fertőzi meg, a COMMAND.COM kivételével.

Ismert átirata:

VHP-627: Mindenben hasonlít a VHP-623-hoz, csak a hossza tér el három bájttal, azaz 627 bájt.

A vírus neve: W13

Egyéb elnevezése: Toothless, W13-A.

Hossza: 534 bájt.

Kódtípusa: Parazita, nincs rezidens része, a .COM állományokat fertőzi.

Azonosítása: Scan V63+, F-Prot, IBM Scan, Pro-Scan 1.4+, VirexPC, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: Clean V63+, F-Prot, Pro-Scan 1.4+, VirexPC, AVTK 3.5+, VirHunt 2.0+.

Leírása: A W13 vírus a .COM állományokat fertőzi meg, kivéve ha azok már fertőzöttek. Nagyon silány munka. A programozási hibákat a szerző utólag igyekezett korrigálni. Lengyelországban bukkant fel 1989 decemberében. Születési helye a Szovjetunió. Magyarországon szórványosan találkozhattunk vele, főleg kutatóintézetekben. Nem károsítja az állományokat, csak ráépül azokra. Változatai:

W13-A: 534 bájt hosszú. (Az eredeti változat, sok hibával.)

W13-B: 507 bájt hosszú. (Egy javított kiadás.)

A vírus a dátum és az időpont könyvtári bejegyzésnél a hónap mezőben 13-ast állít be, a másodperceknél pedig 62-t, hogy jelezze a fertőzést.

A vírus neve: Casper

Egyéb elnevezése: Még nem ismeretes.

Hossza: 1200 bájt.

Kódtípusa: Nem rezidens, önmagát titkosító vírus, .COM fertőző.

Azonosítása: Scan V67+, Pro-Scan 2.01+.

Eltávolítása: Törölni a fertőzött álományokat.

Leírása: Fridrik Skulason izolálta Izlandon 1990 augusztusában. A vírus szerzője is ismeretes: Mark Washburn.

A vírus nem rezidens, a .COM állományokat fertőzi meg, beleértve a COMMAND.COM-ot is. Miután a kód lefut, egy véletlenszerűen kiválasztott .COM állományt fertőz meg az aktuális meghajtón. A hossznövekedés 1200 bájt, a kód az állomány végére épül be. A program igen bonyolult módon kódolva a következő üzenetet tartalmazza:

```
Hi! I'm Casper The Virus, And On April 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>
```

(Hello! Én Casper vagyok, a vírus, és április elsején teljesen szétbaszom a merevlemezed! Tényleg lehetetlen lesz helyreállítani! Na, most mihez kezdesz! <Vigyorgás>)

Ha április elsején ezzel a vírussal fertőzött programot futtatunk, az felülírja — a szabályostól eltérő szektorszámmal és szektorhosszal alacsony szinten for-

mázza — a lemez első sávját, ahol a boot, a FAT és a főkönyvtár található. Ennek eredményeként a későbbiek során a „Sector not found" rendszerüzenetet kapjuk és nem férünk többé hozzá adatainkhoz. A vírus dekódolva szinte teljesen a Vienna vírus, de titkosítási algoritmusát a V2P6 vírustól vette át.

Fridrik Skulason információi szerint — aki a vírusgyártó iparos címét is közölte — a vírusírónak az volt a célja, hogy csakis ő tudja eltávolítani a vírust.

A vírus 1200 bájtot tesz hozzá a fertőzött állományhoz. Ebből az első 39 bájt csak egyszerű titkosító rutin, hasonló a Potyogóséhoz. Van azonban egy fontos eltérés is. Egy vagy két bájt méretű változót ad hozzá a dekódoló algoritmushoz. Ezek az extra parancsok nem befolyásolják a vírus működését, de alaposan megzavarják a vírusfelismerő programok működését. Ennek ellenére megmaradt egy kisméretű állandó fejléc, a dekódoló rutin, amelynek alapján az F-Prot mégis képes azonosítani a vírust. A Casper nevet, mint a szövegből kitűnik, maga a szerző adta vírusának.

Mark Washburn az amerikai számítógépes alvilág ismert alakja. A V2P6 vírus, illetve az ebből kiterebélyesedő sorozat is az ő műve. Árusítja a saját vírusait kitakarító programokat, s akik másként nem képesek megbirkózni szörnyszülötteivel, bizony kénytelenek hozzá fordulni az ellenszerért. Üzlet, de nagyon ocsmány módon. Mindenesetre gyanús, hogy az Egyesült Államok különben minden hasonló cselekményre kényes hatóságai ebben az ügyben a fülük botját sem mozgatták.

A vírus neve: 1260

Egyéb elnevezése: V2P1.

Hossza: 1260 bájt.

Kódtípusa: Parazita, nincs rezidens része, titkosítja magát, a .COM állományokat fertőzi.

Azonosítása: Scan V57+, IBM Scan, Pro-Scan 1.4+, F-Prot 1.12+, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: Clean V57+, Pro-Scan 1.4+, F-Prot 1.12+, VirHunt 2.0+.

Leírása: Az 1260-as vírust először Amerikában, 1990 januárjában észlelték Minnesota (Kalifornia állam) egyetemén. Írója Mark Washburn, aki antivírus programjainak forgalmát igyekezett növelni azzal a vírussal, amelyet ő maga írt. A vírus nem ül be rezidensen a memóriába, ennek ellenére kifejezetten virulens, robbanásszerűen terjed. A fertőzés bekövetkezte után a .COM állomány hossza 1260 bájttal megnő. A beépülés a vírus titkosításával fejeződik be. A titkosító kulcs minden fertőzés alkalmával kicserélődik. A vírusok új, változékony generációjának első jellegzetes darabja.

Az 1260-as a Vienna vírus (DOS 62) egyik változata. A fertőzés során a fertőzött állományok rendszeridejét 31-re írja át. Elsőként a DOS megadott hozzáférési útvonalai mentén lévő könyvtárakban fertőzi meg a .COM állományokat, kivéve a COMMAND.COM parancsértelmező programot. A vírus kódolt formában épül be az egyes állományokba, és a kódoló rutint a felismerés megnehezítésére véletlenszerűen változtatja. A vírus a debuggerek ellen néhány programozási trükköt is tartalmaz. Az 1260-as vírus lehetséges támadáspont-

jai a helyi hálózatok, beleértve az állománykiszolgáló központi gépeket (file server) és a munkaállomásokat is. A vírust kifejezetten felkészítették ezekre.

A vírus neve: V2P2

Egyéb elnevezése: Még nem ismeretes.
Hossza: 1426–2157 bájt.
Kódtípusa: Nem rezidens, .COM fertőző, parazita.
Azonosítása: Scan /X V67+, Pro-Scan 2.01+.
Eltávolítása: Törölni a fertőzött állományokat.
Leírása: Mark Washburn úr újabb találmánya ez a vírus, amelyet 1990 júniusában kezdett terjeszteni működési területén, Minnesota városban. A vírus nem rezidens, és a .COM állományokra ül rá.

Amikor a kód lefut, az aktuális könyvtárban megfertőz egy másik .COM állományt, amelynek hosszát 1426–2157 bájt közötti értékkel növeli meg, olyan kódolási eljárást alkalmazva, hogy eltávolítását az lehetetlenné tegye. Csak olyan állományt fertőz meg, amelyikben még nincs benne a víruskód.

Hasonlóan a 1260-ashoz, igen komplex titkosítási algoritmussal dolgozik, a szerző ebben éli ki fantáziáját. Néhány szoftver a V2P2-t is 1260-asnak azonosítja és természetesen rosszul szedi le, ami nyilvánvalóan a szerző egyik célja is volt.

A vírus neve: V2P6

Egyéb elnevezése: Még nem ismeretes.
Hossza: 1946–2111 bájt.
Kódtípusa: Nem rezidens, parazita, öntitkosító vírus.
Azonosítása: Scan /X V67+, Pro-Scan 2.01+.
Eltávolítása: Törölni a fertőzött programokat.
Leírása: Mark Washburn újabb terméke, amit 1990 júliusában kezdett terjeszteni antibaci programjainak keresletét növelendő. A vírus nagyon hasonlít a Vienna bázisán kitenyésztett 1260, V2P2 és a V2P6 vírusok sorozatához. Nem rezidens, általános .COM fertőző.

Fertőzési hossza a kódolási algoritmus változtatásából következően 1946–2111 bájt között van. A kód lefutása közben az aktuális meghajtó aktuális könyvtárában megfertőz egy másik .COM programot, ha az még nincs megfertőzve. A kód az állomány végéhez kapcsolódik hozzá.

E víruscsaládban alkalmazott egymásra épülő titkosítási algoritmusok felismerése igen nehéz. Sajnos ezzel a rendszerrel iskolát teremtett, ami a hadi célokra is alkalmazható vírusok kifejlesztéséhez vezetett. Nem lehetetlen — és erre sok jel utal —, hogy Washburn is a hadi algoritmusok kikísérletezésén dolgozik, és sérthetetlensége ennek köszönhető.

A vírus neve: V2P6Z

Egyéb elnevezése: Még nem ismeretes.

Hossza: 2076–2364 bájt

Kódtípusa: Önmagát titkosító, .COM fertőző parazita programvírus.

Azonosítása: Sajnos nincs hozzá megfelelő eljárás, a hossznövekedés lehet a ráutaló jel.

Eltávolítása: Törölni a fertőzött programot.

Leírása: Az előbbi sorozatnak szinte a tökéletességig fejlesztett darabja Mark Washburn műhelyéből. Eredeti termék, amely a korábbi vírusokhoz hasonlóan általános .COM fertőző. Az aktuális könyvtárban akkor fertőz, ha ott még talál legalább egy nem fertőzött .COM állományt.

A kód az állomány végére épül be. A hossznövekedés a változó kódolási algoritmus következtében különböző lehet, 2076–2364 bájt között van. Algoritmusa olyan, hogy nincs vírusazonosító jelsorozata. Ebből a szempontból nehezebb eset, mint a hasonlóan durva Whale, ahol legalább a vírusfejet meg lehet találni.

A vírus neve: Adolph

Egyéb elnevezése: Még nem ismeretes.

Hossza: 2109–2445 bájt.

Kódtípusa: Parazita, nem rezidens, .COM fertőző vírus, amely önmagát titkosítja.

Azonosítása: F-Prot 1.16+, VIRx 1.6+, NAV 1.5+

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: 1991 májusában engedték el Európában. Kódja hihetetlenül szövevényes, változó hosszúságban fertőzi a .COM programokat, beleértve a COMMAND.COM-ot is. A V2P6 variációja.

Amikor a kód lefut, megnézi az aktuális meghajtó aktuális könyvtárát, hogy van-e ott fertőzött program. Ha nincs, akkor egyetlenegyet megfertőz. Csak .COM programokra vadászik és nem épül be többször ugyanabba az állományba.

A vírus biztos azonosítása csak aktivizálódásakor lehetséges, amikor az alanti — minősíthetetlenül ocsmány — üzenetben veszi célba Alan Solomont, az Angliában népszerű antivírus-szakembert. A szöveg a német argó jegyeit tükrözi. Egyik elképzelhető forrása a FISH6 vírust készítő csoport az NSZK-ban. Ennek azonban ellentmondanak a szövegben lévő alapvető német helyesírási hibák. A számítógépes bűnözéssel foglalkozó egyes szakemberek is azt feltételezik, hogy a szerző szintén a V2Px sorozat gátlástalan „antibaci"-szakembere, Mark Washburn, hiszen az USA piacán neki áll érdekében kollégájának a lejáratása.

```
********** NAZI P o W e W !!!! **********
Diese Program (c) 1991 Adolph Hitler. Fick Die
Mutti !!! Die Anti Viren Programierer .
konnte viel spass heben fuer nichts HA HA... NAZI !!!,
Ich suche gute fickbar frauen!, Gute Blasen.
Der Idea ist von S&S, Ich glaube er heisst
```

```
so Alan Zolomon oder so, Veiliecht er hatte eine
Kleine Schwanz HA Ha !!!!
rufen sie mal an (+44) 877-882 Fick die Oma Auch Du
Arsch!)
(c) 91 Zolomon S&S Shwanz!
```

(Ez az Adolf Hitler program. B... meg az anyád! Az antivírus programozók jól szórakozhatnak a semmiért. Ha-ha... Náci! Keresek jól kefélhető nőket, jó szopókat. Az eszme az S&S-től van, azt hiszem, Alan Zolomon a neve, vagy valami ilyesmi. Talán neki van olyan kis farka! Hívjon fel +44 877-882. B... meg a nagymamát is, te seggfej! (c) 91 Zolomon S&S Farok!)

A program a fenti üzenetből kapta a nevét. Az Adolph vírus változó hosszal (2109–2445 bájt) fertőz, a víruskódot az állomány végére rakja. A program kiforrott „levélhordozónak" tűnik.

A vírus neve: Leprosy

Egyéb elnevezése: Leprosy 1.00, News Flash.

Hossza: 666 bájt.

Kódtípusa: Nem rezidens, .COM és .EXE fertőző, felülíró.

Azonosítása: Scan /X V67+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: A vírus szintén extrém szaporaságáról híres. Napjainkra már egész víruscsaládot alkot, amelynek első tagját 1990. augusztus 1-jén izolálták San Francisco környékén. Az eredeti hordozóprogram egy segédprogramnak álcázva a BBS-ekben bukkant fel egy 486COMP.ZIP nevű állományba beépítve. A vírus nem rezidens, felülíró, a .COM és az .EXE programokat fertőzi meg. A COMMAND.COM-ot is megtámadja.

Már többb mint négy mutánsa forog közkézen. A vírus hossza 321 és 370 bájt között van. Fertőzése során egyszerűen felülírja a fertőzött programot. A McAfee-féle dokumentáció is azt javasolja, hogy töröljük a fertőzött programot, mert az állomány elejének felülírása miatt semmilyen szoftveres vírusölő program nem gyógyítja meg. Csak behatolásának megelőzésére törekedhetünk.

Amikor a program fertőz, állománytípusra való tekintet nélkül egyszerűen beírja magát a program elejébe. Az aktuális könyvtárnál egy szinttel lejjebb lévő könyvtárat is meg tud fertőzni. Ha az aktuális könyvtár a főkönyvtár, akkor ott minden programot egy menetben megfertőz. A megfertőzött állományokat első látásra nem vesszük észre, mert a bejegyzett hossz marad, csak a kód eleje válik vírussá.

Amikor felülírja az állományokat, a következő üzenetet jeleníti meg a monitoron:

```
Program to big to fit in memory
```

(DOS üzenet: A program túl nagy ahhoz, hogy beférjen a memóriába.)

Más esetekben a vírustól a következő üzenetet kapjuk:

```
NEWS FLASH!! Your system has been infected with the
incurable decay of LEPROSY 1.00, a virus invented by
PCM2 in June of 1990. Good luck!
```

(Gyorshír! Az ön rendszerét megfertőzte a Leprosy 1.00 gyógyíthatatlan nyavalya, egy vírus, amelyet a PCM2 talált fel 1990 júniusában. Sok szerencsét!)

Ez utóbbi szöveget hét fertőzés közül egy esetben olvashatjuk. A vírus tipikus felülíró vírus. Programozástechnikailag is ez a legegyszerűbb megoldás, úgy okozza a legnagyobb kárt, hogy közben nem is kell törődni az eredeti program formátumával és működőképességével. Ha a floppyn vagy a merevlemezen a COMMAND.COM fertőzött, akkor egyszer vagy kétszer megjeleníti a következő üzenetet:

```
Bad or missing Command Interpreter
```

(Rossz vagy hiányzó parancsértelmező)

Természetesen a rendszerbetöltési folyamat sem képes lefutni. Még azután sem, hogy egy másik bootlemezt tettünk be a gépbe. Ilyenkor csak a Reset gomb segít. Az üzeneteket a vírus kódolva tárolja. A fertőzést a következő hexadecimálisan megadott karaktersorozat azonosítja:

```
740AE8510046FE06F002EB08
```

Ismert változatai:

Leprosy B: Abban tér el alapvetően az eredeti Leprosy vírustól, hogy más titkosítási módszert használ önmaga kódolásához. Emiatt hagyományos eljárásokkal nem vehető észre. Amikor a kód lefut, ez a változat négy másik .COM vagy .EXE programot fertőz meg az aktuális meghajtó aktuális könyvtárában. Ha nem talál négy megfertőzhető programra az adott könyvtárban, akkor egy szinttel feljebb megy a könyvtárfán, és ott keresi meg a fertőznivalót. Az első 666 bájtot felülírja. Hogy miért a 666-ot választotta? Talán mert az is apokaliptikus szám.

Üzenete is eltér az eredetiétől:

```
ATTENTION! Your computer has been afflicted with
the incurable decay that is the fate wrought by
Leprosy Strain B, a virus employing Cybernetic
Mutation Technology (tm) and invented by PCM2 08/90.
```

(Figyelem! Az ön számítógépét gyógyíthatatlan kór sújtotta. Ez a sorscsapás a Leprosy B vírusfajta, amely a kibernetikai mutációs technológiát alkalmazza, és amelyet a PCM2 talált fel 1990 augusztusában.)

Más esetekben az első vírushoz hasonló hibaüzenetet jelenít meg:

```
Program too big to fit in memory
```

Leprosy C: Az .EXE programokat megtámadó és azokat felülíró vírus. Futtatásakor az aktuális könyvtárban lévő első három nem fertőzött állomány első 321 bájtját felülírja, ezáltal ott helyreállíthatatlanul tönkreteszi a programokat. Ha egy ily módon megrongált programot akarunk elindítani, a vírus által felülírt rész a továbbiakban a szerzőt ajánlja.

Leprosy D: A .COM és az .EXE programokat felülíró vírus, beleértve a COMMAND.COM-ot is. A megfertőzött gépet újraindítva a „Bad or Missing Command Interpreter" üzenetet kapjuk a COMMAND.COM tartalmának felülírása miatt. Ez a vírus is az állományok első 321 bájtját írja felül. Egyéb működése megegyezik a Leprosy C víruséval.

A Leprosy vírusok fertőzése során a fájlok mérete nem változik meg. Ha az általuk megfertőzendő fájl mérete kisebb, mint a vírus hossza, akkor a fertőzés

után az állomány a vírussal azonos hosszúságú (és tartalmú) lesz. A vírus a fertőzés során a fájl könyvtári dátumbejegyzését és idejét megjelöli, és erről ismeri fel a fertőzött állományt, hogy elkerülje a többszörös fertőzést.

A Leprosy C azonosító szekvenciája (hexadecimálisan):

56 33 F6 E8 51 00 0B C0 74 0A E8 18 00 46 FE 06

A Leprosy vírusokra általában jellemző fejléc:

56 33 F6 E8 4D

Made in Hungary

Turbo Kukac, Kukac, Monxla, Monxla-B,
Töltögető, Polimer, Phantom.

Sokáig azt hittük, hogy „programozói nagyhatalom" vagyunk. Valójában Magyarországnak csak jó kódolói voltak, akik a nyugati munkakörülmények között kiváló kreatív napszámosoknak, bedolgozóknak bizonyultak. Ha végignézünk a világ szoftverkínálatán, nagyok kevés olyan terméket találunk, amelyet teljes egészében Magyarországon fejlesztettek ki, és a benne lévő ötletek a felszín megvakarása után is eredetinek minősülnek.

Bezzeg a vírusoknál! Ott rögtön érvényesült alkotói fantáziánk és ötletességünk. Már középiskolás tanuló is készített olyan vírust, amely mind a mai napig a vírusvédő kártyák és programok egyik legkeményebb próbatétele világszerte. Magyar eredetű a hardverhibát szimuláló vírusok ötlete is, amelyek őse adott volt: Magyarországon széles körben alkalmazzák a büntető, romboló másolásvédelmeket...

A vírus neve: Turbo Kukac

Egyéb elnevezése: Turbo @ v.9.9., Turbo Kukac 9.9, Polish-2.

Hossza: 512 bájt.

Kódtípusa: Parazita, van rezidens része és a .COM állományokat fertőzi meg.

Azonosítása: CHKSeq v.1.0. ,Scan V71+.

Eltávolítása: CHKVir v.4.01, Sysdoki 1,0.

Leírása: A vírus először 1990 novemberében bukkant fel. Ha aktív, akkor a Shift–Print Screen billentyűkombinációra a „Turbo Kukac 9.9" szöveget írja ki. Képes bemászni a Novell hálózatok csak végrehajtható (execute only) típusú programjaiba is. Eddig csak szűk körben jelent meg néhány fejlesztő laboratóriumban. Valamelyik hazai egyetemi központban készült. Különböző szintekig visszafejtett forráskódjait sokan ismerik, ezért új változatainak megjelenésétől is tartani lehet.

A vírus memóriarezidens, a memóriában a COMMAND.COM területére telepszik, más rezidens programok előtt. A rendszermemóriát 1040 bájttal csökkenti. Az INT 05-öt és az INT 21-et magára irányítja. Nem használja a rendszer szabványos rezidens memóriaszegmensét, mert egy „memórialyukba" épül be. Ezt a technikát elsőként alkalmazó vírus volt.

Nem a programok futtatásakor, hanem az állományok kezelésekor, megnyitásakor fertőzi meg a .COM programokat. (Betekintés, másolás stb.) Így példá-

ul, ha jelen van a memóriában és egy .COM állományt másolunk, akkor az eredeti és a másolat is fertőzött lesz. A fertőzött állomány 512 bájttal lesz hosszabb és a víruskód az állomány végére épül be. A könyvtári bejegyzés dátumát átírja a fertőzéskor aktuális dátumra és rendszeridőre. A fertőzött állományok végén a következő karakteres azonosító sorozat látható:

```
Turbo Kukac 9.9 $
```

Ha rezidens antivírus program figyeli a megszakítások átirányítását, akkor a vírus nem aktív. Miután a rendszer három állományt beolvasott, a negyedik program megnyitására „File not found" rendszerüzenetet kapunk.

A vírus neve: Kukac

Egyéb elnevezése: @, Turbo 448, @ Virus, Turbo @.

Hossza: 448 bájt.

Kódtípusa: Parazita, a .COM állományt fertőzi meg, rezidens része van.

Azonosítása: Sysdoki, Scan V71+.

Eltávolítása: Sysdoki, vagy törölni a fertőzött állományokat.

Leírása: Ez a vírus valószínűleg a Turbo Kukac korábbi verziója, bár átírás is elképzelhető. Eredeti magyar fejlesztés. Célja a bosszantás. A .COM állományokat fertőzi meg, beleértve a COMMAND.COM-ot is. A COMMAND.COM után, a memória „árnyékban lévő" részében válik rezidenssé, a commmand interpreter (parancsértelmező) után. Látszólag nem csökkenti a szabad memóriát. A vírusban a következő szöveg található:

```
Üdv minden nagytudásúnak ! Turbo @ ... ...
```

Az INT 21-et magára irányítja. Csak állománynyitásra és nem programvégrehajtásra fertőz, ami felfedezését alaposan megnehezíti. Az egyes állományok hossza 440 bájttal nő meg, a víruskód az állományok végére kerül. A könyvtári fájlbejegyzéseket átírja a fertőzés közbeni rendszeridőre és dátumra. Az antivírus programokkal szemben hasonlóan viselkedik, mint a másik kukacvírus.

A vírus neve: Monxla

Egyéb elnevezése: Time.

Hossza: 939 bájt.

Kódtípusa: A .COM állományokat fertőző, műszaki hibát szimuláló parazita programvírus, rezidens résszel.

Azonosítása: Scan V71+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: Magyar eredetű programvírus. 1990 novemberétől ismerjük. Általános .COM fertőző, beleértve a COMMAND.COM-ot is.

A vírussal fertőzött program lefutása után a vírus beépül a memóriába, ellenőrzi a rendszeridőt, és ha a pillanatnyi időpont — az óra leolvasható utolsó két jegye — több mint 32/100 másodperc, akkor a vírus saját roppant kicsi rezidens részét installálja a memóriába, a 640 K-s konvencionális DOS memória felső részébe. Utána elkapja az INT 20 és az INT 2F megszakítókat. Érdekes az INT 2F, mert annak utolsó használata dönti el a vírusnak a memóriában tör-

ténő allokációját. A Monxla ugyanis több helyre is képes magát elhelyezni. Ugyanakkor ez a rezidens része nem fertőzi az állományokat.

Amikor a Monxla egy megfertőzhető programot keres, alapfeltétele, hogy annak hossza a 3840 és a 64000 bájt közötti tartományba essen. Először az aktuális könyvtárban keres, majd rátér a DOS-ban meghatározott keresési útvonalakra. Amint a feltételeknek megfelelő első állományt megleli, megfertőzi azt.

Ha ekkor valamely hónapnak nem a 13. napja van, 939 bájtot ad hozzá a fertőzendő állományhoz, mégpedig a fájl végére. Ha viszont 13-a van, akkor aktivizálódik a vírus kártevő funkciója. Az, hogy ilyenkor mit csinál, függ a rendszeróra pillanatnyi állásától. Három lehetőség áll előtte:

1. Amikor a rendszerórán jelzett másodperc értéke nagyobb, mint 60/100, a processzor 4 HLT (halt) parancsot kap, amelyet egy véletlen INT hívással a fertőzött program elejére helyez. Ezt követően a program meglehetősen furcsa károkat okoz. A kár mértéke és jellege attól függ, hogy éppen melyik INT funkciót és hogyan hívta meg a víruskód.

2. Ha a másodperc értéke nagyobb, mint 30/100, de kisebb, mint 60/100, akkor a vírus két INT 19 hívást helyez a megfertőzött program elejére. A programot végrehajtva biztosan újraindítás (reboot) lesz a végeredmény, de elegánsan megoldva! Ehhez kapcsolódik a harmadik lehetőség: az INT 00h-val és az INT 1Ch-val való manipulálás, amelyek magára irányításával a rendszert kiakasztja.

3. A harmadik lehetőség az, amikor a másodperc értéke 00/100 és 30/100 között van. Ekkor INT 20 hívást helyez a fertőzött program elejére, amely az indítás után rögtön az adott programból való kilépést eredményezi.

A Monxla rezidens része játszik a RAM felfrissítésével, és néha véletlenszerűen módosítja azt, így a BIOS tisztázatlan eredetű paritáshibákat jelez.

A vírus neve: Monxla B

Egyéb elnevezése: Time B.
Hossza: 535 bájt.
Kódtípusa: Parazita, rezidens, .COM fertőző.
Azonosítása: Scan V74+.
Eltávolítása: Törölni a fertőzött állományokat.
Leírása: A Monxla B vírus Magyarországról 1991 januárjában került ki külföldre. Forrása valószínűleg az eredeti vírus írója, mert a kód módosítására lehet következtetni. A program a .COM állományokat fertőzi meg, beleértve a COMMAND.COM-ot is. Egy programot megfertőz az aktuális könyvtárban, egyet pedig tönkretesz.

A Monxla B rezidens része szintén a rendszeridőt nézi. Ha a rendszeridő neki megfelelő, akkor megfertőz egy vagy több .COM programot, amit vagy az aktuális könyvtárban, vagy pedig a rendszer elérési útvonalán keres. Úgy teszi tönkre a kiválasztott .COM állományt, hogy az első öt karaktert felülírja a hexa 004D004F4D jelsorozattal, ami karakteresen is érdekes:

```
M OM
```

A tönkretett program hossza természetesen nem változik. Ha ezt a progra-

mot futtatni akarjuk, akkor a rendszer úgy kiakad, hogy csak a főkapcsolós újraindítás segít.

Ha a rezidens rész érzékelése szerint a rendszeridő nem nulla, akkor a Monxla az aktuális könyvtárban egy vagy több .COM programot megfertőz, de ha itt nem talál alanyokat, akkor a rendszerútvonalon megkeresi a fertőzhető többit. A fertőzött .COM program 535 bájttal lesz hosszabb, a kód a fájl végére épül be. A vírus a fertőzött állományok könyvtári bejegyzésének adatait a fertőzéskori aktuális rendszeridőre és dátumra cseréli ki.

A vírus neve: Töltögető

Egyéb elnevezése: Filler, Fill, Arc.

Hossza: Nincs rá adat.

Kódtípusa: Rezidens résszel rendelkező, bootszektort fertőző, a partíciós táblát teszi tönkre. A „stealth" (lopakodó) technikát alkalmazza.

Azonosítása: Bootkill 1.04, Sysdoki, SCAN 71+.

Eltávolítása: Bootkill 1.04, Sysdoki, Clean 80+.

Leírása: Aktivizálódásának feltétele, hogy a számítógép belső rendszerórája 1990. július elsejét vagy annál későbbi dátumot mutasson. A vírus ugyanis addig az időpontig csak terjedt. Ezt követően viszont a 21. rendszerindításra tönkreteszi az A: meghajtóban található floppyt, valamint a merevlemez FAT-tábláját. Járványt a nyári iskolai szünidőben, azaz július 1. és szeptember 1. között okoz. Az XT-ket nem támadja meg, csak szaporodik rajtuk. Azokról kerül azután az AT gépekre, ahol — miután elérkezett az ideje — pusztít.

Ez a bootszektort megtámadó vírus egyike a legintelligensebb vírusprogramoknak, amelyet valaha is írtak. Szerzője felhasználta benne mindazt a programozói tudást, ami a bootvírusokról eddig napvilágra került. A vírus jelenléte a lemezen semmilyen megszokott eszközzel nem deríthető fel. Ha a memóriában van, akkor mindig az általa elraktározott sértetlen bootszektor képét mutatja be, bármilyen segédprogrammal vizsgáljuk is a lemezt. A (c) Brain vírus hagyományait követve védekezik a direkt lemezírással dolgozó segédprogramok ellen is.

A Bootkill programcsomag eredetileg még azt tartalmazta, hogy a bootvírus lecseréli a bootszektort. Ismeretlen vírusok jelenlétéről éppen az árulkodik, hogy nem a megszokott szöveges rendszerüzenetet találjuk ebben a szektorban. Nos, a Töltögető az első olyan bootvírus, amely miután a merevlemezen fertőz, nem az egész partíciós táblát cseréli le, hanem annak csak a programját, a rendszerüzeneteket pedig változatlanul hagyja. A Bootkill program 1.04 verziója már nemcsak képes kiirtani ezt a vírust a memóriából, hanem a legtöbb esetben a merevlemezt is helyreállítja a vírus „felrobbanása" után. Ha a Töltögető a Stoned vírussal kombináltan fertőzte meg lemezünket, akkor azt nem lehet ilyen egyszerűen megtenni, mert a két program „összedolgozva" eltünteti a partíciós tábla programját. A vírusmentesítő programnak ezt fel kell ismernie, és újra generálnia, amire azonban csak a Sysdoki képes.

A vírus csak rendszerlemezzel terjed, de ha a memóriában van, elegendő egy

táblában nem fér el, hiszen a programvírusokhoz viszonyítva hatalmas, több mint 4 kilobájt a kód hossza. Ezért az eredeti bootprogramot és saját testének nagy részét a 360 kbájtos floppy 40. sávjára helyezi el úgy, hogy előzőleg formázza az ottani szektorokat. Rendszerüzeneteit kódolva tartalmazza, így azok szövegkereséssel sem ismerhetők fel. Profi munka. A vírust winchesterkezeléséről ítélve egy 20 Mbájtos merevlemezes egységgel rendelkező gépen fejlesztették ki.

Felrobbanása során a vírus a következő rendszerüzenetet írja magyar nyelven a képernyőre:

```
Hahaha, vírus van a gépben!!
Ez egy eddig még nem közismert vírus.
De hamarosan az lesz.
A neve egyszerüen töltögető. Ezt a nevét onnan kapta,
hogy feltöltögeti a FAT-táblát különböző alakzatokkal.
Ez már meg is történt!
```

A FAT-táblát valóban feltölti az ASCII 01 karakterrel (halálfej), úgy, hogy ezek felnagyított formában hasonló alakzatot rajzolnak ki, mint amilyen maga a karakter. Egy szektorba 8 ilyen holdarc-ábrát tesz. Hasonlóan a Vacsina magyarországi eredetű (zenélő) átirataihoz, még a Ctrl-Alt-Del gombokkal történő rendszerindítás után is a tárban marad. Csak a főkapcsoló képes onnan eltávolítani, no meg a megfelelő vírusölő...

A Töltögető 1990 hosszú forró nyarán okozott nehéz perceket a felhasználóknak és kemény munkát a vírustalanítással foglalkozó szakembereknek. A vírust valószínűleg 1990 március végén eresztette el tréfás kedvű fejlesztője. Az első időszakban Komárom, Tatabánya, Budapest környékéről jeleztek fertőzéseket. A vírus fejlesztési helye Székesfehérvár. Sajnos a vírus írójától kikerült a teljes fejlesztői programkészlet. A forráskódállományok ugyan kódolva vannak, de a lemezen rajta van a megfejtő segédprogram, a PMFEJT.COM is, amely jelszóra (password) indul, és elég könnyen megfejthető. A fejlesztő a PathMinder kódolójával rejtjelezte a kódot. A lemez maga is vírusfertőzött, elindítása épp ezért veszélyes. A később felbukkant hasonló tartalmú lemezekről a vírust már eltávolították. Aki a megfejtett rutinokat megérti, maga is zseni, mert azokat szerzőjük nem kommentezte fel. A lemez tartalma:

```
antivira.com     1252     4-19-90
indit.000        1245     4-18-90
indit.001         293     4-18-90
kimenta.com      1365     3-11-90
osszes.000       4166     4-18-90
pmfejt.com       3984     4-06-90
virita.000        271     4-18-90
virusa.000      18415     4-18-90
virusa.asm      12209     3-14-90
virusa.com      12968     4-03-90
virusa.vir      12968     4-03-90
```

A lemez igen gyorsan elterjedt. Most már lemez.txt-vel kiegészített változata is ismert, ahol a lemez nem vírusos, de a lemez.txt tartalmazza azt a számot,

amlynek alapján vissza lehet fejteni a titkosított szövegeket. A titkosított kódot alapnak használva többen is megpróbálkoztak vírusváltozatok írásával, míg mások csak a terjedési algoritmust használták fel. Jelzések szerint a forráskód átírására az oroszországi vírusművészek vállalkoztak legnagyobb számban, azért újabb variációk felbukkanása elsősorban abból az irányból várható.

A vírus neve: Polimer

Egyéb elnevezése: Polimer Tapeworm.

Hossza: 512 bájt.

Kódtípusa: Parazita, rezidens része nincs, a .COM állományokat fertőzi meg.

Azonosítása: Scan V71+, Pro-Scan 2.01+.

Eltávolítása: Törölni kell a fertőzött állományokat.

Leírása: 1990 nyarán jelent meg a Polimer magnókazettát népszerűsítő fájlvírus. Működési elvét tekintve hasonló az Április 1. vírushoz, ami annyit jelent, hogy csak .COM programokat fertőz meg. Ha a fertőzött programot elindítjuk, akkor egy pillanatra a következő szöveg jelenik meg a képernyőn:

```
A le'jobb kazetta a POLIMER kazetta! Vegye ezt!
```

Nem a mi sajtóhibánk! A „g" betű helyett valóban aposztrófot gépelt be a vírusíró. A szöveg a fertőzött állományok végén található. A vírus hossza 512 bájt. Eredeti magyar fejlesztés. Írója valószínűleg a kazetta gyártójának akart kellemetlen perceket szerezni. A vírusnak semmi köze az általa „reklámozott" Polimer Kisszövetkezethez!

Miután ez az üzenet megjelent, a vírus megkeres egy fertőzhető másik állományt az aktuális könyvtában, az aktuális meghajtón. A vírus megvizsgálja, hogy a .COM állomány megfelel-e a fertőzéshez szükséges kritériumoknak, azaz 512 és 64758 bájt között van-e. Ilyenkor egyetlen állományt fertőz meg, mert ennyire van ideje, anélkül, hogy feltűnnének a hosszadalmas lemezműveletek. A vírusnak van egy programozási hibája is: Ha az állomány „read only" attribútummal rendelkezik, akkor nem fertőződik meg, helyette a monitoron felvillan a következő üzenet:

```
$ERROR
```

A vírus ugyan 456 bájt hosszú, de az egyes állományoknál okozott növekedés a szemét hozzámásolása miatt 512 bájt.

A vírus neve: Phantom

Egyéb elnevezése: Netinfo.

Hossza: 2274 bájt.

Kódtípusa: Parazita, rezidens része van, a .COM, az .EXE és az overlay állományokat fertőzi meg.

Azonosítása: PC-Scan 1.0, Scan 80+.

Eltávolítása: Clean 80+.

Leírása: A Phantom vírushoz a VirNet BBS-en keresztül jutottunk hozzá. A felhasználó elsősegélyként a NETINFO.ZIP állományt küldte fel ellenőrzés céljából.

A NETINFO.ZIP fájl tartalma:

```
Length Method   Size  Ratio Date     Time   CRC-32   Attr Name
  48   Stored     48   0%   11-11-90 17:49  30b5ed4e --w START.BAT
 445   Implode   347  23%   11-11-90 17:23  8a2aaae6 --w LEVEL.TXT
1339   Implode   893  34%   11-11-90 17:23  c6f1b5fd --w INFO.TXT
4227   Implode  2188  49%   15-12-90 17:55  3a67fee1 --w UDV.COM
 282   Shrunk    260   8%   11-11-90 17:13  6f344ddb --w MORE.COM
 539   Implode   303  44%   11-11-90 18:16  c34af666 --w RENDEL.TXT
6880           4039  42%                                6
```

Megvizsgálva a ZIP állományt, abban a START.BAT batchfájl az alábbi tartalmú:

```
echo off
break off
type info.txt | more
udv
```

```
            REMÉLEM ÖNT IS ÜDVÖZÖLHETJÜK A
NN    NN  EEEEE  TTTTTT  II  NN    NN  FFFFFF     0000
NNN   NN  EE       TT    II  NNN   NN  FF       00    00
NN N  NN  EEEE     TT    II  NN N  NN  FFFF     00    00
NN   NNN  EE       TT    II  NN   NNN  FF       00    00
NN    NN  EEEEE    TT    II  NN    NN  FF         0000
                          Rt.
                TAGJAINAK SORÁBAN!
```

```
NETINFO Rt.
MISKOLC Pf.: 43
Telefon: 46 11-253
Telefax: 46 11-452
```

A batchfájl végén az UDV.COM Phantomvírusos program fut le, ezzel megfertőzve a felhasználó számítógépét.

A ZIP fájl a NETINFO cég reklámszövegét tartalmazza, amelyben felhívást intéznek a felhasználókhoz, olcsó nemzetközi információkhoz történő hozzájutást ajánlva. A cég nemcsak hogy nem létezik, de nem is létezett ezeken a neveken és telefonszámokon. A vírusfertőzés oka az, hogy önvédelmi, önellenőrző rendszer nélkül szöveges állományt átkonvertáltak .COM kiterjesztésű programmá, majd útjára engedték. Ezt a programmodult tudatosan fertőzték meg, és így terjedhetett tovább, míg el nem jutott hozzánk.

A Phantom vírus hossza 2203 bájt. A vírus kódolt formában az alábbi szöveget tartalmazza, amelyből válogatott részletekkel a monitoron is találkozhatunk. Íme a vírus szövegállománya, amely kódolt formában (és zagyva angolsággal) található benne:

```
The PHANTOM Was HERE - Sorry...HI ROOKIE!
I'm a THESEASE! I live YOUR computer - sorry
Thanks to Brains in the Computer Siences!
```

```
Copyright (c) PHANTOM -- This virus was designed in
HUNGARIAN VIRUS DEVELOPING LABORATORY. (H.V.D.L.) v1
```

„A Phantom járt itt. Elnézést... Helló, újonc! Én egy (?) vagyok. Az ön számítógépében élek. Köszönet a számítógéptudományokban dolgozó agyaknak! Szerzői jogok (c) Phantom. Ezt a vírust a Magyar Vírusfejlesztő Laboratórium (MVL) tervezte. v.1."

Terjedése a naptárhoz kötötten eltérő módokon történik: A vírus június 23-ig csak .COM programokat fertőz. Ezt követően az .EXE programokat a copyright jelsorozattal (109 bájt) fertőzi, plusz a hét napjától függően különböző toldalékokat tesz hozzá. Vasárnap a „The PHANTOM Was HERE - Sorry..." szöveget, a hét többi napján 7–14 bájt hosszúságú különböző értelmetlen sztringeket (hétfőn 8, kedden 7, szerdán 9, csütörtökön 14, pénteken 8, szombaton 10 bájtot).

És ez még nem minden. Az ARC és DBF állományok elejére a copyright sztringjét írja be. A DBF állományok elején az adatbázis fejléce, vagyis a struktúra leírása van, tehát az adatbázis használhatatlanná válik. Az ARC állományok tagjaiból lehet kiszámítani a következő elemet, ezért minden ARC állomány meg fog sérülni. A Phantom a sokoldalúan pusztító vírusok közé tartozik. Mellesleg a videó kontroller kikapcsolását is elvégzi. Egy felhasználó jó pár napig szenvedett, végül a kép visszakapcsolására külön kis programot írt, mire rájött, hogy mi a hiba oka.

A vírus a következő megszakítókat cseréli le: INT 20, INT 21, INT 24, INT B2. A bootszektorral is manipulál valamit. Visszafejtése a könyv nyomdába adásáig még nem fejeződött be. Az biztos, hogy INT 25-tel és INT 26-tal kezdi, vagyis közvetlen lemezolvasási és lemezírási műveleteket végez.

A mi számunkra van e vírusnak még egy pikantériája. Június 23., azaz a 06.23. számsor Farmosi István egykori munkatársunk születési dátuma is. Farmosi előszeretettel használta szoftvereiben családtagjai és a saját személyi számát. Így került A PRGDOKI v2.11 belsejébe is egyedi azonosítóként a 06.23-as. A vírus visszafejtése során Farmosi annak idején meglepetten közölte, hogy a vírus éppen az ő születési dátumához igazodva viselkedik különbözőképpen. Az biztos, hogy a vírust nem Farmosi írta, de szinte az is biztosnak mondható, hogy neki szánták hitelrontás céljából. Addig ezek a gusztustalan módszerek távol maradtak a magyar vírusíróktól. Mint annyi rossz, a Phantommal ez is megérkezett.

De ebből az is fontos tanulság, hogy a személyünkre vonatkozó információkat (név, becenév, személyi szám, telefonszám, a közvetlen környezet által ismert jellegzetes szófordulatok) nem szabad azonosítóként, illetve jelszóként megadni.

Távol-keleti üdvözlet

Azusa, Blood, Bloody!, 382 Recovery, 1575, 1575-B, 1575-C, 1253, Plastique, HM2, Plastique 4.51, Plastique Cobol, Plastique-B, Invader, Fu Manchu, Taiwan, Taiwan-B, Taiwan-3, Taiwan-4, Disk Killer, Korea, MusicBug, Stoned, Stoned-A, Stoned-B, Stoned-C, Stoned-D, , Rostov, Sex Revolution V1.1, Sex Revolution V2.0, Stoned-E, Stoned-F, Stoned II, Donald Duck, Wolfman, Joshi, Fellowship, Ashar, Brain, Brain-B, Brain-C, Clone, Clone-B, Ohio, Pentagon, Den Zuk, 1381.

A Távol-Kelet országai igen gyorsan bekapcsolódtak a vírusok kibocsátásába. Érdekes módon ők ezzel a módszerrel részben a forgalmazók ár- és szerződésdiktátumainak megtörésére törekedtek. A vírusok terjesztése — sok esetben a gyártók tudta nélkül — a Távol-Keletről szállított szoftvereken, illetve az installált gépek merevlemezein történik. A nagyvolumenű gépkibocsátás miatt ez komoly járványokat okozhat.

Fejezetünkben azokat a vírusokat tárgyaljuk, amelyek az utóbbi években a szakirodalom szerint bizonyíthatóan a Távol-Keletről terjedtek el. Ezek közül néhány programozástechnikailag igen bonyolult megoldásokat is tartalmaz. A több verzióban készült vírusok egy része ugyanúgy programhibákkal terhelt, mint sok ottani eredetű szoftver. Nem véletlen, hogy e vírusok kirajzási pontjai a kalóz szoftverek kirajzási pontjaival esnek egybe (Malajzia, Tajvan stb.)

A vírus neve: Azusa

Egyéb elnevezése: Még nem ismeretes.

Hossza: Nem értelmezhető.

Kódtípusa: Bootszektort és partíciós táblát fertőz, rezidens része is van.

Azonosítása: Scan V75+.

Eltávolítása: Clean V75+.

Leírása: 1991 februárjában egy Távol-Keletről származó komputer-szállítmánnyal került az USA-ba ez a boot- és partícióstábla-vírus, amelynek érdekessége, hogy a COM1 és az LPT1 csatlakozási pontokat letiltja.

Amikor fertőzött lemezről hívunk rendszert, akkor a vírus beépül a memóriába, de még a hagyományos 640 K-s DOS területen belül, s többek között magára láncolja az INT 12-t, annak visszatérését tartja teljesen ellenőrzése alatt.

A rendszermemóriából 1024 bájt területet lefoglal magának. Ha merevlemezre installálja magát, akkor a partíciós táblába írja be magát. A vírus csak azokat az információkat tárolja, amelyek elegendőek a rendszer zavartalan működéséhez, az eredeti partíciós táblát a helyreállítás során a vírusból kell kibányászni vagy a partíciós tábla mentését visszatölteni.

A vírus figyeli, hogy amikor a memóriában van, megnyitották-e az állományt írásra. Ha igen, akkor egy Ctrl-Alt-Del rendszerindítást végez, aminek eredménye például dBase állományok esetén az adatok teljes elvesztése. Floppylemeznél azonban más a helyzet, ott kénytelen elmenteni az eredeti bootszektort. Ezt elhelyezi a floppy 40. sávjának 8. szektorában, magát pedig beteszi a bootrekord helyére. Ez azzal is járhat, hogy ha a floppy nem 360 K-s, hanem 1,2 megás, akkor a boot a lemez közepe tájára kerül és felülír más állományokat.

Az Azusa vírus számolja, hányszor indítottunk rendszert a fertőzött lemezről. 32 indítás után egy körre letiltja az LPT1 és a COM portokat, majd nullázza ezt a számlálóját. A következő rendszerindításnál viszont már működnek ezek a csatlakozópontok.

Magyarországon is fellépett egy furcsa, ebbe a sorozatba tartozó átirat. Többször megkerestek bennünket, hogy Bloody vírusuk van, és nem tudják kiirtani. Floppyn ezt a változatot tényleg annak ismeri fel a Scan 80, de a merevlemezen a Clean problémamentesen irtotta Azusaként.

A vírus neve: Blood

Egyéb elnevezése: Blood2.

Hossza: 418 bájt.

Kódtípusa: Nem rezidens, parazita, a .COM programokat fertőzi meg.

Azonosítása: Pro-Scan 2.0+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: A Dél-Afrikai Köztársaságban lévő Natalból származik a vírus, amelyről először Fidrik Skulason számolt be 1990-ben. A rendszerrel szállított számítógépeken indult el terjesztése az USA-ban. Szerencsére ritka.

A vírus általános .COM fertőző, a COMMAND.COM-ot is megtámadja. Másik változata, a Blood2 szintén hasonlóan viselkedik. Nem rendelkezik rezidens résszel. Amikor egy vírussal fertőzött programot elindítunk, megfertőz a C: lemez főkönyvtárában egy másik .COM állományt. A hossznövekedés ilyenkor 418 bájt. Ha ez a program a COMMAND.COM, akkor rendszerindítás következhet be. Ehhez járulhat a karakterek potyogása, és a kurzor lemegy a képernyő alsó sarkába. Ha újra akarjuk indítani, akkor a lemezhozzáférés közben a rendszer kimerevedik. A parancssor alatt a vírus által a memóriából véletlenszerűen válogatott idegen karakterek jelennek meg.

A vírust Natalban egy egyetemi hallgató írta. Miként a Kennedy vírus, ez is csak olyan .COM programokat tud megfertőzni, amelyek első pozícióin E6h (JMP) parancsot talál. A fertőzött program néhány esetben a következő üzenetet jeleníti meg:

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

Augusztus 15-e és az év vége között a vírus nem terjed. A fertőzött program elindítása a rendszer teljes kiakadását okozza.

Ismert átirata:

Blood2: Hasonló az eredeti vírushoz, de az automatikus rendszerindítás, a kiakadás és a potyogtatás rövid idő múltán fellép. Ez a változat augusztus 15-e után is ugyanúgy viselkedik, mint annak előtte.

A vírus neve: Bloody!

Egyéb elnevezése: Még nem ismeretes.

Hossza: Nem értelmezhető.

Kódtípusa: Partícióstábla- és bootvírus.

Azonosítása: Scan V72+.

Eltávolítása: Manuális módszerrel, Norton Utility segítségével a partíciós tábla visszamásolása a merevlemez 0. oldal, 0. sáv, 6. szektoráról vagy újraparticionálás és formázás.

Leírása: Tajvanból származó gépekkel és szoftverekkel 1990 decemberében érkezett Európába ez a protestáló vírus. Írói a kínai hadsereg pekingi, Tienamnen téri vérengzése miatta ezúton akartak tiltakozni.

A vírus rohamosan terjedt Európában és az USA-ban, és a járvány azóta is újra feléled, valahányszor előveszik az akkori gyári lemezeket. A vírus floppyn a bootszektort, a merevlemezen a partíciós táblát támadja meg. A betöltési folyamat során a vírus a hagyományos 640 K-s rendszermemória felső részén 2048 bájt helyet foglal magának, és ellenőrzése alá vonja az INT 12 visszatérését. A rendszerindítás ideje többszörösére nő. A merevlemez partíciós táblája is károsodhat.

A vírus számlálja a rendszerindításokat. 128 indítás után a következő üzenetet jeleníti meg a monitoron, a pekingi vérengzésre utalva:

```
Bloody! Jun. 4, 1989
```

Utána ezt már tíz indításonként újra megjeleníti. A szöveg a vírusban nem látható, mert kódolva van. Amikor memóriarezidens, akkor fertőz, ha egy állományt írásra vagy olvasásra megnyitottunk. Az egyszerű DIR parancsra ez a vírus nem fertőz.

Rokona a magyar Töltögető vírusnak. Onnan vette át azt az ötletet, hogy a floppy bootszektora látszólag normális DOS hibaüzeneteket tartalmaz. Utána vágta el az eredeti bootrekordot, és építette be magát a víruskódot. Az eredeti bootszektor a 11. szektorra van kimásolva, ami a 360 K-s floppyn a főkönyvtár része. Ha sok bejegyzés van a főkönyvtárban, akkor azt — miként a Stoned is teszi — felülírja.

A merevlemezen az eredeti partíciós táblát egészében elmenti a 0. oldal, 0. sáv, 6. szektorába, ahonnan úgy kell visszamásolni, miután egy tiszta rendszerlemezről rendszert indítottunk. Rendszerfloppyk esetében eltávolítható a tiszta rendszerről kiadott SYS paranccsal.

A vírus neve: 382 Recovery

Egyéb elnevezése: 382.

Hossza: 382.

Kódtípusa: Felülíró, .COM és .EXE fertőző.

Azonosítása: Scan V66+, Pro-Scan 2.01+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: A vírust elsősorban tajvani számítógépszállítmánnyal terjesztették az USA-ban. Valószínűleg a piaci háború részeként. akárcsak az újabb tajvani vírusok esetében. A célország az USA volt, Európában eléggé ritka.

A vírus a megtámadott állományok első 382 bájtját felülírja. A .COM és az EXE állományokat egyaránt fertőzi, beleértve a COMMAND.COM-ot is. Amikor a víruskód lefut, a vírus megnézi, hogy az aktuális meghajtó aktuális könyvtárában van-e fertőzetlen .COM állomány. Ha van, akkor annak első 382 bájtját felülírja. Ha a hossza ennél kisebb volt, akkor új mérete pontosan ennyi lesz. A felülírt részen helyezkedik el a vírus, az eredeti program pedig futásképtelenné és helyreállíthatatlanná válik.

Amennyiben már nem talál fertőzhető .COM állományt, úgy elkezdi fertőzni az .EXE állományokat is. A vírus csak a kiterjesztést nézi, ha átnevezzük az állományt, nem találja meg.

Ha a fertőzött programot megpróbáljuk futtatni, minden indítási kísérlettel csak a vírust indítjuk el, újra és újra. A vírus végül kiakasztja a rendszert. Jellemző viselkedésmódja az idegen karakterek megjelenítése, amelyeket a memóriából véletlenszerűen tesz ki a parancssorba. Legvégső trükkje, hogy kikapcsolja a lemezmeghajtók motorját, és csak a gép ki- és bekapcsolása tudja feloldani a zárlatot.

A 382 Recovery az újabb generációs romboló-felülíró irányzat egyik első képviselője.

A vírus neve: 1575

Egyéb elnevezése: 1577, 1591, Green Caterpillar.

Hossza: 1575 bájt.

Kódtípusa: Parazita, rezidens résszel rendelkezik. A .COM és az .EXE állományokat támadja meg.

Azonosítása: Scan V74+.

Eltávolítása: Scan V74+, Clean V74+, vagy törölni a fertőzött állományokat.

Leírása: A tajvani vírusfejlesztő laboratóriumok remekműve. Kanadában 1991 januárjában bukkant fel, Tajvanról érkezett gépeken és programlemezeken. Németországban már egy hónappal előtte megkezdte körútját. Ott tud csak terjedni, ahol Tajvanból „gyárilag" szürke vagy fekete DOS verzióval installálták a gépet. A Microsoft elleni tajvani vírusháború egyik lépése, megtorlás a Microsoft kemény fellépéséért az illegális tajvani másolatok miatt.

A vírus jelenlétét a .COM és .EXE állományok méretnövekedéséből, a rendszer szabad memóriájának csökkenéséből, valamint onnan lehet észrevenni, hogy a DOS DIR parancsát csak vánszorogva hajtja végre. Fertőzés után meg-

változik az állomány időpont- és dátumbejegyzése is. A COMMAND.COM-ot is megfertőzi, ezért viszonylag hamar észrevehető.

Amikor lefut a víruskód, a rezidens rész a rendszer memóriájának tetején foglal el magának 1760–1840 bájtnyi helyet, de nem képes beülni a HIMEM-be. A saját maga által elfoglalt memóriaterületet nem jegyzi be a memória-ellenőrző FCB-be (file control block), hogy ne bukjon le hamar. Így viszont ezt a területet más program felülírhatja. A vírus a 21-es megszakítót irányítja magára. A COMMAND.COM-ot a C: meghajtó gyökérkönyvtárában keresi, s megfertőzi, ha ott találja.

Az aktivizálódás a DOS DIR vagy COPY parancsához kötött. Ha ezt az utasítást kiadjuk, akkor az aktuális meghajtón minden alkalommal egy .COM és egy .EXE állomány fertőződik meg. Ilyenkor a fertőzött állomány ideje és dátuma a fertőzés időpontjában érvényes rendszeridő és dátum lesz. A hossznövekedés 1577–1591 bájt lehet, a paragrafushatártól függően. A vírus a megtámadott állományok végére épül be. Amikor a fertőzött programot futtatjuk, a vírus nem terjed, csak installálódik. A beépülés a DIR vagy a COPY parancsra történik.

Ismert változatai:

1575-B: Teljesen ugyanazt teszi, mint az alapverzió. Eltérés a memóriakezelésében van, ugyanis a 12-es megszakító vektort ez a változat nem irányítja magára.

1575-C: Hasonló a 1575-B változathoz. Aktivizálódása nemcsak a DIR és a COPY parancsra történik meg, hanem akkor is terjed, ha a programot végrehajtatjuk az operációs rendszerrel. A COMMAND.COM-ot megfertőzvén a rendszer kiakad.

A vírus neve: 1253

Egyéb elnevezése: AntiCAD, V-1.

Hossza: 1253 bájt.

Kódtípusa: Parazita, rezidens része van, a .COM állományokat és a partíciós táblát fertőzi meg.

Azonosítása: ViruScan V66+, Pro-Scan 2.01+.

Eltávolítása: Pro-Scan 2.01+, MDisk /P.

Leírása: Az 1253-as vírus 1990 augusztusában kezdett el terjedni Ausztriából kiindulva. Forrása Tajvan, ahol az Autodesk cég elleni első megtorló lépésnek szánták. A később még inkább eldurvult kereskedelmi háborúnak kettős oka volt: egyrészt az Autodesk szokatlanul keményen fellépett az úgynevezett „22 dolláros AutoCAD" illegális verzió ellen, másrészt megakadályozta, hogy egyes forgalmazók a másolásvédelem nélküli amerikai kópiákat értékesítsék, amiért pedig a felhasználók még a hivatalos árnál többet is hajlandók fizetni. A vírust egyes AutoCAD és más CAD rendszerek hivatalos kópiáira ráültetve, lejáratási céllal terjesztették. (Az Anticad vírus-sorozatból — és a hardlockos kópiákból — tapasztalhattuk, hogy a háború tovább eszkalálódott. Ez a vírusháború továbbterjedhet Európában olyan szoftverekre, amelyeket nem az amerikai feltételek és árarányok alapján forgalmaznak. Ezt a felhasználók túlnyo-

mó többségének csendes szimpátiája kíséri. Ugyanakkor a felhasználók is keresik a helyettesítő alternatív termékeket.)

A vírus általános .COM fertőző, beleértve a COMMAND.COM-ot. Ugyanakkor kettős természetű lévén, bootvírusként megfertőzi a floppy bootszektorát, illetve a merevlemez partíciós tábláját. Amikor installálja magát, a memória alsó részén foglal le magának 2128 bájtnyi helyet, mintha szokásos rezidens program lenne, s közben teljesen magára irányítja a INT 08, az INT 13, az INT 21 és az INT 60 vezérlését. Ha még nem lenne megfertőzve, beül a partíciós táblába a merevlemezen. Ha egy fertőzött programot floppyról indítuk, annak bootrekordját fertőzi meg.

Amikor a .COM program lefut, a vírus hozzáfűzi saját kódját az állomány végéhez, mégpedig úgy, hogy az első pár utasítást lecseréli olyan ugróutasításra, amely.k a vírus startpontjára mutat. A fertőzött állomány hossznövekedése 1253 bájt. A vírus ezt a növekedést nem rejti el a DIR parancs elől. A fertőzött állományok felismerhetőek a vírusazonosító karaktersorozatról: 562D31h. Karakteresen: V-1. Innen kapta a vírus egyik nevét.

A vírus akkor fertőzi meg a floppy bootrekordját, ha aktív a memóriában. Írásvédett lemezre nem tud írni, s ilyenkor különböző hibaüzeneteket kapunk. Ha lemezt formázunk vagy egy tiszta lemezről adjuk ki a DIR parancsot, akkor is rámegy. Igen gyorsan terjed, de a későbbi vírusok ismeretében ez a vírus inkább csak a terjedési algoritmusok próbájának tekinthető.

A vírus romboló rutinjának aktivizálódási feltétele, hogy december 24-i vagy annál későbbi rendszerdátumú gépen egy fertőzött programot indítsunk el az A: meghajtóból. (Ez a kulcslemezes másolásvédelmek sajátossága!) Ilyenkor a vírus 9 szektort felülír a program egyes részleteinek összekevert mozaikjával. Utána szép komótosan újra felülírja a lemezeket, és ezen ténykedésének folytatását csak a hálózati főkapcsolóval lehet megakadályozni.

Amikor megfertőzött partíciós táblájú merevlemezről vagy fertőzött bootrekordú floppyról hívunk rendszert, a vírus rezidensen installálja magát a memória tetejére, de még a hagyományos 640 K-s szegmensen belül. A rendszer memóriájának méretét lecsökkenti 77840 bájtra, legalábbis ennyit látunk belőle a CHKDSK paranccsal. Ekkor minden lefuttatott .COM program fertőzötté válik. Néhány esetben azonban nem ez történik, hanem a merevlemezről a rendszer újra betöltődik.

A vírus jelenlétének másik következménye a furcsa lemezaktivitás, egyes műveletek átirányítása. Például ha a C: meghajtóról formázni akarjuk az A: meghajtóban lévő lemezt, azt mondjuk, a B: meghajtóban keresi, s örülhetünk, ha nem a D: merevlemez partíciónkat formázza le.

A vírustól úgy lehet megszabadulni, hogy először is tiszta rendszert indítunk, leragasztott rendszerlemezről. Utána az összes fertőzött .COM állományt kiirtjuk, végül a McAfee-féle M-DISK /P paranccsal a megfelelő verzióhoz szükséges szoftverváltozatot alkalmazva visszatesszük az eredeti partíciós táblát. Erre a célra alkalmasak a Clean program 80-as utáni verziói. (DOS 5.0 esetén csak ez felel meg.) Sajnos a helyreállítás sok esetben nem sikerül, és a merevlemez adatai elvesznek, például ha más vírusokkal van tik-tak fertőzés-

ben. Akinek viszont van elmentett partíciós táblája és bootrekordja, azt ilyen veszély nem fenyegeti, mert az eredeti felállás egyszerűen visszatölthető.

A vírus neve: Plastique

Egyéb elnevezése: Plastic Bomb, Plastique 3012, Plastique 1.

Hossza: 3012 bájt.

Kódtípusa: Rezidens, parazita, .COM és .EXE fertőző.

Azonosítása: Scan V66+, Pro-Scan 2.01+.

Eltávolítása: Clean V72+. Pro-Scan 2.01, vagy törölni a fertőzött állományokat.

Leírása: Az Autodesk ellen indított vírushadjárat jegyében az ismeretlen tajvani csapat a korábbi „anticad" tapasztalatokat felhasználva kibocsátotta az Invader/Plastique vírusokat, amelyek sajnos Magyarországra is bejöttek, a Margaréta csomagküldő szolgálat által közvetlenül Tajvanról, a rendszerrel együtt importált laptopgépekkel. Óriási kárt okozott a többnapos leállás, míg sikerült megtisztítani a teljes számítástechnikai rendszert. Ugyanakkor a cég — ellentétben másokkal — szembenézett a fertőzés tényével, a nyilvánosság előtt is vállalta a történteket és megtette a szükséges intézkedéseket. Ezáltal nem csökkent, hanem nőtt a hitelük az ügyfelek szemében is.

A Plastique 1990 júliusában indult el Tajvanról. A vírus a Jerusalem, illetve a Fu Manchu távoli rokonsági körébe tartozik, de terjedelmesebb, hogy a szükséges intelligenciát bele tudják zsúfolni. Például a 4096 bájtos változat azért olyan hosszú, mert egy komplett bootszektort is tartalmaz.

A vírus célpontja nyilvánvalóan az AutoCAD program. Ha egy ACAD.EXE programot futtatunk a vírus jelenlétében, vagy pedig Ctrl-Alt-Del gombokkal újraindítunk, akkor a vírus aktivizálódik, alaposan felülírva szeméttel a merevlemezt és a floppyt, s összekeverve a CMOS setup RAM adatait is.

A vírus általános .COM és .EXE fertőző, de nem támadja meg a COMMAND.COM-ot. A fertőzött program végrehajtása során rezidensként installálja magát a rendszer alsó memóriatartományában, 3264 bájt helyet foglalva le magának. Az INT 21-et természetesen magára irányítja.

Miután a vírus rezidenssé vált, minden végrehajtott .COM és .EXE állományt megtámad. Sok programhiba is terheli ezt a különben elég intelligens vírust. A fertőzés nem mindig sikerül, ugyanis nem tud megbirkózni azokkal az állományokkal, amelyek a visszafejtés megakadályozására többszörös ugró utasítással kezdődnek. Ha sikeresen fertőz, akkor a hossznövekedés a .COM állományok esetén 3012 bájt, az .EXE állomány esetén pedig 3012–3020 között van. A nyitott állományok megfertőzésekor is sokszor hibázik.

A vírus nemcsak az ACAD.EXE programra vadászik. Károkozó rutinja szeptember 20. és január 1. között aktivizálódik. Két algoritmus között választ, véletlenszerűen. Az egyik esetben a rendszert alaposan lelassítja, mintegy 70%-kal. A másik esetben viszont a hangszórón keresztül bombarobbanás hangját imitálja.

Ismert változatai és átiratai:

HM2: Egy nem szaporodó, fejlesztési példány. Ha véletlenül vele fertőzött ál-

lomány kerül a gépbe, rendszerkiakadást okoz, amit csak újraindítással lehet megszüntetni. Hordozó-fertőző programja ismeretlen. Tajvanból érkezett szoftverszállítmányokban fordult elő 1990 májusában, júliusában. Ma már igen ritka.

Plastique 4.51: A vírus majdnem mindenben megfelel az eredeti Plastique vírusnak. Az eltérés kódolási algoritmusában van. Tajvan 1990 júliusától kezdte kibocsátani. Az átírás során a szoftverhibákat kijavították benne, és más a keresési szekvenciája is.

Plastique Cobol: A szoftverháború újabb lépése, ezúttal a Cobol programnyelv ellen. A vírus minden olyan programra vadászik, amelyik a COBOL.EXE programmal indítható. Rezidenssé válva a rendszermemóriából 3248 bájtot lefoglal. A programvírust azt követően indították el, hogy 1991 közepén a Microfocus Cobol korábban védelem nélküli változatát (néhány forglmazó nyomására) hardverlock-kal szerelték fel.

A megfertőzött .COM program 3004 bájttal, az .EXE állomány pedig 3004–3019 bájttal nő. A vírusban lévő belső keresési sztring ACAD.EXE helyett COBOL. A COMMAND.COM-ot nem fertőzi meg. Aktivizálódási feltételei is eltérnek. A január 1. és szeptember 21. közötti időszakban a rendszer működési sebességét felére-negyedére csökkenti. Aktivizálódása után 20 perccel a rendszer felgyorsul (visszaáll) eredeti sebességére („bemelegedési effektus"). Újabb 30 perc elteltével kikapcsolja a billentyűzetet, majd alaposan összekeveri a CMOS setup RAM tartalmát. Szeptember 21-től az év végéig nem aktivizálódik, hanem csak csendben lapul és szaporodik.

A vírus neve: Plastique-B

Egyéb elnevezése: Plastic Bomb, Plastique 5.21, Plastique 2.
Hossza: 4096.
Kódtípusa: Parazita, rezidens résszel rendelkező, .COM, .EXE és bootvírus.
Azonosítása: Scan V66+, Pro-Scan 2.01+.
Eltávolítása: Clean V72+, vagy törölni a fertőzött állományokat.
Leírása: 1990 júliusától ismert a Plastique-B, amely a korábbi vírus erősen módosított átirata. Nem fertőzi a COMMAND.COM-ot, de bootvírusként is viselkedik, fájlvírusként pedig általános .COM és .EXE fertőző. Szeptember 20-a előtt tudja csak magát rezidenssé tenni a memória alsó tartományában, 5120 bájt helyet szabályosan lefoglalva. Magára veszi az INT 08, az INT 09, az INT 13, valamint az INT ED megszakítókat.

Ha a rendszeróra szeptember 20-a utáni dátumot mutat, akkor a memória felső szegmensébe épül be. Végrehajtásra vagy állománynyitásra fertőzi a .COM és az .EXE állományokat. A hossznövekedés ebben az esetben 4096 bájt. Ebben a változatban sok korábbi programozási hibát kijavítottak. Bootvírusként is beépülhet, akkor a fertőzött lemezről való indításkor válik rezidenssé.

A pusztító rutin aktivizálhatóságának letelte után másképpen épül be a memóriába, mintegy 60%-kal lelassítja a rendszer működését és a hangszóróban időnként bombarobbanás hangját produkálja. A felülírás attól a dátumtól függ, amelyet a vírusban beállítottak. Több olyan változata ismert, amely csak a fel-

ülírás dátumának kezdeti és végpontjában tér el. Amikor felülír, akkor az elérhető meghajtók FAT, boot és főkönyvtári területeit írja felül.

A vírus neve: Invader

Egyéb elnevezése: Plastique Boot.

Hossza: 4096 bájt.

Kódtípusa: Rezidens résszel rendelkező, .COM és .EXE fertőző programvírus, amely bizonyos esetekben bootvírusként is beépülhet.

Azonosítása: Scan V67+, Pro-Scan 2.01+.

Eltávolítása: Scan /D, CleanUp V67+, vagy a fertőzött állományok törlése.

Leírása: A vírust Tajvanban készítették és eresztették útjára 1990 szeptemberében. Hordozói azok a gépek voltak, amelyeket Tajvanból installálva szállítottak, illetve amelyekhez 1990 szeptembere és decembere között programlemezt mellékeltek. Komoly járványt okozott. Lényegében a Plastique B továbbfejlesztett és bővített kiadása. Bootvírusként is képes beépülni, amellett megfertőzi a .COM és az .EXE állományokat, kivéve a COMMAND.COM-ot.

Amikor az Invader víruskódja lefut, a rendszermemória alsó részére épül be, 5120 bájt helyet szabályosan lefoglalva magának. Magára veszi az INT 08, az INT 09, az INT 13, valamint az INT 21 vezérlését. Akkor válik bootvírussá, amikor először lesz rezidens. Ekkor lecseréli a bootszektort egy látszólag teljesen normális 3.30-as MS-DOS bootrekordra. Ha erre véletlenül ránézünk, könnyen észrevehetjük, hogy baj van, mert a hibaüzenetek karaktersorozatai a szektor végén, nem pedig közben találhatóak, mint az igazi bootrekordokban.

Amikor jelen van a memóriában, minden megnyitott .COM és .EXE állományt megfertőz, a COMMAND.COM kivételével. A .COM állományok hossznövekedése 4096 bájt, a víruskód az állomány elejére épül be. Az .EXE állományoknál okozott hossznövekedés 4096–4110 bájt között van, és a vírus az állomány végére épül be. S ha még nem lenne ott, a nem írásvédett lemez bootrekordjába is sürgősen beépül.

A vírus aktivizálódása 30 perccel rezidenssé válása után történik. Ilyenkor a 286-os processzorú gépeken előbb zenél, majd rendszerindítást végez. A 386-os processzorúakon nem zenél.

A vírus neve: Fu Manchu

Egyéb elnevezése: 2080, 2086.

Hossza: 2086 bájt (.COM fájlhoz) vagy 2080 bájt (.EXE fájlhoz).

Kódtípusa: Parazita, rezidens része van. A .COM és az .EXE állományokat fertőzi meg.

Azonosítása: Scan, F-Prot, IBM Scan, Pro-Scan, VirexPC, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: F-Prot, Pro-Scan 1.4+, VirHunt 2.0+, VirexPC.

Leírása: Amikor a Fu Manchu vírus fertőz, a .COM állományok kezdetére, illetve az .EXE állományok végére fűzi be magát. A kód elemzéséből megállapítható, hogy a Jerusalem vírus átirata. Valószínűsíthető keletkezési dátuma

1988. október 3. A vírus jellegzetes azonosító (ID) karaktersorozattal rendelkezik:

`sAXrEMHOr`

Amennyiben óra van a gépünkben, egy véletlenszerű időtartam után hatvan esetből egyszer a következő üzenettel hökkenti meg a gép használóit:

`The world will hear from me again!`

(A világ ismét hallani fog rólam!)

És ekkor természetesen újraindítja a gépet. Meglehetősen kellemetlen, ha éppen egy dBase állománnyal dolgoztunk, ami nyitva maradt... A melegstartot (warm reboot) a vírus ráadásul túléli a memóriában. 1989. augusztus 1. után a vírus a billentyűzet-pufferen keresztül egyes politikusok nevéhez jelzőket biggyeszt a monitoron. Akkor kezd szövegelni, ha például a következő nevek bármelyikét begépeljük: Thatcher, Reagan, Botha, Waldheim. A jelzők különböző durvasági fokozatúak. A Botha neve után írt bastard (fattyú) és a Waldheim nevéhez biggyesztett nazi (náci) az enyhébbek közé tartozik.

Az üzeneteket a vírus kódolva tartalmazza! Néhány változata előszeretettel épül be átfedő (overlay), .SYS, valamint .BIN állományokba. Az USA-ban a szakirodalmi adatok szerint igen ritka, viszont Európában és a Közel-Keleten elég gyakori.

A vírus neve: Taiwan

Egyéb elnevezése: Taiwan 2, Taiwan-B

Hossza: 743 bájt.

Kódtípusa: Nem rendelkezik rezidens résszel, parazita, .COM fertőző.

Azonosítása: Scan V56+, F-Prot, Pro-Scan 1.4+, VirexPC.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: A vírust a R.O.C. (Republic of China = Kínai Köztársaság azaz Tajvan) területén izolálták, nem sokkal elkészítése után, 1990 januárjában. A vírus a .COM állományokat támadja, belelértve a COMMAND.COM-ot is, de nem marad rezidensen a memóriában.

Amikor a víruskód lefut, a vírus igyekszik a memóriában legalább három .COM állományt megfertőzni. Ha az aktuális könyvtárban nem talál alanyokat, akkor tovább keresgél a C: meghajtó főkönyvtárában, majd lefelé a könyvtári fa ágain. Amikor talál fertőzhető állományt, akkor kivesz annak elejéről 43 bájtot, bemásolja magát a helyére és a kivett állományrészletet áthelyezi a fertőzött állomány végére. A vírusban ennél a műveleti rutinnál van egy programhiba: ha a vírus 743 bájt hossznál kisebb .COM állományt fertőz meg, akkor a fertőzött programból egy 1486 bájt hosszú állományt kreál, mert induláskor nem ellenőrzi, hogy belefér-e. Ezzel pedig önmagát menti el még egyszer.

A vírus igen romboló természetű. Minden hónap 8. napján abszolút lemezformázást és felülírást végez a 0. logikai szektortól a 160. logikai szektorig, ami tartalmazza a FAT, a boot és a partíciós tábla, valamint a főkönyvtár információit.

Ismert változata:

Taiwan-B: Egy korábbi, kidolgozatlan verzió. Rossz a fertőző rutinja, a fer-

tőzött program futtatása során a gép kiakad. Fertőzési mechanizmusa már a végleges változatéhoz hasonló.

A vírus neve: Taiwan 3

Egyéb elnevezése: Még nem ismeretes.

Hossza: 2900 bájt.

Kódtípusa: Parazita, rezidens résszel rendelkezik, a .COM és az .EXE programokat támadja meg.

Azonosítása: Scan V64+, Pro-Scan 2.01+.

Eltávolítása: Clean V71+, vagy törölni a fertőzött programokat.

Leírása: Tajvanban a vírusháború részeként bocsátották szárnyra 1990 júniusában, a Disk Killerrel és más tajvani vírusokkal együtt. A Fu Machu-val mutat rokonságot.

Amikor lefut a víruskód, a vírus rezidenssé teszi magát a rendszermemória alsó részén, 3152 bájttal csökkentve a szabad memória méretét. Csak az INT 21 vezérlését veszi magára. A vírus a programok végrehajtásakor fertőz. A .COM állományok hosszát 2900 bájttal növeli meg, míg az .EXE állományok növekedése 2900–2908 bájt között van. Overlay állományokat is fertőz. Aktivizálódási feltételei számunkra még nem ismeretesek.

A vírus neve: Taiwan 4

Egyéb elnevezése: 2576.

Hossza: 2576 bájt.

Kódtípusa: Rezidens résszel rendelkező parazita vírus. A .COM és az .EXE állományokat támadja meg.

Azonosítása: Scan V71+, Pro-Scan 2.01+.

Eltávolítása: Clean V71+, vagy törölni a fertőzött állományokat.

Leírása: Thaiföldön, Tajvanban és az USA-ban egyszerre kezdték terjeszteni az AutoCAD elleni vírusháború újabb meneteként. Első előfordulása 1990 szeptember végén volt. Biztosra vehető, hogy szerzője azonos a Taiwan 3 vírusával, annak bázisán megírt programvírus, amely általános .COM és .EXE fertőző, de a COMMAND.COM-ot nem támadja meg.

Mindig ellenőrzi, hogy ott van-e már a memóriában. Ha nincs, akkor beépül a rendszermemória alsó részébe, ott szabályosan 2832 bájt helyet foglal le magának. Az INT 08 és az INT 21 vezérlését veszi magára. Rögtön lefékezi a rendszer működését, majd 30 perc elteltével további harminc százalékkal lassítja. Ha aktív a memóriában, a .COM és az .EXE állományokat végrehajtáskor fertőzi meg. A .COM állományok hossznövekedése ilyenkor 2576 bájt az állomány elején, az .EXE állományoké 2576–2590 bájt között van, és a vírus az állomány végére épül be. A következő levélszerű üzenetet tartalmazza:

```
To Whom see this: Shit! As you can see this document,
you may know what this program is. But I must tell you:
DO NOT TRY to WRITE ANY ANTI-PROGRAM to THIS VIRUS.
This is a test-program, the real dangerous code will
implement on November. I use MASM to generate varius
```

virus easily and you must use DEBUG against my virus hardly, this is foolish. Save your time until next month. OK? Your Sincerely, ABT Group., Oct 13th, 1989 at FCU.

„Annak, aki látja: Szar úgy! Amint ezt a dokumentumot olvassa, már tudhatja, mi ez a program. De meg kell hogy mondjam, ne próbáljon ellenprogramot írni erre a vírusra. Ez egy tesztprogram, a valóban veszedelmes kód novemberben jelenik meg. Én a MASM (Microsoft Assembler Macro) segítségével könnyedén létrehozok különböző vírusokat, ön pedig keményen küszködik, hogy a visszafejtő programokkal próbáljon tenni valamit ellenük. Hát nem baromság! Takarékoskodjon az idejével a következő hónapig. Rendben? Üdvözlettel, ABT Csoport, 1989. október 13. FCU."

Ezen kívül a vírus tartalmaz még egy karakteres részletet:

ACAD.EXECOMMAND.COM

A vírus neve: Disk Killer

Egyéb elnevezése: Computer Ogre, Disk Ogre, Ogre, Bootkiller.

Hossza: 3072 bájt.

Kódtípusa: Rezidens része van, a bootszektort támadja meg.

Azonosítása: Scan V39+, F-Prot, IBM Scan, Pro-Scan, VirexPC, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: MDisk, CleanUp, CHKVir v.4.01, F-Prot, Bootkill, Sysdoki vagy a DOS SYS parancsa.

Leírása: A Disk Killer vírus a bootszektort megfertőzve saját elrejtőzéséhez kijelöl magának három nem használt blokkot a floppylemezen vagy a merevlemezen. Ezt a helyet a floppyn a FAT-táblában hibás blokként jelöli meg, így azt nem tudják felülírni. Ráadásul a bootszektort a saját ízlése szerint írja át. Amikor rendszert indítunk, betöltődik — mégpedig elsőként éppen ő — a memóriába. Így azonnal lehetősége van rá, hogy megfertőzzön új lemezeket.

A merevlemezen elhelyezkedő vírus belső számlálója regisztrálja, hogy hány floppyt tudott megfertőzni. Aktivizálódásának feltétele egy előre beállított érték elérése. Az alapverzióban ez összesen 48 órányi működési időtartamot jelent, ami a gép igénybevételétől függően 1–6 hét elteltét is jelentheti a vírus felvitele után. A destruktív folyamat elindulásakor megjelenik a vírusra jellemző üzenet. Amíg üzenget, egy karakterrel véletlenszerűen, keresztül-kasul felülírja az állományokat. Nekünk már csak a lemez újraformázása a dolgunk, majd a korábban floppyra elmentett állományokból rekonstruálhatjuk az eredeti állapotot... (Mármint ha rendszeresen lementettük anyagainkat!)

Mivel a Disk Killer fertőzése során lecseréli a megtámadott lemez bootszektorát és rendszerindításkor az eredeti bootszektor programja helyett először a víruskód töltődik be a memóriába, rendszerünk csak ezt követően érkezik el a DOS alapprogramjaihoz. Minden lemez bootrekordja a lemezre jellemző információkat is tartalmazza, s ha olyan parancsokat használunk, amelyek végrehajtásához a bootszektorban levő információkra van szükség — például CHKDSK, FORMAT —, akkor a vírus azonnal lecseréli önmagára a bootszektor tartalmát!

Floppylemezek fertőzése esetén a vírus véletlenszerűen beépül valamelyik állomány közepébe (lehet szöveges állomány is), és példányonként 3072 bájtnyi

hibás szektort jegyez be a FAT-táblába. Erről tehát könnyen felismerhető a DOS CHKDSK nevű programjával. Előfordul, különösen 1,2 Mbájtos floppylemezeknél, hogy a vírus nem aktívan épül be az állományokba, így csak 2560 bájt hibás szektort jelöl meg.

Merevlemez fertőzése esetén a vírus nehezebben észlelhető. Ott a DOS operációs rendszer egy sávot (track-et) lefoglal magának, amely tartalmazza a lemez partíciós tábláját, a szektorkiosztás feljegyzésének helyét. A standard DOS programok számára ez a sáv elérhetetlen. A Disk Killer a bootszektort lecserélve ezen a rejtett sávon bújik meg mindaddig, amíg nem tudja aktivizálni magát. Ennek megtörténtekor a következő üzenet jelenik meg a képernyőn:

```
Disk Killer - Version 1.00 by COMPUTER OGRE 04/01/1989
Warning!!
Don't turn off the power or remove the diskette while
Disk Killer is Processing! PROCESSING!
Now you can turn off the power. I wish you Luck!
```

(Disk Killer — 1.00 változat a Számítógépevő Óriástól, 1989. I. 4. Figyelmeztetés! Ne kapcsolja ki az áramot, ne vegye ki a lemezt. A Lemezgyilkos dolgozik! DOLGOZIK! No, most már kikapcsolhatja az áramot. Sok szerencsét!)

A Disk Killer aktivizálódása után teljesen tönkreteszi a merevlemez tartalmát. Nullával feltölti a bootszektort, és ezzel elvész a partíciós tábla információja is. ASCII karaktereket ír az állományelhelyezkedési táblába (FAT), és hexa E5 karakterekkel felülírja a katalógusterület (directory) tartalmát. A vírus a merevlemezen nem jelöl be hibás szektorokat és nem épül be semmilyen állományba.

Amikor az üzenet megjelenik, a gép kódolja a merevlemez tartalmát. Előző könyvünkben azt írtuk, hogy az így roncsolt lemez helyreállíthatatlan. Időközben egyik kollégánk elmondta, hogy igen sok munkával ugyan, de a lemez helyreállítható. Mindenekelőtt nem szabad kikapcsolni a gépet, amíg a vírus be nem fejezi művét. Ugyanis a vírus a merevlemez teljes tartalmát a szektorok XOR-olásával (XOR 0AAAAh és 05555h) titkosítja. Ez pedig visszafejthető.

Ha a merevlemezen megtaláljuk a Disk Killer nevet, akkor az csak floppyról, az adott állomány bemásolásával kerülhetett oda. Ebben az esetben a vírus nem aktív a merevlemezen, de a floppyn már az lehet. A Disk Killer csak önálló merevlemezes gépeken és munkaállomásokon fertőz. A Novell hálózatban sem a szerver winchesterét, sem a többi munkaállomást nem fertőzi meg.

A vírus jelenlétéről sok hibás floppylemez-művelet és téves lemezfelismerés árulkodik. Magyarországon először egy Disk Manager v3.3 gyári programlemezen találtuk meg, és az valószínűleg az NSZK-ból került hozzánk.

A vírus neve: Korea

Egyéb elnevezése: LBC Boot.
Hossza: Nem értelmezhető.
Kódtípusa: Rezidens, csak a floppy bootszektorát fertőzi meg.
Azonosítása: Scan V61+, VirHunt 2.0+.
Eltávolítása: M-Disk, vagy a DOS SYS parancsa.

Leírása: A Korea vagy másik elterjedt nevén LBC bootvírust 1990 márciusában izolálták Szöulban, a Koreai Köztársaságban. A vírus memóriarezidens, a bootszektort fertőzi meg, de kizárólag 360 K-s 5,25"-os floppylemezen. Külföldön a koreai gyártmányú gépekhez és PC bővítőkártyákhoz adott programlemezeken terjedt el.

A vírus láthatóan nem szándékos pusztítás céljára készült, legalábbis jelenlegi formája kizárólag csak terjed. Ilyenkor kénytelenek vagyunk feltételezni, hogy egy terjedési eljárás tesztelésére létrehozott eszközről van szó. Ennek ellenére — hasonlóan a Stone/Marijuana vírushoz – kárt is okoz. Mégpedig azzal, hogy az eredeti bootszektort elmenti a 11. szektorra, amelyik a gyökérkönyvtár utolsó szektora. Ha sok állomány vagy alkönyvtár van a lemezen, akkor az ide bejegyzett állományok, illetve könyvtárak elvesznek.

A vírus neve: MusicBug

Egyéb elnevezése: Music Boot, Music Bug.
Hossza: Nem értelmezhető.
Kódtípusa: Bootszektort, illetve partíciós táblát fertőz.
Azonosítása: Scan V72+.
Eltávolítása: Patríciós tábla mentésének visszatöltése vagy Mdisk /P.
Leírása: 1990 decemberében terjedt el, tajvani gépekkel és programlemezekkel. Tajvanból származó vírus, amely merevlemezeken a partíciós táblában, a floppykon pedig a bootszektorban telepszik meg.

Fertőzött rendszerlemezről való betöltés után épül be a memóriába úgy, hogy a DOS csak 638 K rendszermemóriát jelez installáltnak. A vírus a rendszermemória tetején foglalja le a helyet, az INT 12 visszatérését manipulálja. Mialatt a rendszer betöltődik, a vírus zenél. Rezidens része ezt követően minden lemezműveletnél néhány hangot hallat, olyanokat, mint mikor egy vulkán kitör. A merevlemezen a partíciós táblába és a bootrekordba egyaránt beül. A floppyn 4 K hibás szektort jelöl be, oda teszi el az eredeti bootrekordot. A rossznak jelzett szektorban a következő szöveges üzenet van:

```
MusicBug v1.06. MacroSoft Corp.
Made in Taiwan
```

A floppyról, ha az rendszerlemez, úgy takarítható le, hogy egy tiszta rendszerlemezről a SYS paranccsal ismét feltesszük a rendszert, majd utána egy tiszta floppyra fájlmásolással átvisszük annak tartalmát. A merevlemezen először a rossznak bejelölt szektorok jelölését feloldva kell azok tartalmát kitakarítani, majd a SYS C: paranccsal a rendszert ismét felrakva a bootszektort felülírni. Az esetek többségében a merevlemez ennek ellenére nem kerülheti el az alacsony szintű formázást, vagy pedig nem lesz bootolható. Ha van mentésünk a bootszektorról és a partíciós tábláról, akkor annak visszatöltése után csak a rossznak bejelölt szektorokat kell letakarítani.

A vírus neve: Stoned

Egyéb elnevezése: Hawaii, Marijuana, New Zealand, Rostov, San Diego, Sex Revolution, Smithsonian.

Hossza: Nem értelmezhető.

Kódtípusa: Bootvírus, rezidens része van, floppyn a bootszektort fertőzi meg, a merevlemezen a partíciós táblát (master boot sector).

Azonosítása: Scan, F-Prot, IBM Scan, Pro-Scan, VirexPC, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: CleanUp, MDisk, CHKVir v.4.01, F-Prod, Bootkill, Sysdoki, Pro-Scan 1.4+.

Leírása: A Stoned vírust először Új-Zélandon, Wellingtonban észlelték, 1988 elején. Az eredeti vírus csak a 360 kilobájtos, 5 1/4"-os floppyt fertőzte meg, a későbbi változatok viszont már a merevlemezt is. A Magyarországon előforduló változat megfertőz minden floppyt, a 3 1/2"-os 720 kbájtos és 1,44 Mbájtos, illetve az 5 1/4"-os 360 kbájtos és 1,2 Mbájtos lemezeket egyaránt, míg a merevlemez fertőzése esetén csak a C: lemezegységre „mászik" rá. Eddig számtalan változatáról tud a nemzetközi szakirodalom.

Amikor a Stoned megfertőzi a floppyt, átteszi az eredeti bootszektort (0. szektor) a 11-dikre és magát a 0-dikra másolja rá. Ez a 11. szektor a normál 360 K-s floppyn a főkönyvtár utolsó szektora. Ha sok bejegyzésünk van a főkönyvtárban, ami ide kerül, az elvész. Néhány speciális DOS verzió ide, a 11. szektorra teszi a FAT-ot, amire azután a vírus ráírja magát. A merevlemezen a Stoned az eredeti partíciós táblát kiteszi a 0. oldal, 0. fej, 7. szektorra, és önmagát elhelyezi ennek eredeti helyén, a 0. oldal, 0. sáv, 1. szektoron. Ha nem DOS-szal, hanem olyan szoftverrel formáztuk a merevlemezt, amely máshova teszi a partíciós táblát, akkor a merevelemez a fertőzéskor teljesen tönkremegy. (Például ha Novell szervert vagy egyéb lemezformázó-meghajtó segédprogramokat használtunk.)

A vírus akkor válik memóriarezidenssé, amikor egy fertőzött floppyról indítanak rendszert. A memóriából 2 kilobájtnyi helyet foglal le magának és magára veszi az INT 12 vezérlését. Amikor rendszerlemezt készítünk, ráteszi magát, de ha a memóriában van, akkor már bármilyen hozzáférési műveletre, például egy tartalomjegyzék behívásakor is, ráteszi magát a lemezre. Nyolc rendszerindítás közül egy esetben a vírus a következő rendszerüzenettel lepi meg a gép használóját:

`Your computer is now stoned. Legalize Marijuana`

(Az ön számítógépe most ki van nyírva. Engedélyezzék a marihuánát)

Szövegváltozata:

`Your PC is now Stoned!`

A Stoned volt 1990 februárjában az egyik legelterjedtebb vírus. Miután a floppy bootszektorát fertőzte meg, a merevlemezen pedig a partíciós táblát cserélte le, kétféle fertőzési mechanizmussal működött. Változatai legtöbbször csak annyiban különböznek egymástól, hogy a szöveg második mondata hiányzik (tehát az átíró nem követeli a marihuána szabad forgalmazását), vagy az üzenet töredékes, illetve még tisztázatlan szerepű bináris kódot tartalmaz. A

magyarországi változat megtámadja a merevlemezt is, és valószínűnek látszik, hogy az egy itthon „továbbfejlesztett" termék.

A Stoned vírus fertőzése különösen a 3 1/2"-os floppykra veszélyes, mert azokat teljesen használhatatlanná teszi. E fertőzött floppyk használata során a következő DOS-üzenetek jelennek meg:

```
Error reading directory.
Sector not found.
Abort, Retry, Ignore?
```

(Katalógusolvasási hiba. A szektort nem találom. Vége, Újra, Tovább?)

A Stoned vírus sem a floppyn, sem a merevlemezen nem jelöl be hibás szektorokat, ezért lefülelése nehezebb a hagyományos vírusokénál. Vírusölő program használata nélkül a merevlemezről ez a vírus csak alacsony szintű (low level) formázással távolítható el. A vírus rezidens része 4 kilobájt.

A Stoned vírus ismert változatai:

Stoned-A: Csak szűk körben fordult elő az USA-ban. Hasonló, mint az eredeti, de kizárólag floppyt fertőz és a „Legalize Marijuana" szövegrész sohasem jelenik meg a monitoron. A bootrekordban lévő szöveg teljesen azonos.

Stoned-B: Az eredetitől csak annyiban tér el, hogy a merevlemez partíciós táblájába épül be. Ennek egyik alváltozata terjedt el Magyarországon, többféleképpen átírt szöveggel. Ha RLL kontrollert használunk, a vírus gyakran tönkreteszi a rendszert, mert ezt a kontrollert nem tudja korrekt módon kezelni, ezért a rendszert kiakasztja. Alapváltozatában a szöveg:

```
Your computer is now stoned. LEGALISE MARIJUANA
```

A szöveg sohasem jelenik meg a monitoron.

Stoned-C: Majdnem azonos az eredeti Stoned vírussal, de a rendszerüzenetet valaki teljesen kitörölte belőle.

Stoned-D: Teljesen hasonló az alapváltozathoz, de kifogástalanul kezeli az 5,25"-es 1,2 MB-os, és a 3,5"-es 720 K-s, illetve 1,44 MB-os floppykat is.

Rostov: A Stoned-B átirata, de a szövegek sohasem jelennek meg a monitoron. A vírus a következő szövegeket tartalmazza:

```
Non-system disk
Replace and strike
```

(Nem rendszerlemez. Cserélje ki és nyomjon meg egy gombot)

1990 decemberétől terjedt el, bizonyosan a Szovjetunióból. Valószínű forrása a Moszkvai Informatikai Intézet. Rokonságban van a STONED-F verzióval, ami feltehetően szintén ott készült.

SexRevolutionV1.1: 1990 decemberétől ismert. A szexuális forradalom exportját hirdető szövegváltozata megjelenik a monitoron is:

```
EXPORT OF SEX REVOLUTION ver. 1.1
```

Sex Revolution V2.0: 1990 decemberétől ismert. A benne lévő szöveg:

```
EXPORT OF SEX REVOLUTION ver. 2.0
```

Stoned-E: Amikor a PC kinyírásáról szóló épületes szöveg megjelenik, a hangszóró ennél a változatnál fütyül egyet. A LEGALISE.. szöveg előfordulhat a bootszektorban vagy a partíciós táblában.

Stoned-F: A Stoned-E átirata, a hangszóró sípol, amikor az eredeti Stoned

szöveggel azonos jelentésű, de lengyel nyelvű és ékezés nélküli feliratot kiírja a monitorra:

```
Twoj PC jest teraz bel
```

A vírus neve: Stoned II

Egyéb elnevezése: Donald Duck.

Hossza: Nem értelmezhető.

Kódtípusa: Rezidens, bootszektort fertőző.

Azonosítása: ViruScan V66+, Pro-Scan 1.4+, VirHunt 2.0+.

Eltávolítása: CleanUp V66+, MDisk, Pro-Scan 1.4+.

Leírása: Gyakorlatilag a Stoned-B változata, de számos antivírus program külön vírusként jelöli ezt a Donald Kacsának becézett vírusverziót. 1990 júniusától Új-Zélandban lépett fel. A kódot egy köztes visszafejtett állapotból újraírták. Európában viszonylag ritka, a vírusokkal foglalkozó szakemberek gyűjteményében viszont általában megvan. Az alapkódot is módosították, de csak annyira, hogy a hagyományos Stoned-keresők ne ismerjék fel. Két szövegváltozata ismert, a Version 2 tűnik az eredetinek:

Stoned II-A:

```
Your PC is now Stoned! Version 2
```

Stoned II-B:

```
Donald Duck is a lie.
```

(A Donald Kacsa hazugság)

A szöveg Version 2 része töredékes, és amikor a vírus másolja magát, akkor részben szeméttel töltődik fel. Az üzeneteket véletlenszerűen jeleníti meg. Önmagát és az elmentett eredeti bootszektort ugyanúgy helyezi el, mint az eredeti Stoned.

A vírus neve: Wolfman

Egyéb elnevezése: Még nem ismeretes.

Hossza: 2064 bájt.

Kódtípusa: A .COM és az .EXE programokat támadja meg. Parazita vírus, rezidens résszel.

Azonosítása: Scan V66+, Pro-Scan 2.01+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: Tajvanról származik a Wolfman (farkasember) vírus. 1990-ben engedték szabadjára. A .COM és az .EXE állományokat fertőzi meg, beleértve a COMMAND.COM-ot is.

A vírus memóriarezidensként installálódik, két blokkot foglal le magának. Az első 68032 bájt hosszú, a második 4544 bájt. Összesen tehát 72460 bájt helyet vesz el. A kettős helyfoglalás értelme, hogy nehezebben lehessen megtalálni és kiirtani a memóriából. A rendszer alsó részén telepszik le, és a két rész egymással szoros kapcsolatban marad. A vírus magára irányítja a következő megszakításokat: INT 09, INT 10, INT 16, INT 21, INT 2F, INT ED, INT F5.

A fertőzött .COM állomány hossza 2064 bájttal nő meg, a kód pedig a .COM állomány kezdetére épül be. Az .EXE állományoknak a végére tapad, hasonló

hosszal. A fertőzés feltétele, hogy az állományoknak 2064 bájtnál hosszabbaknak kell lenniük. Egyéb aktivizálódási feltételei jelenleg ismeretlenek. Eddig viszonylag ritkán bukkant fel. A kód visszafejtése folyamatban van.

A vírus neve: Joshi

Egyéb elnevezése: Happy Birthday Joshi.
Hossza: Nem értelmezhető.
Kódtípusa: Bootszektort és partíciós táblát fertőz.
Azonosítása: Scan V64+, Pro-Scan 1.4+.
Eltávolítása: Clean V66+, Pro-Scan 1.4+, RmJoshi, vagy alacsony szintű formázás.
Leírása: A Joshi vírust 1990 júniusában eresztették el Indiában, a szoftverháború részeként, mert onnan ered a kalózmásolatok jelentős része. A vírus az 5,25"-es floppyk bootszektorába ül bele, a merevlemezen pedig a partíciós táblába.

Rezidens résszel rendelkezik, ami egy fertőzött lemezről történő rendszerindítással kerül a gépbe. Ekkor 6 K-val csökkenti a DOS számára rendelkezésre álló memóriát. Hasonló a Stoned vírushoz, ahogy a merevelemez partíciós táblájába ül bele, és a Brain vírushoz, ahogy a bootszektor fertőzésének mechanizmusa működik. A bootszektor változásait álcázza, s ha valamilyen segédprogrammal szeretnénk azt megnézni, akkor az elmentett, sértetlennek látszó bootszektort mutatja be nekünk.

Minden év január 5-én aktivizálódik. Ekkor rendszerindításkor kiakasztja a rendszert, és megjeleníti azt az üzenetet, amelyről a vírus a nevét is kapta:

```
type Happy Birthday Joshi
```

Ha ezután a felhasználó begépeli, amit a vírus kért, akkor a rendszer újra használhatóvá válik. A vírussal csak akkor lehet elbánni, ha tiszta, írásvédett DOS rendszerlemezről töltjük be a rendszert. Ilyenkor például a Norton Diskedit programmal már meg tudjuk nézni a bootrekordot. Ha a bootszektor első két bájtja hexában EB 1F, akkor lemezünk fertőzött. Ugyanis ez a két bájt a víruskód elejére való ugrás gépi kódja. A vírus magát a 41. sáv 1.–5. szektoraiban helyezte el a 360 K-s, 5,25"-os floppyn. Az 5,25"-os 1,2 MB-os floppyn a vírus a 81. sáv 1.-5. szektoraiban található.

Ha a merevlemezen a partíciós tábla első két bájtja hexa EB 1F, akkor a winchester fertőzött. A vírus a 0. sáv 2.-6. szektoraiban ül, az eredeti partíciós táblát viszont a 0. sáv 9. szektora tartalmazza.

A szakirodalom mindezek ismeretében is a merevlemez alacsony szintű formázását ajánlja. A floppyn minden mentesítés után egy nem futtatható verzió marad vissza a 41. sávon.

A vírus neve: Fellowship

Egyéb elnevezése: 1022.
Hossza: 1022 bájt.
Kódtípusa: Rezidens résszel rendelkező parazita vírus, a .COM és az .EXE állományokat fertőzi meg.
Azonosítása: Scan V66+, F-Prot 1.12+, Pro-Scan 2.01+.

Eltávolítása: F-Prot 1.12+, vagy törölni a fertőzött állományokat.

Leírása: Malajzia IC-gyártó nagyhatalom, de vírust szerencsére nagyon keveset bocsátott ki a számítógépes szoftverforgalomba. Ez egyike vírusritkaságainak. Egy Ausztráliába menesztett gépszállítmány szoftvereivel terjedt el, 1990 júliusától. A vírus 1022, illetve 1019 bájt hosszú — ez utóbbi adat Fridrik Skulasontól ered —, és az utolsó 28 bájtot felülírja a megfertőzött programban. Nem lehet irtani, csak felismerni.

A vírus 2048 bájtot foglal el a memória alsó részén. Az INT 21-et magára irányítja, így válik rezidenssé. Bár Skulason azt írja, hogy csak .COM állományokat fertőz meg, a többi szakirodalom szerint .EXE állományokat is, amikor hossznövekedése 1019–1027 bájt, és a víruskód az állomány végére kerül.

A megfertőzött COMMAND.COM állományok végén a következő (névadó) üzenet van:

```
This message is dedicated to all fellow PC users on Earth
Toward A Better Tomorrow
And a better Place To Live In
03/03/90 KV KL MAL
```

(Ezt az üzenetet ajánlom a Földön minden PC-felhasználó társamnak. Egy jobb holnap felé. Amelyben jobb lesz élni.)

A szöveg végén lévő rövidítés egy vírusíró műhelyre utal Kuala Lumpurban, Malajziában.

A vírus neve: Ashar

Egyéb elnevezése: Shoe_Virus, UIUC.

Hossza: Nem értelmezhető.

Kódtípusa: Rezidens része van, a bootszektort fertőzi.

Azonosítása: ViruScan V41+, F-Prot, IBM Scan, Pro-Scan 1.4+, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: MDisk, Clean V41+, Pro-Scan 1.4+, F-Prot, CHKVir v.4.01 Sysdoki vagy a DOS SYS parancsának kiadása.

Leírása: Az Ashar vírus a bootszektort fertőzi meg. A Brain variációja vagy átírása. Eltér viszont tőle abban, hogy ez a vírus a floppyt és a merevlemezt egyaránt képes megfertőzni. A vírus egy rendszerüzenetet is tartalmaz:

```
VIRUS_SHOE RECORD, v9.0. Dedicated to the dynamic memories
of millions of virus who are no longer with us today
```

(CIPŐ-VÍRUS ÁLLOMÁNY, v9.0. Azon dinamikus vírusmilliók emlékének szentelve, akik ma már nincsenek velünk)

A vírusoknál megszokott szlenget és hibás angolságú szöveget nem mindig lehet magyarra átültetni. A cipő elnevezés nyilvánvaló gúnyos utalás a bootvírus jellegre, miután a boot egyik eredeti angol jelentése csizma. A fenti rendszerüzenet sohasem jelenik meg a monitoron. A vírusazonosító sztring „ashar", amelyet normális esetben a vírus elejétől hexa 04A6 eltolással (offset) találhatunk meg a vírus kódjában. Léteznek az Ashar vírusnak változatai is, Ashar-B vagy Shoe_Virus-B nyilvántartási nevek alatt. A v9.1 rendszerüzenete eltér a v9.0-étól.

A vírus neve: Brain

Egyéb elnevezése: (c) Brain, Pakistani, Pakistani Brain.

Hossza: Nem értelmezhető.

Kódtípusa: Rezidens része van, a bootszektort fertőzi.

Azonosítása: Scan, F-Prot, IBM Scan, CHKSeq v.1.0, Sysdoki. AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: MDisk, CleanUp, F-Prot,CHKVir v.4.01, Sysdoki. Pro-Scan vagy a DOS SYS parancsának kiadása.

Leírása: A bootvírusok egyik „mintadarabja", nagyon sokat cikkeztek róla. A Brain vírus Pakisztánból, Lahore városából származik. A bootrekordot fertőzi, azt felülírja saját kódjával, eredeti tartalmát pedig elmenti a lemeznek a FAT-táblában megjelölt másik pontjára, ami 3072 bájt (3 cluster, 6 szektor). Azzal jelzi, ha egy floppyt már megfertőzött, hogy kicseréli a lemezcímke (label) állományát a következőre: (c) Brain.

A vírus kódjának egy részét a fertőzött lemez logikai 0., azaz bootszektorába helyezi el. Működése során a vírus először tárrezidens részét bocsátja ki magából, amely a RAM-ban 3–7 K-nyi részt foglal le magának. A Brain vírus igen ügyesen elrejti magát a felderítés elől: számos megszakítást (interrupt) magára irányít. Sok lemezeditort azzal tud megtéveszteni, hogy önmagán keresztül a lemeznek arra a helyére irányítja, ahová az eredeti bootrekordot elrakta. Így a gyanútlan felhasználó az eredeti bootot látja, a vírus pedig mintha ott sem lenne... Ezt a trükköt az újabb lemezkezelő programok már „nem veszik be". Az átírások során a vírus egyes változataiból a felderítés megnehezítésére a vírusazonosítót hordozó „(c) Brain" szöveget távolították el.

Az eredeti Brain csakis floppyt fertőz. Ez felkeltette néhány vírusíró szakmai becsvágyát, akik az eredeti vírust „továbbfejlesztették", a merevlemez megtámadására is alkalmassá tették.

A Brain vírus eddig ismert változatai:

Brain-B/Hard Disk Brain/Houston: Ez a verzió már a merevlemezt is megfertőzi.

Brain-C: Mint a Brain-B, de a „(c) Brain" lemezcímkét gondos kezek eltávolították.

Clone: Olyan Brain-C, amelybe visszaírták az eredeti copyright lemezcímkét.

Clone-B: Az előbbi alaposan átírt változata. 1992. május 5-től kell elpusztítania a FAT-ot, ha sikerült valahol meglapulnia.

Magyarországon nagyobb (c) Brain fertőzés, valamint az Ashar verzió egyik átiratának felbukkanása 1990 júliusában és augusztusában volt.

A vírus neve: Ohio

Egyéb elnevezése: Még nem ismeretes.

Hossza: Nem értelmezhető.

Kódtípusa: Rezidens része is van, csak a floppy bootszektorát fertőzi meg.

Azonosítása: Scan, F-Prot, IBM Scan, Pro-Scan, VirexPC, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: MDisk, F-Prot, VirexPC, Pro-Scan 1.4+, vagy pedig a DOS SYS parancs kiadása.

Leírása: Az Ohio vírus memóriarezidens résszel rendelkező, bootszektort fertőző vírus. Csak a 360 kilobájtos floppylemezekre tud felmászni. Sok mindenben hasonlít a Den Zuk vírus viselkedéséhez, annak esetleg egy korábbi verziója. Az általa már megfertőzött lemez immunis a Pakistani (c) Brain vírus fertőzésével szemben, ha viszont ő találja ott a Braint vagy a Den Zuk-ot, akkor kiirtja őket, és önmagát teszi fel a helyükre, vagyis tudatosan készítették fel a velük való találkozásra. Elemzés során felmerült az is, hogy esetleg egy félresikerült, a (c) Brain vírus ellen vírustechnológiával védekező megoldással állunk szemben, vagy pedig egy eddig még nem ismert program átiratával.

Az Ohio vírusban az alábbi, inkább csak névjegyszerű szöveget találhatjuk:

```
V I R U S
b y
The Hackers
Y C 1 E R P
D E N Z U K O
Bandung 40254
Indonesia
(c) 1988, The Hackers Team....
```

A vírus neve: Pentagon

Egyéb elnevezése: Még nem ismeretes.

Hossza: Nem értelmezhető.

Kódtípusa: Rezidens része van, csak a floppy bootszektorát fertőzi meg.

Azonosítása: Scan, F-Prot, CHKSeq v.1.0.

Eltávolítása: MDisk, CleanUp, vagy pedig a DOS SYS parancsának kiadása.

Leírása: A Pentagon vírus az MS-DOS 3.20 bootszektorában, az ott előforduló IBM szó helyére beleírja a következő karaktersorozatot: HAL. Ezen kívül további két állományt is módosít. Az első ilyen módosított állománynak új nevet ad a 0F9 hexadecimális karakterek felhasználásával. Ez az állomány tartalmazza a víruskódnak azt a részét, amelyet nem tudott begyömöszölni a bootszektorba, valamint az eredeti bootszektort is ide teszi. A második állomány neve PENTAGON.TXT, de ez már nem tartalmaz semmilyen használható adatot. A vírus a nevét erről az állományról kapta. A 0F9 állományt a vírus egyben abszolút tárcímként is kezeli, a vírusrészletek kódoltak. A Pentagon vírus csakis a 360 kilobájtos floppykat támadja meg. Megnézi azt is, hogy van-e rajta (c) Brain vírus. Ha rátalál, akkor azt eltávolítja onnan és önmagával helyettesíti. Memóriarezidens része 5 K helyet foglal el a RAM-ban, és túléli a Ctrl-Alt-Del melegstartot is.

A vírus neve: Den Zuk

Egyéb elnevezése: Search, Venezuelan.

Hossza: Nincs rá adat.

Kódtípusa: Van rezidens része, csak a floppy bootszektorát fertőzi meg.

Azonosítása: Scan, F-Prot, IBM Scan, Pro-Scan, VirexPC, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: MDisk, F-Prot, vagy a DOS SYS parancs kiadása.

Leírása: Kizárólag 360 K-s, 5 1/4" formátumú floppylemezeken fertőzi meg a bootszektort. Ha utána ilyen lemezről töltjük az operációs rendszert, akkor rezidens módon felmegy a tárba. Ha ebben az esetben a rendszert a Ctrl-Alt-Del gombokkal újraindítjuk, a vírus CGA, EGA, illetve VGA monitorokon grafikus üzemmódban kiírja a „DEN ZUK" rendszerüzenetet. Eredeti verziója nem károsít semmit sem. Vannak olyan átiratai, amelyek magukban egy számlálót működtetnek. A számláló beállítása a vírusverzió függvényében 5 és 10 között lehet. Amennyiben ezt az értéket eléri, akkor a floppyt újraformázza. Azon a floppyn, amelyet a Den Zuk vírus megfertőzött, a következő zavaros belső rendszerüzenetet találhatjuk a víruskódban:

```
Welcome to the Club The HackerS - Hackin' All The Time
The HackerS
```

(Légy üdvözölve a hackerek klubjában. Folyton feltörni. A hackerek.)

A megfertőzött lemeznek a címkéjét kicseréli a következőre:

```
Y.C.1.E.R.P.
```

A Den Zuk vírus elpusztítja a Brain vírust is, utána pedig rögtön önmagát rakja fel helyette. (Hasonlóképpen viselkedik, mint az Ohio vírus, amely hármuk közül a legerősebb, és akár a Den Zukkal, akár a Brainnel találkozik, mindegyiket törli és önmagát ülteti a helyére.) A Den Zuk megírásában közreműködhettek azok, akik az Ohio vírust készítették, amire a fentieken kívül az is utal, hogy az „Y.C.1.E.R.P." karaktersorozat mindkettőben előfordul.

A vírus neve: 1381

Egyéb elnevezése: Internal.

Hossza: 1381 bájt.

Kódtípusa: Parazita, rezidens rész nélküli, .EXE fertőző.

Azonosítása: Scan V64+, Pro-Scan 2.01+.

Eltávolítása: A fertőzött állományt törölni kell.

Leírása: A vírus a hardverhibát szimuláló vírusok csoportjába tartozik. Az .EXE állományok növekedése árulja el jelenlétét, általános .EXE fertőző. Algoritmusa szerint az éppen aktuális meghajtón terjed, ami elég rapszodikussá teszi terjedését, és nehezen kideríthetővé a fertőzés forrását. 1990 júniusától ismerik, valószínűsíthető származási helye Bulgária.

A víruskód lefutásonként csak egyetlen másik .EXE állományt fertőz meg az aktuális meghajtón. Az állománynövekedés a paragrafushatárok miatt 1301–1309 bájt hosszig terjedhet. Az állomány végére épül be, mint a klasszikus .EXE vírusok. A fertőzött állományban olyan „hibaüzenetet" találhatunk, ami-

lyen természetesen nincs sem a gép BIOS-ában, sem pedig az operációs rendszerben:

```
INTERNAL ERROR 02CH.
PLEASE CONTACT YOUR HARDWARE MANUFACTURER IMMEDIATELY !
DO NOT FORGET TO REPORT THE ERROR CODE !
```

(Belső hiba 02Ch. Sürgősen vegye fel a kapcsolatot a hardver gyártójával! Ne felejtse el közölni a hibakódot!)

Aktivizálódásának feltétele még nem ismert, és az sem, hogy mikor örvendeztet meg bennünket ezzel a szöveggel. Szakirodalmi feltételezések szerint elképzelhető nyugat-európai eredete is.

Adatbűnözés

Datacrime, Datacrime-B, Datacrime-II, Datacrime-IIB, AirCop, Datalock, Mirror, Flip, Syslock, Advent, Macho-A, Machosoft, 5120, Cookie, Zero Bug, Agiplan, Typo Boot, Typo.COM, 4870 Overwriting, Yukon Overwriting, RaubKopie, VCOMM, Microbes, Crew-2480, Deicide, Dot Killer, EDV.

Fejezetünkben azokat a vírusokat mutatjuk be, amelyek bár nem hadviselési céllal készültek, nagyon gonoszak és pusztítóak. E vírusok szerzői a számítástechnika vandáljai. Lényegében ugyanazt teszik, mint azok, akik megrongálják a köztéri padokat és lámpákat vagy a járművek belső berendezését. A többnyire pillanatnyi (vagy elhúzódó) pszichés zavarokból fakadó cselekedetek elkövetőinek személye általában még a legszűkebb szakmai körök előtt is örökre homályban marad. Amint erről az Új víruslélektan című kötetben részletesen is írtunk, még sehol nincs kiforrott jogi gyakorlat ezeknek a bűncselekményeknek a kezelésére.

A vírus neve: Datacrime

Egyéb elnevezése: 1168, Columbus Day.

Hossza: 1168 bájt.

Kódtípusa: Parazita, rezidens része nincs. Titkosítja, azaz elkódolja magát. A .COM állományokat fertőzi meg.

Azonosítása: Scan /X V67+, F-Prot, IBM Scan, Pro-Scan, VirexPC, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: AntiCrim, Scan /D /X, VirexPC, Pro-Scan 1.4+, F-Prot, VirHunt 2.0, vagy a fertőzött állományok törlése.

Leírása: A vírust eredetileg Európában „fogták el", nem sokkal azután, hogy 1989-es márciusi változata megjelent. A Datacrime vírus átirata. Forrása valószínűleg az USA. A vírusprogram hozzáfűzi magát a .COM állományokhoz, azok hosszát 1280 bájtttal megnövelve. Az eredeti programban az első 3 bájtot átírja, mert ide helyezi el azt az ugróutasítást, amely a program elindításakor a hordozóprogram végére s ott a víruskód elejére ugratja az operációs rendszert, hogy a víruskód lefuthasson. Ezt az átírt 3 bájtot azonban tárolja magában, mert arra azért szüksége van, hogy a gazdaprogram is zavartalanul lefuthasson. A vírusgyártásnak ez a klasszikus programozási fogása már a Cascade

típusú vírusoknál megjelent, azzal a különbséggel, hogy ott az eredeti ugrócím kódolva van.

Terjedése során a vírus végigpásztázza az alkönyvtárakat .COM állományok után kutatva. A lebukás veszélyének csökkentése érdekében a COMMAND.COM-ot nem fertőzi meg Ugyancsak nem fertőzi meg azokat a .COM állományokat, amelyekben az állománynév hetedik betűje D. Előbb a merevlemez partíciókat vizsgálja végig, és csak utána a floppymeghajtót. A vírus minden esztendőben október 12-ig terjed. Amikor elérkezik ez a dátum, akkor az addig kódolva tárolt alábbi üzenetet jeleníti meg a monitoron:

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

Ilyenkor alacsony szintű szektor- vagy cluster-formázást végez a merevlemezen. Nagyon valószínű, hogy a felhalmozódó hibás területek következtében a rendszer hamarosan összeomlik. Ennek a vírusnak másik megfigyelt változata abban tér el az alapverziótól, hogy április elseje után nem terjed és nem fertőz állományokat. Érdekes vírusprogramozási hibát derített ki az ismert számítógép-virológus, a Hollandiában dolgozó Jan Terpstra: ha a PC kontroller RLL vagy SCSI típusú, vagy speciális AT-BIOS van a gépben, a vírus nem mindig tudja az alacsony szintű formázást elvégezni. Az MFM és az elterjedt RLL kontrollereket kezeli, de az újabban bevezetett Advanced RLL típusú kontrollerek esetén szintén nem működik.

A vírus a .COM állományok megfertőzése során a kódban véletlenszerű hibát okoz, ami előbb-utóbb a rendszer összeomlását okozza. Ellentétben a többi Datacrime változattal, az eredeti vírus minden év április 1-jéig nem szaporodik és nem fertőzi az állományokat.

A vírus neve: Datacrime-B

Egyéb elnevezése: 1280, Columbus Day.

Hossza: 1280 bájt.

Kódtípusa: Parazita, nincs rezidens része. Általános .EXE fertőző.

Azonosítása: Scan, F-Prot, IBM Scan, CHKSeq v.1.0.

Eltávolítása: AntiCrim, Scan /D, F-Prot.

Leírása: Az eredeti Datacrime vírus változata. Az eltérés a vírus hosszában és abban van, hogy az eredeti csak a .COM, ez pedig csak az .EXE állományokat fertőzi meg.

A vírus neve: Datacrime II

Egyéb elnevezése: 1514, Columbus Day.

Hossza: 1514 bájt.

Kódtípusa: Nincs rezidens része. Titkosítja, azaz elkódolja magát. A .COM és az .EXE állományokat fertőzi meg.

Azonosítása: Scan /X V67+, F-Prot, IBM Scan, Pro-Scan, VirexPC, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: AntiCrim, Scan /D /X, Pro-Scan 1.4+, VirexPC, F-Prot, VirHunt 2.0+.

Leírása: A Datacrime II az eredeti Datacrime vírus változata. 1989 szeptemberében bukkant fel. Eltér az állományok mögé bemásolt hosszúságban, ami itt 1514 bájt. Az eredetivel ellentétben nemcsak a .COM, hanem az .EXE állományokba is bemászik. A COMMAND.COM-ot is megfertőzi. Titkosítási mechanizmusa azonos az eredeti verzióéval. Sajátossága, hogy hétfői napon nem formázza sem a merevlemezt, sem a floppyt. Más napokon viszont igen...

A vírus neve: Datacrime IIB

Egyéb elnevezése: 1917, Columbus Day.

Hossza: 1917 bájt.

Kódtípusa: Nincs rezidens része. Átkódolva titkosítja magát, .COM és .EXE állományokat egyaránt megfertőz, beleértve a COMMAND.COM-ot is.

Azonosítása: Scan /X V67+, F-Prot, IBM Scan, Pro-Scan, VirexPC, VirHunt 2.0+.

Eltávolítása: AntiCrim, Scan /D /X, F-Prot, VirexPC, VirHunt 2.0.

Leírása: A Datacrime IIB a Datacrime II vírus változata, amelyet 1989 novemberében fedezett fel Hollandiában Jan Terpstra. Az átirat holland eredetű, visszafejtett eredeti kód alapján készült.

A vírus a .COM és az .EXE állományokat fertőzi meg, beleértve a COMMAND.COM-ot is. Alacsony szintű formázást végez egyes clustereken és véletlenszerű helyeken. Hétfői napokon nem formáz. Ez a vírus ugyanolyan, mint az eredeti Datacrime II, de titkosítási mechanizmusa eltérő, így mind a mentesítés, mind a felderítés mechanizmusa különböző.

A vírus neve: AirCop

Egyéb elnevezése: Még nem ismeretes.

Hossza: Nincs adat.

Kódtípusa: A floppy bootszektorába ül be, rezidens része van.

Azonosítása: ViruScan V66+, Pro-Scan 2.01+.

Eltávolítása: DOS SYS parancsa vagy Mdisk.

Leírása: Az AirCop vírus a tajvani vírusgyártó műhelyek remekmívű darabja. 1990 júliusában okozott nagyobb járványt az USA Washington államában. Tajvanról behozott gépek programlemezeivel kezdte meg kártevését. Európában viszonylag ritka. A vírus kizárólag az 5,25"-es, 360 K-s floppy bootszektorába telepszik be. Amikor a fertőzött lemezzel dolgozunk, installálja magát a memóriába. Egyaránt képes használni a HIMEM területet és a hagyományos DOS memória felső végét. 1024 bájttal csökkenti a más programok számára rendelkezésre álló memóriaterületet. A 13-as megszakítót manipulálja.

Ha a memóriában ücsörög, minden olyan 5,25"-es 360 K-s floppyt megfertőz, amely nincs írásvédelemmel ellátva. Amikor lecseréli a bootrekordot, azt elmenti a 719-es sorszámú szektorra (1. oldal, 39. sáv, 9. szektor), míg saját magát a 0, azaz a bootszektorba teszi.

A fertőzött lemez jellegzetessége, hogy a boot végén a következő szöveget találjuk:

```
Non-system...
```

Az AirCop vírus fertőzés után rendszer- és gépfüggően két hibajelenséget okozhat. Az egyik esetben véletlenszerű időközönként a következő rendszerüzenetet jeleníti meg a képernyőn:

```
Red State, Germ Offensive.
AIRCOP.
```

(Vörös Állam, baci offenzíva. Légizsaru.)

A másik esetben a vírus egyik rendszerfüggő programozási hibája jelentkezik. Megjelenik a „Stack overflow error" üzenet és a rendszer lemerevedik. Ilyenkor a normál Reset is hatástalan, csak a főkapcsoló segít.

A vírus nem tudja megfertőzni a merevlemezt, csak a floppykat. Tiszta rendszerről a DOS SYS parancsával kitakaríthatjuk őt a bootszektorból.

A vírus neve: DataLock

Egyéb elnevezése: DataLock 1.00, V920.

Hossza: 920 bájt.

Kódtípusa: Parazita, rezidens résszel rendelkezik. A .COM és az .EXE állományokat fertőzi meg, beleértve a COMMAND.COM-ot is.

Azonosítása: Scan V71+, Pro-Scan 2.01+.

Eltávolítása: Clean V71+, vagy a fertőzött állományok törlése.

Leírása: Az USA-ban bukkant fel 1990 november elején. A vírus a .COM és az .EXE állományokat megfertőző rövid vírus. A fertőzött COMMAND.COM hatására rezidensen installálódik a memória felső részében, de a hagyományos 640 K-s tartományon belül. A rendszermemóriából 2048 bájtot foglal le, és magára irányítja az INT 21-et.

Ha a vírus már rezidens, akkor minden futtatott .EXE állományt megfertőz. A hossznövekedés 920 bájt. A könyvtári bejegyzés dátumát kicseréli a fertőzéskori aktuális dátumra és időpontra. A vírusfertőzött állományok végén rejlik az üzenet, amelyből a vírus a nevét kapta:

```
DataLock version 1.00
```

A vírus egy átmeneti járvány után gyakorlatilag kiveszett, de a kódja még ma is forrásmű. A minél kisebb víruskód megírásának babérjára pályázók részben innen merítik az ötleteket.

A vírus neve: Mirror

Egyéb elnevezése: Még nem ismeretes.

Hossza: 927 bájt.

Kódtípusa: Parazita, rezidens, .EXE fertőző.

Azonosítása: Scan V67+, Pro-Scan 2.01+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: A vírus 1990 októberében bukkant fel. Bár a szakirodalom egy része szerint ismeretlen eredetű, bizonyos, hogy az akkori Szovjetunió egyik nagy vírusfejlesztő laboratóriumában készült, egyesek szerint Szentpéterváron (Leningrádban). A vírus az .EXE állományokat támadja meg, és pontosan meg nem határozott feltételek esetén bináris nullával (00h) tölti fel — hihetetlenül gyorsan — a teljes merevlemezt.

Amikor a fertőzött program lefutása után, a vírus beépül a memória felső részébe, ott 928 bájtot foglal le, és elkapja az INT 21 vezérlését. Ekkor az aktuális könyvtárban megfertőzi az .EXE programokat, 927–940 bájt hossznövekedést okozva, az állomány végére épülve be. A vírus azonosítója a fertőzött program végén található, két karakter hosszúságú szöveg: IH.

A vírus, mint arra neve is utal, a monitoron szabálytalan időközönként a képet saját tükörképévé alakítja. Ezt a műveletet igen gyorsan és látványosan hajtja végre. Veszélyessége mellett ezért is ezt használtuk vírusvédő kártyánk működésének illusztrálására 1991-ben, a tavaszi Budapesti Nemzetközi Vásáron.

A vírus neve: Flip

Egyéb elnevezése: Még nem ismeretes.

Hossza: 2343 bájt.

Kódtípusa: A .COM és az .EXE állományok fertőzése mellett bootvírusként is működik.

Azonosítása: F-Prot 1.14+.

Eltávolítása: F-Prot 1.14+.

Leírása: Fridrik Skulason dokumentációjában jelezte ennek a kettős természetű vírusnak a felbukkanását. A vírus meglehetősen hosszú, mert benne egy teljes bootszektor kódja is megtalálható a bootverzió működéséhez. Floppyn sohasem fertőz bootvírusként, csak merevlemezen. Amikor aktivizálódik, akkor vízszintesen elmozgatja a monitorképet és átkapcsolja az EGA és VGA monitorokat a speciális, negatív képet adó karakterkészletre. A vírus aktivizálódása minden hónap második napján, 16:00 — 16:59 közötti időpontban történik. A boot fertőzésének mechanizmusa a V-1 néven ismert vírusból lett kiemelve, de csak winchestert fertőz.

A vírus neve: SysLock

Egyéb elnevezése: 3551, 3555.

Hossza: 3551 bájt.

Kódtípusa: Önmagát tikosító, nem rezidens, .COM és .EXE állományokat fertőző vírus.

Azonosítása: Scan, F-Prot, Pro-Scan, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: 1988 novemberében bukkant fel az USA-ban ez az önmagát titkosító vírus. Az adatállományokat is károsítja. A vírus nem válik rezidenssé, hanem a kód lefutása közben az aktuális lemez aktuális alkönyvtárában megfertőzi az .EXE és a .COM programokat, majd véletlenszerűen tönkretesz egy állományt. A fertőzött állomány 3551 bájttal nő meg, ami szembetűnő változás. A következő DOS-üzenetet jeleníti meg:

```
Error writing to device AUX
```

(Íráshiba a külső csatlakozó eszköznél)

A vírus írója a szoftver vírusháború jegyében a Microsoftnak üzent hadat. A

vírus ugyanis megkeresi az egyes programokban az akár kis-, akár nagybetűvel, vagy a kettő kombinációjával írt Microsoft nevet, és kicseréli a következőre:

```
MACROSOFT
```

A vírus onnan kapta a nevét, hogy a környezeti (environment) változóban keresi a következő sort:

```
set Syslock = @
```

Ha itt ez be van állítva, azaz megtalálja a környezeti sztringben a @ azaz az ASCII 64 (hexa 40) karaktert, akkor a vírus nem fertőz, illetve nem cseréli le a Microsoft nevet Macrosoftra.

Ismert változatai:

Advent: Egyelőre csak a létéről tudunk, Fridrik Skulasonhoz és a többi antivírus központba csak lebutított változatai kerültek, úgy tűnik, célzatosan. Lehet, hogy egyesek által víruscsere céljára átírt, de elfuserált változatról van szó.

Macho-A: Teljesen ugyanaz, mint az eredeti Syslock, de a Microsoft karaktersorozatot a következőre cseréli le: MACHOSOFT. A Macho-A készítője nagyon utálhatta a neves szoftvercéget, mert a vírus a károsítandó állományokat úgy választja ki, hogy az megkeresi bennük a Microsoft szövegrészt, bármilyen írásmódban legyen is az.

A vírus neve: Machosoft

Egyéb elnevezése: 3551.

Hossza: 3551 bájt.

Kódtípusa: Parazita, öntitkosító, nincs rezidens része, a .COM állományokat fertőzi meg. (A COMMAND.COM-ot is.)

Leírása: A Machosoft vírus a programkódhoz kapcsolódó vírus, amely önmagát titkosítja. Nemcsak a rendszert és a .COM állományokat fertőzi meg, hanem az adatokat is tönkreteszi a megtámadott rendszerekben. Mivel nincs rezidens része, úgy fertőz, hogy végigpásztázza az aktuális könyvtárat a program futása alatt. Ha talál benne .COM állományokat, kinéz azokból egyet, és beletéve saját kódját, megfertőzi azt. A kiválasztás a véletlen műve. A fertőzött állomány 3551 bájttal nő meg, ami szembetűnő változás. Amíg a COMMAND.COM meg van fertőzve, a fertőzés megállítható az alábbi utasítással:

```
set VIRUS=OFF
```

Ez azonban csak a rendszer újraindításáig hatásos. A vírus a megtámadott rendszerben IBMIONET.SYS „hidden/read only" állományt hoz létre. A vírus fertőzése során a DOS INT 25h megszakítását használja, 20 szektort beolvasva a fertőzendő állományból. A fertőzés során a vírus a fájlokban található „MICROSOFT" copyright szöveget „MACHOSOFT"-ra cseréli le. Ezt a vírust gyakran összekeverik a hasonló hosszúságú Syslock vírussal. A vírus a DOS 4.xx verzió alatt hibásan működik!

A vírus neve: 5120

Egyéb elnevezése: VBasic, Basic.

Hossza: 5120 bájt.

Kódtípusa: Nem rezidens, parazita, .COM és .EXE fertőző.
Azonosítása: Scan /X V67+, Pro-Scan 1.4+, F-Prot 1.12+.
Eltávolítása: Scan /D /X, Pro-Scan 1.4+, F-Prot 1.12+, Pro-Scan 2.01+.
Leírása: 1990 májusában lépett fel először ez a nem rezidens, általános .COM és .EXE fertőző vírus. A COMMAND.COM-ot is megtámadja. A vírust Turbo Basic programnyelven írták, assembler rutinokkal megspékelve, ami komoly programozástechnikai teljesítmény, mert a kód ehhez képest nagyon rövid.

Miután a víruskód lefut, megfertőz egy .COM és egy .EXE állományt az aktuális meghajtó aktuális könyvtárában. Idő hiányában véletlenszerűen kiválaszt még egy harmadik .COM vagy .EXE állományt is a C: meghajtó valamelyik könyvtárában. Az .EXE állományok hossznövekedése 5120 és 5135 bájt között van.

A vírus nem érzékeli, ha iráshiba történik, amikor fertőzi a programot, mert ennek vizsgálatára egyszerűen nincs ideje, ha észrevétlen akar maradni. Éppen ezért a fertőzött rendszer nem minden esetben tud hozzáférni a lemezhez. Az iráshibák végül rendszerösszeomláshoz vezetnek. Ugyanakkor az adatállományok azáltal rongálódnak meg, hogy a vírus töméntelen mennyiségű keresztkapcsolt szektorblokkot (clustert) hoz létre.

A vírus végén a Turbo Basic-re jellemző alábbi karakteres szövegrészletek találhatók:

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

A szakirodalom beszámol a vírusnak egy másik, igen ritka verziójáról is, amely nagyon egyszerűsített fertőzési metodikával dolgozik és nincsenek benne a fenti szövegek.

A vírus neve: Cookie

Egyéb elnevezése: Még nem ismeretes.
Hossza: 2232 bájt.
Kódtípusa: Nem rezidens, parazita, .COM fertőző.
Azonosítása: Scan, F-Prot, VirexPC.
Eltávolítása: Törölni a fertőzött állományokat.
Leírása: A valószínűleg angol eredetű programvírus 1990 december végén és 1991 januárjában bukkant fel Európában. A SysLock kódjának módosításával keletkezett. Olyannyira szoros ez a rokonság, hogy több antivírus program is Syslock-nak ismeri fel. Tulajdonságai azonban eltérőek, mert ez a nem rezidens vírus a COMMAND.COM-ot, a többi .COM és az .EXE programokat is megtámadja.

A víruskód lefutása közben az aktuális könyvtár aktuális meghajtójában az elsőnek meglelt .COM állományt fertőzi meg. Mindig megnézi, hogy az adott ál-

lományban már benne van-e. Ha igen, akkor továbblép, ha nem, akkor fertőz. Ha nincs .COM állomány, akkor hasonló logikával fertőzi meg az .EXE állományokat. Az egyes fertőzések során a hossznövekedés 2232 és 2251 bájt között van. A vírus a fertőzött állományok végére épül be. A könyvtári bejegyzés dátum és időpont adatait a vírus nem módosítja. A vírus által megfertőzött rendszer számos program futtatásánál kiakad, illetve egy adott futásszám után nem működik többé. A szakértők egyetértenek abban, hogy ez a vírus valamelyik másolásvédelmi rendszer része lehet, mert károkozásában és funkciójában megfelel az értékesítés oldaláról igényelt büntető másolásvédelmeknek.

A vírus esetenként kiírja a következő (névadó) rendszerüzenetet:

```
I want a COOKIE!
```

(Kérek egy tortát!)

A vírus neve: Zero Bug

Egyéb elnevezése: Palette, 1536.

Hossza: 1536 bájt.

Kódtípusa: Parazita, rezidens része van, a .COM állományokat fertőzi meg.

Azonosítása: Scan /X V67+, F-Prot, Pro-Scan 1.4+, VirexPC, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: Scan /D /X, CleanUp V66+, F-Prot, Pro-Scan 1.4+, VirHunt 2.0+ vagy pedig a fertőzött állományok törlése.

Leírása: A Zero Bug vírust először Hollandiában különítette el az ismert ottani vírusvadász, Jan Terpstra és csapata, 1989 szeptemberében. A vírus memóriarezidens. A megfertőzött .COM állományok hossza megnő ugyan 1536 bájttal, de a hossznövekedés a tartalom bejegyzésében nem jelenik meg, mert a DOS-nak nem engedi a változást átkönyvelni. A vírus fő célja a COMMAND.COM-nak (és másolatainak) megfertőzése. A lelőhelyet a DOS environment bejegyzésben a COMSPEC kiolvasása során tudja meg. Ha a COMSPEC-ben nem lel semmire, akkor rezidensen installálja magát úgy, hogy átirányítja önmagán a 21h megszakítást. Miután a vírus megfertőzte a COMMAND.COM-ot vagy tartósan beült a memóriába, megkezdi a .COM állományok fertőzését. A COPY és az XCOPY parancs hatására keletkező állománymásolatok is fertőzést kapnak. Végül minden .COM állomány és az egész rendszer fertőzött lesz.

Amennyiben a vírus által fertőzött COMMAND.COM töltődik be a gépbe, az elveszi az 1Ch időmegszakítót, és átirányítja önmagán. Bizonyos idő elteltével megjelenik egy holdarc karakter (ASCII 01), és körbeszaladva a monitor ernyőjén, jó étvággyal elfogyasztja a 0 számjegyeket... (Kifejezetten „előnyös" lehet a könyveléshez és az adónyilvántartáshoz... de talán mégsem ez a jó megoldás.) A vírus a viszonylag jóindulatúbbak közé tartozik, mert a fenti mókával is beéri, nem töröl állományokat és nem formázza a lemezt.

A vírus neve: Agiplan

Egyéb elnevezése: Még nem ismeretes.

Hossza: 1536 bájt.

Kódtípusa: Parazita, rezidens része van, a .COM állományokat fertőzi meg.

Azonosítása: F-Prot.
Eltávolítása: Törölni a fertőzött állományokat.
Leírása: 1991 elején jelentette Fridrik Skulason, hogy az NSZK-ban az Agiplan cégnél felbukkant egy olyan vírus, amely 1536 bájttal növeli a .COM állományokat. Amikor aktivizálódik, íráshibát okoz. A vírus dél-afrikai eredetű, a Zero Bug igen közeli rokona, valószínűleg átirata.

A vírus neve: Typo Boot

Egyéb elnevezése: Mistake.
Hossza: Nem értelmezhető.
Kódtípusa: Rezidens résszel rendelkező, bootszektort fertőző vírus.
Azonosítása: Scan, F-Prot, IBM Scan, Pro-Scan, AVTK 3.5+, VirHunt 2.0+.
Eltávolítása: MDisk, Pro-Scan 1.4+, F-Prot, Bootkill, vagy pedig a DOS SYS parancs kiadása.
Leírása: A Typo bootvírust először Yasrael Radai izolálta, 1989 júniusában, Izraelben. A vírus memóriarezidens része a rendszermemória végén 2 kilobájtnyi helyet foglal el magának. E vírusnak az a mániája, hogy megreformálja a helyesírást. Ha egy rendszert megfertőzött, akkor a DOS nyomtatási rutin vagy az arra épülő egyéb programok használatakor a karaktereket felcseréli azok kiejtés szerinti, fonetikus írásmódjára. Hogy a hecc teljes legyen, a számokat is valami mással helyettesíti. Csak a nyomtatás reformjával törődik, az adatokat és a képernyőn megjelenő szövegeket nem bántja. Viszont nem nyelvzseni, sem a héber, sem a cirill karaktereket nem ismeri, s az ilyen betűkkel írt szövegeket teljesen összezagyválja.

A Typo bootvírus lopott ötletre épül. Ismeretlen szerzője a Ping Pong vírust írta át: a pingpongozó rutint cserélte ki karakterhelyettesítő táblára és rutinra. Olyannyira kópiája az eredeti Ping Pong vírusnak, hogy annak detektorai és killerei vele szemben is alkalmazhatók!

A vírus neve: Typo COM

Egyéb elnevezése: Fumble, 867.
Hossza: 867 bájt.
Kódtípusa: Parazita, rezidens része is van, a .COM állományokat fertőzi meg.
Azonosítása: Scan /X V67+, F-Prot, IBM Scan, Pro-Scan, AVTK 3.5+, VirHunt 2.0+.
Eltávolítása: Scan /D /X, F-Prot, Pro-Scan 1.4+, VirHunt 2.0+, vagy a fertőzött állományok törlése.
Leírása: Brighton városában, 1989 novemberében találta meg Joe Hirst. A Typo COM vírus a Typo bootvírus szülője. Létrehozza a bootverziót, ugyanakkor minden karakterátirányítást ugyanúgy csinál a nyomtatón, mint a bootverzió, ha a DOS printer rutinját használjuk a soros vagy a párhuzamos kimeneten keresztül.

A vírus a DOS INT 21h megszakításának 31h funkciójával válik rezidenssé. Ha vírussal fertőzött állományt futtatunk, a vírus megkeresi az első tiszta

.COM fájlt és megfertőzi azt, majd aktivizálódása után véletlenszerűen összekeveri a klaviatúrán lenyomott billentyűket. (Nagyon szórakoztató. Majdnem annyira, mint egy jól eltalált KEYBHU billentyűzetkiosztás! Inkább azt ajánlom, mert kevesebb kárt okoz. — K.J.)

A vírus neve: 4870 Overwriting
Egyéb elnevezése: Még nem ismeretes.
Hossza: 4870 bájt.
Kódtípusa: Nem rezidens, .COM és .EXE fertőző programvírus.
Azonosítása: A jelenségek alapján megvizsgálni az állományokat.
Eltávolítása: Törölni a fertőzött állományokat.
Leírása: A vírus egy új technológia első darabja. A vírust a memóriában kicsomagolódó formában az LZEXE programmal tömörítették. Agresszív. 1991 februárjától terjed, nem rezidens, a .COM és az .EXE programokat megfertőzi, beleértve a COMMAND.COM-ot is.

Miután a víruskód betöltődött, először futásképes állapotba helyezi magát a memóriában. Itt nagyon nehezen lehet követni a tömörítésre használt program, az LZEXE.EXE 0.91 verziójának speciális memóriaműveletei miatt. Amikor már kibontva ott van a memóriában, keres az aktuális meghajtó aktuális könyvtárában egy még nem megfertőzött .COM vagy .EXE programot, és magát 4870 bájt hosszban egyszerűen rámásolja, ekképpen megfertőzve azt, s a felülírással a víruskódnyi szakaszt helyreállíthatatlanul tönkretéve! A megtámadott program mérete olyankor nem változik, ha előzőleg hosszabb volt 4870 bájtnál. Ha viszont rövidebb volt, akkor éppen ekkorára nő, csak tartalmilag az eredeti programból már nem lesz benne semmi, mert az egész maga a vírus — idegen név alatt. Az időpont- és dátumbejegyzés nem tér el az eredetitől. A fertőzött program helyett ezután már a vírus fut. Ha csak egy fertőzendő programot tud elérni, és abban már ott ül, akkor egyszerűen kilép a DOS-ba, és nem tesz semmit sem.

Detektálására kidolgozott eljárás még nincs. A fertőzés jele, ha a program első 4870 bájtján előfordul az LZEXE 0.91 verziójának jelzése. Különösen gyanús, ha a COMMAND.COM-ban lelünk ilyenre, mert az nem tömöríthető! E vírus fertőzésekor törölnünk kell a megtámadott állományokat.

A vírus neve: Yukon Overwriting
Egyéb elnevezése: Még nem ismeretes.
Hossza: 151 bájt.
Kódtípusa: Nem rezidens, a .COM állományokat felülírja.
Azonosítása: Manuálisan, editorprogrammal, szemrevételezéssel.
Eltávolítása: Csak a fertőzött állományok törlésével.
Leírása: E vírus jó helyezést érhetne el a legrövidebb vírusok megírásáért folyó „nemes" vetélkedőben. 1991 januárjában bukkant fel Kanadában. A vírus nem rezidens, a .COM állományokat és a COMMAND.COM-ot is felülírja saját kódjával.

A felülírás után a programból csak a víruskódrészlet marad futásképes. Ha

elindítjuk, akkor az aktuális könyvtár minden .COM állományában felülírja az első 151 bájtot saját kódjával. Az állománybejegyzés adatai viszont nem változnak.

Miután az aktuális könyvtárban elfogytak a fertőzendő állományok, a program végrehajtása során a Divide Overflow hibaüzenetet kapjuk az operációs rendszertől. Azaz csak látszólag attól, mert ezt tulajdonképpen a vírus üzeni nekünk. A vírusban található karakteres szöveg:

```
Divide Overflow$
```

Ez az állomány elejétől a 07h eltoláson (offset) található, és ez a vírus azonosítására az egyetlen biztos lehetőség. A vírus megoldásaiban igen primitív. Agresszivitása miatt szerencsére nem tudott elterjedni.

A vírus neve: Raubkopie

Egyéb elnevezése: Még nem ismeretes.

Hossza: 2219 bájt.

Kódtípusa: A .COM és az .EXE állományokat fertőzi, nem rendelkezik rezidens résszel.

Azonosítása: Scan V76+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: A vírus egy játék másolásvédelmébe volt beleépítve. Eredete nehezen bizonyítható, ugyanakkor tudatosítja a felhasználóval, hogy neki másolásvédelem-büntetést kell elszenvednie. Az ismeretlen forgalmazónak sikerült a Német Szövetségi Köztársaság határain túl terjedő járványt elindítania. Mi a vírust 1991 április táján kaptuk kézhez.

A vírus nem rendelkezik rezidens résszel, a .COM és az .EXE állományokat fertőzi meg, köztük a COMMAND.COM-ot is. A szövegek szempontjából igen bőbeszédű és agresszív. Amikor kódja lefut, a vírus legalább öt .COM programot akar megfertőzni. Ha nem talál ennyit az aktuális meghajtó aktuális könyvtárában, akkor az elérhető .EXE állományokkal igyekszik a megfertőzött állományok számát 5-re kiegészíteni. A .COM programok a fertőzés után 2219 bájttal lesznek hosszabbak, a víruskód az állomány elejére épül be. Az .EXE programok hossznövekedése 2475–2491 bájt között van, és a kód az állomány végére kerül. A könyvtári bejegyzés dátumát és időpontját nem változtatja meg.

Az .EXE programoknál a fertőzés kicsit bonyolultabb a szokásosnál. Módszereiben a magyar Phantom vírusra emlékeztet, bár nem valószínű, hogy annak szerzője ismerte ezt a szörnyeteget. Ha az .EXE állomány hosszabb, akkor lép életbe a program második fertőzési algoritmusa. A kiszemelt .EXE állományhoz 0–16 bájt közötti értéket tesz hozzá úgy, hogy a teljes hossz osztható legyen 16-tal. Utána a második menetben a program végéhez ad 256 bájt 00h karaktert. Ilyenkor sem változtatja meg a könyvtári bejegyzést. A trükk abban rejlik, hogy a 00h-t a víruskeresők egy része vagy programnak, vagy szemétnek értelmezi.

Közli a felhasználóval, hogy programja fertőzött, és úgy beszélget vele, mint az oktató vírusokról szóló fejezetben ismertetett Burger demóvírus. Itt a prog-

ram egyes üzenetei titkosítva, nem karakteres formában vannak a kódban. Íme az első épületes üzenet, amelyről a nevét kapta:

```
A C H T U N G
-------------------------
Die Benutzung einer RAUBKOPIE ist strafbar!
Nur wer Original-Disketten, Handbucher,
oder PD-Lizenzen besitzt, darf Kopien verwenden.
Programmierung is muhevolle Detailarbeit:
Wer Raubkopien verwendet, betrugt
Programmierer un den Lohn ihrer Arbeit.
-------------------------
```

(Figyelem! A kalózmásolat használata büntetendő! Másolatokat csak az használhat, akinek birtokában vannak az eredeti lemezek, kézikönyvek vagy szabadszoftver-engedélyek. A programozás fáradságos, aprólékos munka, és aki kalózmásolatot használ, az becsapja és megfosztja munkabérétől a programozót.)

Ezután egy kis szünet következik, majd a vírus válaszunkat várva felteszi a következő kérdést:

```
Bist Du sauber ? (J/N)
```

(Te tiszta vagy? Igen/Nem.)

Ha a német igennek (ja) megfelelő J gombbal válaszolunk, akkor megjelenik a következő szöveg, és a programkód lefut.

```
Ich will glauben, was Du sagst .....
```

(Elhiszem, amit mondtál...)

Ha a német nemnek (nein) megfelelő N gombbal válaszolunk, akkor a vírus a következőt üzeni:

```
CPU-ID wird gespeichert...
**** LO<garbled>
```

(A CPU azonosítót eltárolom. Meghamisítva.)

Még egy szöveget rejt magában titkosítva a vírus kódja:

```
**** Losche dieses Programm ****
```

(Törlöm ezt a programot)

A programvírus formázza a rendszer bootszektorát, ha a rendszeróra dátuma szerint az adott hónapban már elmúlt 12-e, vagy ha az időpont későbbi, mint 17:00 óra (5:00 PM). Az eredeti programkód még a „normális ágon" végigfutva sem mindig képes futni, a vírus több programhibával terhelt.

A vírus neve: Striker #1

Egyéb elnevezése: Még nem ismeretes.

Hossza: 461 bájt.

Kódtípusa: Nem rezidens, parazita, a .COM állományokat fertőzi meg.

Azonosítása: Scan V76+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: E programvírus az USA keleti partvidékén bukkant fel 1991 márciusában. A vírusnak nincs rezidens része, a fertőzött program indításakor közvetlenül fertőz, és a COMMAND.COM-ot is megtámadja. Amikor lefut a kódja, csak egyetlen másik .COM programot fertőz meg.

Az eredeti és a fertőzött program az első 13 bájtban tér el egymástól, a vírus többi része az állomány végére kerül. Az első rész tartalmazza azokat az ugró és allokációs parancsokat, amelyek eredményeként a víruskód hátrakerülhet a .COM állományban, és a debugger elvű vírusdetektorok nem tudják felfedezni. A végő hossznövekedés 461 bájt, de a könyvtári dátum- és időpontbejegyzések nem változnak. A „Striker #1" vírusazonosító megtalálható a fertőzött állományok végén.

A vírus neve: Vcomm

Egyéb elnevezése: Vircomm.

Hossza: 637 bájt.

Kódtípusa: Parazita, de rezidens része is van, az .EXE állományokat fertőzi meg.

Azonosítása: F-Prot, Scan V60+, IBM Scan, Pro-Scan, VirexPC, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: F-Prot vagy a fertőzött állományok törlése.

Leírása: Ha a Dark Avengerrel vagy pedig az Ivánnal vetjük össze, írója még kezdő volt ebben a műfajban. Mégis, ez az a kelet-európai eredetű (lengyel) vírus, amely — talán éppen primitívsége miatt — nagyon gyorsan átlépte az országhatárokat és Németországban is, az USA-ban is felbukkant. 1989 decemberében kezdett elterjedni.

Ha egy fertőzött állományt elindítunk, az aktuális könyvtárban egy másik .EXE állományt is megfertőz. Amikor a Vcomm a fájl belsejébe (!) épül be, a fájl hossza az 512 bájt többszörösével nő. Ha pedig a végéhez kapcsolja magát, akkor 637 bájtot tesz hozzá az .EXE állomány eredeti méretéhez. A vírus memóriarezidens része figyelemmel kíséri, hogy mikor akar írni a rendszer a lemezre, és az írás műveletét kicseréli olvasásra. A memóriában a COMMAND.COM rezidens részébe rejti el magát.

A vírus a benne lévő rutinokkal, például az állományok belsejébe való beépüléssel, alaposan megelőzte korát. Utána csak 1991 júliusában jelentek meg az első olyan vírusok, amelyek a STACK területére vagy az állományok belsejébe úgy épülnek be, hogy az eredeti program is futásképes. Ilyen fertőzéskor már csak törölni lehet a megtámadott programállományt.

A vírus neve: Microbes

Egyéb elnevezése: Még nem ismeretes.

Hossza: Nem értelmezhető.

Kódtípusa: Bootvírus, a floppyt és a merevlemezt egyaránt megtámadja. Memóriarezidens résszel rendelkezik.

Azonosítása: Scan V64+, Pro-Scan 1.4+.

Eltávolítása: M-Disk, Pro-Scan 1.4+, vagy a DOS SYS parancsa.

Leírása: A vírust 1990 júniusában kezték terjeszteni Indiában. A bootszektort támadja meg, memóriarezidens résszel rendelkezik.

Amikor elindítunk egy vírussal fertőzött lemezt, akkor a rendszerbetöltési (boot) folyamat közben kiakad. Ha ilyenkor beteszünk egy másik lemezt, a ví-

rus azt is megfertőzi. XT gépekben a vírus írásvédett lemezre is képes rámenni, amit a más típusú kontrollerrel ellátott AT-n már nem tud megtenni. Az XT-n azonban, ha nem kapcsoljuk ki a gépet, továbbra sem tudunk rendszert indítani, csak tovább fertőzzük a betett lemezeket. A vírus biztonságosan kitakarítható a rendszerlemezekről tiszta rendszerrel történt indítás után a DOS SYS parancsának kiadásával, vagy a megfelelő szoftverekkel.

A vírus neve: Crew-2480

Egyéb elnevezése: 2480.

Hossza: 2480 bájt.

Kódtípusa: Nem rezidens, parazita vírus. A .COM állományokat fertőzi meg.

Azonosítása: Egyedi azonosítással.

Eltávolítása: A fertőzött állományok törlése.

Leírása: A vírus 1991 februárjában bukkant fel. Memóriarezidens résszel rendelkezik. A COMMAND.COM-ot is beleértve minden 10 bájtnál nagyobb .COM állományt megtámad.

Rezidenssé válása után olyan állományt keres, amely megfelel feltételeinek. Ha a COMMAND.COM-ot találja meg, akkor az megfertőzve már csak egy dologra képes: rendszerindítást csinál. A fertőzés során az állományok hossznövekedése 2480 bájt, a vírus a fertőzött program végére épül be. A könyvtárbejegyzések rendszerideje és dátuma nem változik.

Ha nem a COMMAND.COM-ot fertőzi meg, akkor indításakor a rendszer kiakad. Ez azonban nem általános, más programok ilyenkor lefuthatnak. A monokróm monitorokat rosszul kezeli, ami szintén rendszerkiakadáshoz vezet.

A vírus neve: Deicide

Egyéb elnevezése: Glenn.

Hossza: 666 bájt.

Kódtípusa: Felülíró, nem rezidens, .COM fertőző.

Azonosítása: Egyedi eszközökkel, az állományok megvizsgálásával.

Eltávolítása: A fertőzött állományok törlése.

Leírása: Üzenete alapján egy ifjú vírusíró első műve. A szakirodalom szerint a vírus egy hollandiai BBS-ről került elő. Nem rezidens, a .COM állományokat a COMMAND.COM kivételével felülírja a víruskóddal.

Amikor a kód lefut, a vírus az aktuális könyvtárban keres egy még fertőzetlen *.COM* állományt. Ha megtalálja, akkor az első 666 bájtot felülírja. Ha a .COM program rövidebb, mint 666 bájt, akkor ekkorára nő a hossza, ha hosszabb, akkor az eredeti méretadatok nem változnak. Amikor a vírus tönkretesz egy állományt, a következő üzenetet jeleníti meg a monitoron:

```
File corruption error.
```

Ha a vírus nem talál fertőzhető állományt, akkor a következő üzenetet kapjuk tőle, miközben leformázza a merevlemez első 80 szektorát.

```
DEICIDE!
Glenn (666) says : BYE BYE HARDDISK!!
```

`Next time be carufull with illegal stuff`
(Deicide! Glenn (666) mondja: Isten veled, merevlemez! Legközelebb legyél óvatos az illegális anyaggal.)

Ha talál megfertőzhető állományokat, akkor nem tarolja le merevlemezünket, és minden fertőzött állományban megtaláljuk azt az üzenetet, amely homályosan és nem egészen korrekt angolsággal utal a szerző személyére:

```
This experimental virus was written by Glenn Benton
to see if I can make a virus while learning machinecode
for 2,5 months. (C) 10-23-1990 by Glenn.
I keep on going making virusses.
```

(Ezt a kísérleti vírust Glenn Benton írta, hogy megnézze, tud e készíteni egy vírust 2,5 hónapnyi gépikód-tanulás alapján. Folytatom a víruskészítést.)

A vírus neve: Dot Killer

Egyéb elnevezése: Doteater, 944, Point Killer.

Hossza: 944 bájt.

Kódtípusa: Parazita, de nincs rezidens része, a .COM állományokat fertőzi meg.

Azonosítása: Scan76+.

Eltávolítása: Clean76+.

Leírása: Újabb bosszantási ötlet, ezúttal Lengyelországból. Ez a vírus onnan kapta nevét, hogy a képernyőről minden pontot (.), azaz ASCII 46-os karaktert kipucol. A vírusnak nincs rezidens része, minden .COM állományt megfertőz, a COMMAND.COM-ot is. Igen primitív tákolmány.

Amikor a kód lefut, megkeres az aktuális könyvtárban egy másik .COM állományt, amibe beleépül. Hosszát 944 bájttal megnöveli, és a fertőzés során a programkód végére épül be. A vírus vizsgálja a COMSPEC környezeti változót is, mert ennek alapján akarja megtalálni a COMMAND.COM-ot. De ezt a rutint alaposan elszúrták, mert nem működik. Ehelyett, ha a COMMAND.COM az éppen aktuális könyvtárban van, akkor mint egy közönséges .COM programot, azt is megfertőzi.

A vírus neve: EDV

Egyéb elnevezése: Cursy.

Hossza: Nem értelmezhető.

Kódtípusa: Rezidens résszel rendelkező, bootot és partíciós táblát fertőző vírus.

Azonosítása: Scan V58+, IBM Scan, Pro-Scan 1.4+, VirHunt 2.0+.

Eltávolítása: MDisk /P, Clean V67+, Pro-Scan 1.4+.

Leírása: Le Havre környékén, Franciaországban bukkant fel ez a vírus még 1988-ban, és Jean-Luc Nail jelezte előkerülését. Ekkor úgy tűnt, hogy csak kísérleti darabbal állunk szemben. Két évvel később ugyanez a vírus már járványokat okozva lépett ismét színre. Ekkor, vagyis 1990 januárjában kapta az EDV vírus elnevezést.

A vírus memóriarezidens résszel rendelkezik, floppyn a boot rekordot, a me-

revlemezen pedig a partíciós táblát támadja meg. A rendszermemória felső területére épül be. Az INT 12 visszatérését magához igazítja, így amikor a memóriában van, a lemezhozzáféréseknél a nem írásvédett floppykat megfertőzi, és az eredeti bootszektort elmenti a floppy 1. oldal 39. sáv 0. szektorába, önmagát pedig a 0. abszolút szektorba, vagyis a boot helyére másolja be. A winchesteren az eredeti partíciós táblát átteszi a 1. oldal 39. sáv 8. szektorára, helyére pedig ő ül be. A partíciós tábla programjaként az elmentett információkat tölti be.

Amikor a vírus már hat lemezt megfertőzött, aktivizálódik, letiltja a billentyűzetet és az első három sávot (FAT, boot és a főkönyvtár egy része) felülírja. Utána jelenlétét a következő üzenettel közli:

`That rings a bell, no? From Cursy`

(Ez megkondít egy harangot, ugye? Cursytól.)

Végezetül kiakasztja a gépet, és már csak a főkapcsoló segít. Utána meg nem tudjuk elérni a merevlemezt. Ugyanakkor, ha jelen van a memóriában, a segédprogramoknak az elmentett eredeti bootrekordot mutatja be. Ilyenkor tiszta lemezről kell rendszert indítani. A vírusos floppy bootszektorában vagy a merevlemez partíciós táblájában ott láthatjuk a névadó vírusazonosítót:

`MSDOS Vers. E.D.V.`

Nem nagyon terjedt el, mert a vírus túl rövid ideig vár a beépülés és az aktivizálódás között.

Hírhedt vírusok

Cascade, 1701-B, 1704-D, 1704-Y, Cunning, Cascade-B, 1704-C, Icelandic, Icelandic-II, Icelandic-III, Saratoga, Swedish Disaster, MIX/1, Armagedon, Australian 403, Dutch 555, Groen Links, Holland Girl, Sylvia 2, Halloechen, Sorry, Perfume, Swiss 143, Italian 803, Italian 803-B, Paris, 903, Hybryd.

Sajnos a vírusírók többségének kiléte titok marad, de a vírusok származási országa többnyire kiderül, tehát saját hazájuknak szereznek negatív hírnevet. Könyvünk ezen fejezetében olyan vírusokat mutatunk be, amelyek megjelenésükkel felhívták a figyelmet egy-egy országra, vagy maguk a vírusok váltak híressé és elterjedtté. Például a Potyogós a kevés számítástechnikai ismerettel rendelkezők számára maga „a" számítógépvírus.

A vírus neve: Cascade

Egyéb elnevezése: Fall, Falling Letters, 1701, 1704, Herbst, Poty #1, Potyogós COMMAND.COM, Austrian #2.

Hossza: 1701 vagy 1704 bájt.

Kódtípusa: Parazita, rezidens része van. Titkosítja, azaz alaposan átkódolja magát, a .COM állományokat fertőzi.

Azonosítása: Scan, F-Prot, IBM Scan, DXU2, CHKVir régi változatok, CHKSeq v.1.0, Sysdoki, Pro-Scan, VirexPC, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: M-1704, CleanUp, F-Prot DXU2, Prgdoki, Serum, Serum2, Serum3, CHKVir v.4.01, Sysdoki.

Leírása: Magyarországon ez volt az első komoly vírusjárványt okozó programvírus. Trójai funkcióként ültették be egy hasznos segédprogramba, amelynek a rendszerindításkor bekapcsolva maradó Num Lock gombot kellett alaphelyzetbe visszaállítania. A vírus viszont lehullatta a karaktereket a képernyő aljára. 1987 végén valaki a trójai program alapján megírta a csak .COM állományokat fertőző, memóriarezidens vírust.

A vírus izraeli eredetű, de feltételezik, hogy más szempontból is manipuláltak a kóddal. A vírus maga a programozás klasszikusának számít, sok technikai fogás itt jelentkezett először. Ahhoz, hogy valaki egyáltalán elkezdjen a vírustalanítás szakmai kérdéseivel foglalkozni, valahol itt kell kezdenie az is-

merkedést. Sajnos a teljes, kellően dokumentált forráskódot a vírusíró nem publikálta. E könyv szerzőinek birtokában is csak egy visszafejtett kód van.

Az eredeti vírus hossza 1701 bájt. A fertőzés célpontjai az IBM PC-k klónjai voltak. A 3 bájttal hosszabb változat azt is megvizsgálja, hogy a BIOS-ban van-e eredeti IBM copyright jelzés. Ha van, akkor fertőzés és egyéb ténykedés nélkül kilép, a kód el sem indul. Maga a vírus néhány egyedülálló megoldással rendelkezik. Itt alkalmazták először a víruskódot titkosító algoritmust, amely a detektálást, visszafejtést és a mentesítést bonyolulttá teszi. Az aktivizálódást is több feltétel megléte indítja el. Ezek megállapítására szerepel ténykedései között például a gép és a monitor típusának vizsgálata. Az aktivizálódás attól is függ, hogy van-e belső óra a gépben.

A vírus aktivizálja magát minden olyan gépen, amelyikben CGA, EGA vagy VGA monitorkártya van. Néhány változata IBM PC/AT klónokon nem aktivizálódik, csak terjed. Potyogtató funkciója az 1980–1988 közötti időszakban, azon belül is csak szeptember, október, november és december hónapokban működött. Ezen túl — tehát napjainkban is — csak terjed. Igen sok (olykor csak minimálisan megváltoztatott) átirata ismeretes. Többek között a potyogtatás időpontját aktualizálták.

Ha elindítunk egy Potyogós vírussal fertőzött programot, először a vírus aktivizálódik. Bemásolja magát a gép memóriájába, átveszi az operációs rendszertől néhány ellenőrzési pont — az idő (timer), a képernyőkezelő (video) megszakítások — kezelését. Ilyenkor még nem veszünk észre semmit, hiszen mindez nagyon gyorsan történik. A memóriában elbújva azután megkezdi tevékenységét. Először csak egy, később egyre több betű lepotyog a képernyőn, elrontva az ott lévő szövegeket, így lehetetlenné téve a munkát. A vírus egyes változatai a karakterek potyogtatása közben hangeffektusokat is adnak. Egyetlen vírusos program is elegendő teljes elszaporodásához. A külső (floppy) és a belső adathordozókon (merevlemez) vagy a helyi hálózatokon lévő állományokra egyaránt veszélyes. A kezdeti időben ártalmatlannak vélve sajnos sokan tudatosan terjesztették.

A Cascade vírusnak a következő átiratai váltak ismertté:

1701-B: Azonos az 1701-essel, csak az időfeltételt írták át, így minden esztendő őszén potyogtatja a betűket a képernyőn.

1704-D: Azonos az 1704-essel, csak annyiban tér el attól, hogy nem lép akcióba, ha egy IBM copyright információt tartalmazó BIOS van a gépben.

1704-Y: Azonos az 1704-essel, csak a vírusazonosító kódot írták át Jugoszláviában. A szakirodalomban ismert másik elnevezése: 17Y4.

Cunning: A potyi víruskódjának visszafejtésével, átírásával és újrafordításával készült átirat. Zenél.

(Lásd még az 1704 Format vírus adatait is!)

A vírus neve: Cascade-B

Egyéb elnevezése: Blackjack, 1704-B, Poty #2, 1704/Cascade, Black Jack 17+4=21.

Hossza: 1704 bájt.

Kódtípusa: Parazita, rezidens része van, saját magát titkosítja, azaz átkódolja. A .COM állományokat fertőzi meg.

Azonosítása: Scan, F-Prot, IBM Scan, CHKSeq v.1.0, Prgdoki, Sysdoki.

Eltávolítása: M-1704, M-1704C, CleanUp, F-Prot, Prgdoki, CHKVir v.4.01, Sysdoki.

Leírása: A Cascade-B vírus hasonlóan működik, mint a Cascade. A fő különbség, hogy a betűpotyogtatást valaki a rendszer újraindítását eredményező rutinnal cserélte fel. Egyes változatai azonban potyogtatnak is. Ami lényeges: a vírus aktivizálódását követően egy véletlenszerű időpontban a rendszer újraindul (reboot).

A következő változatát sikerült elkülöníteni:

1704-C: Azonos az 1704-B vírussal, csak annyi az eltérése, hogy minden esztendőben, december hónapban potyogtat. A megszokott detektorok kimutatják, de a mentesítés más eljárással történik.

A vírus neve: 1704 Format

Egyéb elnevezése: Formázó Potyogós.

Hossza: 1704 bájt.

Kódtípusa: Parazita, rezidens része van, kódolja magát, a .COM állományokat fertőzi.

Azonosítása: Scan, F-Prot, IBM Scan, Pro-Scan, VirexPC, AVKT 3.5+, VirHunt 2.0+.

Eltávolítása: M-1704, Clean, Scan /D, CHKSeq v.1.0, F-Prot, Prgdoki, Sysdoki, Pro-Scan, VirexPC, VirHunt 2.0+.

Leírása: Teljesen azonos a Cascade vírusssal, csak amikor aktivizálódik, egyúttal formázza is a lemezeket. A vírus tevékenységéből egy évet kihagy, ugyanis nem aktivizálódik 1993 évben. Egyébként minden év október, november és december hónapjában pusztít.

A vírus neve: Icelandic

Egyéb elnevezése: 656, One In Ten, Disk Crunching, Saratoga 2.

Hossza: 656 bájt.

Kódtípusa: Van rezidens része, parazita, az .EXE állományokat fertőzi.

Azonosítása: Scan V67+, F-Prot, CHKSeq v.1.0.

Eltávolítása: Scan /D, F-Prot.

Leírása: A vírus egy család első tagja. Izland szülötte, ott kapta a „Disk Crunching", azaz a Lemezropogtató nevet. Első változata 1989 júniusában bukkant fel. A vírus csak az .EXE állományokat fertőzi, amelyek hossza ezáltal a tapasztalatok szerint 651 vagy 671 bájt értékkel nő meg. A növekedés hossza a 16 többszörösével változhat. (A DOS paragrafushatárai miatt.) A vírus jelzi

magának, hogy beült egy állományba, és ne telepedjen oda másik példánya. Az erre szolgáló jelsorozat az állomány végén található, hexadecimálisan 4418,5F19.

Az Icelandic vírus a fertőzött program első futásakor átmásolja magát a szabad memória végére. Elrejti magát a memóriát feltérképező programok elől. Amikor pedig a program utoljára ide akar írni, a rendszer összeomlik. Ha a vírust keressük, nem szabad arról megfeledkezni, hogy az INT 13 hívóvektort (hooked) jó pár olyan program is használhatja — teljesen legálisan —, amely nem fertőzött. Ha pedig a memóriateszt során az INT 13 nem jelentkezik hívóvektorként, azaz éppen nem használják, akkor a fertőzés minden tizedik programfuttatáskor bekövetkezik.

Ha a rendszerben csak egy floppymeghajtó van, vagy pedig 10 Mbájtnál kisebb a merevlemez, akkor semmi sem ösztönzi a vírust a rombolásra. Egyébként pech! A 10 Mbájtnál nagyobb merevlemezen a vírus kiválaszt egy nem használt FAT belépési pontot. Itt bejelöli annak a rosszra (bad) állított logikai egységnek (cluster) a belépési pontját, ahol ő lakik, s így minden pillanatban készen áll a fertőzésre.

A vírus neve: Icelandic-II

Egyéb elnevezése: System Virus, One In Ten.

Hossza: 632 bájt.

Kódtípusa: Parazita, rezidens része van, az .EXE állományokat fertőzi meg.

Azonosítása: Scan V76+, F-Prot, CHKSeq v.1.0.

Eltávolítása: Scan /D, F-Prot.

Leírása: Az Icelandic-II átírt változata az eredeti Icelandic vírusnak. Először 1989 júliusában vették észre, ugyanott, ahol elődjét. Fő jellemvonásaik megegyeznek, de van néhány kellemetlen eltérés, sőt programozási hibákkal is alaposan terhelt.

Amikor az Icelandic-II fertőz, módosítja az állományok keletkezési dátumait. Innen bárki észreveheti, hogy valami történt a szoftverrel. Hasonlóképpen programozási hiba, hogy amikor fertőzés céljából leveszi a csak olvasási (read-only) attribútumot, utána elfelejti visszatenni, ha már beépült a programba. Innen látható, hogy a program írója nem valami mélyen nyúlt a normál DOS szintje alá. Az sem kizárt, hogy tulajdonképpen ez korábbi, a kijavítatlan programváltozat, csak később indították el, vagy később észlelték.

Az Icelandic-II akkor is tud programot fertőzni, ha a 21-es megszakításra ráültetünk egy rezidens programokat figyelő TSR monitorprogramot, mint például a Magyarországon is jól ismert FluShot+ szabadszoftvert. Ha a winchester nagyobb mint 10 Mbájt, akkor nem jelöl be rossz szektorokat a FAT-táblába, ellentétben az eredeti Icelandic vírussal.

A vírus neve: Icelandic-III

Egyéb elnevezése: December 24th.

Hossza: 853 bájt.

Kódtípusa: PRE. Parazita, rezidens része van, az .EXE állományokat fertőzi meg.

Azonosítása: Scan V57+, F-Prot, CHKSeq v.1.0.

Eltávolítása: F-Prot, Scan /D vagy törölni a fertőzött állományokat.

Leírása: Nagyrészt ugyanazok a tulajdonságai, mint a korábbi Icelandic változatoknak. Magát a vírust is ugyanott azonosították 1989 decemberében, mint társait. Írója valami sajátos logikával így ünnepelte a karácsonyt. Az Icelandic-III azonosító jelsorozata (sztringje) az utolsó két szó a program végén. Hexadecimálisan: 1844,195F — ahol ezek szavanként fordítottjai az Icelandic vírusban előfordulóknak. Ezen kívül még egy adag üres utasítást (NOP = no operation) is hozzáadott a szerző az átírás során. Sajnos ez a NOP átírási technika Magyarországon is népszerű lett. Egyszerű, de hatásosan akadályozza meg a hagyományos eljárásokkal történő azonosítást.

Feltételezhető, hogy valóban ez a változat a harmadik az evolúciós sorban. Mielőtt fertőzne, mindig körülnéz, hogy testvérei nem fertőzték-e már meg a programot. Ha igen, akkor nem bántja az állományt. z fertőzés során az egyes állományok hossza a paragrafushatárok miatt 853–868 bájt közötti hosszúsággal nő. Ha a programot véletlenül december 24-én futtatják, akkor a következő üzenetet írja ki a képernyőre:

```
Gledileg jol
```

(Boldog karácsonyt)

A vírus neve: Saratoga

Egyéb elnevezése: 642, One In Two.

Hossza: 642 bájt.

Kódtípusa: Parazita, rezidens része is van, az .EXE állományokat fertőzi meg.

Azonosítása: Scan, F-Prot, CHKSeq v.1.0.

Eltávolítása: Scan /D, F-Prot, vagy törölni kell a fertőzött állományokat.

Leírása: A vírust először 1989 júliusában találták meg Kaliforniában. Nagyon hasonlít az Icelandic és az Icelandic-II vírusokhoz. (Az alapinformációkat lásd ott.) A vírus a memória-ellenőrző blokkon (MCB) keresztül válik rezidenssé, ezért hasonlóan az Icelandic vírushoz, olyan rezidens antivírus programok mellett is tud fertőzni, amelyek a 21-es megszakítást figyelik. Az MCB block manipulációi miatt védi a más programok általi felülírástól a memóriának azt a területét, ahol dolgozik. Így például a népszerű FluShot+ mellett is „röhögve" betolakszik. Az Icelandic-II vírushoz hasonlít abban, hogy a csak olvasható (read-only) attribútumú állományokat is meg tudja fertőzni. Utána nem állítja vissza a fertőzött program ezen tulajdonságát.

A vírus neve: Swedish Disaster

Egyéb elnevezése: Még nem ismeretes.

Hossza: Nem értelmezhető.

Kódtípusa: Bootszektort és partíciós táblát fertőző vírus, rezidens résszel.

Azonosítása: Scan V74+.

Eltávolítása: Mdisk /P.

Leírása: A vírust Svédországban eresztették el 1991 januárjában. Svédországból viszonylag kevés vírus jutott el külföldre. (És jóval több a jelentéktelennek látszó Izland szigetéről!) A vírus a floppyn a bootszektort fertőzi meg, a merevlemezen pedig a partíciós táblára ül rá.

Amikor rendszert hívunk egy fertőzött floppyról, akkor a vírus rezidenssé válik és megfertőzi a merevlemez partíciós tábláját. Az eredeti partíciós táblát a 0. oldal, 0. sáv 6. szektorára teszi le. A rendszermemória felső területeire épül be és 2048 bájt helyet foglal el, de a programok számára rendelkezésre álló területet 6994 bájttal csökkenti. Az INT 12 visszatérését alaposan módosítja.

Ha a memóriában ül, akkor a lemezhozzáférési műveletek (katalógusolvasás, másolás stb.) közben ráteszi magát a floppyra, ha az nem fertőzött és nem írásvédett. A szabványos 360 K-s 5,25"-es floppy esetében az eredeti bootrekordot átrakja a gyökérkönyvtár egyik utolsó szektorára, a 11-es sorszámúra. Miként a Stoned vírusnál, itt is elvesznek azok az állományok, amelyeknek az adatait ide írta fel a rendszer. A vírus azonosítójaként használt szöveg meglelhető a fertőzött floppy bootrekordjában, illetve a merevlemez partíciós táblájában, mint oda nem tartozó üzenet:

`The Swedish Disaster`

(A svéd csapás)

Floppyk esetében a bootrekordot kell visszamásolni eredeti helyére, merevlemezeken a 4.xx DOS verzióig az Mdisk /P opcióval lehet helyreállítani az eredeti partíciós táblát. Afelett a partíciós tábla mentésének visszatöltése segít.

A vírus neve: MIX/1

Egyéb elnevezése: MIX1, Mixer 1.

Hossza: 1618 bájt.

Kódtípusa: Parazita, rezidens része van, az .EXE állományokat fertőzi meg.

Azonosítása: Scan V37+, F-Prot, CHKSeq v.1.0.

Eltávolítása: Scan /D, Virus Buster vagy F-Prot.

Leírása: Igazság szerint ennek a vírusnak nem itt, hanem a hadicélú vírusok fejezetében lenne a helye. Mivel azonban a grönlandi vírusok kódjával nagyfokú rokonságot mutat, inkább mégis itt tárgyaljuk. A terrorcélzattal készült vírusok sorában érdekes színfolt ez a kártevő. 1989. augusztus 21-én egyszerre bukkant fel számos szabad hozzáférésű izraeli eletronikus adatbankban, azaz BBS-ben. A vírus hozzáépül az állományokhoz. Ha egy fertőzött programot futtatunk, a memóriában a vírus 2048 bájtot foglal le a RAM-ból.

A megtámadott állomány hossza minden fertőzés alkalmával 1615–1635 bájt közötti hosszal nő meg, az eredeti állomány paragrafushatárainak függvé-

nyében. A vírus nem támadja meg a 8 kbájtnál kisebb állományokat. Egyszerű eszközökkel úgy azonosítható, hogy a megfertőzött állományok utolsó négy bájtját megnézzük. Ha a vírus beépült az állományba, akkor ott a következő karaktersorozatot kell lelnünk: MIX1. Ha pedig Debuggert használunk és a 0:33C címen található bájt értéke egyenlő hexa 77-tel, a vírus a memóriában van.

A vírus alaposan megkavarja a soros és a párhuzamos csatlakozókra kiküldött jeleket, a Num Lock-ot pedig nem lehet kikapcsolni. A hatodik fertőzés után a rendszerbetöltés összeomlik, mert a vírus hibákat okoz a programkódban. Ugyanakkor megjelenik egy pont-karakter a képernyőn, a „labda", amely ide-oda bolyong. Ennek a vírusnak vannak olyan változatai is, amelyek nem okoznak rendszerösszeomlást, és csak a 16 kilobájtnál hosszabb állományokat fertőzik meg.

A vírus neve: Armagedon

Egyéb elnevezése: Armagedon The First, Armagedon The Greek.
Hossza: 1079 bájt.
Kódtípusa: Rezidens része van, a .COM állományokat fertőzi.
Azonosítása: ViruScan V64+, F-Prot 1.12+, Pro-Scan 2.01+.
Eltávolítása: F-Prot 1.12+ vagy törölni a fertőzött állományt.
Leírása: Viszonylag ritka és érdekes vírus. 1990. június 2-án bukkant fel Görögországban. George Spiliotis izolálta először, Athénben. Fridrik Skulason tanulmányozta alaposan a vírust és jött rá egy érdekes tulajdonságára. Ha a gépben Hayes-kompatibilis modem van installálva, akkor a vírus elkezdi folyamatosan tárcsázni a következő telefonszámot: 081-141. Nem csekély nyomozás után sikerült kideríteni, hogy Kréta szigetén ezen a telefonszámon lehet felhívni a pontos időt.

A .COM állományokat fertőzi meg, azok hossza 1079 bájttal nő. A kódot a program elejéhez adja hozzá. Amikor a program rezidenssé válik, a vírus elkapja a 8-as valamint a 21-es megszakítót. Ezután minden olyan .COM állományt megfertőz, amelyik a vírus rezidenssé válása után lefut. A vírus a következő szöveget küldözgeti különböző időközönként a .COM kimenetekre:

```
Armagedon the GREEK
```

(Armagedon, a görög)

Naponta 5:00 és 7:00 órakor jön rá a telefonálhatnék, amikor a Krétai pontos időt kergeti. Ha sikerült a kapcsolat, akkor a vonalat tartja, anélkül, hogy a felhasználót figyelmeztetné. A gép addig használja a vonalat, amíg csak hagyjuk neki. Károkozása mindössze annyi, hogy nem fizeti ki a telefonszámlát. A megvalósításban egy kicsit hebehurgya volt ennek az ötletnek a kiagyalója, mert Kréta szigetén kívül a trükk nem igazán működik, hiszen mások a körzetszámok és a hívószámok.

A vírus neve: Australian 403

Egyéb elnevezése: Még nem ismeretes.

Hossza: 403 bájt.

Kódtípusa: Parazita, rezidens résszel rendelkező, .COM fertőző vírus.

Azonosítása: Egyedileg, az állományokat „szemrevételezve".

Eltávolítása: A fertőzött állományok törlése.

Leírása: A kenguruk kontinensének, Ausztráliának is megvannak a maga vírusai, csak a távolság miatt azok nem jutnak el hozzánk olyan nagy számban. Ez a vírus 1991 februárjában bukkant fel Ausztráliában, ahonnan a szakirodalomban Colin Keeble ausztráliai számítógép-bakterológus nyomán értesülhettünk megjelenéséről.

A vírus viszonylag rövid, de semmi köze nincs a Bulgáriából világpolgárrá vált népes Tiny családhoz. Memóriarezidens, .COM fertőző, megtámadja a COMMAND.COM-ot is. Magát a rendszermemória alsó részére installálja, ahol rezidensként 720 bájtot foglal, és magára irányítja az INT 21-et.

A vírus cseretrükkel dolgozik: amikor memóriarezidenssé válik, az aktuális meghajtó aktuális könyvtárában két .COM állományt lecserél egy-egy 403 bájt hosszú állományra, vagyis saját magára. Éppen ezért nem lehet vele semmi mást kezdeni, mint törölni. A fájl nevét meghagyja, de a könyvtári bejegyzést a változásnak megfelelően valóságossá teszi, tehát a vírus hosszát és a fertőzéskor aktuális rendszerdátumot és időpontot tünteti fel. Ha ezt az állományt naivan futtatni akarjuk, akkor csak a vírust indítjuk el ismét...

A vírus neve: Dutch 555

Egyéb elnevezése: 555.

Hossza: 555 bájt.

Kódtípusa: Parazita, rezidens résszel rendelkező vírus, a .COM és az .EXE állományokat támadja meg.

Azonosítása: Scan V75+.

Eltávolítása: Törölni a fertőzött programokat.

Leírása: Hollandia vírustulipánja a rövid, de igen durva vírusok közé tartozik. 1991 februárjában izolálta Richard Zwienenberg.

A vírus a .COM és az .EXE állományokat, valamint a COMMAND.COM-ot is megtámadja. A rendszermemória felső részére épül be, azt 560 bájttal csökkentve, és az INT 12 visszatérését alaposan átalakítva. Azt INT 21-et magára irányítja. Amikor rezidens, a futtatott .COM és .EXE programokba írja be magát az állományok végére.

A vírus neve: Groen Links

Egyéb elnevezése: Green Left.

Hossza: 1888 bájt.

Kódtípusa: Rezidens résszel rendelkező, a .COM és az .EXE programokat fertőző, propagandavírus.

Azonosítása: Scan V67+, Pro-Scan 2.01+.

Eltávolítása: Scan /D, Pro-Scan 2.01+ vagy törölni a fertőzött programokat.

Leírása: A hadibacikról már szóltunk könyvünkben. Az eszmék háborús kellékéhez, a propagandához Hollandiában a militáns Zöldek használták fel a számítógépvírust. A holland Groen Left (a Zöld ellenzék) választási felhívását öntötték vírus formájába, amely 1990 márciusában került forgalomba.

A Jerusalem-B vírus volt az átírás forrása, de olyannyira sikerült átbarkácsolniuk, hogy teljesen új vírus lett belőle, ezért is került ebbe a fejezetbe. A vírus a .COM és az .EXE állományokat támadja meg, de nem bántja a COMMAND.COM-ot. Amikor a vele fertőzött program kódja lefut, installálja magát a rendszermemória alsó részén, és ott 1872 bájt helyet foglal le magának. Az INT 21 és az INT CE interruptokat irányítja magára. A fertőzött .COM programok hossza 1893 bájttal nő meg, és a vírus a program végére épül be, az .EXE programok 1888–1902 bájttal lesznek nagyobbak, és a kód a program végére telepszik. Többszöri fertőzés esetén minden újabb alkalommal 1888 bájttal növeli meg a programállomány hosszát. Az .EXE programokba ismételten is beépülhet, a .COM állományokba csak egyszer. A vírus azonosítója minden fertőzött állományban karakteresen látható:

GRLKDOS

Miután a vírus rezidenssé vált, elkezdi választási propaganda-hadjáratát. Minden harmincadik percben eljátssza a Zöld Baloldal „Stem op Groen Links", azaz „Szavazz a Zöld Balokra" című választási indulóját.

A vírus neve: Holland Girl

Egyéb elnevezése: Sylvia, Netherlands Girl.

Hossza: 1332 bájt.

Kódtípusa: Van rezidens része, parazita, a .COM állományokat fertőzi meg.

Azonosítása: Scan V50+, F-Prot, CHKSeq v.1.0. IBM Scan, Pro-Scan, VirexPC, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: F-Prot, Pro-Scan 1.4+, VirHunt 2.0+, Scan /D vagy a fertőzött állományok törlése.

Leírása: Első felbukkanását Jan Terpstra jelentette Hollandiából. A vírus memóriarezidens, csak a .COM állományokat fertőzi meg, kivéve a COMMAND.COM-ot. A fertőzött állományok 1332 bájtttal lesznek hosszabbak, de nem keletkezik más kár. A vírus neve onnan származik, hogy tartalmazza egy Sylvia nevű hollandiai lány nevét, címét, telefonját, és egy felszólítást, hogy küldjenek neki levelezőlapot. A vírust a lány egyik volt barátja írta. A vírusírást pedig leülte egy kényelmes fegyintézeti cellában. A lány viszont kénytelen volt a vírusban megadott címről elköltözni. Előző könyvünk óta kézhez kaptuk a szokatlan szerelmi közvetítésre hivatott vírust is. Íme az üzenet:

```
This
     program
             is
               infected
                        by
                          a
                            HARMLESS
                                     Text-Virus V2.1
Send a FUNNY postcard to : Sylvia Verkade,
                           Duinzoom 36b,
                           3235 CD Rockanje
                           The Netherlands.
You might get an ANTIVIRUS program.....
```

(Ezt a programot egy ártalmatlan Szöveg-Vírus V2.1 fertőzte meg. Küldjön egy tréfás levelezőlapot az alábbi címre: Sylvia Verkade, ... Biztosan van egy antivírus programja...)

Miután a fenti üzenet megjelenik, lefut a fertőzött program, s utána jön egy trágár zárószöveg, amit a program kódolva tárol:

```
FUCK YOU LAMER !!!!
system halted...$
```

(Kb.: Te faszkalap! A rendszer leállítva.)

Utána a program kimerevedik, csak az újraindítás segít. A vírus az üzengetés közben legalább öt .COM állományt megfertőz az aktuális meghajtón. A vírus 1301 bájtot tesz hozzá az állomány elejéhez és 31 bájtot a végéhez. A rejtett rendszerállományokat nem bántja.

A vírus neve: Holland Girl 2

Egyéb elnevezése: Sylvia 2.

Hossza: 1332 bájt.

Kódtípusa: Rezidens, .COM fertőző, parazita vírus.

Azonosítása: Ha a Scan nem azonosítja az előző vírusként (Holland Girl), akkor csak az állományok „szemrevételezésével" lehet azonosítani.

Eltávolítása: A fertőzött állomány törlése.

Leírása: 1991 januárjában Kanada New Brunswick nevű városában valaki átbarkácsolta a holland kislánynak írt szerelmi vírust. A szöveget teljesen változatlanul hagyta, talán nem akart a kódolás visszafejtésével foglalkozni, helyette a könnyebb megoldást választva a terjesztő rutint írta át egy kicsit, hogy a korábbi eljárásokkal ne lehessen azonosítani. A vírus mérete és az aktivizálódás módja sem változott. Újdonság viszont benne a fertőzendő állományok keresési sorrendje.

A vírus megfertőzi a COMMAND.COM-ot is. Így amíg a vírus üzenget, az is legalább öt állományt fertőz meg, először a C: meghajtó főkönyvtárában keresgélve, majd pedig az aktuális meghajtó aktuális könyvtárában. A hossznövekedés 1332 bájt, ami a fertőzött program elejére kerül.

A vírus neve: Halloechen

Egyéb elnevezése: Még nem ismeretes.

Hossza: 2011 bájt.

Kódtípusa: Parazita, a .COM és az .EXE állományokat fertőzi meg. Rezidens része van.

Azonosítása: Scan V57+, Pro-Scan 1.4+, VirexPC, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: Scan /D, VirHunt 2.0+, vagy a fertőzött állományok törlése.

Leírása: Halloechen vagy ahogy nálunk ismerik, Holle anyó a német mesevilág figurája. Amikor megrázza ágyának párnáit, havazás kezdődik a Földön, és beköszönt a tél. A vírus erről a mesealakról lett elnevezve.

A Halloechen vírust Christoff Fischer Németországban, az Universität Karlsruhe számítógépes rendszerében fedezte fel. Amikor fertőzött programállományt futtatunk, a billentyűről beadott karaktereket alaposan összezagyválja, így nem tudunk értelmes szavakat beírni. (Mellesleg hasonlót produkál néhány „magyar ékezetesre átalakított" PC is, ha eredeti angol programot futtatunk. Ez nem vírus, hanem hozzánemértés, inkompatibilis kódkiosztás...)

A vírussal fertőzött program lefutása után épül be a memóriába. Minden olyan futtatott állományt megfertőz, amely nagyobb mint 64 K, vagy az állomány dátuma megegyezik az aktuális rendszeridő hónapjával és évével. Ha pedig a hossza 64 K-nál nagyobb és az adott időn kívül esik, akkor fertőz. Az állományhossz 2011 bájtos víruskóddal, plusz esetleg a 16 többszörösével nő.

A vírus neve: Sorry

Egyéb elnevezése: G-Virus V1.3.

Hossza: 731 bájt.

Kódtípusa: Rezidens résszel rendelkező, parazita, .COM fertőző.

Azonosítása: Scan V64+, F-Prot, Pro-Scan 2.01+.

Eltávolítása: Scan /D, Pro-Scan 2.01+, vagy törölni a fertőzött állományokat.

Leírása: Számos antivírus program 4711-nek vagy Perfume-nek véli felismerni, pedig nem sok köze van hozzájuk. Nevét elnézést kérő szöveges üzenetéről kapta. 1990-ben több gócponton lépett fel az NSZK-ban. Azóta szórványosan kerül elő.

A fertőzött program lefutása után a víruskód a rendszermemória felső részébe épül be, azt 1024 bájttal csökkentve. Az INT 21-et magára láncolja. A COMMAND.COM-ot érdekes módon manipulálja: amikor a vírus memóriarezidens, akkor a COMMAND.COM nem fertőzött, de a víruskód lefutása után átmenetileg ismét fertőzötté válik. Ennek a „hol fertőzött, hol nem fertőzött" játéknak az a célja, hogy a vírus a gép kikapcsolása után újraindításkor ismét rezidenssé válhasson. Amikor a vírus bent ül a memóriában, minden futtatott .COM állományt megfertőz, azok hossza 731 bájttal nő meg, és a kód a program végére épül be.

A vírus az állományban is megtalálható alábbi üzenetet írja ki a monitorra:

```
G-VIRUS V1.3
Bitte gebe den G-Virus Code ein:
```

(G-Vírus V1.3. Kérem, adja meg a G-Vírus kódját.)

A „G" a geheim (titkos) rövidítése lehet. Ha ezek után megadunk egy számot, a következő üzenet érkezik:

```
Tut mir Leid !
```

(Nagyon sajnálom!)

Még nem sikerült kideríteni, mi az igazi kód, amit elfogad. A Perfume rokonságból sejteni lehet, hogy ha eltaláljuk, akkor a vírus hagyja a programot lefutni, egyébként pedig a fenti sajnálkozó üzenettel kilép a DOS-ba. A vírus többnek látszik, mint egy apró hecc. Elképzelhető, hogy valamilyen nagyobb hordereju fejlesztés kísérleti darabja vagy köztes terméke.

A vírus neve: Perfume

Egyéb elnevezése: 765, 4711.

Hossza: 765 bájt.

Kódtípusa: Parazita, nincs rezidens része, .COM fertőző, beleértve a COMMAND.COM-ot is.

Azonosítása: Scan V57+, F-Prot, CHKSeq v.1.0.

Eltávolítása: F-Prot vagy a fertőzött állományok törlése.

Leírása: A Perfume vírus német eredetű, de első előfordulását Lengyelországban regisztrálták 1989 decemberében. A vírus a .COM állományokat fertőzi, de a COMMAND.COM megfertőzésével egészen addig vár, amíg talál más fertőzendő állományokat. Az állomány a vírus beépülése után 765 bájttal lesz hosszabb. Érdekessége, hogy válaszol a felhasználó kérdésére. Ha vírusfertőzött program fut és a felhasználó begépeli a 4711 karaktersorozatot, megtudhatja, hogy az egy német parfüm neve. A vírus innen kapta elnevezését. Ennek a vírusnak számos változata van. Többek között olyan is, amelyik a kérdésre válaszolva felülírja azt különböző karakterekkel.

A vírus neve: Swiss 143

Egyéb elnevezése: Még nem ismeretes.

Hossza: 143 bájt.

Kódtípusa: Nem rezidens, a .COM állományokat támadja meg, beleértve a COMMAND.COM-ot is.

Azonosítása: Scan V74+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: A vírus 1991 januárjában jelent meg Svájcban. A víruskód lefutása közben az aktuális meghajtó aktuális könyvtárában minden .COM állományt megfertőz. 143 bájttal növeli meg a .COM programok hosszát, és azok végére épül be. A könyvtárbejegyzés idejét és dátumát fertőzés közben az aktuális rendszeridőre és dátumra írja át.

A vírus neve: Itavir
Egyéb elnevezése: 3880.
Hossza: 3880 bájt.
Kódtípusa: Nem rezidens, parazita, az .EXE programokat fertőzi meg.
Azonosítása: Scan V60+, Pro-Scan 1.4+.
Eltávolítása: Törölni a fertőzött programokat.
Leírása: Olaszországban a Milánói Technikai Főiskola egyike a vírusok kirajzási gócának. Ott találták 1990 márciusában ezt a vírust.

A vírusnak nincs rezidens része. A víruskód lefutása közben fertőz, a megfertőzött állomány 3880 bájttal lesz hosszabb. A fertőzés során készít a lemezen egy COMMAND.COM nevű állományt, amelynek első karaktere egy nem nyomtatható jel. Ezt arra használja a vírus, hogy innen kapcsolja rá a kódot más állományokra.

A vírus aktivizálásának feltétele, hogy a rendszer egyvégtében több mint 24 órát menjen. A vírus tönkreteszi a bootszektort, így a rendszer nem tud újraindulni. Az ANSI.SYS-t felhasználó, úgynevezett ANSI-bombák technikáját is alkalmazza, ugyanis az ANSI escape szekvenciák (ESC-jellel kezdődő különleges jelsorozatok) segítségével 0–255 között teljesen véletlenszerűen irányítgatja át az I/O csatlakozási pontokat. Több monitort villogtat is.

A vírus neve: Italian 803
Egyéb elnevezése: Még nem ismeretes.
Hossza: 803 bájt.
Kódtípusa: A .COM és az .EXE állományokat fertőző parazita vírus. Nincs rezidens része.
Azonosítása: A jelenség alapján vizsgálva az állományokat.
Eltávolítása: Törölni a fertőzött állományokat.
Leírása: Az olasz vírusgyártó kisüzemek terméke, 1991 márciusából, az olasz vírusírás fellendülésének időszakából. Nincs a vírusnak rezidens része, de megtámadja a .COM és az .EXE állományokat, közöttük a COMMAND.COM-ot is. Amikor a kód lefut, a vírus keres magának nem fertőzött .EXE állományt az aktuális meghajtón. Ha talál, akkor megfertőzi. Ha nem talál, akkor beéri .COM állománnyal, és megfertőzi azt — ha van.

A hossznövekedés 803–817 bájt, és a vírus az állományok végére épül be. Az idő- és dátumbejegyzést a könyvtári listában nem változtatja meg. A vírus képes ugyanazt az állományt ismételten megfertőzni. Ezt akkor teszi meg, amikor egy másik fertőzött program éppen fut a memóriában. A második vagy további fertőzés esetén a hossznövekedés mindig 816 bájt.

Átirata:

Italian 803-B: Teljesen hasonló az eredetihez, mindössze egy bájtot írt át valamelyik nem túl szorgalmas vírusgyártó.

A vírus neve: Paris

Egyéb elnevezése: Még nem ismeretes.

Hossza: 4909 bájt.

Kódtípusa: Nem rezidens, parazita, a .COM, az .EXE és az overlay állományokat fertőzi.

Azonosítása: Scan V66+, Pro-Scan 2.01+.

Eltávolítása: Törölni a fertőzött állományt.

Leírása: Franciaországban 1990 augusztusában bukkant fel. Az ország határain túl nem nagyon okozott járványt, feltehetően a francia nyelvű programok iránti kisebb érdeklődés miatt.

A vírus békén hagyja a nagyon kicsi .COM állományokat. Megnézi azt is, hogy a C: meghajtón a COMMAND.COM fertőzött-e. Ha nem találja annak, akkor ktüntetett figyelmet fordít megfertőzésére. A hossznövekedés a fertőzések során 4909–4925 bájt között van, a vírus a kód végére épül be.

A vírus neve: 903

Egyéb elnevezése: Még nem ismeretes.

Hossza: 903 bájt.

Kódtípusa: Rezidens résszel rendelkező, .COM fertőző, parazita.

Azonosítása: Scan V74+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: 1991 az „új esztendő, új vírus" jegyében köszöntött be a francia számítógépes szakmának. Ekkor jelent meg ez a nem romboló, inkább kellemetlenkedő, igen rövid programvírus. A COMMAND.COM-ot és a .COM programokat károsítja, azokba épül be. Amint általában a francia eredetű vírusok, ez sem terjedt el nagyon a világban.

A vírus hosszához képest szokatlanul nagy helyet foglal le magának a rendszermemória alsó részén, mint rezidens program. Az INT 21-et magára láncolja. Amikor a COMMAND.COM-ot fertőzi meg, 903 bájtot ad hozzá az elejéhez. A könyvtári bejegyzés időpontját és dátumadatait nem változtatja meg. A vírus a fertőzés során a következő rendszerüzenetet küldi:

```
Fichier introuvable
```

(Az állomány nem található)

Más források szerint ez az üzenet sohasem jelenik meg, a mi példányunknál azonban igen. Ha a COMMAND.COM fertőzött, akkor a rendszer a legtöbb esetben lemerevedik. Amikor a vírus memóriarezidens, akkor az aktuális meghajtó aktuális könyvtárában megfertőz három másik állományt. Ha később a fertőzött eredeti programot ugyanitt újra futtatjuk, akkor már nem fertőz tovább. A DOS copy parancsával csak akkor fertőz, ha a kiindulás és a cél ugyanabban a könyvtárban található.

A vírus neve: Hybryd

Egyéb elnevezése: Hybrid.

Hossza: 1306 bájt.

Kódtípusa: Rezidens résszel rendelkezik, parazita, a .COM állományokat fertőzi meg.

Azonosítása: Scan V74+.

Eltávolítása: Törölni a fertőzött programokat.

Leírása: A lengyel vírusírás kezd felzárkózni a bolgár mellé. Ezt elősegíti, hogy a vírusgyártókat semmilyen szankció nem sújtja, miként Magyarországon sem. A Hybryd vírus 1990 decemberében jelent meg Lengyelországban, és 1991 jan. ában már az USA-ba is eljutott.

Közvetlenül támadó, a .COM programokra veszélyes vírus. A COMMAND.COM-ot is megfertőzi. Ha a fertőzött program lefut, a vírus megnézi az aktuális könyvtárat, hogy talál-e ott fertőzetlen .COM állományt. Ha igen, akkor beépül a végére, azt 1306 bájttal megnövelve. Ezt azonban mindaddig nem észleljük, amíg a vírus a memóriában aktív, mert a lopakodó technikát alkalmazva az eredeti adatokat mutatja be. A Hybryd vírusban a következő, közvetlenül nem olvasható, kódolt ajánlást találjuk, ékes lengyel nyelven:

```
(C) Hybryd Soft
Specjalne podziekowania dla
Andrzeja Kadlofa i Mariusza Deca
za artykuly w Komputerze 11/88"
```

(Külön köszönet Andrzej Kadlof és Mariusz Dec részére a Komputer című lap 1988/11. számában megjelent cikkükért.)

Ezen kívül egy nem kódolt szöveg is található a programban, amely azt sugallja, mintha ezt a bacit az IBM írta volna:

```
Copyright IBM Corp 1981,1987
Licensed Material - Program Property of IBM
```

(Szabadalmaztatott program, az IBM tulajdona)

Nagyon a „bögyükben lehetett" a Nagy Kék, amely ebben az esetben ártatlan... A vírus aktivizálódásának dátuma 1992 péntek 13. (Milyen népszerű ez a nap!) Ha egy ilyen dátum után elindítunk egy Hybryd vírussal fertőzött állományt, akkor a vírus felülírja az aktuális meghajtó bootszektorát. Ha erre nincs lehetősége, akkor is megkárosítja azt az állományt, amelyik éppen fut.

Váltogatott ötletek

1392, Form, Jeff, Jerk, JoJo, JoJo 2, July 13th, June 16th, Kennedy, Keypress, IKV 528, Lazy, Lehigh, Lehigh-2, Lehigh-B, Liberty, Liberty B, Little Pieces, Loa Duong, Mardi Bros.

Itt olyan vírusokat mutatunk be, amelyek a korábbi fejezetek „háziállataival" ellentétben kevésbé hajlamosak a családalapításra, és nehezen tehetők más csoportba. A vírus általában a szerzők egyetlen fellángolása volt, és művüket mások sem tartották alkalmasnak arra, hogy megpatkolva újra és újra feltámasszák. Kevés kivételtől eltekintve ezek egyike sem tartozik az elterjedt vírusok közé. Sajnos életben tartja viszont őket a maszek víruscsere, mert van aki vírust, van, aki bélyeget gyűjt, s a vírusnak is akkor nagyobb az értéke, ha ritkaság.

A vírus neve: 1392
Egyéb elnevezése: Amoeba.
Hossza: 1392 bájt.
Kódtípusa: Parazita, rezidens, .COM és .EXE fertőző.
Azonosítása: Scan V61+, VirexPC 1.1+, F-Prot 1.12+, VirHunt 2.0+.
Eltávolítása: Scan /D, F-Prot 1.12+, VirHunt 2.0+, vagy törölni kell a fertőzött állományt.
Leírása: Indonéziában készült vírus, amelyet 1990 márciusától ismerünk. A vírus a .COM és az .EXE állományokat fertőzi meg, beleértve a COMMAND.COM-ot is. A fertőzés során az állományok könyvtári bejegyzésének adatait kicseréli a fertőzéskor aktuális adatokra. A vírus azonosítását a következő belső rendszerüzenet segíti:

```
SMA KHETAPUNK - Nouvel Band A.M.O.E.B.A
```

A .COM állományok megfertőzésekor kódjának egy részével felülírja az első 1089 bájtot, 303 bájtot pedig az állomány végére másol. Európában ritka.

A vírus neve: Form
Egyéb elnevezése: Még nem ismeretes.
Hossza: Nem értelmezhető.
Kódtípusa: Bootvírus, rezidens résszel.
Azonosítása: Scan V64+, F-Prot 1.12+, VirHunt 2.0+.
Eltávolítása: MDisk, vagy a DOS SYS parancsa.
Leírása: 1990 júniusa óta ismert svájci eredetű vírus. Svájcból nem sok ví-

rus származik, ezért is érdekes ez a ritkaság. A floppy és a merevlemez bootrekordját támadja meg, s egyszerűen eltávolítható.

A vírus a fertőzött lemezről történt rendszerindítással kerül a memóriába, majd megfertőzi az általa elérhető lemezek bootrekordjait. A vírusban levélszerű üzenet található, amely egyes esetekben ASCII karakteresen is olvasható, máskor kódolva van a vírusban.

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

(A Form vírus mindenkinek üdvözletét küldi, aki olvassa ezt a szöveget. A Form nem teszi tönkre az adatokat! Nem kell pánikba esni! ...???)

Ha a vírus a memóriában van, akkor a hangszóró minden hónap 24-én olyasféle kattogásokat hallat, mint amikor rendszerindításkor a gép számol. A vírus akár a McAfee-féle Mdisk programmal, akár a DOS SYS parancsával egyszerűen eltávolítható, feltéve ha tiszta lemezről hívtunk előtte rendszert, és így a vírus nincs a memóriában. Viszonylag jóindulatú vírus, célja inkább csak a boszszantás.

A vírus neve: Jeff

Egyéb elnevezése: Még nem ismeretes.

Hossza: 814 bájt.

Kódtípusa: Nem rezidens, parazita, .COM fertőző.

Azonosítása: Scan V72+, Pro-Scan 2.01+.

Eltávolítása: Törölni a fertőzött állományt.

Leírása: Ha az előző vírusról azt mondhattuk, hogy jóindulatú, akkor ez a programvírus kifejezetten dúvadnak számít informatikai állatseregletünkben. A vírus 1990 decemberében bukkant fel az USA-ban.

Nem rendelkezik rezidens résszel. A .COM állományokat támadja meg, beleértve a COMMAND.COM-ot is. Miközben a fertőzött programmal együtt a víruskód is lefut, a vírus keresi a fertőzhető állományokat a C: meghajtó főkönyvtárából kiindulva. Atikor talál egy még tiszta .COM állományt, megfertőzi, éspedig úgy, hogy hosszát 814–828 bájt közötti értékkel megnövelve, annak végére épül be.

A vírusban kódolva található a következő (névadó) üzenet, amit károkozáskor, azaz egyes szektorok felülírásakor alkalomszerűen megjelenít a monitoron:

```
Jeff is visiting your hard disk
```

Ha pedig „Jeff meglátogatja az ön merevlemezét", akkor könnyen felülírhatja azok kényes részeit, a FAT-táblát, a bootrekordot, a partíciós táblát. Ilyenkor az állományok természetesen hozzáférhetetlenné válnak, és részlegesen sem állíthatók helyre...

A vírus neve: Jerk

Egyéb elnevezése: Talentless Jerk, SuperHacker.

Hossza: 1077 bájt.

Kódtípusa: Nem rezidens, parazita, a .COM és az .EXE állományokat támadja meg.

Azonosítása: A jelenségek alapján „szemrevételezve" az állományokat.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: Ha hinni lehet a Jerk vírusnak, van valahol az USA-ban egy Craig Murphy nevű programozó, aki nagy programfeltörőnek tartja magát, de a Jerk vírus szerzője szerint csak egy tehetségtelen pasas. Ebben a vírusban ez a személyeskedés az üzenet lényege.

A Jerk a .COM és az .EXE programokat egyaránt megtámadja, de nem kíméli a COMMAND.COM-ot sem. Programozási stílusa alapján azonos szerzőtől származhat, mint a korábban bemutatott Jeff. A vírus egy fertőzött programmal betöltődik a memóriába, majd végigpásztázza a C: meghajtó könyvtári struktúráját, keresve a fertőzhető állományokat. Erről az is árulkodik, hogy ha floppyról futtatunk programot, a vírus akkor is folyton a merevlemezen vakar, amit a lámpa villogása jelez. Ha megtalálta a fertőzhető .COM és .EXE állományokat, akkor fertőzés után azok első kilenc bájtja tér el az eredetitől és a víruskód a programnak a végére épül be. Jelenlétét időnként tehetségtelen programozó kollégájának „leleplezését" tartalmazó üzenettel adja tudtul:

```
Craig Murphy calls himself SUPERHACKER but he's just a
talentless jerk!
```

(Craig Murphy önmagát szuper programfeltörőnek nevezi, de csak egy tehetségtelen pasas!)

Ezt a szöveget közvetlenül nem lehet olvasni az állományban, mert kódolva van benne. A fertőzött állomány hossznövekedése 1077 bájt, és megtalálható benne a MURPHY karaktersorozat is, mégpedig a fertőzött állomány negyedik bájtjától kezdve. Egy másik szöveges rész viszont kódolatlanul van az állományban:

```
COMMAND.COM *.COM *.EXE Bad command or file name
```

Aktivizálódásának egyéb feltételei még ismeretlenek számunkra. A vírus igen ritka, eddig csak a víruscsere csatornáin bukkant fel.

A vírus neve: JoJo

Egyéb elnevezése: Még nem ismeretes.

Hossza: 1701 bájt.

Kódtípusa: Parazita, rezidens része van, és saját magát is titkosítja, azaz átkódolja. A .COM állományokat fertőzi meg (a COMMAND.COM-ot is beleértve).

Azonosítása: Scan V63+, Pro-Scan 1.4+, VirexPC, F-Prot 1.12+.

Eltávolítása: Scan /D, F-Prot 1.12+, Pro-Scan 2.01+.

Leírása: A JoJo vírus Izraelben és Spanyolországban szinte egyszerre bukkant fel. (Skulason adatai szerint.) Valószínűleg terrorista szándékkal készült, bár egyes jelek inkább a Cascade vírus készítőinek irányába mutatnak. Nem

rokona ugyana a Cascade vírusnak, de lehet, hogy szerzőjük közös. Ha ez a feltevés igaz, akkor a forrás valahol Hollandiában található egy fejlesztőintézetben.

A vírus minden 63800 bájtnál rövidebb .COM állományt megfertőz. A memóriaellenőrző blokkon (MCB) keresztül, nem szabványos módon válik rezidenssé. A fertőzött lemezegységek első sávját véletlenszerűen felülírja. Feltűnő, hogy a vírus működőképessége az IBM copyright jelének a gépben való jelenlététől függ. Ha az F000:E008 memóriacímem, ami a BIOS része, ott van az IBM copyright, akkor a vírus nem működik, nem bánt semmit sem, csak kilép. Ha viszont nincs ott a Nagy Kék névjegye, akkor a vírus kárt okoz a monitoron nem látható alábbi üzenet kíséretében:

```
Welcome to the JOJO Virus.
Fuck the system (c) - 1990
```

(Üdvözöl a JoJo vírus. Baszhatod a rendszert (c) – 1990)

A vírus nem veszi igénybe a fertőzéshez az INT 13-at, ha azt másik program éppen használja. Ilyenkor letörli a képernyőt és kiakasztja a rendszert, reboot után pedig benn marad a memóriában. Máskor viszont az INT 13-at magára irányítja. A memória szabad területét 2048 bájttal csökkenti. A hossznövekedés fertőzés után 1701 bájt.

A vírus neve: JoJo 2

Egyéb elnevezése: Még nem ismeretes.

Hossza: 1703 bájt.

Kódtípusa: Rezidens, a .COM állományokat támadja meg. Parazita.

Azonosítása: Az általa okozott jelenségek alapján.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: A vírus érdekes módon az USA-ban bukkant fel 1991 januárjában. Benne a Cascade titkosítási eljárását alkalmazták, és több kódrészletük is azonos. Szerzője ugyanakkor a JoJo vírus forráskódjának bázisán dolgozott.

Amikor a vírus rezidenssé válik, minden végrehajtott .COM programot megfertőz. A hossznövekedés 1703 bájt, és a vírus a programállomány végéhez épül hozzá. Memóriarezidens része — hasonlóan a JoJo alapvírushoz — a parancsértelmezővel vetélkedve ugyanarra a területre épül be, lefoglalva egy újabb 48 bájtos blokkot. A vírusban található üzenet kicsit eltér az eredetitől, közölve, hogy „a JoJo vírus újra lecsap":

```
The JOJO virus strikes again.xxxxxxxxxxxx zzz
Fuck the system 1990 - (c)
141$FLu
```

A JoJo2 néhány program fertőzött változatának futtatásakor rendszerkiakadást okoz. Üzenete második sorát néhány esetben megjeleníti a monitoron is. A harmadik karakteres azonosító sor a FluShot antivírus program jellegzetes belső azonosítója. Úgy tűnik, hogy ez a vírus a FluShot ellen különösen jól fel van vértezve. Más esetekben a fertőzött program végrehajtása során a „Not enough memory" hibaüzenetet kapjuk. Végezetül a JoJo2 jellegzetes

tünete még az is, hogy ha rezidens a memóriában, akkor a kurzort a ténylegeshez képest mindig egy pozícióval visszafelé állítja.

Ezt a programvírust a közforgalomban lévő antivírus programok összekeverik a JoJo és a Cascade/1701/1704 vírusokkal, bár az utóbbiakhoz semmi köze.

A vírus neve: July 13th

Egyéb elnevezése: Még nem ismeretes.

Hossza: 1201 bájt.

Kódtípusa: Nem rezidens, parazita, az .EXE programokat fertőzi meg.

Azonosítása: Scan V64+, VirexPC, F-Prot 1.12+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: A vírust 1990 áprilisában Madridban azonosította Guillermo Gonzalez García antivírus-szakértő. Dél-Európában a vírus járványszerűen előfordult. Az .EXE állományokat támadja meg, de nincs memóriarezidens része.

A fertőzött program lefutása közben fertőzi meg azokat az .EXE programokat, amelyek hosszabbak a vírusnál, 1201 bájtnál. A fertőzés során a hossznövekedés 1201–1209 bájt között lehetséges. Minden év július 13-án aktivizálódik, amikor is bolyongó labdaként jelenik meg a monitoron az ASCII 9-es tabulátorjel. A képenyőgörgetés során ez abbamarad. Az állományokba való beépülésén és ezen a jelenségen kívül más kárt nem okoz.

A vírus neve: June 16th

Egyéb elnevezése: Pretoria.

Hossza: 879 bájt.

Kódtípusa: A .COM állományokat fertőzi meg, nem rezidens.

Azonosítása: Scan V62+, Pro-Scan 1.4+, VirexPC, AVTK 3.5+, F-Prot 1.12+, VirHunt 2.0+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: 1990 áprilisában bukkant fel Dél-Afrikában. A vírus önmagát titkosítja, rezidens résszel nem rendelkezik. A .COM állományokat fertőzi meg.

Amikor a vele fertőzött program lefut, akkor az aktuális meghajtó minden alkönyvtárában minden .COM állományt megvizsgál és megfertőz. Ezért a lemezhozzáférési idő igencsak megnyúlik, nagy merevlemez esetén egy-két percre is! Aktivizálódása napján, június 16-án a főkönyvtárban és a FAT-ban minden állomány belépési címe helyett a következő bejegyzést helyezi el: ZAPPED. És közben természetesen minden állomány és adat elvész.

A vírus neve: Kennedy

Egyéb elnevezése: Dead Kennedy, 333.

Hossza: 333 bájt.

Kódtípusa: Parazita, nem rendelkezik rezidens résszel, .COM fertőző.

Azonosítása: Scan V62+, Pro-Scan 1.4+, VirexPC, F-Prot 1.12+, VirHunt 2.0+.

Eltávolítása: F-Prot 1.12+, VirHunt 2.0+, vagy törölni a fertőzött programokat.

Leírása: A Víruslélektan első kiadásának lezárása után kaptuk kézhez ezt a vírust, amelyet az USA-ban 1990 áprilisában izoláltak. A vírus COMMAND.COM-ot is beleértve, általános .COM fertőző.

A vírus Kennedy-ek átkának a krónikása, mert aktivizálódási dátumai a Kennedy család tragikus eseményeinek évfordulójára emlékeztetnek:

Június 6. — Robert Kennedy meggyilkolása 1968-ban.

November 18. — Joseph Kennedy halála 1969-ben.

November 22. — John F. Kennedy meggyilkolása 1963-ban.

Amikor a vírus aktivizálódik, a következő üzenet jelenik meg a monitoron:

```
Kennedy is dead - long live 'The Dead Kennedys'
```

(Kennedy halott. Éljenek sokáig „a halott Kennedyk")

Létezik egy másik változata, amelynek szövegébe Dániában idegen karaktereket kevertek, bár a mondanivalón nem változtattak. (Erről Skulason számolt be a szakirodalomban.)

```
Kennedy er dœd - længe leve "The Dead Kennedys"
\command.com
The Dead Kennedys
```

A fertőzött rendszernél rendkívül sok keresztkapcsolt cluster képződik, és a FAT is elromlik. Ilyenkor megjelenik az erre utaló DOS üzenet: File Allocation Table is Bad.

A vírus neve: Keypress

Egyéb elnevezése: Még nem ismeretes.

Hossza: 1232 bájt.

Kódtípusa: Parazita, rezidens résszel. A .COM és az .EXE állományokat támadja meg.

Azonosítása: Scan V71+, Pro-Scan 2.01+.

Eltávolítása: Clean V71+, vagy törölni a fertőzött állományokat.

Leírása: Az USA-ban találtak erre a vírusra 1990 októberében. A .COM és az .EXE állományokat megtámadja, de nem kíméli a COMMAND.COM-ot sem. A fertőzött program lefutása után beépül a hagyományos DOS memória felső tartományába.

Installálódása után magára irányítja az INT 1C és az INT 21 megszakító vektorokat. A rendszer által használható memória méretét 1232 bájttal csökkenti. Rezidenssé válása után keresi a megfertőzhető állományokat, de csak azokat fertőzi meg, amelyek hosszabbak nála, vagyis 1232 bájtnál. A megfertőzött a program könyvtári bejegyzésének időpontját a fertőzéskor aktuális dátumra és időadatokra cseréli ki. A .COM állományok a fertőzés után 1234–1248 bájttal, az .EXE programok viszont 1472–1486 bájttal lesznek hosszabbak, s a vírus mindegyik esetben az állomány végére épül be.

A vírus rezidenssé válása után kezdi meg bosszantó tényked ését, ami abból áll, hogy a billentyűleütéseket meghatszorozza. Ha ilyenkor valaki begépeli például a DOS DIR parancsát, a rendszer nyilvánvalóan nem tudja azt végrehajtani, hiszen az alábbi karaktersorozatot kapja:

```
ddddddiiiiiirrrrrr
```

Minden vírusfertőzött program végén a következő, itt hexa kódban közölt karakterzagyvalék található: 4333C98E1E2901CD21.

A vírus neve: IKV 528

Egyéb elnevezése: Még nem ismeretes.
Hossza: 528 bájt.
Kódtípusa: Nem rezidens, a .COM állományokat támadja meg.
Azonosítása: Scan V74+.
Eltávolítása: Törölni a fertőzött állományokat.
Leírása: Az 1991 januárjában izolált vírus valószínű keletkezési helye Magyarország. Nem rezidens, a COMMAND.COM-ot is fertőző, .COM állományokat megtámadó vírus.

Amikor a kód lefut, akkor az aktuális könyvtárban két .COM programot fertőz meg. A hossznövekedés 528 bájt és a vírus a fertőzött program végére épül be. A könyvtári bejegyzés adatait nem cseréli le, azok maradnak az eredetiek.

A vírus neve: Lazy

Egyéb elnevezése: Még nem ismeretes.
Hossza: 720 bájt.
Kódtípusa: Rezidens résszel rendelkező, parazita, .COM állományokat fertőző.
Azonosítása: Scan V75+.
Eltávolítása: Törölni a fertőzött állományokat.
Leírása: 1991 februárjában bukkant fel az USA-ban. A .COM állományokat támadja meg, belelértve a COMMAND.COM-ot is.

Amikor beépül a memória alsó szegmensébe, nem foglalja le magának szabályosan a helyet, ő is felül tud írni, de őt is felülírhatja egy másik program, ami rendszerkiakadásokra vezet. A vírus magára irányítja az INT 10 valamint az INT 21 megszakítókat. Ennek eredményeként a rendszer és a képernyőkezelés csigatempóra lassul le.

A végrehajtatott .COM programokat akkor fertőzi meg, amikor a memóriában ül. Az eredeti programhoz 720 bájtot ad hozzá, és a végre ül be. A könyvtári bejegyzés dátumát és időadatait átállítja a fertőzéskor aktuálisra. A program arról a szóról kapta nevét (jelentése: lusta), amelyet minden fertőzött állomány végén megtalálunk: lazy.

Ha a rendszer fertőzött, akkor érthetetlen kiakadásokat és memóriafelülírásokat okoz a szabálytalan memóriabeépülési eljárás következményeként. Ha a Scan memóriavizsgálatot tart, akkor a vírus és a rendszer kiakad, ami jelzi a fertőzést.

A vírus neve: Lehigh

Egyéb elnevezése: Lehigh University.

Hossza: Nem értelmezhető.

Kódtípusa: Felülírja az állományt, rezidens része van, a COMMAND.COM-ot fertőzi meg és manipulálja a FAT-táblát.

Azonosítása: Scan, F-Prot, IBM Scan, Pro-Scan, VirexPC, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: A COMMAND.COM felülírása egy tiszta példányról, vagy pedig az F-Prot, ami itt ugyanezt teszi.

Leírása: A Lehigh vírus csak a COMMAND.COM állományt fertőzi meg a rendszerlemezen (floppyn vagy merevlemezen). A fertőzés mechanizmusa itt az, hogy felülírja a verem (stack) számára fenntartott üres helyet. Ha véletlenül olyan rendszerlemez kerül a látókörébe, amelyet még nem fertőzött meg, akkor mulasztását sürgősen pótolja.

A vírus egy számlálót tartalmaz, amelynek állapota a másolatokon mindig nulla. Amikor megfertőz egy másik COMMAND.COM-ot, akkor ennek értékét eggyel növeli. Ha a számláló értéke elérte a négyet, akkor kezdi pusztítását a vírus. Ennek mechanizmusa az, hogy felülírja a FAT-táblát és a bootszektort, aminek következtében az adatok elvesznek.

Ismert átiratai:

Lehigh-2: Abban tér el az alapváltozattól, hogy a fertőzéseket számláló rutinja a RAM-ban működik, és nem ír vissza a lemezre. Ha a számlálásban eléri a tízet, akkor megrongálja a bootszektor és a FAT adatait. Az adatok ilyenkor is elvesznek.

Lehigh-B: Teljesen hasonló az eredetihez, csak a kódot változtatták meg aképpen, hogy a megszokott eljárással ne lehessen felismerni.

A vírus neve: Liberty

Egyéb elnevezése: Még nem ismeretes.

Hossza: 2862 bájt.

Kódtípusa: Rezidens résszel rendelkezik, a .COM, az .EXE és az overlay állományokat támadja meg.

Azonosítása: Scan V63+, Pro-Scan 1.4+, VirexPC, F-Prot 1.12+, VirHunt 2.0+.

Eltávolítása: VirHunt 2.0+, Clean V72+, vagy törölni a fertőzött programokat.

Leírása: A vírust Ausztráliában, Sydney városában izolálták 1990 májusában. A vírus Indonéziából származik, megfertőzi a COMMAND.COM-ot, a .COM és .EXE állományokat, de beépül az overlay állományokba is. A megfertőzött .EXE programok utolsó 3 kilobájtja tartalmazza a vírust, míg a .COM programoknál az állomány elejére épül be.

A felső memóriatartományban 8496 bájt helyet foglal le magának, átvéve a INT 21 és INT 24 vezérlését. A fertőzött állományok hossznövekedése 2862–2887 bájt között van. Az fertőzött állományok végén mindog a következő, itt hexa kódban megadott keresési szekvencia található: 80722D80FA81772880.

A vírus a nevét a LIBERTY szóról kapta, amelyet beleír az állományba. Az első 128 bájtot a következő szöveggel írja felül:

`- M Y S T I C - COPYRIGHT (C) 1989-2000, by SsAsMsUsEsL`

Az .EXE állományokban ugyanezt a 00h karakterekkel teszi. Önmagát kódolja és felülíró jellege miatt nagy pusztítást végez.

Ismert átirata:

LibertyB: 1990 novemberében került elő. Funkcionálisan ugyanazt teszi, mint az eredeti vírus, csak az azonosító karaktereket változtatták meg 04 C4 04 64 84 20 20 EB hexa sorozatra. Hossza 2867 bájt. E mellett a MAGIC szó jópárszor megtalálható a fertőzött állományok belsejében. Valószínűleg nem átiratról, hanem köztes kísérleti termékről van szó, amit valamilyen okból kieresztettek.

A vírus neve: Little Pieces

Egyéb elnevezése: Még nem ismeretes.

Hossza: 1374 bájt.

Kódtípusa: Rezidens résszel rendelkező, .EXE állományokat fertőző parazita vírus.

Azonosítása: Scan V74+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: 1991-ben kezdett működni Olaszországban ez a vírusbennszülött. Érdekes ötlettel a rendszer alsó részén foglal memóriát, és ha valamelyik segédprogrammal azt nézzük, hogy melyik programnak a része az ott leledző 1392 bájtos rezidens rész, a rendszer a COMMAND adatterületet jelzi vissza. A COMMAND.COM rezidens része ezzel lesz hosszabb más programok számára. Az INT 13, az INT 16 valamint az INT 21 megszakításokat magára irányítja.

Az .EXE programokat végrehajtáskor fertőzi meg. Ilyenkor a megfertőzött állomány hossza 1374 bájttal nő meg, és a vírus az állomány végére épül be. A könyvtári bejegyzéseket — dátum és időpont — nem módosítja. A vírus egy gyors és váratlan fordulattal, billentyűlenyomás után letörli a képernyőt. Ezt követően jeleníti meg — de nem minden esetben — a következő üzenetét:

`One of these days I'm going to cut you into little pieces`
(E napok egyikén apró darabokra vagdoslak)

Az állományban az üzenetet nem lehet látni, mert a vírus kódolja. Vírusfertőzés után a rendszer időnként váratlanul és logikátlanul kiakad, és ilyenkor néha szintén megjelenik az üzenet.

A vírus neve: Loa Duong

Egyéb elnevezése: Még nem ismeretes.

Hossza: Nem értelmezhető.

Kódtípusa: Rezidens résszel rendelkező bootvírus.

Azonosítása: Scan V80+.

Eltávolítása: Clean V80+, vagy pedig az Mdisk.

Leírása: A könyv befejezésekor kaptuk kézhez ezt az érdekes, muzsikáló

thaiföldi vírust, amely 1991 májusában került elő. A vírus rezidens, a floppy valamint a merevlemez bootrekordját támadja meg.

Az INT 12 visszatérését manipulálja, a rendszermemória felső részére épül be. A DIR parancsra megfertőzi a floppyt, ha a memóriában már jelen van. A DOS CHKDSK programja a memóriában 1024 bájt helyfoglalást jelez.

A vírus az eredeti bootrekordot a merevlemezen a 0. oldal, 0. sáv, 8. szektorába menti el. Az 1,2 MB-os floppyn az eredeti bootszektor helye a 28. szektoron van, míg a 360 K-s lemezen ennek helye a 11. szektor. Ezek általában a főkönyvtár utolsó szektorai. Ha itt könyvtári bejegyzés van, akkor azok az állományok vagy könyvtárak, amelyekre ez hivatkozik, természetesen elvesznek. (Ezt az ötletet már alkalmazta a Stoned vírus...) Minden 128 lemezhozzáférési művelet után a vírus dalra fakad és valami keleti melódiát játszik. A szakirodalom szerint ez egy „laoszi temetési gyászének".

A vírus neve: Mardi Bros

Egyéb elnevezése: Még nem ismeretes.
Hossza: Nem értelmezhető.
Kódtípusa: Bootvírus, memóriarezidens résszel.
Azonosítása: Scan V66+.
Eltávolítása: Mdisk, vagy a DOS SYS parancsa.
Leírása: A vírus 1990 júliusa óta boldogítja a franciaországi számítógépfelhasználókat. Csak floppyt támad meg, a merevlemez partíciós tábláját és bootszektorát nem bántja. Ha fertőzött floppyról indítunk rendszert, akkor mászik fel a memóriába, ahol annak tetején, a rendes DOS tartományon belül 7160 bájtot foglal le magának.

A vírus a nem írásvédett floppykat fertőzi meg, a lemezcímke-állományt is lecseréli. Ha a CHKDSK paranccsal megnézzük az új lemezcímkét, akkor a következő szokatlan dolgot láthatjuk a monitoron:

```
Volume Mardi Bros created ira 0, 1980 12:00a
```

A bootszektorból hiányoznak az eredeti DOS rendszerüzenetek, helyettük a következő szöveg van odaírva:

```
Sudah ada vaksin
```

Nem tudjuk, milyen nyelven írták és mi a jelentése. Várjuk olvasóink megfejtését. A vírus elég jóindulatú. Ha nincs a memóriában, akkor a legegyszerűbb praktikákkal, például a DOS SYS parancsával eltávolíthatjuk.

Kellemes karácsonyt!

Father Christmas, Christmas, Christmas in Japan, Ontario, Oropax, Parity, Evil, Evil-B, Phoenix, PhoenixD, Ping Pong, Ping Pong-B, Ping Pong-C, The Plague, Polish 217, Polish 217 B, Polish 529, Polish 583, Ambulance Car, Revenge Attacker.

Az informatikai bestiáriumban most olyan agyszüleményeket mutatunk be, amelyekből a későbbi vírusírók sok ötletet merítettek. Nem a kódrokonságot vettük alapul, hanem a kisebb-nagyobb járulékos fogásokat, trükköket, mint például a képernyőn pingpongozó karakter vagy a karácsonyi jókívánság.

A vírus neve: Father Christmas
Egyéb elnevezése: Choinka.
Hossza: 1881 bájt.
Kódtípusa: Nem rezidens, parazita, .COM fertőző.
Azonosítása: Scan V71+.
Eltávolítása: A fertőzött állományok törlése.
Leírása: 1990 karácsonyára készült ez a meglepetés Lengyelországban. Igen távoli rokonságban van a Vienna vírussal. Nem rezidens, a .COM állományokat fertőzi meg, beleértve a COMMAND.COM-ot is.

Amikor a víruskód lefut, keres egy fertőzhető állományt az aktuális meghajtó aktuális könyvtárában. Ha ilyet nem talál, akkor a DOS megadott elérési útvonalain keresgél tovább. Ha talál, akkor egy menetben egyetlen egyet megfertőz. A kód az állomány végére épül be, és a hossznövekedés 1881 bájt. A vírus sok keresztkapcsolt szektort hoz létre és „elvesznek" a clusterek.

A vírus karácsonyi üdvözletként minden esztendőben december 19. és december 31. között aktív. Ekkor grafikusan megjelenít a monitoron egy karácsonyfát és a következő szöveget adja mellé:

```
Merry Christmas
       &
  a Happy New Year
for all my lovely friends
       from
  FATHER CHRISTMAS
```

(Kellemes karácsonyt és boldog új évet minden kedves barátomnak Karácsony apótól)

Egy billentyű lenyomása után a felirat eltűnik és a program futás nélkül kilép a DOS-ba.

A vírus neve: Christmas

Egyéb elnevezése: Tannenbaum, XA1, 1539.

Hossza: 1539 bájt.

Kódtípusa: Parazita, nincs rezidens része, a .COM állományokat fertőzi meg.

Azonosítása: ViruScan V61+, VirexPC, VirHunt 2.0+, Pro-Scan 2.01+.

Eltávolítása: VirHunt 2.0+, Pro-Scan 2.01+, vagy a fertőzött állományok törlése.

Leírása: A vírus minden esztendőben április elsején tönkreteszi a FAT-ot. December 24. és január 1. között pedig karácsonyfát rajzol a képernyőre, de akkor nem rombol. 1990 márciusában az NSZK-ban észlelte először Christoff Fischer. A vírus kizárólag a .COM állományokat támadja meg.

A vírus neve: Christmas in Japan

Egyéb elnevezése: Xmas in Japan.

Hossza: 600 bájt.

Kódtípusa: Nem rezidens, parazita, a .COM állományokat fertőzi meg.

Azonosítása: Scan V67+, Pro-Scan 2.01+.

Eltávolítása: A fertőzött állományok törlése.

Leírása: A vírust már 1990 szeptemberében izolálták Tajvan szigetén, de igazi nagy járványt csak ugyanazon év decemberében okozott Japánban. A mindössze 600 bájt hosszú vírus a COMMAND.COM-ot és a .COM állományokat támadja meg.

Amikor a program végrehajtódik, a vírus vagy nem fertőz, vagy pedig egy .COM állományt fertőz meg az aktuális könyvtárban. Ha a fertőzés megtörténik, a hossznövekedés 600 bájt, és a vírus az állomány végére épül be. Ha december 25-én vírusos programot futtatunk, a következő karácsonyi üdvözlet jelenik meg a monitoron:

```
A merry christmas to you
```

Az üzenet felvillan a monitoron és a program normálisan lefut. Ha újabb fertőzött programot indítunk el, akkor a jelenség megismétlődik.

A vírus neve: Ontario

Egyéb elnevezése: Még nem ismeretes.

Hossza: 512 bájt.

Kódtípusa: Önmagát titkosító, parazita, .COM és .EXE fertőző.

Azonosítása: Scan V66+, Pro-Scan 2.01+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: Mike Shields izolálta a kanadai Ontarióban, 1990 júliusában. A vírus bonyolult kódolási mechanizmussal rendelkezik. Memóriarezidens része van, a .COM és az .EXE állományokat támadja meg, beleértve a COMMAND.COM-ot is.

Amikor a víruskód lefut, a vírus beépül a memóriába a hagyományos DOS tartomány felső részébe. A memória csökkenése a kódhoz képest igen nagy, 2048 bájt. A fertőzés során a .COM állományok hossznövekedése 512 bájt. Az .EXE állományoknál és az overlay programoknál ez az érték 512–1023 bájt közötti érték. Ezt úgy produkálja, hogy az 512 bájt mögé változó hosszúságú, de szemetet másol be. A végleges értéket pedig mindig teljes szektorhosszal még növelni is tudja. (A magyar Phantom ezt még napi variációkkal is megtoldotta, de az ötlet valószínűleg innen volt.) A vírus merevlemezhibákat, elvesző és keresztkapcsolt clustereket okoz.

A vírus neve: Oropax

Egyéb elnevezése: Musician.

Hossza: 2756–2806 bájt.

Kódtípusa: Parazita, rezidens része van, a .COM állományokat fertőzi meg.

Azonosítása: Scan V53+, F-Prot, CHKSeq v.1.0. IBM Scan, Pro-Scan, VirexPC, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: Scan /D, F-Prot, VirexPC, Pro-Scan 1.4+, VirHunt 2.0+, vagy a fertőzött állományok törlése.

Leírása: Az Oropax vírust könyvünk első kiadása óta sikerült Magyarországon begyűjtenünk. Korábban Magyarországi jelenléte csak a tisztázatlan eredetű üzemzavarokból volt valószínűsíthető.

A vírus véletlenszerűen aktivizálódik. Öt perccel az állomány megfertőzése után három eltérő melódiát játszik le, hétperces időközönként ismételve azt. A magyarországi változat valószínűleg azonos az európai verzióval, amely hat különböző melódiát fütyül el, szintén hétperces időközönként. (Megjegyzendő, hogy a Prgdoki különböző magyar kiadásaiban ezt a vírust tévesen azonosították az Ötórai Tea/Yankee Doodle vírussal.) Az Oropax 2756 és 2806 bájt közötti változó értékkel növeli a fertőzött állomány hosszát, mindig úgy, hogy a teljes állományhosszúság osztható legyen 51-gyel.

A valószínűleg NSZK eredetű vírus megjelenését először 1989 decemberében jelezték. A .COM programokat, köztük a COMMAND.COM-ot is megtámadja. Aktivitását a vírusban található véletlenszám-generáló rutin vezérli. Amíg a memóriában van, a futtatott programokat nem fertőzi meg, de egyéb DOS műveletek, mint könyvtármegnyitás, állománytörlés vagy másolás kiváltják a fertőzést.

A vírus neve: Parity

Egyéb elnevezése: Még nem ismeretes.

Hossza: 441 bájt.

Kódtípusa: A .COM állományokat megfertőző, rezidens résszel rendelkező parazita vírus.

Azonosítása: F-Prot 1.12+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: A vírus igen rövid programkódot tartalmaz. Ha a memóriában van, futtatáskor mindig megfertőz egy .COM programot. Nevét onnan kapta, hogy

a számítógépen paritáshibát szimulál. Egyike a hardverhibát szimuláló legelső vírusoknak, talán a magyar Monxla is innen vette néhány trükkjét. A vírus szórványosan bukkan fel. Amikor aktivizálódik, a rendszerleállás előtt megjelenik a képernyőn az alábbi felirat: PARITY CHECK 2.

A vírus neve: Evil

Egyéb elnevezése: P1, V1701New.

Hossza: 1701 bájt.

Kódtípusa: Parazita, rezidens résszel rendelkező .COM fertőző programvírus.

Azonosítása: Scan V66+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: A vírus Bulgáriából származik, onnan jelezte előfordulását Veszelin Boncsev, 1990 júliusában. Egy háromtagú család (Phoenix-Evil) tagja, valószínűsíthetően egyazon szerzőtől.

Az Evil (= gonosz) memóriarezidens, megfertőzi a COMMAND.COM-ot és a többi .COM állományt. A Phoenix család legfejlettebb tagja, „apja" a PhoenixD vírus volt. Miután rezidenssé vált, a szabad 640 K feletti memóriatartományban installálja magát, ahol 8192 bájt helyet foglal le magának, közben magára irányítja az INT 2A megszakítást. Ezután végigmegy az aktuális meghajtón, megkeresi a COMMAND.COM-ot. Ha megtalálja, akkor megfertőzi az Evil binárisan felülíró részével, és kicseréli a fejlécinformációkat aképpen, hogy a külső szemlélő semmi változást sem lát. A C: meghajtón ugyanez zajlik le, ha merevlemezes géppel dolgozunk. Miután rezidenssé vált, minden elindított .COM állományt megfertőz. A hossznövekedés 1701 bájt. Gyorsan terjed. Nem ismeri fel, hogy korábban már megfertőzte-e az állományt, ezért ismételten megfertőzi azt, újabb 1701 bájtot adva hozzá.

Állománynyitásra is fertőz, vagyis — ha a memóriában aktív — egy egyszerű COPY parancs kiadása esetén mind a kiinduló, mind a célállomány fertőzött lesz. A CHKDSK lefuttatásával egyszerre az egész rendszer fertőzötté válik. Ha melegindítást végzünk, a rendszert csak látszólag indítja újra, s közben a memóriában marad. A vírus szabálytalan időközönként maga is végez ilyen melegindítást. (Jele: nem számolja végig a RAM tesztet, és ha nincs ott az AUTOEXEC.BAT, akkor nem kérdez rá a dátumra és az időre.) Bár hosszúsága azonos, semmi köze az 1701/1704 vírushoz!

A vírus igen bonyolult kódolási mechanizmust használ, ami nagyon megnehezíti kiirtását. Normális sztringkereséssel egyáltalán nem található meg.

Ismert átirata:

Evil-B: Biztos, hogy egy korábbi, kísérleti verzió. Nagyon rosszul szaporodik, mert ezt a rutinját írója akkor még nem dolgozta ki. A fertőzött program sok esetben nem is indul el, a rendszer kiakad.

A vírus neve: Phoenix
Egyéb elnevezése: P1.
Hossza: 1704 bájt.
Kódtípusa: Rezidens résszel rendelkező, parazita, a .COM állományokat támadja meg.
Azonosítása: Scan V66+, Pro-Scan 2.01+.
Eltávolítása: Törölni a fertőzött állományokat.
Leírása: 1990 júliusában találta meg az ismert bolgár antivírus-szakértő, Veszelin Boncsev. A Phoenix család „atyja" ez a vírus, mely memóriarezidens résszel rendelkezik, a .COM állományokat fertőzi meg, beleértve e COMMAND.COM-ot is.

A vírus a szabad DOS feletti memóriatartományba installálja magát (a 640 K és az 1024 K közé), ott 8192 bájt helyet foglalva le magának. Az INT 2A megszakítást magára irányítja. Ha olyan floppyról indították, ahol nincs COMMAND.COM, akkor üzenetben kéri, hogy azt a floppyt tegyük be a meghajtóba, amelyen a COMMAND.COM jelen van. A Phoenix a COMMAND.COM-ba saját bináris felülíró részét építi be, és közben átírja annak fejlécét is, ezért a hosszcsere sehol nem látszik. A COMMAND.COM-ot alapértelmezésben a C: meghajtó gyökérkönyvtárában keresi. Rosszul szaporodik, mert reprodukciós rutinja igen poloskás. Ha mégis sikerül szaporodnia, akkor a kódot az állomány végére építi be, amelynek hossznövekedése 1704 bájt. Többszörösen is megfertőzhet egy állományt, ilyenkor a hossznövekedés az 1704 többszöröse. A melegindítást ennek a vírusnak a rezidens verziója (szerencsére) nem éli túl. A vírus véletlenszerű rendszerindításokat okoz. A CHKDSK futtatásával az egész rendszer minden fertőzhető állománya fertőzötté válik, és az egyes állományok különbözőképpen csonkolódhatnak. Kódolása igen bonyolult, ezért hagyományos keresési eljárásokkal a vírus nem detektálható.

A vírus neve: PhoenixD
Egyéb elnevezése: P1.
Hossza: 1704 bájt.
Kódtípusa: Parazita, rezidens résszel rendelkező, .COM fertőző vírus.
Azonosítása: Scan V66+, Pro-Scan 2.01+.
Eltávolítása: Törölni a fertőzött állományokat.
Leírása: Bulgáriából jelezte előfordulását 1990 júliusában Veszelin Boncsev. A vírus a Phoenix család középső tagja, az első Phoenix alaposan átdolgozott és poloskamentesített verziója. A vírus magát a memória felső részében helyezi el, a hagyományos DOS terület fölé, ott 8192 bájt helyet foglalva le magának. Mint a család többi tagja, ez is az INT 2A megszakítást veszi el a rendszertől.

Az aktuális meghajtó főkönyvtárában keresi a COMMAND.COM-ot, hogy abba beletegye reprodukciós részét. Utána a fejinformációt is kicseréli, tehát a vírus jelenléte a COMMAND.COM-ban nem észlelhető. A vírusszerző kijavította a szaporodó rutint, s ez a vírus már kifejezetten jól szaporodik. Az állományok hossznövekedése 1704 bájt, vagy többszörös fertőzés esetén ennek

többszöröse. Szaporodásánál újdonság az eredeti állományhoz képest, hogy a fertőzés nemcsak állomány-hozzáféréskor, hanem futtatáskor is megtörténik. A COPY parancs kiadásakor ugyancsak fertőzött lesz mind az eredeti, mind pedig a másolati állomány. A vírus időnként rendszerindítást csinál, amit azonban tárrezidens része minden gond nélkül túlél és aktív marad a memóriában.

A vírus komplex titkosítási mechanizmusa miatt egyszerű sztringkereséssel — mint amilyet a TBSCAN keresőprogram alkalmaz — nem detektálható. Semmi köze az 1701/1704 vírushoz!

A vírus neve: Ping Pong

Egyéb elnevezése: Bouncing Ball, Bouncing Dot, Italian, Vera Cruz.

Hossza: 1024 bájt.

Kódtípusa: Rezidens része is van, csak a floppylemez bootszektorát fertőzi meg.

Azonosítása: Scan, F-Prot, IBM Scan, CHKSeq v.1.0. VirexPC, Pro-Scan, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: MDisk, CleanUp, CHKVir v.4.01, F-Prot, Bootkill 1.03, Sysdoki, vagy a DOS SYS parancs kiadása.

Leírása: A Ping Pong vírus a bootszektort fertőzi. Első felbukkanását 1988-ban jelezték. Az eredeti változat csakis floppyt támad meg. A vírus aktivizálódása véletlenszerűen történik. Ekkor megjelenik a monitoron egy erőteljes pont, a „pingponglabda", s ott bolyong a jelek között. Ezt a jelenséget csak úgy tudjuk megszüntetni, hogy a gépet kikapcsoljuk. Ennek a verziónak más hatását eddig nem tapasztaltuk, viszont sokan ezt vették alapul, hogy kártékonyabb vírussá dolgozzák át.

A vírus neve: Ping Pong-B

Egyéb elnevezése: Pingpongozó, Bouncing Ball Boot.

Hossza: Nem értelmezhető.

Kódtípusa: Rezidens része van, a bootszektort fertőzi meg.

Azonosítása: Scan, F-Prot, IBM Scan, CHKSeq v.1.0, Bootkill, Sysdoki. Pro-Scan, VirexPC, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: CleanUp, MDisk, CHKVir v.4.01, F-Prot, Bootkill Pro-Scan 1.4+, VirexPC, vagy pedig a DOS SYS parancsa.

Leírása: A Ping Pong-B vírus az eredeti Ping Pong egyik változata. Fontos különbség, hogy a merevlemezt és a floppyt egyaránt meg tudja fertőzni. Magyarországon — igaz, elszigetelt környezetben, főként nagy floppyforgalmú, szövegfeldolgozással foglalkozó cégeknél — kiadós járványokat okozott.

Ez a bootvírus csak az IBM PC/XT számítógépek merevlemezét fertőzi meg, ami arra enged következtetni, hogy a vírusok korábbi generációjához tartozik. Fertőzése során floppy és merevlemez esetén is 1024 bájt hibás szektort jegyez be a FAT-táblába. A vírus nem írja felül a lemezegységen található információkat, hanem az első szabad területre épül be. Működését több lépcsőben tapasztalhatjuk:

1. Kis rombusz jelenik meg a képernyőn, és a betűk között pattog. Ekkor a vírus még nem pusztít, csak jelzi jelenlétét.

2. Egy nagyobb ponttal a képernyő teleíródik. A vírus még mindig nem töröl adatokat, de számítógépünk kiakad és az operációs rendszert újra be kell töltenünk.

3. A képernyőn az ASCII 01 karakter jelenik meg. Ez a „röhögő pofának", „halálfejnek" vagy „holdarcnak" is becézett figura, miközben a monitoron állandóan ide-oda ugrál, a winchesteren jókora adatpusztítást végez.

A vírus valószínűleg Olaszországból származik, Magyarországra pedig Csehszlovákián keresztül érkezett. A kiirtására alkalmas egyik legelső program szintén északi szomszédunkban készült.

Ismert változata:

Ping Pong-C: Hasonló a Ping Pong-B-hez, csak ez a verzió nem pingpongozik a monitoron a karakterekkel. A vírust valaki 1990 júniusában vakarta át Argentínában.

A vírus neve: The Plague

Egyéb elnevezése: Még nem ismeretes.

Hossza: 590 bájt.

Kódtípusa: Nem rezidens, .COM és .EXE fertőző vírus, amely felülírja az állományokat.

Azonosítása: A jelenségek alapján az állományokat megvizsgálva.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: 1991 januárjában bukkant fel az USA-ban. A vírus a .COM és .EXE állományokat, a COMMAND.COM-ot is beleértve, megtámadja. Amikor a programkód lefut, a vírus keres az aktuális meghajtón az aktuális könyvtárból kiindulva három megfertőzhető programot. Semmivel sem törődve egyszerűen ráhelyezi aaját magát a program első 509 bájtjára. Az időpont és egyéb könyvtári bejegyzési adatok nem változnak.

A megfertőzött program nem fut le. Helyette a következő DOS rendszerüzenet jelenik meg a monitoron:

```
Program too big to fit in memory
```

Ha a Plague (magyarul Pestis) vírus már nem talál több fertőzni való programot, akkor aktivizálódik. Ennek során a következő üzenetet mutatja be a monitoron:

```
Autopsy indicates the cause of
death was THE PLAGUE
Dedicated to the dudes at SHHS
VIVE LE SHE-MAN!
```

(A boncolási jegyzőkönyv mutatja, hogy a halál oka a Pestis volt. Ajánlva SHHS jampeceinek. Éljen a nő!)

Amikor a fenti üzenet megjelenik, akkor az aktuális meghajtót felülírja memóriaszeméttel, és azt — miként általában a felülíró vírusok pusztítását — nem lehet helyreállítani.

A vírus neve: Polish 217

Egyéb elnevezése: 217, Polish Stupid.

Hossza: 217 bájt.

Kódtípusa: Parazita, nem rezidens, a .COM állományokat támadja meg.

Azonosítása: Scan V71+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: A vírust 1990 októberében izolálták Lengyelországban. Nem rendelkezik rezidens résszel, a .COM programokat támadja meg, beleértve a COMMAND.COM-ot is.

Amikor a víruskód lefut, a vírus megkeresi az aktuális könyvtárban megfertőzhető első programot, és beépül abba. A hossznövekedés 217 bájt, a kód a program végére kerül. A fertőzés jeleként a program végén megtaláljuk a következő azonosítót: 5757 (hexadecimálisan értve). A könyvtári bejegyzéseket nem változtatja meg. Ha a COMSPEC változó rámutat a fertőzött COMMAND.COM-ra, akkor a rendszer melegindítást hajt végre. A vírus szerzője egy alkalommal alaposan átírta művét.

Ismert átirata:

Polish 217 B: Amikor a COMMAND.COM-ot megfertőzi, nem végez rendszerindítást. Helyette a fertőzött COMMAND.COM futtatásakor a következő DOS üzenetet kapjuk:

```
Specified COMMAND search directory bad
```

Amikor egy fertőzött program lefut, még egy hibaüzenetet kapunk:

```
????????COM
Path not found.
```

A felismerés módja eltér az eredeti változatétól. A Scan V72 ezt a verziót nem tudja azonosítani.

A vírus neve: Polish 529

Egyéb elnevezése: 529.

Hossza: 529 bájt.

Kódtípusa: Rezidens résszel rendelkező, parazita, .COM állományokat fertőz meg.

Azonosítása: Scan V71+.

Eltávolítása: A fertőzött állományok törlése.

Leírása: 1990 szeptemberétől terjed, Legyelországból kiindulva. Nagyobb járványokat eddig szerencsére még nem okozott. A .COM állományok mellett a COMMAND.COM-ot is megtámadja.

Szabályosan instalállja magát a DOS memória alsó részbe, ahol 1664 bájt helyet foglal le, és magára irányítja az INT 21 vezérlését. Amikor a vírus rezidens, minden fertőzött .COM állomány 1600 bájtnyival hosszabbnak látszik. Valójában a hossznövekedés 529 bájt, és a kód a fertőzött állomány végére kerül. Ennek a trükknek az a célja, hogy a hosszvizsgálat alapján dolgozó antivírus programokat félrevezesse, és azok a vírus jelenlétében rossz méretet csonkoljanak.

A vírus neve: Polish 583

Egyéb elnevezése: Még nem ismeretes.

Hossza: 583 bájt.

Kódtípusa: Nem rezidens, parazita, a .COM állományokat támadja meg.

Azonosítása: A jelenség alapján szemrevételezve az állományokat.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: Nem rendelkezik rezidens résszel, és szerencsére eddig még nem okozott járványokat. Szórványosan előfordult Lengyelországban 1990 decemberétől. A vírus a .COM állományokat támadja meg, beleértve a COMMAND.COM-ot is.

Amikor a kódja lefut, az aktuális meghajtó aktuális könyvtárában egyetlen .COM állományt fertőz meg. A hossznövekedés 583 bájt, és a vírus a programkód végére épül be. A könyvtár időpont és dátum adatain nem változtat. Károkozása eddig még nem ismert, valószínűleg egy terjedési rutin tesztvírusának szánták.

A vírus neve: Ambulance Car

Egyéb elnevezése: RedX.

Hossza: 796 bájt.

Kódtípusa: Parazita, nem rezidens, a .COM állományokat fertőzi meg.

Azonosítása: Scan V64+, F-Prot 1.12+, Pro-Scan 2.01+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: 1990 júniusban találkoztak vele először az NSZK-ban. A vírusnak nincs rezidens része, és a .COM programokat támadja meg.

Amikor a kód lefut, megfertőz egy .COM állományt a C: meghajtón. A vírus soha nem az elsőnek bejegyzett .COM állományt támadja meg, és könyvtáranként mindig csak egyetlen .COM állományba épül be. Ha a COMMAND.COM-ot megtalálja a főkönyvtárban, és ott nincs más fertőzött állomány, akkor azt normális .COM-ként kezelve megfertőzi. Grafikus üzemmódot használva a képernyőn véletlenszerűen megjelenik egy mentőautó képe, ASCII blokk-karakterekből kirajzolva, és áthajt egyik saroktól a másikig. (Innen a neve: Mentőautó.) Ezalatt a számítógép hangszórója a mentőautó szirénájának hangját utánozza. A mentőautó megjelenítésének módja nagymértékben függ a gépben lévő grafikus adaptertől.

A vírus neve: Revenge Attacker

Egyéb elnevezése: 777.

Hossza: 1127 bájt.

Kódtípusa: Parazita, rezidens résszel rendelkezik, .COM fertőző.

Azonosítása: Scan V80+.

Eltávolítása: A fertőzött állományok törlése.

Leírása: A 777-est 1991 júniusában találták meg a Fülöp-szigeteken. Memóriarezidens, .COM fertőző, a COMMAND.COM-ot is megtámadja.

Amikor installálja magát, szabványos rezidens programként a DOS memó-

ria alsó részébe épül be, ahol 1392 bájt helyet köt le magának. Az INT 21 vezérlését teljesen átveszi. Ha a COMMAND.COM még nem lenne fertőzött, megfertőzi azt. Mindig a végrehajtott programot fertőzi meg. Ilyenkor az állomány hossznövekedése 1127 bájt, a könyvtári bejegyzés dátumát és időpontját megváltoztatja a fertőzéskor aktuális értékekre. A víruskód a programok végére épül be.

Jelenlétét a fertőzött állományban a 777 karaktersorozattal jelzi. Két másik szöveges rész is van a vírusban:

```
*** 777 - Revenge Attacker V1.01 ***
*.COM
```

Amikor a vírus a memóriában van, alaposan megzavar számos DOS funkciót. Például a DIR parancsra az első könyvtári bejegyzést látjuk az aktuális könyvtári bejegyzés helyett, majd utána a rendszer kiakad. Aktivizálódásának feltétele, hogy az aktuális könyvtárban minden megfertőzhető állomány fertőzött legyen. Ekkor a *** 777-tel kezdődő rendszerüzenete hétszer ismételve megjelenik a képernyőn. Miközben ezt a jelenséget mutatja, felülírja a merevlemez 0. oldal, 1. sávjának, 0. szektorát. A FAT megrongálódik és a gyökérkönyvtár is károsodik.

Vegyes vírussaláta

RPVS, RPVS-B, VFSI, VP, Yap, ZK900, Saturday 14. Scott's Valley, Sentinel, Shake, Slow, 1554, 1575, 1575-B, 1575-C, Sparse, Spyer, Staf, StarDot 600, StarDot 801, Stone'90, Subliminal 1.10, Solano 2000, Solano 2000-B, Dyslexia 2.00, SVir, SVir-A, SVir-B, Swap, Traceback, Traceback-B, Traceback-B2, Traceback II, Traceback II-B, 1008, 1210, Chaos, Arf, Flash, DBASE, 8 Tunes, Carioca.

Sajnos ennek a könyvnek egy végtelen történetről kell véges beszámolót adnia. A víruspanoptikum folyamatos átrendeződése miatt folyton ki kellene bővítenünk és át kellene írnunk. Mi a könyv végső nyomdai zárásáig menet közben több frissítést is elvégeztünk, a beszerzett és megvizsgált vírusok, illetve az azóta hozzánk eljutott szakirodalmi információk alapján. Ebbe a fejezetbe azok a vírusok kerültek, amelyek a különböző ismérvek alapján alkotott előző csoportok egyikébe sem fértek bele, annyira vegyesek. Egy közös rendező elvük talán mégis van: az itt ismertetett vírusok eredeti darabjaival a közelmúltban, könyvünk írása közben sikerült kiegészítenünk gyűjteményünket.

A vírus neve: RPVS
Egyéb elnevezése: 453.
Hossza: 453 bájt.
Kódtípusa: A .COM állományokat fertőzi meg, nincs rezidens része.
Azonosítása: Pro-Scan 2.01+.
Eltávolítása: Pro-Scan 2.01+, vagy törölni a fertőzött állományokat
Leírása: A vírust 1990 augusztusában fedezték fel az NSZK-ban. Nevét a vírusban lévő betűszóról kapta, ami azonban nem szöveg, hanem egy jól elrejtett Assembly PUSH parancs.

```
TUQ.RPVS
```

A vírus nem rendelkezik rezidens résszel, és a .COM állományokat támadja meg. Nagyon eredeti megoldásokat tartalmaz. Amikor a vírussal fertőzött kód lefut, a vírus az aktuális könyvtárban keres magának egy megfertőzhető állományt. Fertőzöttségének megállapítására ellenőrzi az utolsó két bájtot. Ha az nem hexa 9090, akkor 453 bájtot rápakol az állomány végére, és elvégzi a vírus

működéséhez szükséges egyéb tennivalókat is. Egy futásra csak egy fájlt fertőz meg. Megfertőzése után a COMMAND.COM rendellenesen működik.

Ismert változata:

RPVS-B: Hasonló az eredetihez, csak néhány plusz bájtot is hozzáad a fertőzött program végéhez, ezért a fertőzésvizsgálat eredménytelen, és a vírus többször is beépülhet az állományba. Ilyenkor a legelső könyvtári bejegyzésű .COM állományt fertőzi meg akárhányszor.

A vírus neve: VFSI

Egyéb elnevezése: 437, Happy Day.

Hossza: 437 bájt.

Kódtípusa: Parazita, nem rezidens, a .COM állományokat fertőzi meg.

Azonosítása: Scan V71+, Pro-Scan 2.01+.

Eltávolítása: Scan /D, Pro-Scan 2.01+.

Leírása: A vírust 1990 szeptemberében Szvisztov bolgár városban egy felsőfokú pénzügyi továbbképző intézetben izolálták. A vírus helyi tervezésű, viszonylag agresszív. A .COM állományokat, közöttük a COMMAND.COM-ot is megtámadja. Nincs rezidens része.

Amikor a kód lefut, keres az aktuális meghajtó aktuális könyvtárában másik olyan állományt, amelyet megfertőzhet. Csak olyanok jöhetnek szóba, amelyek hossza a 16 többszöröse. Ha talál ilyet, akkor beépül annak végére, 437 vagy 452 bájt hosszal növelve a fájlt. A fertőzött állományok azonosíthatók a 3A483F244B6F636E706C74 hexa szekvencia keresésével. Aktivizálódáskor a vírus a belsejében közvetlenül nem olvasható (kódolt) alábbi üzenetet villogtatja a monitoron:

```
HELLO!!! HAPPY DAY and SUCCESS
from virus 1.1 VFSI-Svistov
```

(Helló! Jó napot és sok sikert a VFSI-Svistov 1.1 vírustól.)

A vírus neve: VP

Egyéb elnevezése: Még nem ismeretes.

Hossza: 913 bájt.

Kódtípusa: Parazita, nem rezidens, a .COM állományokat fertőzi meg.

Azonosítása: Scan V64+, Pro-Scan 1.4+, AVTK 3.5+, F-Prot 1.12+, VirHunt 2.0+.

Eltávolítása: Scan /D, Pro-Scan 1.4+, F-Prot 1.12+, VirHunt 2.0+.

Leírása: 1990 májusától ismert, nem rezidens, .COM fertőző vírus. A COMMAND.COM-ot is megtámadja. Amikor a kód lefut, a vírus keres egy másik fertőzhető .COM állományt. Ha ez a COMMAND.COM, akkor binárisan megjeleníti tartalmát a monitoron, a gép sípol, „csillag-halálfej" jeleket küld a képernyőre, majd a fertőzött program kiakad. Más program viszont gond nélkül lefut.

Az állományok a fertőzés során 913 bájttal növekednek. A fertőzött programok végén található a 4503EB1808655650 hexa azonosító jelsorozat.

A vírus neve: Yap

Egyéb elnevezése: Még nem ismeretes.

Hossza: 6258 bájt.

Kódtípusa: Rezidens résszel rendelkező, parazita, .COM fertőző.

Azonosítása: Scan V75+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: E viszonylag nagyméretű vírus az USA-ból indult el 1991 márciusában. A COMMAND.COM-ot is megtámadja. Amikor rezidenssé válik, a rendszermemória alsó tartományába szabályosan épül be, majd elveszi az INT 09 és az INT 21 vezérlését. A lefoglalt terület igen nagy, 11344 bájt, de ekkorára csak a grafika miatt van szüksége. A .COM programokat futtatásuk során fertőzi meg. A hossznövekedés 6258 bájt, és a víruskód a program végére kerül. A könyvtári bejegyzések dátumát és időadatait nem változtatja meg.

Ha a vírus aktív és a felhasználó az Alt billentyűt és valamelyik másik gomb kombinációját lenyomja, akkor a monitoron számos grafikus poloska jelenik meg, és megeszi a kérpernyő tartalmát. (Ennek a vírusnak a demó változata „Screen eating utility" néven közismert beugró program, amely a vírussal ellentétben ártalmatlan.) Ha ismét megnyomunk egy Alt billentyűkombinációt, akkor a képernyő tartalma visszatöltődik. Gyorsan terjed, mert szép grafikai megoldásai miatt az idétlen viccelődők előszeretettel terjesztik.

A Yap a Potyogós vírus kódolásának módosított változatát felhasználva titkosítja magát. Irtása helyett a szakirodalom egységesen a fertőzött programok törlését javasolja. Szinte kipusztíthatatlan.

A vírus neve: ZK900

Egyéb elnevezése: Pray.

Hossza: 900 bájt.

Kódtípusa: Rezidens résszel rendelkező, a .COM és az .EXE programokat megtámadó vírus.

Azonosítása: A jelenségei alapján az állományokat megvizsgálva.

Eltávolítása: Törölni a fertőzött programokat.

Leírása: A legkisebb zenélő vírusok közé tartozik, David Chessm, az IBM egyik programozója 1991 áprilisában izolálta. A vírus rezidens résszel rendelkezik. A COMMAND.COM-ot és a többi .COM és .EXE programot is megtámadja.

A hagyományos DOS rendszermemória felső területére épül be, magára irányítva az INT 1C valamint az INT 21 megszakítókat. A vírus a programok végrehajtatásakor fertőz. A hossznövekedés 900 bájt, a vírus a program végére épül be. A könyvtári dátumot és az időadatokat nem változtatja meg. A fertőzött programok legvégén megtaláljuk a zx karakteres vírusazonosítót:

Zenei képességeit a vírus három- vagy ötpercenként fitogtatja. A szakirodalom szerint ilyenkor a „Pray for the dead, and the dead will pray for you" című, Amerikában népszerű gyermekdalról van szó. (Imádkozz a holtakért, és a holtak imádkozni fognak érted.)

A vírus neve: **Saturday 14**

Egyéb elnevezése: Durban, Saturday The 14th.

Hossza: 685 bájt.

Kódtípusa: Parazita, rezidens része van, a .COM, az .EXE éa az overlay (átfedő) állományokba épül be.

Azonosítása: Scan V61+, Pro-Scan 1.4+, VirexPC, AVTK 3.5+.

Eltávolítása: VirHunt 2.0+, Pro-Scan 2.01+.

Leírása: A vírust a Dél-Afrikai Köztársaságban, Durban városában izolálták 1990 márciusában.

Rezidenssé válásához nem használja a DOS INT 21h és 27h megszakításait. Az .EXE és a .COM állományokat fertőzi meg, a COMMAND.COM kivételével. A hossznövekedés 669-684 bájt között van. Nevének megfelelően akkor aktivizálódik, amikor a hónap 14. napja szombatra esik. Ekkor a lemezegység első 100 szektorát felülírja a C:, a B: és azután az A: meghajtóban. Ez a lemez teljes tartalmának helyreállíthatatlan elvesztését jelenti a bootszektor, a FAT-tábla és a katalógus-terület információinak megsemmisülése miatt.

A vírus neve: **Scott's Valley**

Egyéb elnevezése: 2131.

Hossza: 2131 bájt.

Kódtípusa: Parazita, rezidens résszel rendelkező, .COM és .EXE fertőző.

Azonosítása: Scan V67+, Pro-Scan 2.01+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: A vírus kaliforniai izolálási helyéről kapta nevét, ahol 1990 szeptemberében bukkant fel. A .COM és az .EXE állományokat egyformán megtámadja, de mellőzi a COMMAND.COM megfertőzését. Rezidens része van. A víruskód lefutása után tárrezidens programként szabályosan installálja magát a hagyományos DOS memória alsó részébe, ahol 2384 bájtot foglal le magának, és átveszi az INT 21 feletti ellenőrzést is. Amikor a vírus már rezidenssé vált, akkor minden végrehajtatott .COM és .EXE program fertőzötté válik. A .COM állományok hossznövekedése 2131 bájt, az .EXE programoké pedig 2131–2140 bájt. A *fertőzött programokat a következő hexadecimális kódban megadott* azonosító alapján lehet detektálni: 5E8BDE909081C63200B912082E

A vírus neve: **Sentinel**

Egyéb elnevezése: Még nem ismeretes.

Hossza: 4625 bájt.

Kódtípusa: Parazita, rezidens vírus, a .COM és az .EXE állományokat fertőzi meg.

Azonosítása: Scan V74+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: Egy bolgár vírusíró műhely bocsátotta ki 1991 januárjában, nem kis bosszúságára a Sentinel floppygyártó cégnek és a Borlandnak, hogy az ő nevüket használták.

A vírus rezidens résszel rendelkező .COM és .EXE fertőző vírus. a COMMAND.COM-ot is megtámadja. Turbo Pascal forráskódban is terjesztik, így több más vírus forrásává is válhat. Amikor installálódik a hagyományos DOS memória felső részén, magára irányítja az INT 12 vektort, illetve annak visszatérési címét manipulálja. Az INT 21 vezérlését teljesen átveszi. Ha a COMMAND.COM még nem lenne fertőzött, legkésőbb a rezidenssé válás után megfertőzi. Minden 1 K-nál nagyobb .COM és .EXE állományt megnyitáskor, illetve végrehajtáskor fertőz és a program végére épül be. A hossznövekedés 4625 bájt. Az állományok könyvtári bejegyzésének időpontját és dátumát nem változtatja meg. A Sentinel vírusban a következő rendszerüzenet található:

```
You won't hear me, but you'll feel me....
(c) 1990 by Sentinel
With thanks to Borland.
```

(Engem nem fog hallani, csak érezni... 1990 by Sentinel. Köszönet a Borlandnak.)

A vírus neve: Shake

Egyéb elnevezése: Még nem ismeretes.

Hossza: 476 bájt.

Kódtípusa: Parazita, rezidens résszel rendelkező, .COM fertőző programvírus.

Azonosítása: Scan V63+, Pro-Scan 1.4+, VirexPC, F-Prot 1.12+, VirHunt 2.0+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: Bolgár vírusgyártók 1990. májusi terméke, először Daniel Kalcsev ismertette. Általános .COM fertőző, a COMMAND.COM-ot is beleértve. Amikor rezidenssé válik, létrehozza a COMMAND.COM alteregóját (hasonmását) a memóriában, s az átveszi a parancsirányítást. Ennek eredményeképpen a DIR használhatatlanná válik, és alaposan összekeverednek a DOS belső funkciói.

Fertőzéskor a .COM állományok hossznövekedése 476 bájt. A fertőzött állományok futtatásakor küldött üzenet:

```
Shake well before use !
```

(Használat előtt jól felrázandó!)

Utána a program vagy lefut, vagy pedig kilép. Ez nem a vírustól, hanem attól a programtól függ, amelyikre ráépült.

A vírus neve: Slow

Egyéb elnevezése: Slowdown.

Hossza: 1701 bájt.

Kódtípusa: Rezidens, parazita, .COM és .EXE fertőző.

Azonosítása: Scan V63+, Pro-Scan 1.4+.

Eltávolítása: Clean V67+, Scan /D, Pro-Scan 2.01+.

Leírása: A vírust 1990 májusában Ausztráliában izolálták. A COMMAND.COM kivételével a .COM, .EXE és az overlay (átfedő) állományokat támadja meg.

A hagyományos DOS memória alsó részére épül be, ott szabályos rezidens programként 1984 bájt helyet foglalva le. Az INT 21-et magára irányitja. Amikor egy programot végrehajtunk, akkor a vírus megfertőzi. A .COM állományok hossznövekedése 1721 bájt, az .EXE programoké 1716–1728 bájt. A vírus-kód a programok végére épül be, de a program elején a vezérlésátadó utasításokat ennek megfelelően módosítja. Nevéhez híven a vírus alaposan lelassítja a rendszer működését, számos esetben pedig kiakasztja, és újra kell indítani. A Jerusalem-B vírus kódjából kiindulva barkácsolták össze.

A vírus neve: 1554

Egyéb elnevezése: Ten Bytes, 9800:0000, V-Alert, 1559.

Hossza: 1554 bájt.

Kódtípusa: Rezidens résszel rendelkező, parazita, .COM és .EXE fertőző.

Azonosítása: Scan V58+, IBM Scan, Pro-Scan 1.4+, VirexPC 1.1+, AVTK 3.5+, F-Prot 1.12+, VirHunt 2.0+, NAV.

Eltávolítása: Scan /D, F-Prot 1.12+, VirHunt 2.0+, Pro-Scan 2.01+.

Leírása: A vírus egy hálózaton át elkövetett informatikai merénylet eredményeképpen, a New Yorkban üzemelő VALERT-L rendszerrel jutott el 1990. február 13-án több mint 600 előfizetőhöz.

Amikor a vírus rezidenssé válik, a .COM és az .EXE programokat fertőzi meg, beleértve a COMMAND.COM-ot is. A fertőzés az .EXE programoknál 1554–1549 bájt méretnövekedést eredményez. Szeptember, október, november és december hónapban aktív. Ilyenkor felülírja a programok első tíz bájtját, az állomány végére pedig szintén tíz karakternyi szemetet másol hozzá. A program- és adatállományok ezáltal tönkremennek, helyreállíthatatlanná válnak.

Ha a vírust 640 K-nál kisebb memóriájú gépen indítjuk el, a rendszer azonnal lefagy. Alternatív elnevezését a hibás programok hibaüzenetéről, illetve a tíz felülírt bájtról kapta. Sajnos már Európában is felbukkant.

A vírus neve: Sparse

Egyéb elnevezése: Még nem ismeretes.

Hossza: 3840 bájt.

Kódtípusa: Rezidens résszel rendelkező, parazita, .COM fertőző vírus.

Azonosítása: A jelenségek alapján megvizsgálva az állományokat.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: 1991 áprilisától fordul elő. Forrása valószínűleg Anglia. A vírus általános .COM fertőző, a COMMAND.COM-ot is megtámadja.

A hagyományos DOS memória alsó részén válik rezidenssé, 3072 bájt területet foglal el, és magára irányítja a következő megszakítókat: INT 21, INT D1, INT D3. Ha már rezidens, akkor minden végrehajtott .COM programot megfertőz, 3840 bájt hossznövekedést okozva. A kód a fertőzött állomány elejére épül be, annak könyvtári dátumát és időadatait kicserélve a fertőzéskor aktuálisakra.

A vírusban van egy-két érdekesség is. A vírus által megfertőzött programban a második és harmadik bájt helyén az UK karaktereket látjuk. A vírus tartal-

maz másik karaktersorozatot is: SHELLC. Ezt annak a programnak a neve követi, amelyik elindításával a vírus rezidenssé vált.

A vírus neve: Spyer

Egyéb elnevezése: Még nem ismeretes.

Hossza: 1181 bájt.

Kódtípusa: Rezidens résszel rendelkező, a .COM és az .EXE programokat megtámadó vírus.

Azonosítása: Scan V71+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: 1990 novemberében Tajvan szigetéről indult el. Rezidens résszel rendelkezik, a .COM és az .EXE állományokat támadja meg, de nem bántja a COMMAND.COM-ot.

A kód lefutása után a vírus szabályos rezidens programként beépül a memóriába, s ott 1760 bájt helyet foglal le magának. Az INT 21 és INT 22 megszakításokat magára irányítja. A programokat futás közben megfertőzi, ha azonban már megfertőzött programba ütközik, akkor a rendszer kiakad, csak az újraindítás segít. A .COM állományok hossznövekedése 1181 bájt, az .EXE állományoké 1181–1195 bájt. A víruskód az állomány végére épül be, s abban található a CBDFD9DE848484 hexa vírusazonosító karaktersorozat.

A vírus neve: Staf

Egyéb elnevezése: Staff.

Hossza: 2083 bájt.

Kódtípusa: Nem rezidens, parazita, a .COM programokat fertőzi meg.

Azonosítása: Scan V76+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: A vírus a Burger demóvírusnak rosszindulatú átirata. Első előfordulását 1991 áprilisában jelentették. Nem rezidens, a .COM állományokat és a COMMAND.COM-ot fertőzi meg. Amikor a víruskód lefut, a következő üzenetet küldi a képernyőre:

```
This program has been infected by:
Virus Demo Ver.: 1.1 - Handle with care!
By STAF (Tel.: (819) 595-0787)
Generation #nnnnn
Infecting: xxxxxxxx.COM
Press any key to execute original program...
```

(Ezt a programot a Vírus demó 1.1 változata fertőzte meg. Óvatosan kezelendő! ... Nyomjon meg egy gombot, hogy lefusson az eredeti program...)

Az nnnnn helyén a vírus generációs száma jelenik meg, az xxxxxxxx.COM helyén pedig a vírus által megfertőzendő állomány nevét láthatjuk, ami a könyvtárban elsőként bejegyzett .COM állomány. Ha meg tudja fertőzni, akkor a vírusos program normális lefutása után kiírja, hogy éppen fertőz (infecting), majd a következő üzenetben bújik ki a vírus igazi arca:

```
I have infected all your files in the current directory!
```

`Have a nice day!`
(Megfertőztem minden állományt az aktuális könyvtárban. Szép jó napot!)
Ha valami miatt nem tud fertőzni, akkor hibaüzenetet küld, közölve a fertőzési folyamat leállítását:
`VIRUS ERROR #nn - Aborting process.`
A sikeres fertőzések során az állományok hosszát 2083 bájttal növeli meg, a kód elejére épülve be. A programok eredeti könyvtári dátumát és időadatait nem változtatja meg.

A vírus neve: StarDot 600

Egyéb elnevezése: Még nem ismeretes.
Hossza: 600 bájt.
Kódtípusa: Nem rezidens, az .EXE állományokat fertőzi meg.
Azonosítása: A jelenségek alapján megvizsgálni az állományokat.
Eltávolítása: Törölni a fertőzött állományokat.
Leírása: A vírus 1991 áprilisában jelent meg. Eredete valószínűleg Olaszország. Nem rezidens, az .EXE állományokat fertőzi meg, mégpedig az aktuális könyvtárban minden futása során egyet. A vírus 604–616 bájttal növeli meg az újonnan fertőzött állományokat, és az eredeti programok végére épül be. A könyvtári bejegyzések időpont- és dátumadatai a fertőzés során nem változnak meg.

A vírus neve: StarDot 801

Egyéb elnevezése: Még nem ismeretes.
Hossza: 801 bájt.
Kódtípusa: Nem rendelkezik rezidens résszel, a .COM és az .EXE programokat fertőzi meg.
Azonosítása: A jelenségek alapján megvizsgálni az állományokat.
Eltávolítása: Törölni a fertőzött állományokat.
Leírása: 1991 áprilisa óta ismert, olasz eredete valószínűsíthető. Szerencsére viszonylag ritka. A vírus nem rendelkezik rezidens résszel, megfertőzi a COMMAND.COM-ot, valamint a .COM és az .EXE állományokat.
Amikor a memóriában van, keres magának egy nem fertőzött másik programot az aktuális meghajtó aktuális könyvtárában. Ha nincs .EXE állomány, akkor a .COM is jó neki. Közülük a könyvtári bejegyzésben elöl állót kiválasztja, és a kód végéhez hozzáfűzi magát. A hossznövekedés 804–814 bájt, a könyvtári bejegyzések változatlanok maradnak. A vírus rendszerkiakadást okoz. Az előzőekhöz hasonlóan tesztvírus lehet, amellyel alkotójuk a terjesztő rutin működését akarta kipróbálni. A vírus programhibái miatt sok rendszerkiakadást okoz.

A vírus neve: Stone'90

Egyéb elnevezése: Polish 961, Stone-90.
Hossza: 961 bájt.
Kódtípusa: Nem rezidens, parazita, a .COM állományokat fertőzi meg.
Azonosítása: Scan V74+.
Eltávolítása: Törölni a fertőzött állományokat.
Leírása: Egy megtévesztő vírussal állunk szemben, amelynek semmi köze nincs az eredeti Stoned vírushoz. Ez ugyanis fájlvírus. Lengyelországban írták, 1990 decemberében. A .COM programokat, közöttük a COMMAND.COM-ot is megtámadja.

Amikor a kód lefut — hogy ne tűnjön fel keresgélése —, az aktuális meghajtó aktuális könyvtárában keres magának egy másik fertőzhető .COM programot. Ha talál, akkor megfertőzi, annak hosszát így 961 bájttal megnöveli, és a végére épül be. A fertőzött állományok ismertetőjele az alábbi komolytalan szöveg, de azt soha nem jeleníti meg a monitoron:

```
Sorry, I'm INFECTED!
I'm already NOT infected!
(C) Stone'90
```

(Elnézést, fertőzött vagyok! Már nem vagyok fertőzött! ...)

A vírus neve: Subliminal 1.10

Egyéb elnevezése: Még nem ismeretes.
Hossza: 1496 bájt.
Kódtípusa: Rezidens résszel rendelkező, parazita, .COM fertőző.
Azonosítása: Scan V64+, Pro-Scan 1.4+.
Eltávolítása: Scan /D, Pro-Scan 1.4+, vagy törölni a fertőzött állományokat.
Leírása: Kaliforniában izolálta Jay Parangalan, 1990 májusában. A név a vírus által alkalmazott kódolási módszerből ered, amelynek eredményeként számos nullával határolt bájt van a víruskódban. A vírus kódolása során a XOR műveletet rendszeresen FFh értékkel végzi el. A vírus által módosított állományok dátuma 02OCT89. A Solano 2000 kísérleti példányának tűnik.

Rezidenssé válása után a vírus minden végrehajtott .COM programot megfertőz. A hossznövekedés 1496 bájt. A vírus hatására a monitor villódzik, esetenként pedig a bal alsó sarokban megjelentet egy elmúlt szerelemre emlékeztető üzenetet is:

```
LOVE, REMEMBER?
```

Az üzenet megjelenési gyakorisága erősen függ a gép processzorának sebességétől, mert a vezérlő rutin egy bizonyos számú meddő ciklus végrehajtására van beállítva.

A vírus neve: Solano 2000

Egyéb elnevezése: Dyslexia 2.01.

Hossza: 2000 bájt.

Kódtípusa: Rezidens, parazita, .COM fertőző.

Azonosítása: Scan V60+, Pro-Scan 1.4+, VirexPC, F-Prot 1.12+, VirHunt 2.0+.

Eltávolítása: Scan /D, Pro-Scan 2.01+, vagy a fertőzött állományok törlése.

Leírása: Virulens természete és nagyfokú kártevő képessége miatt ennek a vírusnak igazság szerint a Hadibacik fejezetben is helye lenne. Edward Winters 1990 márciusában a USA-ban, a Kalifornia állambeli Solano County (= megye) területén izolálta. (Innen a neve.) A vírust azonban korábban is ismerték, akkor Dyslexia V2.01 néven regisztrálta Jay Parangalan, szintén Solano County-ban.

A vírus egyik ismertetőjele, hogy a fertőzött állományok könyvtári bejegyzését 08FEB90 dátumra változtatja. A vírus általános .COM fertőző. Miután beépült a memóriába, minden elindított .COM állományt megfertőz. A vírus érdekessége, hogy a fertőzött állományban 1168–1152 bájtot felülír nyitó zárójel (28h) karakterekkel. Ezen ötletet egy hazánkban is alkalmazott hardverlock büntető rutinja szintén előadja, csak annál a kérdőjel és az egyenlőségjel a felülíró karakter...

Másik sajátossága, hogy a képernyőmemóriában a numerikus karakterek színattrbútumát átállítja. A vírus hatására számos program, például a CopyQM, a DOS DiskCopy parancsa megzavarodik. A leggyakoribb hibaüzenet ilyenkor a NON-DOS DISK vagy az Invalid Drives Specification. Szerencsére a vírus nem éli túl még a melegstartot, azaz a Ctrl-Alt-Del gombokkal való rendszerhívást sem. Mintegy 3 K-nyi helyet foglal el a gép memóriájában.

Átiratai:

Solano 2000-B: Csak annyi az eltérés, hogy a felülíró karakter nem a 28h, hanem a DAh, és a felülírt tartomány 1168–1912 bájt.

Dyslexia 2.00: A Solano 2000-hez hasonló, csak a felülíró karakter nem a 28h, hanem a 00h, azaz bináris nulla. A videomemóriában a számok kiírását lelassítja. A fertőzött állományokban elhelyezett jellegzetes dátum is más: 08FEB90 helyett 22JAN90.

A vírus neve: SVir

Egyéb elnevezése: Még nem ismeretes.

Hossza: 512 bájt.

Kódtípusa: Nem rezidens, parazita, .COM fertőző.

Azonosítása: A jelenségek alapján megvizsgálni az állományokat.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: 1990 szeptemberétől ismerik. A vírus nem rezidens, az .EXE állományokat támadja meg.

Minden végrehajtás során egy másik .EXE állományt fertőz meg. A hossznövekedés 516–526 bájt között van, s a kódot a program végén találhatjuk meg. Ha nem talál fertőzhető állományt, akkor addig pörgeti a lemezt, amíg a gépet

ki nem kapcsoljuk. Csak az A: meghajtón fertőz, ezért feltehetően oktató vírus, vagy pedig kísérleti példány. Előfordulása kuriózum.

Változatai:

SVir-A: Patricia M. Hoffman által beszerzett példány Lengyelországból, programhiba miatt nem szaporodik.

SVir-B: Skulason gyűjtéséből származó, immár szaporodóképes példány. Mi is ehhez jutottunk hozzá a nemzetközi csatornákon keresztül.

A vírus neve: Swap

Egyéb elnevezése: Falling Letters Boot, Israeli Boot.

Hossza: 740 bájt.

Kódtípusa: Rezidens része is van, a floppy bootszektorát fertőzi meg.

Azonosítása: Scan, F-Prot, CHKSeq v.1.0. IBM Scan, VirexPC, VirHunt 2.0+.

Eltávolítása: MDisk, CleanUp, CHKVir v.4.01, F-Prot, vagy a DOS SYS parancs kiadása.

Leírása: A Swap első felbukkanását 1989 augusztusában jelentették. Csak floppykat támad meg. Rezidens része 2 kilobájtot foglal le a RAM-ból. A lemez fertőzésekor hibásként jelöl meg egy logikai egységet (clustert) a 39. sáv 6. és 7. szektorát, hogy oda betelepedjen. A fejhez már nem ragaszkodik. Ha a lemez annyira tele van, hogy a fenti hely sem szabad, akkor semmit nem ír felül, és nem is tud fertőzni.

A Swap vírus 10 perccel memóriarezidenssé válása után aktivizálódik. Elkezdi potyogtatni a monitoron a karaktereket, ahogy a Potyogós vagy a többi Cascade-változat teszi. Nevét onnan kapta, hogy első megfogásakor a 39. sáv 7. szektorában, a 00B7-00E4 bájton a következő szöveges üzenet bukkant fel:

```
The Swapping-Virus. (C) June, 1989 by the CIA
```

Ezt a szöveget csak bizonyos idő után hozza létre, a frissen fertőzött floppykon még nem találjuk meg. A Norton Utilities segítségével könnyen felismerhetjük a fertőzött floppykat, mert a bootszektor végén normális esetben hibaüzeneteket találunk, ha viszont bootvírus fertőzte meg, akkor itt tömör kód van.

A vírus neve: Traceback

Egyéb elnevezése: 3066.

Hossza: 3066 bájt.

Kódtípusa: Parazita, rezidens része van, a .COM és az .EXE állományokat fertőzi meg.

Azonosítása: Scan /X V67+, F-Prot, IBM Scan, Pro-Scan, VirexPC, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: M-3066, VirexPC, Pro-Scan 1.4+, VirHunt 2.0+ VirClean, F-Prot, vagy a fertőzött állományok törlése.

Leírása: Ha a Traceback vírus beépül a .COM és az .EXE állományokba, azok 3066 bájttal lesznek hosszabbak. Amikor a fertőzött állományt elindítjuk, egy memóriarezidens rész válik ki belőle, amely bennmarad az operatív tárban.

Ha a rendszerdátum 1988. december 5. utáni, akkor az aktuális könyvtárban megfertőz egy .COM vagy .EXE állományt. Ha ott nincs megfertőzhető állomány, vagy pedig a vírus már mindegyikben benne ül, akkor keresi a további jelölteket az egész lemezen, a főkönyvtárnál kezdve. A keresési folyamat leáll, ha megtalálta új áldozatát, vagy pedig a lemezen már mindegyik állomány fertőzött lett.

A fertőzött állományokat megtalálhatjuk a DOS elérési útvonalán (path). Így visszafelé nyomon lehet követni, hogy a fertőzés honnan indult el. Innen a név: Traceback, azaz „nyomkövetés visszafelé". Másik jellegzetessége, hogy ha a vírus megfertőzi egy másik kópiáját ugyanannak a programnak, mint amelyikből elindult a memóriába, akkor törli magát az eredeti hordozóból, és áttelepszik a másik példányba.

A Traceback vírussal történt fertőzés első jele, hogy amennyiben a rendszerdátum 1988. december 28-a utáni, és a vírus beült a memóriába, a betűk elkezdenek potyogni. (Hasonlóképpen, mint a közismert Cascade/Potyogós vírus esetében.) Ez a jelenség a fertőzés után egy óra elteltével bekövetkezik. Ha ekkor a billentyűzettel szeretnénk valamit begépelni, akkor egy perc időtartamra a rendszer lemerevedik. Utána a betűk ismét eredeti helyükre ugranak, és minden visszaáll, mintha semmi sem történt volna. Ezt a játékot egyórás időközönként megismétli. (Lásd még: Traceback II.)

Ismert átiratai:

Traceback-B: Ez a Spanyolországból előkerült átirat hasonló, mint az eredeti vírus, csak a karakterek potyogtatása egy órával a vírus rezidenssé válása után indul el. Az állományban más a karakteres azonosító is: MICRODIC MSG. Ha fertőzött COMMAND.COM-ról hívunk rendszert, akkor a rendszer memóriaallokációs hibával lemerevedik. 1990 márciusa óta ismerik.

Traceback-B2: Teljesen hasonló, mint az előző, csak a vírusazonosító szöveg új: XPO DAD. 1990 májusában bocsátották útjára ismeretlen hispániai átvakarói.

A vírus neve: Traceback II

Egyéb elnevezése: 2930.

Hossza: 2930 bájt.

Kódtípusa: Parazita, rezidens része van, a .COM és az .EXE állományokat fertőzi meg.

Azonosítása: Scan /X V67+, F-Prot, IBM Scan, Pro-Scan, VirexPC, AVTK 3.5+, VirHunt 2.0+.

Eltávolítása: Scan /D /X, F-Prot, VirexPC, Pro-Scan 1.4+, VirHunt 2.0+, vagy törölni a fertőzött állományokat.

Leírása: A Traceback II vírus a korábban felismert Traceback (3066) változata. Ugyanazt teszi, mint elődje, de kódja valamivel rövidebb (2930). A .COM és az .EXE állományokat fertőzi, rezidens része van. A COMMAND.COM-ot nem bántja. A potyogtatás után, ha lenyomunk egy gombot, visszaáll az eredeti monitorkép.

Átirata:

Traceback II-B: A vírusnak ez az átirata a COMMAND.COM-ot is megfertőzi. A potyogtatás után nem adja vissza az eredeti képet, ezért csak a rendszer újraindítása segít.

A vírus neve: 1008

Egyéb elnevezése: Suomi, Oulu.

Hossza: 1008 bájt.

Kódtípusa: Parazita, van rezidens része, a .COM állományokat fertőzi meg.

Azonosítása: Scan V64+, F-Prot 1.12+, Pro-Scan 2.01+.

Eltávolítása: Scan /D, F-Prot 1.12+, Pro-Scan 2.01+, vagy a fertőzött állományok törlése.

Leírása: 1990 júniusában Petteri Jarvinen bukkant rá Helsinkiben, és Soumi vírusnak nevezte el. A vírus jellegzetes .COM fertőző. A COMMAND.COM-ot is megfertőzi, így igen gyorsan „lebukik". Viszonylag ritka.

A fertőzés során először lefut a víruskód, és rezidenssé válik a vírus. Ekkor a COMMAND.COM is megfertőződik, és a vírus hosszával, azaz 1008 bájttal lesz nagyobb. Amíg jelen van a memóriában, addig nem láthatjuk az állománynövekedést. A vírus a lopakodó technika érdekes képviselője, nem tartozik a terrorista célzatú vírusok közé, bár elképzelhető, hogy egy terjedési rutint teszteltek vele.

Ha fertőzött COMMAND.COM-mal indítunk rendszert, akkor tapasztalhatjuk néhány gépnél az „Internal Stack Error, System Halted" üzenettel való elszállást, ami nagy valószínűséggel vírusprogramozási hiba következménye. Ezen tünete megtévesztő, mert a rebootvírusra tereli a gyanút.

A vírus neve: 1210

Egyéb elnevezése: Prudents.

Hossza: 1210 bájt.

Kódtípusa: Parazita, rezidens része is van, .EXE fertőző.

Azonosítása: Scan V61+, Pro-Scan 1.4+, F-Prot 1.12+, VirHunt 2.0+.

Eltávolítása: Scan /D, F-Prot 1.12+, VirHunt 2.0+, vagy a fertőzött állományok törlése.

Leírása: Barcelonában izolálták 1989 decemberében. Szerencsére igen ritkán fordul elő. Memóriarezidens, az .EXE állományokat akkor fertőzi meg, amikor azok végrehajtódnak. A vírus minden évben május 1-től 4-ig rombol, különben csakis terjed. Aktivizálódásakor megcseréli a lemezírás és lemezellenőrzés műveleteit.

A vírus neve: Chaos

Egyéb elnevezése: Még nem ismeretes.

Hossza: Nem értelmezhető.

Kódtípusa: Rezidens, a bootszektort fertőzi.

Azonosítása: Scan V53+, CHKSeq v.1.0.

Eltávolítása: MDisk, CleanUp, vagy a DOS SYS utasítása.

Leírása: Első észlelője James Berry volt, Kentben (Anglia), 1989 decemberében. A Chaos mind a floppyn, mind pedig a merevlemezen megfertőzi a bootszektort. Mint szabályos bootvírusnak, neki is van memóriarezidens része. Amikor megfertőzi a bootszektort, felülírja az ott lévő eredeti információkat, de előbb a lemez másik helyére elmenti annak tartalmát. A fertőzött bootszektor vége üzenetet tartalmaz, ami olyan programok segítségével kiolvasható, amelyek a bootszektorban is keresnek. (Például PC-Tools, Norton Utilities.) A nem egészen korrekt angol helyesírású üzenet:

```
Welcome to the New Dungeon
Chaos
Letz be cool guys
```

(Üdvözöllek az új vártoronyban. Káosz. Srácok, őrizzük meg a hidegvérünket.)

A Chaos vírus már akkor rossznak jelzi a szektort, amikor az még olvasható. Aktivizálódásának feltételei ismeretlenek.

A vírus neve: Arf

Egyéb elnevezése: Rigor Mortis, Thor.

Hossza: 1000 bájt.

Kódtípusa: Nem rezidens, parazita, .COM fertőző.

Azonosítása: Scan V75+.

Eltávolítása: Törölni a fertőzött állományokat.

Leírása: 1991 márciusában az USA-ban egy magát Thor-nak nevező számítógép-szabotőr csoport jelentkezett ezzel a vírussal, amely kísérleti terméknek tűnik. A víruskód alapja egy alaposan átbarkácsolt Vienna vírus, ezért a legelterjedtebb antivírus programok tévesen annak azonosítják és úgy próbálják íratni. A vírusnak nincs rezidens része, a .COM programokat fertőzi meg, beleértve a COMMAND.COM-ot is.

Futtatása előtt ellenőrzi, hogy fertőzött-e a COMMAND.COM. Ha nem, akkor megfertőzi és a következő szöveget jeleníti meg a monitoron:

```
Rigor Mortis !!!
I am Hi.pas
```

(Hullamerevség! Én Hi.pas vagyok.)

A vírus ezen ténykedése után az aktuális könyvtárban egy .COM állományt keres, amit megfertőz. Ilyenkor kapjuk a következő épületes üzenetet:

```
Arf krad krad krad
krad krad kr
```

A vírus ellenőrzi, hogy a B: meghajtóban, talál-e fertőzhető állományt. Ha igen, azt is megfertőzi. A hossznövekedés 1000 bájt, a vírus az állomány végére épül be.

A vírus neve: Flash

Egyéb elnevezése: Még nem ismeretes.

Hossza: 688 bájt.

Kódtípusa: Rezidens résszel rendelkezik, .COM és .EXE állományokat fertőz meg.

Azonosítása: Scan V64+, Pro-Scan 2.01+.

Eltávolítása: Pro-Scan 2.01+, vagy a fertőzött állományok törlése.

Leírása: 1990 júliusában az NSZK-ban kibocsátott programvírus. A COMMAND.COM kivételével az .EXE és a .COM programokat támadja meg.

A memóriának a felső részén 976 bájtot foglal magának. Magára láncolja az INT 00, INT 23, INT 24, INT 30, INT ED, INT F5 és az INT FB megszakításokat, szinte a teljes rendszervezérlést magára irányítva. A memóriafoglalást ezért a DOS nem is érzékeli.

Amikor rezidens, minden futtatott .COM és .EXE programot megfertőz, az .EXE állományokat azt követően, hogy az eredeti programkód már végrehajtódott. A .COM állományokat csak akkor fertőzi meg, ha azok hossza több mint 500 bájt. A fertőzés során a hossznövekedés 688 bájt.

A vírus aktivizálódásának kulcsdátuma 1990. június 1. volt. A monitorokon villogó képet hoz létre, műszaki hiba illúzióját keltve — minden hetedik percben. Azt is megteszi, hogy hétpercenként üres képernyőt mutat, lekapcsolva a videojelet. (Ezt a magyar Phantom vírus is megteszi.)

A vírus neve: Dbase

Egyéb elnevezése: Még nem ismeretes.

Hossza: 1864 bájt.

Kódtípusa: Parazita, rezidens része van, a .COM, valamint az átfedő (overlay) állományokba is beépül.

Azonosítása: Scan V47+, F-Prot, CHKSeq v.1.0.

Eltávolítása: Scan /D vagy F-Prot.

Leírása: A DBASE vírust New Yorkban találta meg Ross Greenberg, 1988-ban. Érdekessége, hogy kifejezetten vadászik a .DBF kiterjesztésű (dBase) állományokra. Innen kapta nevét is. Ha nyitott .DBF állományra lel, akkor abban véletlenszerűen áthelyezgeti, összekavarja a bájtokat, mérhetetlen kárt és káoszt okozva az adatokban. Ugyanakkor könyveli, hogy milyen adatokat alakít át, és ezt az állományt, amely BUG.DAT névre hallgat, elhelyezi egy ugyanolyan nevű alkönyvtárban, mint az általa átírt .DBF állomány. Amikor olvasásra megnyitjuk az állományokat, a vírus az elmentett eredeti adatokat visszatölti, így kívülről úgy tűnik, mintha minden rendben lenne. A BUG.DAT állomány létrehozása után 90 nappal azonban a vírus immár véglegesen tönkreteszi — felülírja — a FAT-táblát és a gyökérkönyvtár bejegyzéseit.

A vírusokkal foglalkozó szakemberek feltételezése szerint szerzője ezt a programot eredetileg másolásvédelemnek szánta. Valószínűleg azokat akarta megbüntetni, akik az USA-ban szokásos 90 napos áruvisszaküldési határidő után sem fizettek, de tovább használták a programot. Minden bizonnyal az úgynevezett regisztrációs lemezen volt a leszedő program, amit a pénz beérke-

zése után az ügyfél megkapott. Miként azonban a seprű Goethe bűvészinasa kezében, itt a program kelt önálló és ellenőrizhetetlen életre.

Amikor azonosítottuk a vírust, a dBase programot kell törölni és tiszta kópiával pótolni. Azokat a .DBF állományokat mindenképpen elveszítjük, amelyeket a fertőzés időszakában hoztunk létre. A BUG.DAT alapján eddigi ismereteink szerint nem lehet helyreállítani a sérült állományokat.

A vírus neve: Tunes

Egyéb elnevezése: 1971, Eight Tunes, 8 Tunes.

Hossza: 1971 bájt.

Kódtípusa: A .COM, az .EXE és az átfedő (overlay) állományokat fertőzi meg, tárrezidens része van, parazita.

Azonosítása: Scan V62+, Pro-Scan 1.4+, VirexPC, AVTK 3.5+, VirHunt 2.0+

Eltávolítása: Scan /D, VirHunt 2.0+, vagy törölni a fertőzött állományt.

Leírása: Fridrik Skulason fedezte fel Izlandban ezt a muzsikáló vírust, 1990 áprilisában. A vírus jelenléte a zenélésen kívül egyes állományok megnövekedéséről, valamint arról ismerhető fel, hogy a DOS által észlelt memória csökken. Valószínűleg valamelyik Hamburg környéki vírusműhely „ujjgyakorlata".

Ha a víruskóddal fertőzött programkód lefut, akkor a baci rezidenssé válik. Utána gondosan ügyel arra, hogy ne fertőzze meg a COMMAND.COM-ot, mert könnyen felfedezhető lenne. Kíméli a 8 K-nál rövidebb .COM állományokat. Viszont nemcsak az .EXE, hanem az átfedő (overlay) állományokra is veszélyes. A fertőzött program hossza a paragrafushatár függvényében 1971–1985 bájttal megnő. A memória méretét a rezidens vírusrész 1984 bájttal csökkenti.

Nem okoz rendszerösszeomlást, de beépülésével rombol. A zeneszolgáltatást akkor kezdi el, amikor már harminc perce aktív a memóriában. Utána véletlenszerű időközönként nyolc német népdal részleteivel szórakoztat bennünket.

A vírus neve: Carioca

Egyéb elnevezése: Még nem ismeretes.

Hossza: 951 bájt.

Kódtípusa: Rezidens résszel rendelkezik, parazita, .COM fertőző.

Azonosítása: Scan V71+, Pro-Scan 2.01+.

Eltávolítása: Pro-Scan 2.01+, vagy a fertőzött állományok törlése.

Leírása: 1990 novemberétől ismert a vírus, amely rezidens résszel rendelkező, .COM fertőző, de a COMMAND.COM-ot nem támadja meg.

A kód lefutása után szabályos rezidens programként installálja magát a hagyományos DOS memória alsó részében, 1280 bájt helyet lefoglalva, de a rendszer számára rendelkezésre álló terület ennél kicsit többel, 1312 bájttal csökken. Az INT 21 vezérlését magára irányítja. Amikor a memóriában tartózkodik, minden futtatott .COM állományt megfertőz, kivéve a COMMAND.COM-ot. A fertőzés utáni hossznövekedés 951 bájt, és a kód az állomány végére épül be. A vírussal fertőzött állomány legvégén megtalálható az azonosító 2EFF1E1A010203CD21 hexa karaktersorozat.

Túl a PC határain

Szerencsére már Magyarországon is kezdenek kialakulni az országos kommunikációs hálózatok, s azok egyre szélesebb körben hozzáférhetővé válnak mindenki számára. Ennek nyomán viszont várható lesz a hálózati vírusok megjelenése is.

Az Alaplap 1991 áprilisi számában írtunk egy DEC számítógépre készült vírusról. Mivel azonban mi nem ismertük a DEC környezetet, felhívást intéztünk az ezzel foglalkozó szakemberekhez, hogy segítsenek megfejteni a különös szövegállomány-vírus rejtélyét. Végül is Cser László és Balázs Béla volt segítségünkre. Ők az országos kísérleti DECNet hálózat rendszergazdáiként közreműködtek a vírus visszafejtésében. Ebben a fejezetben az általuk írt — és ugyancsak az Alaplapban megjelent — beszámoló alapján igyekszünk a vírustémát a PC határain túli környezetben is felvillantani.

Aki rendszerekkel dolgozik, bizonyára ideges lett attól a hírtől, hogy a Digital Equipment Corporation (DEC) többszintű hozzáférésvédelmi-önvédelmi rendszerét sikerült egy vírusnak kijátszania. Nem eszik azonban olyan forrón a kását! Az a bizonyos .COM kiterjesztésű vírusállomány a VAX/VMS operációs rendszer kommunikációs nyelvén, DCL-ben íródott (DCL = digital command language). Ebben a környezetben a .COM kiterjesztés azonban nem bináris végrehajtható állományra, hanem a command file (parancsfájl) elnevezésre utal, és az hasonló funkciót tölt be, mint PC-s környezetben a .BAT batchfájl.

A parancsfájl analizálása után kiderült, hogy valóban helytelen lett volna az Alaplapban közölni a teljes programlistát, mert olyan trükkök vannak benne, amelyek bizonyos rendszerhiányosságokat használnak ki. A teljes lista alapján vissza lehetett fejteni a programot, amely valóban vírus. Olyan értelemben vírus, hogy terjed a rendszerben. Viszont jóindulatú, mert terjeszkedése során önmagát kivéve nem töröl, illetve nem épül be más programba. Ha a klasszikus vírusosztályozást vennénk figyelembe, akkor a programférgeknek (elfogadott angol nevén: worms) a vírusoknál kevésbé népes, de sok elegáns programozási fogást tartalmazó csoportjába tartozik. E hálózati program jellemzői:

— Nem fertőz, mert más parancsfájlokhoz (.COM) vagy végrehajtható programokhoz (.EXE) nem nyúl. Nem is nagyon tudná megtenni, mert a VAX/VMS többfelhasználós operációs rendszer jól el van látva hozzáférés-védelemmel.

— Nem okoz kárt, mert nem töröl (önmagán kívül) semmit, nem állítja meg a gépet (bár alaposan lelassíthatja), és nem is formattálja a lemezeket. (A VAX/VMS alatt nem is lehet formattálni.) Bosszantásul viszont karácsonyi üdvözleteket küld.

— Terjeszkedik, de csak abban az esetben, ha az a VAX gép, amelyen elin-

dították, része egy számítógép-hálózatnak, és a hálózat DECNet alapú. Adathordozó (hajlékony mágneslemez) közvetítésével nem terjed.

Természetesen a fenti megállapításokkal vitába lehet szállni. Például, miért nem fertőz? Hiszen fertőz, ha a számítógép-hálózatot tekintjük egységes rendszernek, valamiféle „hipergépnek", mert ez a program a hálózat csomópontjai között vándorol, s ott többszörözi magát. Ezek után nézzük, mit is csinál valójában ez a programféreg!

A parancsfájl teljes szövegét természetesen nem tesszük közzé, mert aktivizálódási feltételei pillanatok alatt átírhatók, s akkor már veszélyes is lehet. Ezt a programot kizárólag azért készítette valaki, hogy segítsen a Télapónak szétküldözgetni a karácsonyi üdvözleteket. A programnak 1988. december 24-én nulla óráig volt lehetősége terjeszkedésre, és 24-én nulla órától kezdve csak 30 percen át fejtette ki hatását. Természetesen, ha ezt az időkorlátozást kivesszük belőle, akkor bármikor és bármeddig képes működni, de akkor könnyen lefülelhető. Az évszám is könnyen módosítható. Néhány jellemző tevékenységének ismertetése során ne lepődjünk meg, hogy sok olyan dolgot csinál, mint egy megszokott PC-s vírus. Az elvek, a működés logikája ugyanaz!

— A program futás közbeni saját azonosítóját MAIL_178DC névre változtatja. Ez több okból is „hasznos": álcázza magát, valamint fel tudja venni a kapcsolatot a VAX/VMS MAIL segédprogramjával, amely levelezési lehetőséget biztosít a hálózaton dolgozó felhasználók között.

— Beolvassa önmagát a memóriába, majd a lemezről kitörli magát (DELETE hi.com;*). Ugye, ezt egy PC-s vírus is megtehetné?

— Generál egy hálózati csomópont-azonosítót, kvázi véletlenszerűen, felhasználva az aktuális időt. Ez a csomópont lesz az, ahová átmásolja, majd ott elindítja önmagát. Azt természetesen ellenőrzi, hogy a hálózatban van-e olyan azonosítójú csomópont, amilyet előállított. A másoláshoz és az indításhoz felhasználja, hogy a DECNet hálózatban lévő VAX gépeken általában definiálva van egy alapértelmezés szerinti hálózati bejelentkezési lehetőség. (A VAX/VMS rendszerbe csak felhasználói név és jelszó ismeretében lehet belépni.) Ez az alapértelmezés szerinti belépési lehetőség nem rendelkezik privilégiumokkal.

— Amikor elmúlt a terjeszkedéséhez határidőként megszabott időpont, hozzáfog az üdvözletek szétküldéséhez. Nagyon ügyes fogással megszerzi majdnem az összes felhasználó nevét azon a csomóponton, amelyiken működik.(Például ezért sem közölhető a teljes kód!) Ezek a felhasználók lesznek a címzettek. Felveszi a kapcsolatot a rendszer hálózati levelezést végző programjával és a parancsfájlban lévő üdvözlet szövegét elküldi a kiválasztott címzetteknek a Télapó nevében.

— Kitörli azt a fájlt, amelybe a megszerzett felhasználói neveket tette, majd leállítja önmagát (STOP/ID=0).

Ezután joggal vetődik fel a hálózati felhasználókban, hogy mit lehet tenni egy esetleges ilyen vagy jóval kártékonyabb trükk elkerülésére?

— Szigorúan be kell tartani a VAX/VMS védelmi előírásait.

— A hálózat gépei semmiképpen ne legyenek átjárhatók az alapértelmezés

szerinti, tehát közismert bejelentkezések segítségével. Minden bejelentkezési lehetőség egy-egy konkrét személyhez kapcsolódjon.

— A rendszer használói mindig csak a munkájukhoz feltétlenül szükséges minimális privilégiumokat kapják meg.

— A SYS$SYSTEM:RIGHTSLIST.DAT fájlt ne legyen joga bárkinek elolvasni. Ha ugyanis ehhez valaki hozzáfér, akkor a kulcs egy része már a kezében van a rendszer manipulálásához.

A probléma szerencsére még idejében nyilvánosság elé került. Remélhetőleg a most üzembe lépő nagygépes halózatokon nem kell komolyabb vírusinvázióval vagy az USA ARPANET félkatonai rendszerének leállását előidéző informatikai merénylethez hasonlóval találkozniuk. Ehhez viszont a rendszerüzemeltetőknek és a felhasználóknak komolyan kell venniük az adatbiztonsági szabályokat.

Vírusgeneológia

A számítógépvírusok kiforrott rendszerezésére még valószínűleg sokáig kell várni, de egy nemzetközi vírusdokumentáció kiadója, Patricia M. Hoffman az általa vezetett adatbankban található leírások alapján megkísérelte összefoglalni néhány népes víruscsalád leszármazási fáját.

A vírusgeneológia viszonylag új keletű szakterület. Művelése azért hasznos és szükséges, hogy a vírusprogramokkal foglalkozó szakemberek meg általában a számítógépen dolgozók könnyebben eligazodjanak az egyre több vírus és vírusváltozat között. Hiszen az azonos családba tartozó vírusok standard azonosítója sok esetben megegyezik, de ugyanakkor irtásukhoz már tudni kell, hogy a vírus melyik változatával állunk szemben.

Könyvünk első kiadásában már céloztunk arra, hogy a biológia tudományának kategóriái előbb-utóbb megjelennek a számítógépes vírusokkal foglalkozó szakemberek szótárában. Ilyen számítástechnikai másodlagos értelmet nyert már a törzs (strain), a család (family) és a változat (variation) fogalma.

Törzs: Egymásból leszármaztatható, forráskódjukban jelentősen eltérő vírusok csoportja.

Család: Egymásból leszármaztatható, forráskódjukban csak kisebb mértékben eltérő vírusok csoportja.

Változat: Azonos forráskódú, csupán valamilyen paraméterében különböző vírus. (Például eltérő az aktivizálódás dátuma.)

Tisztázatlan ma még, hogy rendszertanilag hová sorolhatók be azok a vírusvariációk, amelyek .COM és .EXE állományokat is, és/vagy a bootrekordot is fertőzik. Irtásuk, felismerésük ugyanis más-más algoritmust igényel, viszont egymásba átalakulhatnak, ezért fizikailag és logikailag egyetlen vírust képeznek. Talán a forma lenne a megfelelő fogalom. (Mint a pete, hernyó, báb, lepke formaváltozatok.)

Bonyolítja a helyzetet, hogy bizonyos vírusok folyamatosan átalakulnak, egymással kölcsönhatásban élnek. Itt még talán a biológiai értelemben vett nem (szex) fogalma is helytálló lehetne. (A Fish 6 és a Whale, ha találkozik, összeolvadva, majd szétesve más vírusokat hoz létre...) Végső soron tehát a vírusprogramok felfoghatók az élő anyag működőképes számítógépes modelljeinek is.

A vírusok leszármazási tábláit Patricia M. Hoffman kutatásai alapján állítottuk össze. Terjedelmi okokból azonban a családfák törzsi és családi elágazásait, a változatok rokoni szálait nem tudjuk vizuálisan bemutatni, mindössze felsoroljuk a leszármazás alapján összetartozókat.

AircCop: AirCop — AirCop-B
Akuku: Akuku — Metal Thunder
Alameda: Alameda — Alameda-2 — Golden Gate — Golden Gate-B — Golden Gate-C — SF
Anti-Pascal: Anti-Pascal — AP-529 — AP-400 — AP-440 — AP-480
Anti-Tel: Holocaust — Telecom
Arab: 834 — 834-B (Arab)
Azusa: Azusa — Azusa 2
Bad Boy: Bad Boy — Bad Boy 2
Blood: Blood — Blood2
Brain: Brain — Ashar — Clone — Chaos — EDV
Cascade: Cascade (1701) — 1701-B — 1704 — 1704 Format — 1704-B — 17Y4 — Cunning — JoJo — JoJo 2
Darth: Darth-1 — Darth-2 — Darth-3 — Darth-4
Datacrime: Datacrime — Datacrime-B — Datacrime II — Datacrime IIB
Do-Nothing: Do-Nothing — Saddam
Exterminator: Exterminator — BadGuy — Demon
Flip: Flip — Flip-B — Tequila
Fri 13th COM: Fri 13th COM — Fri 13th-B — Fri 13th-C — Virus-B
Happy New Year: Happy New Year — Happy New Year B
HM2-Plastique: HM2 — Plastique — Plastique 4.21 — Plastique 5.21 — Invader — Jerusalem B — Plastique Cobol
Holland Girl: Holland Girl — Holland Girl 2
Icelandic: Icelandic — Saratoga — Icelandic-II — Icelandic-III — Dec 24th — Mix1 — Mix1-B — Mix2
Kemerovo: Kemerovo — Kemerovo-B — Kemerovo-C
Kennedy: Kennedy — Tiny-163
Keypress: Keypress — Keypress-B
Leprosy: Leprosy — Leprosy-B — The Plague — Leprosy-C — Leprosy-D — RMIT
MG: MG — MG-2 — MG-3 — MG-3B
Mini: Mini-45 — Define
Murphy: Murphy — Murphy-2 — Murphy-4 — HIV — Migram — Italian Pest — Smack — Goblin — Swami — Diabolik — Murphy-3 — Finger — Erasmus — AntiChrist — Kamasya — Cemetery
Mutant: Mutant 128 — Mutant 127 — Mutant 123
Naughty Hacker-B: Naughty Hacker-B — Naughty Hacker-A — Horse 2 — Horse — Naughty Hacker-C — Naughty Hacker-F — Naughty Hacker-D — Horse 5 — Naughty Hacker-E — Naughty Hacker-G
Number One: Number One — AIDS
Ohio: Ohio — Den Zuk
Perfume: Perfume — Sorry
Phoenix: Phoenix — PhoenixD — Evil-B — Evil
Ping Ping: Ping Pong — Ping Pong-B — Ping Pong-C — Big Italian — Typo Boot — Print Screen — Print Screen-2 — Ghostballs

Pixel: Pixel — Amstrad — V-847B — V-852 — V-345 — V-299 — V-277 — S-847 — Pixel 2 — Hell — Silly-365 — Silly
Polish 217: Polish 217 — Polish 217 B
Sentinel: Sentinel — Sentinel-3 — Sentinel-5
Stoned/Marijuana: Stoned — Stoned-B — Rostov — Sex Revolution V1.1 — Sex Revolution V2.0 — Stoned-C — Stoned-D — Stoned-E — Stoned-F — Stoned I — Swedish Disaster — PS-Stoned — Evil Empire — Evil Empire-B — Horse Boot — Michelangelo
Suriv: Suriv 3.00 — Jerusalem — Fu Manchu — Taiwan 3 — RAM Virus — Jerusalem B — New Jerusalem — Payday — Sunday — Sunday-B — Sunday-C — Jerusalem C — Jerusalem D — Jerusalem E — Spanish JB — 1720 (PSQR) — Australian — 1210 (Prudents) — Frere Jacques — Anarkia — Anarkia-B — Slow — Scott's Valley — Westwood — 1605 — 1605-B — Park ESS — Skism-1 — Discom — Captain Trips — Swiss 1813 — Phenome — Apocalypse
Sverdlov: Sverdlov — Sverdlov-B
SysLock: SysLock — Macho — Macho-B — Advent — Cookie
Tiny: Tiny-198 — Tiny-167 — Tiny-160 — Tiny-159 — Tiny-158 — Tiny-156 — Tiny-154 — Tiny-143 — Tiny-138 — Tiny-134 — Tiny-133 (A Tiny-163 a Kennedy családba tartozik, ezzel a családdal csak a névrokonsága van meg.)
Terror: Terror — Dark Lord
Traceback: Traceback II — Traceback — Traceback-B — Traceback-B2 — Traceback II-B
Tumen: Tumen V.5 — Tumen V2.0
USSR 1064: USSR 1064 — USSR 1689
V1024: V1024 — Dark Avenger — V651 — V800 — V800M — V2000 — V2000-B — V2100 — M.I.R. — Apocalypse II — Dark Avenger-B — Rabid Avenger — VAN Soft — Diamond — Diamond-B — Gremlin — Damage — Damage-B — Lucifer — Ah
Vienna: Vienna — Father Christmas — NTKC — Lisbon — Lisbon-B — Lisbon-B2 — Ghostballs — 1260 — V2P2 — V2P6 — V2P6Z — V2P6-B — Casper — Adolph — W13 (V-534) — W13-B (V-507) — Wien (Poland) — Vien6 — Vienna-B — Vienna-B 645 — Vienna 822 — Violator — Violator BT — Violator B1 — Violator B2 — Violator B3 — Violator B4 — Violator B4-1 — Violator B4-B — Grither — VHP-348 — VHP-353 — VHP-367 — VHP-435 — VHP-623 — VHP-627 — Iraqui Warrior — Arf-B — Arf — Incom — Monxla — Monxla B — Polish 583
Virus-90: Virus-90 — Virus-101
Wolfman: Wolfman — Wolfman 2
WWT: WWT 01 — WWT 02
Yankee 2: Yankee 2 — Enigma — Bandit
ZeroHunt: ZeroHunt — ZeroHunt B
512: 512 — 512-B — 512-C — 512-D — 512-E — 512-F
1226: 1226 — 1226M — 1226D

1263: 1963 — 1963-B
2560: 2560 — 2560-B — 2560-C — Magnitogorsk 2048
4096: 4096 — 4096-B — 4096-C — Fish — Whale
5120: 5120 — Slayer Family

A fenti felsorolás a teljesség kedvéért tartalmazza azokat a vírusokat is, amelyek a részletes leíró részben még nem szerepelhetnek, mert a kézirat lezárása után bukkantak fel. Ha ezek elemzésének elkészültét is bevárnánk, könyvünk soha nem jelenhetne meg, hiszen állandóan jönnek az új vírusok. Az alapvető paraméterek azonban megtalálhatók a nagy összefoglaló táblázatban, amelynek lehető legkésőbbi, 1992 márciusi változatát közöljük.

Melyik országból jöttek?

Az alábbi felsorolásban azok a vírusok szerepelnek, amelyek első felbukkanási helyét ismerjük. Néhány népszerű vírus eredete, illetve származási országa homályba vész, bizonyos vírusoknál pedig csak a családok és nem a változatok első előfordulási helyét regisztrálták.

Anglia: Chaos, Typo COM, VP

Ausztrália: Australian, Australian 403, Growing Block, Liberty, Possessed, Slow

Ausztria: 1253, Vienna

Bulgária: 512, 1226, 1226D, Anthrax, Anti-Pascal, Anti-Pascal II, Boys, Dark Avenger, Dark Lord, Darth Vader, Destructor V4.00, ETC, Evil, Happy New Year, Horse Boot, Kamikazi, Leech, MG, MG-2, Mini-45, Murphy, Mutant Family, Naughty Hacker Family, Nina, Parity, Phoenix, PhoenixD, Proud, Sentinel, Shake, Tiny Family, V651, V800, V1024, V2000, V2100, Vacsina, VFSI, VHP, VHP2, Warrior, Yankee Doodle, Yankee 2

Dánia: Kennedy, Tiny-163

Dél-Afrika: Blood, Friday The 13th COM, June 16th, Saturday The 14th

Egyesült Államok: 1260, AirCop, Alameda, Arf, DataLock, dBASE, Doom II-B, Frere Jacques, Frog's Alley, Golden Gate, Green Peace, Grither, Guppy, Iraqui Warrior, Jeff, JoJo 2, Keypress, Lehigh, Leprosy, Leprosy-3, Saratoga, Scott's Valley, Solano 2000, Striker #1, Subliminal 1.10, Sunday, Tester, The Plague, V2P2, V2P6, V2P6Z, V801, Violator, Violator B4, Virus-90, Virus-101, Westwood, Wisconsin, Yap, ZeroHunt, ZK900

Finnország:: 1008, Crew-2480

Franciaország: 903, EDV, Mardi Bros, Paris

Fülöp-szigetek: Revenge Attacker

Görögország: Amstrad (Pixel), Armagedon

Hollandia: Datacrime, Datacrime-B, Datacrime II, Datacrime IIB, Deicide, Dutch 555, Groen Links, Holland Girl, New Jerusalem, Payday, Zero Bug

Hong Kong: Azusa

India: Joshi, Microbes, Print Screen

Indonézia: 1392, Den Zuk, Ohio

Izland: Ghostballs, Icelandic, Icelandic-II, Icelandic-III

Izrael: 4096, Alabama, Do-Nothing, Jerusalem, Jerusalem B, JoJo, Mix1, Saddam, Suriv 1.01, Suriv 2.01, Suriv 3.00, Swap, Typo Boot

Japán: Christmas in Japan

Kanada: Evil Empire, Evil Empire-B, Evil Empire-B, Holland Girl 2, NoInt, Ontario, Yukon Overwriting
Korea: Korea
Lengyelország: Dot Killer, Father Christmas, Hybryd, Joker, Nomenklatura, Polish 217, Polish 529, Polish 583, Stone'90, SVir, VComm, W13
Magyarország: Monxla, Monxla B, Phantom, Polimer, Töltögető (Fat Filler), Turbo 448, Turbo Kukac
Malajzia: Black Monday, Fellowship
Málta: Casino
Mexikó: Devil's Dance
Németország: 405, 5120, Ambulance Car, Burger, Cascade, Cascade-B, Christmas Tree, Eight Tunes, Fingers, Fish, Flash, Halloechen, Number One, Perfume, RaubKopie, RPVS, VirDem, VCS, Whale
Olaszország: Ah, AntiChrist, Bandit, Cracker Jack, Damage, Enigma, Erasmus, Goblin, Hero, HIV, I-B, Italian 803, Italian Pest, Itavir, Kamasya, Klaeren, Little Pieces, Lucifer, Migram, PCV, Smack
Pakisztán: Brain
Portugália: Amstrad, Lisbon
Spanyolország: 1210, 1720, Anti-Tel, Holocaust, July 13th, Spanish April Fools, Telecom
Svájc: Burghofer, Flip, Form, Swiss 143, Tequila
Svédország: Swedish Disaster
Szaúd-Arábia: 834
Szovjetunió: 2560, Akuku, Attention!, Best Wishes, Crash, Dir Virus, F-Word, Hymn, Kemerovo, Kiev 483, Lozinsky, Magnitogorsk 2048, MGTU, NTKC, Red Diavolyata, Sverdlov, Tumen V.5, Tumen V2.0, USSR, USSR 311, USSR 492, USSR 516, USSR 600, USSR 707, USSR 711, USSR 948, USSR 1049, USSR 1064, USSR 1689, USSR 2144, Victor, Voronezh
Tajvan: 382 Recovery, 1575, Bloody!, Disk Killer, Invader, MusicBug, Plastique, Plastique-B, Spyer, Taiwan, Taiwan 3, Taiwan 4, Wolfman
Thaiföld: Loa Duong
Új-Zéland: Shadow, Stoned

Két veszélyes „állatfaj"

A fájlvírusoknál is komolyabb veszélyforrássá váltak a floppyk és a merevlemezek bootszektorát megfertőző vírusok. Listájukat ezért külön is közöljük. Nem szabad megfeledkezni arról sem, hogy a floppyn bootvírusként viselkedő egyes vírusok a merevlemezen partícióstábla-vírusként működnek. (A részletes vírusleírásból kell tovább tájékozódni.)

A vírusok különösen veszélyes másik csoportjába azok tartoznak, melyek az úgynevezett „stealth" és „sub-stealth", azaz lopakodó programozási trükkök alkalmazására vannak felkészítve. Ezek a DOS és egyéb programok elől el tudják rejteni az általuk végrehajtott változtatásokat, és a fertőzés leplezésére az eredeti állapotot mutatják.

Bootvírusok:

AirCop, Alameda, Anti-Tel, Ashar, Azusa, Bloody!, Brain, Chaos, Den Zuk, Disk Killer, EDV, Evil Empire, Evil Empire-B, Form-Virus, Golden Gate, Horse Boot, Joshi, Keydrop, Korea, Loa Duong, Mardi Bros, Michelangelo, Microbes, MusicBug, NoInt, Ohio, Pentagon, PingPong, PingPong-B, Print Screen, SF Virus, Stoned, Töltögető (Filler), Swap, Swedish Disaster.

Lopakodók:

512, 1008, 1963, 2560, 4096, Ah, Anti-Tel, Brain, Casino, Damage, EDV, Fish, Gremlin, Holocaust, Joshi, Leech, Lucifer, Magnitogorsk 2048, MG, MG-2, Murphy, Naughty Hacker Family, NoInt, PCV, Sentinel, Telecom, Tequila, V651, V1024, V2000, V2100, Whale, ZeroHunt, Zero Bug.

Mérettáblázat

Táblázatunkban azoknak a vírusoknak a hosszát közöljük, amelyeknél ez mint informatív adat jelentőséggel bír. Tájékozódó jelleggel tudjuk használni olyankor, amikor hossznövekedést tapasztalunk állományainkon. Ne felejtsük el azonban, hogy az ok nem minden esetben vírus! Nő az állomány mérete, ha a programhoz immunrutint építünk (például a Buruzs Tamás-féle SPS szoftverrendszerrel vagy a Sysdokival), illetve ha *ellenőrző* összeget rakunk az állomány végéhez a Scan valamelyik újabb változatával, esetleg az öt MSDOS betűt tesszük immunizálás gyanánt az állomány végéhez a TNT programmal. Az ilyesmire érzékeny programok vírusveszélyt jelezve indokolatlanul is vísítani fognak. Ugyanakkor a lopakodó technikát alkalmazó vírusok esetében az állománynövekedést csak akkor vesszük észre, ha tiszta lemezről rendszert indítva nézzük végig állományainkat. A méret szerinti rendezés sok esetben mégis segíthet az eligazodásban. Ezért állítottuk össze ezt a segédtáblát is, amelyet az első kiadás óta jelentősen kibővítettünk, átdolgoztunk — és helyesbítettünk!

133	Tiny-133
143	Swiss 143
144	144
152	Guppy
163	Tiny
217	Polish 217
256	Nina
256	USSR-256
257	USSR-257
265	BadGuy
270	268-Plus
273	MGTU Virus
299	V-299
308	Kennedy
321	USSR-311
337	337
369	Bljec
394	USSR-394
427	Blood-2
441	Parity
448	Kukac
451	Exterminator
453	453
453	Happy Day
461	Striker
476	Shake
482	Beeper
483	483
488	Love Child
492	USSR-492
510	510
512	Friday 13th COM
512	Polimer
512	Polish-2
512	Turbo Kukac
516	Leapfrog Virus
516	USSR-516
528	IKV528
529	529
529	USSR-529
532	W-13
535	Monxla-B
555	V-555
575	USSR
575	USSR
600	Christmas-J

600 USSR-600
608 Do-Nothing
632 Saratoga
642 Hymn
642 Icelandic
648 Incom
648 Lisbon
648 Vienna-B
648 Vienna/648
651 651
661 Icelandic II
685 Saturday 14th
688 Flash
691 Dir-Vir
696 USSR-696
707 USSR-707
708 Taiwan
711 USSR-711
720 Lazy
723 Shadow Byte
731 Sorry
733 733
765 Perfume
777 777
777 Iraqi Warrior
779 Pixel
796 RedX
801 Star Dot
801 V-801
825 Wisconsin
828 Jeff
830 USSR-830
834 Arab Virus
847 Amstrad
850 S-847
853 Icelandic-3
857 Virus-90
867 Typo/Fumble
897 Suriv01
903 903
919 Saddam
920 DataLock
923 923
928 Mirror
934 Leech
939 Monxla
941 Devil's Dance
944 Dot Killer
948 USSR-948
951 Carioca
961 Stone-90
961 V-961
988 Bandit
1000 Bad Boy
1000 Tester
1004 BeBe
1008 1008
1022 Fellowship
1023 Lozinsky
1024 1024
1024 1024PSRC
1024 Best Wish
1024 Nomenclature
1024 Warrior
1049 USSR-1049
1055 Black Monday
1055 Violator
1067 1067
1074 Vcomm
1079 Armagedon
1085 Terror
1086 Lucifer
1092 Tumen V2.0
1146 Greemlin
1150 Destructor
1154 Horse
1168 Datacrime-B
1181 Spyer
1200 Casper
1201 July 13th
1206 Anthrax - File
1206 Vacsina
1210 1210
1217 Vacsina V05
1226 1226
1232 Keypress
1242 Justice
1253 1253 - COM
1255 Spar
1260 1260
1260 1260
1277 Murphy
1280 Datacrime
1306 Hybrid
1322 Fingers
1332 Sylvia/Holland

1374 Little Pieces
1381 1381
1392 1392
1433 Australian
1446 Growing Block
1480 Cancer
1488 Suriv02
1496 Subliminal
1500 Frogs
1514 Datacrime II
1530 Vacsina V16
1536 1536/Zero Bug
1536 AGI-Plan
1539 XA1
1554 1559
1560 Alabama
1600 Voronezh
1605 1605
1618 MIX1
1636 Sunday
1663 Tumen V0.5
1689 Off Stealth
1701 1701/Cascade
1701 JoJo
1704 1704 Format
1704 1704/Cascade
1704 Cascade-B
1720 1720
1720 1720
1721 Slow
1726 June 16th
1745 Mir
1755 Enigma
1760 Vacsina V24
1800 Dark Avenger
1808 Jerusalem
1808 Jerusalem-B
1808 New Jerusalem
1808 Payday
1811 Frere Jacques
1813 Anarkia
1815 Skism
1864 Dbase
1865 Happy New Year
1881 Father Christmas
1910 Pest
1917 Datacrime II-B
1951 Goblin
1961 Yankee-2
1962 Hymn-2
1962 Sverdlov
1963 1963
1971 1971/8 Tunes
2000 Solano
2000 V2000
2064 Wolfman
2083 Staf
2086 Fu Manchu
2100 V2100
2133 Scott's Valley
2144 USSR-2144
2253 Phantom
2280 Mix2
2343 Flip
2351 Ghost COM
2458 Victor
2504 Doom2
2560 Virus-101
2576 Taiwan4
2772 Yankee Doodle v3
2773 Oropax
2862 Liberty
2885 Yankee Doodle
2890 Yankee Doodle v1
2905 Taiwan3
2930 2930
2932 Yankee - H 3
2940 Yankee Doodle v2
2941 Yankee - H 4
3012 Plastique
3066 Traceback
3445 3445
3551 3551/SysLock
3584 Fish6
3700 Telecom File
3784 Holocaust
3880 ItaVir
4096 4096
4096 Invader
4625 Sentinel
4909 Paris
4909 TCC
5120 5120
5120 Brain Slayer
7808 7808
9216 Whale

Vírusazonosító jelsorozatok

Az alábbiakban a vírusok felismeréséhez használt azonosító sztringeket, az úgynevezett vírusszignatúrákat adjuk meg a HTSCAN szabadszoftver és a hasonló elven működő többi program által használt formában. A vírusnév előtti pontosvesszőt elhagytuk. (Megjegyzendő, hogy néhány vírusnak csak az azonosító szekvenciáját ismerjük.)

Az egyik első víruspánik alkalmával az IBM cég terjesztett az USA-ban, Mexikóban és Venezuelában egy SCAN.EXE (illetve VIRSCAN.EXE) nevű szekvenciális víruskereső programot. Az is egy .LST kiterjesztésű ASCII állományban tárolta a keresési jelsorozatot. Hasonló elven működnek, csak más adatformátumot használnak a McAfee-féle SCAN.EXE programok. Szignatúralistánkban ezeket a megszokottól eltérő szekvenciákat IBM-SCAN megjegyzéssel közöljük, s mivel e szekvenciák kiválasztása sok bizonytalanságot tükröz, csak tájékoztató jelleggel ajánljuk.

Újdonság az első Víruslélektan kötethez képest, hogy listánk jelentősen bővült a Norton Antivírus (NAV) 1.0 változatából visszafejtett, valamint más forrásokból beszerzett elsődleges vírusszignatúra állományokkal. Az előző könyvben még három sorban helyeztük el az egy vírushoz tartozó információkat. Ezt most terjedelmi okokból kétsorosra sűrítettük. (Ami nem fér el, az itt is több.) Az első sorban elöl áll egy legfeljebb 30 karakter hosszú elnevezés, utána kerek zárójelben a pontosítások, megjegyzések, végül pedig szögletes zárójelben az, hogy hol kell keresni [COM, EXE, BOOT, memória] a második sorban megadott, elvileg maximálisan 80 karakter hosszú hexadecimális sorozatot. Amennyiben a memóriában eltérő szekvenciát kell keresni, azt is közöljük, ha ismerjük. A hagyományos DOS memórián kívül néhány vírus képes a HIMEMben is futni, ott azt is jelezzük.

AirCop [BOOT]
DD2EFF2EC001530EE8B1FF0EBB4C00E8ADFF5BCD12

Alabama [COM, EXE]
C606F900013CD375062EC606F90000BB40008EDB33DB8A4717240C3C0C7541

Anarkia [COM, EXE]
5C02B82125CD218E063100268E062C0033FFB9FF7F

Anthrax [BOOT, EXE, COM]
A58ED8BA270451535052CB8EC1B104BEB00583C60EAD3C80

Anti-Pascal [COM]
BF0C018B360C0103F7B95D021E07EA00

Ambulance (RedX) [COM]
BDF0FFBA0000B91000E83F0042E2FAE81600E87B00

April 1st COM [COM]
89263401B419CD2104412EA265
April 1st COM (IBM-SCAN) [COM]
89263401B419CD2104412EA265032EA2B103BF6703578BF2807C013A750D8A0
42EA265032EA2B103
April 1st EXE [EXE]
2EA31700BB17000E1FB4DECD21
April 1st EXE (IBM-SCAN) [EXE]
2EA31700BB17000E1FB4DECD21B42ACD2181FA0104742281F9BC077506E8C
504
Armagedon [COM]
3DDADA7503E999000E1F
Ashar boot (IBM-SCAN) [BOOT]
8CC88ED88ED0BC00F0FBA0067CA2097C8B0E077C890E0A7CE85900
Birthday (IBM-SCAN) [COM, EXE]
2E8B360101FCBF00015703F72E8936F000B90300F3A4B430CD213C037303E9F
801B44ABB75032E031EF000B90400D3EB43CD21BB0800B448CD21
Black Monday [EXE, COM]
AC009C0650EA0000000033C08ED88F0602008F060000FB
Brain, Shoe or Ashar [BOOT]
F4A113042D0700A31304B106D3E08EC0BE007C
Brain (c) Boot (IBM-SCAN) [BOOT]
8CC88ED88ED0BC00F0FBA0067CA2097C8B0E077C890E0A7CE85700
Choinka [COM]
B90080F2AEB90400ACAE75EEE2FA
Companion (AIDSII, 8064) [COM, EXE]
5589E581EC0202BFCA050E57BF3E011E57
Dark Avenger [COM, EXE]
49CD21BBFFFFB448CD2181EBE700727B8CC1F913CB
Dark Avenger 3 (Maszkolt! Terpsta-féle szekvencia) [COM, EXE]
49CD21*5CD2181EBE700727B8CC1F913CB
Dark Avenger/Eddie (IBM-SCAN) [COM, EXE]
E800005E81EE6B00FC2E81BC05074D5A740EFA8BE681C40808FB3B26060073
CD5006561E8BFE33
Datacrime 1168 [COM]
8B36010183EE038BC63D00007503E9FE00
Datacrime 1280 (IBM-SCAN) [COM]
8B36010183EE038BC63D00007503E90201
Datacrime II (IBM-SCAN) [COM, EXE]
5E81EE030183FE00742A2E8A9403018DBC2901
Datacrime II [COM, EXE]
5E81EE030183FE00742A2E8A94
Datacrime IIb [COM, EXE]
2E8A0732C2D0CA2E880743E2F3
DataLock [COM, EXE]
680001C3B4BECD213D3412C31EA12C00508CD8488ED8812E
DBASE [COM]
FB750A86E09DCFE9CE06E9810381FF0AFB742E3D004B

December 24th [EXE]
6803A32400A16A03051000A31C0090
Den Zuk [BOOT]
FA8CC88ED88ED0BC00F0FBB8787C50C3
Devil's Dance [COM]
AD03F3A426C706000003015E1E068CC048
DisCom [COM, EXE]
6B008CC88ED88EC0B43FCD21498BFABE0500F3A67507B43E
Disk Killer (Ogre) [BOOT]
D2F7361A0088163F01A34101C3A14101
Do-Nothing [COM]
C21ECD707219A36F02B442B0028B1E6F02B90000
Do-Nothing-2 [COM]
C21ECD707219A36F00B442B0028B1E6F00B90000
Durban (SAT14) [COM, EXE]
9D02A4E2FD06B82135CD211F891E5302
EDV [BOOT]
DB8ED8C7078118813F8118740D2D00103D00B875ECB800A8
Falling Letters/Potyogós boot [BOOT]
31C0CD13B80202B90627BA0001BB00208EC3BB0001CD139A00010020
Fellow [EXE, COM]
FB039C0650EA0000000033C08ED88F0600008F060200FB
Fish(6) [COM, EXE]
8F06DB0E2E8326DB0EFE2E803EDA0E0075112EFF36DB0E
Flash [COM, EXE]
4ACD218CDA03D3428EC2B455CD2156BF000183EE080E1FB9D002
Flip COM/EXE (Terpsta-féle maszkolt szekvencia!) [COM, EXE]
0EBB*21FB9*2B2??81C1*2EB
Flip — rezidens (Terpsta-féle maszkolt!) [Normál memória és HIMEM]
505152B402CD1A80FD1075
Flip Boot [BOOT]
FBB80300E81F0006B8420050B8C007
Form Boot [BOOT]
B9FF00FCF3A506B89A0050BBFE01B80102
Friday the 13th [COM, EXE]
1E8BECC746100001E80000582DD700B104D3E88CCB03C32D100050
Fu Manchu A [COM, EXE]
72454D484F72
Fu Manchu (2086) B [COM, EXE]
8ED0BC200950B8230250CBFC06
Ghost — Boot átíró verzió [BOOT]
7D83EA247211800EF77D0156579090905F5E8026F77DFE
Ghost — COM verzió [COM]
F281C60A00BF0001B90300F3A48BF2B430CD213C007503E9C601
Golden Gate C [BOOT]
A717800FADBDAD5507173384

Golden Gate C2 [BOOT]
A717DDAFF001233907173385
HAHAHA [COM]
2A546869732046696C6520486173204265656E20496E666563746564204279 20
Halloechen [COM, EXE]
4B00C7065B005555BA4900C706FB003000E8A1FEFF064A01
Icelandic/Saratoga [COM, EXE]
A3030003D8438EC333F633FF0E1FB9D007
Icelandic (IBM-SCAN) [COM, EXE]
8CDB4B8EDBB04DA20000A103002D8000A3030003D8438EC333F633FF0E1FB 9D007
Icelandic/Saratoga II [COM, EXE]
26C6067F03FFB452CD212E8C066D02268B47FE8EC026030603004040
Itavir [COM, EXE]
9B00908A16D70B80FA02741B1E52B41CCD218A075A
Jerusalem (PLO/sUMsDos) [COM, EXE]
FC062E8C0631002E8C0639002E8C063D002E8C0641008CC0
Jerusalem related I. (Vírusátirat, HIMEM-ben is működik!) [COM, EXE]
0510008EC00E1FB9??07D1E933F6
Jerusalem II. (Vírusátirat, HIMEM-ben is működik!) [COM, EXE]
50B8C50050CBFC062E8C0631002E8C0639002E8C063D002E8C
JoJo-1701 [COM]
6DB42CCD2180FD13720AB8CD20A3000153E9C702
Joshi [BOOT]
022D2100BF0000BE007C03F003F8B979012BC8
July13 [EXE]
A012003490BE1200B9B1042E300446E2FA
Khetapunk (1392) [COM, EXE]
2F01C3E80700E83A00E86600C3BF0001A1030180000905E5051B82135CD218C
Khetapunk (1392) (Javított rövid szekvencia) [COM, EXE]
2F01C3E80700E83A00E86600C3BF0001A10301
Kukac [COM]
83EE03BAC10281EA000103F28B1C8B4C02
LDV [BOOT]
A406B8330150CBBB4C008B0F8B5702
Lehigh [COM]
505380FC4B740880FC4E7403E977018BDA807F013A75058A07EB07
Liberty [COM, EXE]
93E8CD0072C2BB13012E813F4D5A7505
Lisbon 648 [COM]
2FCD21895C00908C44029007BA5F009001F2B41A
Marti Bros [BOOT]
FA8CC88ED88ED0BC00F0FBE82700FA31C08ED8A113042D0700
MicroDot [BOOT]
010000C706D9010800C606DB0102B9040051
Mirror [COM, EXE]
CD215A59B80157CD21B43ECD21B82135CD21

Mix 1 [COM, EXE]
2933C08EC02680261704
Mix 1B [COM, EXE]
2733C08EC02680261704
Monxla (Time) (Ugyanaz a memóriakeresésési szekvenciája) [COM]
B42ACD2180FA0D7530B42CCD2180FA3C
Murphy [COM, EXE]
4BCD217203E9??015E568BFE33C0501FC4064C002E
News Flash [COM]
B43BCD21463B36ED027CE1803EF00200740AB8BA0250
Nichols [BOOT]
DD0DDF0FDD0FFF0A000ABA00
Ohio [BOOT]
B106D3E08EC0BE007C33FFB90410FCF3A406B8000450CBB90400
Ohio (Rövid szekvencia mutációszűréshez) [BOOT]
B106D3E08EC0BE007C33FFB90410FCF3A406B8000450
Oropax [COM]
8200C7069C007D098C0E9E00C7068400EE088C0E8600FB2E803E070100
Ping Pong vagy Typo Boot [BOOT]
8ED8A113042D0200A31304B106D3E02DC0078EC0BE007C8BFEB90001
Ping Pong/286 [BOOT]
7D807426BEBE81B90400807C0401740C807C04047406
Plastique (Invader) [BOOT, EXE, COM]
1304B106D3E08ED8833E400EFE751AB8540F1E
Polimer [COM]
E90C01B000B40ECD21BAC000B41ACD21
Polimer (Javított elsődleges szekvencia) [COM]
8B0E6C018CD80500108ED8B440CD21
Pretoria (June14) [COM]
C933D2E85BFFE81200B440BA0001
Prudents [EXE]
2F040175D00E0E1F07BED3042BC92E8A0446410AC0
PSQR [COM, EXE]
A526C606FE03CB580510008EC00E1FB9B306D1E9
PSQR (Javított rövid szekvencia) [COM, EXE]
A526C606FE03CB580510008EC00E1FB9
Print Screen [BOOT]
DBB801038A365F01B90100CD6DE824005A595F5E5B
Shake [COM]
5E50E800005EB80342CD213D34217503
Slowdown [COM, EXE]
DE909081C61B00B990062E8034
Solano [COM]
175858BF00012E893E2101582EA32301
Staf [COM]
E80AFFBA8F02E820FFE801FFB80057CD215152B000

Stoned (Marijuana) [BOOT]
1E5080FC02721780FC0473120AD2750E33C08ED8A03F04A8017503E80700
Stoned/2 [BOOT]
120AD2750E33C08ED8A03F04A8017503E80700
Sunday [COM, EXE]
C80510008ED0BC5D0650B8C40050CBFC062E8C063100
Sunday/2 [COM, EXE]
C80510008ED0BCBE0650B8C40050CBFC062E8C063100
Suriv 1.01 [COM]
81F9C407721B81FA0104
Suriv 2.01 [EXE]
81F9C407722881FA0104
Suriv3 [COM, EXE]
4F0026A0FE032EA2510026C706FC03F3A526C606FE03CB58
Suomi (Terpsta-féle maszkolt szekvencia) [COM]
DDBFA80390EB03*38B87EE03EB02*281C34400EB04*43101EB03
Sylvia [COM, EXE]
8D36030133C933C0AC3C1A7404
Syslock [COM, EXE]
D1E98AE18AC13306140031044646E2F25E5958C3
Svir (S for stupid) [EXE]
E788261900A11D00A32100A11B00A32300C7061B000000
Taiwan [COM]
B90800BEBC03BF00F8FCF3A4B9C4028B364801
Taiwan-2 [COM]
B90800BEDF03BF00F8FCF3A4B9E7028B364001
Töltögető (Nemzetközi nevén: Filler) [BOOT]
26813F5224740BCD13
Turbo @ (Turbo Kukac) [COM]
CD20E80000905E5051B021B435CD21
TP06VIR [COM]
7A75772E833E1200069073922EA10C002EA3DD042E
TP16VIR [COM]
7A7403E98F002E803E16001073852E8A0E17002EA11000
TP23VIR [COM, EXE]
7A7406E98C00E9A201B417F6061B00027402FEC438262200
TP24VIR átirat (Maszkolt szekvencia Terpsta nyomán) [COM, EXE]
7A7406E98C00E99601B4??F606??00027402FEC43826
TP41VIR átirat (Maszkolt szekvencia Terpsta nyomán) [COM, EXE]
7A75*300807E00007507F606??00027401403906020O
Twelve Tricks Trojan Dropper [COM, EXE]
BE640231944201D1C24E79F7
Twelve Tricks Trojan [BOOT]
8CC88ED0BC007C8BF48EC08ED850
Vacsina [COM, EXE]
DA012E890E0800B8014380E1FECD2173

Vacsina EXE2COM konverzió (Első fertőzési lépcső) [COM]
03C8894FFB8B0E160103C8894FF78B0E1001894FF98B0E1401894FF58B3E1801
Vacsina EXE2COM konverzió (Rövid azonosító Terpstrától) [COM]
03C8894FFB8B0E160103C8894FF78B0E1001894FF98B
Vcomm [EXE]
7D02B440CD21E83E00A19B02A33602A19D02A334021E
Victor (Azonos a memóriakereső szekvencia is) [COM, EXE]
BCF308B42CCD2189167200B42CCD218ACA80E10FD3067200
Vienna „A" (DOS 62) [COM, EXE]
8BFE81C71F008BDE81C61F00
Vienna „B" (DOS 62) [COM, EXE]
8BFE83C71F908BDE83C61F90
Virdem [COM]
B200B40ECD21B43B8D16DF03CD21EB4C90B43B8D16DF03
Vírus-90 [COM]
C5030133C033DBB909008D561289D6030043
VHP623 [COM]
2FCD21891C8C4402B82435CD21899C8F008C84910007B82425
VHP435 [COM]
5B83EB18FC8D37BF0001B90300F3A48BF3558BEC83EC7C
VHP348 [COM]
5BBF00015750FC8D77FAA5A48BF38DAFD001B82435CD21
VP [COM]
290332E43A062A037503E94902403D
V1024 [COM, EXE]
4A8EC233FFB943008B55022BD13BD0723CFA26294D03895502
Whale (Terpsta féle memóriakeresési szekvencia)
[Normál memória és HIMEM]
252E890E64255B2E8B0783C3025389C132ED2E302743E2FA
Whale mutánsa (NAV-ból, a Whale.def alapján) #1 [COM, EXE]
2907E2FA5B59EB2A5BFC53C30E1FE8F7FF81EBA323B9C111
Whale mutánsa (NAV-ból a Whale.def alapján) #2 [COM, EXE]
371083C301E2F8585B5956BE6625F8FF14F85E43E82900
Whale mutánsa (NAV-ból a Whale.def alapján) #3 [COM, EXE]
37261383C303E2F78BCB598BD959B460EB1D56E80200
Whale mutánsa (NAV-ból a Whale.def alapján) #4 [COM, EXE]
3786F283C301E2F55AFB5B59FF166625E803004033DE
Whale mutánsa (NAV-ból a Whale.def alapján) #5 [COM, EXE]
37964083C303E2F78CC0588BD859B450EB1E56FDE80200
Whale mutánsa (NAV-ból a Whale.def alapján) #6 [COM, EXE]
49434975F7FF3666258F0699255B59EB03E82F00FF16
Whale mutánsa (NAV-ból a Whale.def alapján) #7 [COM, EXE]
4983C30249C35AE8F4FF742EEBF9520E1FE8230081EA
Whale mutánsa (NAV-ból a Whale.def alapján) #8 [COM, EXE]
49F61F83C30249C35DE8F4FF7430EBF9550EF81FE82300
Whale mutánsa (NAV-ból a Whale.def alapján) #9 [COM, EXE]
5B415956BE6625FF14F85E42505A90E80100F85B81EB9F23

Whale mutánsa (NAV-ból a Whale.def alapján) #10 [COM, EXE]
5B5955FF3666255D3EFFD55DE80000B984235B81EBB623
Whale mutánsa (NAV-ból a Whale.def alapján) #11 [COM, EXE]
5B59B440E8BA01EB0C5B530E1FC3E82A0075FBEBEBE8F1FF
Whale mutánsa (NAV-ból a Whale.def alapján) #12 [COM, EXE]
5BB44059E8BA01EB0C5B0E1F53C3E8290075FBEBEBE8F1FF
Whale mutánsa (NAV-ból a Whale.def alapján) #13 [COM, EXE]
67254EFF14E8020033DE81F676185B5E81EB9F23B98523
Whale mutánsa (NAV-ból a Whale.def alapján) #14 [COM, EXE]
852381EBA923FE0F43E2FB558BEB81C58E0033C03E807E0001
Whale mutánsa (NAV-ból a Whale.def alapján) #15 [COM, EXE]
91FF166625EBEE5BB985230E81EB9F231F8A47FFFEC8
Whale mutánsa (NAV-ból a Whale.def alapján) #16 [COM, EXE]
9383EB1DB9C3118A072847FF4B4BE2F7803E3324017416
Whale mutánsa (NAV-ból a Whale.def alapján) #17 [COM, EXE]
93B9C31183EB1E8A170057FF4BF54BE2F6803E3324017415
Whale mutánsa (NAV-ból a Whale.def alapján) #18 [COM, EXE]
CA8EDAE80300D7EBF65A81EA9D23F987DAB98A2CF881F10F0F
Whale mutánsa (NAV-ból a Whale.def alapján) #19 [COM, EXE]
D7585B59FF166625E80300BB01565B81EB9F23B93489
Whale mutánsa (NAV-ból a Whale.def alapján) #20 [COM, EXE]
DB1F81C361DCE81E00BA02008137060403DAE2F881C38D00
Whale mutánsa (NAV-ból a Whale.def alapján) #21 [COM, EXE]
DB1F81C361DCE81F00B8020081379A239001C3E2F781C38D00
Whale mutánsa (NAV-ból a Whale.def alapján) #22 [COM, EXE]
DB5B81EB9F23E81E00B802008137380101C3E2F881C38D00
Whale mutánsa (NAV-ból a Whale.def alapján) #23 [COM, EXE]
DC5901CB0EB9C4111FFEC943812FFE0043E2F85689DE81C68D00
Whale mutánsa (NAV-ból a Whale.def alapján) #24 [COM, EXE]
DC5958935891B43FFEC4E8810158EBD28CCB8EDB5A52C3
Whale mutánsa (NAV-ból a Whale.def alapján) #25 [COM, EXE]
DCB986230E33C81F8037E801C32BC875F781C38F00FE0F
Whale mutánsa (NAV-ból a Whale.def alapján) #26 [COM, EXE]
DCB9C1118B0743430107E2FA81C39200807F010174E106
Whale mutánsa (NAV-ból a Whale.def alapján) #27 [COM, EXE]
DDEB2AE80100C359BB61DC01CB0EB9C3101FFEC5290F
Whale mutánsa (NAV-ból a Whale.def alapján) #28 [COM, EXE]
DFE82B0087D381C361DCB9C311E8E0FFF6063324FE74E1
Whale mutánsa (NAV-ból a Whale.def alapján) #29 [COM, EXE]
E6FF75FB585BFB59FF3666258F069A25FF169A25E80000
Whale mutánsa (NAV-ból a Whale.def alapján) #30 [COM, EXE]
F9595B87CBE8B501EB078CC88ED8E80200EBF7582D9C23
W13 Family [COM]
D681C60000FCB90300BF0001F3A48BFAB430CD213C007503
XA1 (Tannenbaum) [COM]
FA8BEC5832C08946028146002800

XA1 (Boot) [BOOT]
5B83C30D8CC88ED8E81500EBFE
Yale [BOOT]
BB40008EDBA11300F7E32DE0078EC00E1F81FF56347504FF0EF87D
Yankee Doodle 2772 [COM, EXE]
9F83C4049E7303E9F002B8004233C933
Yankee Doodle 2885 [COM, EXE]
9F83C4049E7303E97A0233C933
Yankee Doodle/Music (IBM-SCAN) [COM, EXE]
E800005B81EBD4072EC6875C00FFFC2E80BF5B00007418BE0A0003F3BF0001
B92000F3A40E2EFFB76400061E50EB138CDA83C2102E03162000522EFF361E
00061E5053BB2C00F8B803C6CD215B7307581F07E898FFCB
Yankee-Go-Home [EXE]
D80E1FBE370881EE030103F38904BE390881EE03
Zapper [BOOT]
FC02721780FC04731222D2750E33C08ED8A03F04A8017503
Zero-Bug (Palette) [COM]
5A45CD602EÇ606250601902E803E2606
V277 [COM]
3FCD210515012EA30F01813E1701554D741633C98BD1B80042
V299 [COM]
3FCD21052B012EA30F01813E2D014956742533C98BD1B80042
V345 [COM]
3FCD21055901902EA30F01813E5B014956741633C98BD1B80042
V512 (4th Bulgarian) [COM, EXE]
B830CD21BE04008EDE80FC1EC5440872
V512X (Memóriában is azonos szekvencia, normál és HIMEM) [COM]
CF8EC33B158E1D8B154A8EDA8BF18BD7B128F3A58EDB
V627 [COM]
2FCD21891C8C440207BA5F009003D6B41ACD210656
333 [COM]
9452028BFAB90300CD21803DE97405E87E00F8
333 (Változat) [COM]
EE0B018BACA00181C503018D94A20133C9B44ECD21727A
405 [COM, EXE]
B8000026A2490226A24B0226A28B0250B419CD2126A24902B4470401
537 [COM, EXE]
8A0789D3B90200B600CD26
541 [COM, EXE]
8A078BDAB90200B600CD26
648 [COM]
FC8BF281C60A00BF0001B90300F3A48BF2B430CD213C007503E9C701
648 (Változat) [COM]
A5A58BF3B44E8D5690B103EB168A46EA241F3C1F740B836EEE0A
765 [COM]
EF408EC70E1FB90004FCBF0000F3A481EC0004
847 [COM]
4FBA5F02CD217202EBA0BA8000B41A

867 [COM]
D681C2050033C9B44FCD2173EF
1253 [BOOT, COM]
CA03562D751726813ECC03314C750E36C7068001000036
1381 [EXE]
7FB91C008B1E27008D160900CD217211813E1B004D5A7409A11700
1624 [EXE]
DE058CD80E1FBEE60681EE030103F38904BEE80681EE030103F3
17XX [COM]
F6872A0101740F8DB74D01BC
1704(B) vagy 17Y4 [COM]
FA8BECE800005B81EB31012EF6
1704-B (IBM-SCAN) [COM]
FA8BEE800005B81EB31012EF6872A0101740F8DB74D01BC850631343124464C
75F8
17Y4 (IBM-SCAN) [COM]
FA8BCDE800005B81EB31012EF6872A0101740F8DB74D01BC85063134312446
4C75F8
1704-C/1704-Format [COM]
F6872A0101740F8DB74D01BC850631343124464C77F8
1971 [COM, EXE]
B7003B445B7219B8907EE8C800B80835CD21895C5D
1813 (IBM-SCAN) [COM, EXE]
8ED0BC000750B8C50050CBFC062E8C0631002E8C0639002E8C063D002E8C06
41008CC0
V2000 (Eddie 2) [COM, EXE]
B413CD2F5A1F2E8994A7072E8C9CA9072E
2086 (IBM-SCAN) [COM, EXE]
8ED0BC200950B8230250CBFC062E8C062C002E8C0634002E8C0638002E8C06
3C008CC0
2730 [COM, EXE]
9177917AA4B7570056000000
2930 [COM, EXE]
2906E8E005B419CD218884E300E8CE048A95E2000E1F7509
2930 (IBM-SCAN) [COM, EXE]
E82906E8E005B419CD218884E300E8CE048A95E2000E1F7509
3066 [COM, EXE]
7106E82806B419CD2189B451018184510184088C8C5301
3445 [COM, EXE]
5983E91F8CC8*5F7E303C183D200
4096 [COM, EXE]
875EECFCC383C30381FBCC0272E95BE8890AE421
5120 [COM, EXE]
FBA10C002EA30001A10E002EA302018C1E2200
9800:0000 (1554) [COM, EXE]
9B00FFFF7203A39B00A19B003DFFFF741FB000
9800-2 [COM]
83EE03BA860103F28B1C8B4C02

ÖSSZEFOGLALÓ VÍRUSTÁBLÁZAT

A McAfee Associates 1992. márciusi listája alapján

Az alábbi táblázat a Scan V89 programmal azonosítható, a PC-kompatibilis számítógépeken működő vírusfajták főbb ismérveit összegezi. A vírusok általában a Clean programmal kiirthatók. A szögletes zárójelben megadott azonosító kódnál csillaggal(*) jelöltük azokat a kivételeket, amikor a SCAN /D, SCAN /D /A vagy az MDISK /P paranccsal lehet megszüntetni a fertőzést.

Önálló vírusok száma: 534

Átírt vírusváltozatok száma: 729

Ismert vírusok száma együtt: 1263

JELMAGYARÁZAT

Méretnövekedés:

Vált. = Változó hosszúságú

N/A = A vírus nem fűződik hozzá az állományhoz

Nincs = A vírus nem változtatja meg a fájlméretet, mert a fájl vége jelhez kapcsolódik

Felülír = A vírus felülírja a fájl elejét, a fájlméret nem változik

Számértékek = A bájtokban megadott méretnövekedés, amennyivel a fájl nagyobb lesz, ha megfertőződik

A károkozás módja:

B = Megrongálja vagy felülírja a bootszektort

D = Megrongálja az adatállományokat

F = Részben vagy teljesen újraformázza, illetve felülírja a lemezt

L = Közvetve vagy közvetlenül megrongálja a fájlkapcsolatokat

O = Az operációs rendszer futtatási műveleteit befolyásolja

P = Tönkreteszi a programállományokat és az átfedő (overlay) fájlokat

Jelölések:

x = Igen

. = Nem

Megjegyzés:

A „crash", azaz „zúzó" típusú vírus futtatásakor rendszerösszeomlást okoz, emiatt egyéb tulajdonságait nem lehet megismerni. (Elképzelhető, hogy más rendszerek vagy más környezeti feltételek között viszont működik.)

MEGNEVEZÉS			MÓD-SZER			FERTŐZÉS HELYE								
Név	Változatok száma	Rövidített névkód	Lopakodó technika	Önmagát titkosítja	Memóriába installálódik	COMMAND.COM	.COM állományok	.EXE állományok	Overlay állományok	Floppy bootszektora	Merevlemez bootszektora	Partíciós tábla	A fertőzött program méretnövekedése	KÁROKOZÁS MÓDJA
1008		[1008]	.	x	x	x	x	.	.	.	.	.	1008	O P D L
1014		[Vienna]	.	.	x	x	x	.	.	.	.	.	1014	O P L
1024	(2)	[Alf]	.	.	x	x	x	.	.	.	.	.	1024	O P
1033		[1033]	.	.	x	.	.	x	x	.	.	.	1033	O P L
1024PSRC		[PS10]	.	.	x	x	x	.	.	.	.	.	1024	O P
1067		[1067]	.	.	x	x	x	.	.	.	.	.	1067	O P L
1210		[1210]	.	.	x	.	x	.	.	.	.	.	1210	O P L
1241		[1241]	.	.	x	x	x	.	.	.	.	.	1241	L O P
1244		[1244]	.	.	x	.	x	x	x	.	.	.	1244	L O P
1253-Boot		[1253]*	.	.	x	.	.	.	.	x	x	x	N/A	B O P D L
1253-COM		[1253]	.	.	x	x	x	.	.	.	.	.	1253	O P D L
1260	(4)	[V2P2]	.	x	.	.	x	.	.	.	.	.	1260	P
1280		[Crime-B]	.	x	.	.	x	.	.	.	.	.	1168	P F
1376		[1376]	.	.	x	x	x	x	x	.	.	.	1376	O P L
1381		[1381]	.	.	.	.	.	x	x	.	.	.	1381	O P
1385		[1385]	.	.	x	x	x	.	.	.	.	.	1385	O P L
1392		[1392]	.	.	x	x	x	x	.	.	.	.	1392	O P L
1559/1554	(2)	[1559]	.	x	x	x	x	x	.	.	.	.	1554	O P L
1575/1591	(5)	[15xx]	.	.	x	x	x	x	.	.	.	.	Vált.	O P L
1605	(2)	[Jeru]	.	.	x	x	x	x	.	.	.	.	1605	L O P D
1661		[1661]	.	.	x	x	x	.	.	.	.	.	1661	O P L
1677		[1677]	.	.	x	x	x	.	.	.	.	.	1677	O P L
1720	(4)	[1720]	.	.	x	.	x	x	x	.	.	.	1720	F O P L
1840		[Alf]	.	.	x	.	.	x	x	.	.	.	1840	O P L D
191		[Tiny]	.	.	.	x	x	.	.	.	.	.	191	L O P
1963		[1963]	x	.	x	x	x	x	x	.	.	.	1963	O P L D
1971/8 Tunes	(2)	[1971]	.	.	x	.	x	x	x	.	.	.	1971	O P

MEGNEVEZÉS			MÓD-SZER			FERTŐZÉS HELYE								
Név	Változatok száma	Rövidített névkód	Lopakodó technika	Önmagát titkosítja	Memóriába installálódik	COMMAND.COM	.COM állományok	.EXE állományok	Overlay állományok	Floppy bootszektora	Merevlemez bootszektora	Partíciós tábla	A fertőzött program méretnövekedése	KÁROKOZÁS MÓDJA
2330		[2330]	.	.	x	x	x	x	x	.	.	.	2330	O P L
2559		[2559]	.	.	.	.	.	x	.	.	.	.	2559	L O P
262		[262]	.	.	x	x	x	.	.	.	.	.	262	O P L
2622		[2622]	.	.	x	x	x	x	x	x	x	x	2622	O P L D
2930		[Spain]	.	.	x	.	x	x	.	.	.	.	2930	P
310		[310]	.	.	x	x	x	.	.	.	.	.	310	O P L
337		[337]	.	.	x	x	x	.	.	.	.	.	337	O L
3445		[3445]	x	x	x	.	x	x	.	.	.	.	3445	O P D L
365		[365]	.	.	x	x	x	.	.	.	.	.	365	O P L
370-B		[370]	.	.	.	.	x	.	.	.	.	.	Nincs	
382	(2)	[382]	.	.	.	x	x	x	.	.	.	.	Felülír	L O P
405		[Burger]	.	.	.	.	x	.	.	.	.	.	Felülír	
408		[408]	.	.	x	x	x	.	.	.	.	.	408	L O P
4096	(9)	[4096]	x	.	x	x	x	x	x	.	.	.	4096	D O P L
482		[482]	.	.	x	x	x	.	.	.	.	.	482	O P
487		[487]	.	.	.	.	x	.	.	.	.	.	Nincs	
510		[VHP]	.	.	.	x	x	.	.	.	.	.	510	O L
512	(5)	[512]	x	.	x	x	x	.	.	.	.	.	N/A	O P L
5120	(3)	[5120]	.	.	.	x	x	x	x	.	.	.	5120	O P D L
555		[BWish]	.	.	x	x	x	x	x	.	.	.	555	O P L
560		[560]	.	.	x	x	x	.	.	.	.	.	560	O P L
621		[621]	.	.	.	x	x	.	.	.	.	.	621	O P D
651		[Alf]	.	.	x	.	x	.	.	.	.	.	651	O P D
709		[709]	.	.	x	x	x	.	.	.	.	.	709	O P
733		[733]	.	.	.	x	x	.	.	.	.	.	733	O P D L
737		[737]	.	.	x	x	x	x	.	.	.	.	737	O P L
748		[748]	.	.	x	x	x	.	.	.	.	.	748	O D L

MEGNEVEZÉS			MÓD-SZER			FERTŐZÉS HELYE								
Név	Változatok száma	Rövidített névkód	Lopakodó technika	Önmagát titkosítja	Memóriába installálódik	COMMAND.COM	.COM állományok	.EXE állományok	Overlay állományok	Floppy bootszektora	Merevlemez bootszektora	Partíciós tábla	A fertőzött program méretnövekedése	KÁROKOZÁS MÓDJA
765		[765]	.	.	x	.	.	x	x	.	.	.	765	O P L
777		[777]	.	.	x	x	x	.	.	.	.	.	777	O P
7808		[7808]	.	.	x	x	x	x	x	.	.	.	7808	O P L D
789		[789]	.	.	x	x	x	.	.	.	.	.	789	O L
7th Son	(4)	[7S]	.	.	.	x	x	.	.	.	.	.	350	O P
812	(2)	[812]	.	.	x	x	x	x	x	.	.	.	812	O D
834/Arab		[Ar]	.	.	x	.	x	.	.	.	.	.	834	O P
855		[855]	.	.	x	x	x	x	x	.	.	.	855	O P L
903		[903]	.	.	x	x	x	.	.	.	.	.	903	O P
905		[905]	.	.	.	.	x	.	.	.	.	.	Nincs	
923		[923]	.	.	x	x	x	x	x	.	.	.	923	O P L D
Ada		[Ada]	.	.	x	x	x	.	.	.	.	.	2600	O P L
AGI-Plan		[AGI]	.	.	.	x	x	.	.	.	.	.	1536	O P L
Ah		[Alf]	.	.	x	x	x	.	.	.	.	.	1173	B L O P
AIDS Trojan	(13)	[Aids]	.	.	.	.	x	.	.	.	.	.	Felülír	
AirCop	(3)	[AirCop]	.	.	x	.	.	.	.	x	.	.	N/A	B O
Akuku	(2)	[Akuku]	.	.	.	x	x	x	.	.	.	.	891	L O P
Alabama	(3)	[Alabama]	.	.	x	.	.	x	.	.	.	.	1560	O P L
Alfa	(2)	[Alf]	.	.	x	x	x	x	x	.	.	.	1150	L O P
Amstrad	(7)	[Amst]	.	.	.	.	x	.	.	.	.	.	847	P
Anthrax-Boot	(2)	[Atx]*	.	.	x	.	.	.	.	.	.	x	N/A	B O P D
Anthrax-File	(4)	[Atx]	.	.	x	x	x	x	.	.	.	.	1206	O P D
Anti-D		[AD]	.	.	x	x	x	.	.	.	.	.	945	O P L
Anti-Pascal II	(4)	[AP-2]	.	.	.	x	x	.	.	.	.	.	400	B L O P
Anti-Pascal	(3)	[AP]	.	.	.	x	x	.	.	.	.	.	605	L O P
Anti-Tel		[A-Vir]	x	x	x	.	.	.	.	x	.	x	N/A	B F L O
Argentina		[Arg]	.	.	x	x	x	.	.	.	.	.	1249	O P D

MEGNEVEZÉS			MÓD-SZER			FERTŐZÉS HELYE								
Név	Változatok száma	Rövidített névkód	Lopakodó technika	Önmagát titkosítja	Memóriába installálódik	COMMAND.COM	.COM állományok	.EXE állományok	Overlay állományok	Floppy bootszektora	Merevlemez bootszektora	Partíciós tábla	A fertőzött program méretnövekedése	KÁROKOZÁS MÓDJA
Armagedon	(3)	[Arma]	.	.	x	x	x	.	.	.	.	.	1079	O P
ASP-472		[472]	.	.	x	x	x	x	x	.	.	.	472	L O P
AT144		[144]	.	.	.	x	x	.	.	.	.	.	144	O P
August 16		[A16]	.	.	.	x	x	.	.	.	.	.	631	O P
Australia		[Aust]	.	.	x	x	x	x	x	.	.	.	1433	O P L D
Azusa	(2)	[Azusa]	.	.	x	.	.	.	.	x	.	x	N/A	D O B L
A-403		[A-403]	.	.	x	x	x	.	.	.	.	.	Felülír	L O P
BackTime		[BT]	.	.	x	x	x	.	.	.	.	.	528	L O P
Bad Boy	(4)	[BB]	.	.	x	x	x	.	.	.	.	.	1000	O P D
BadGuy	(3)	[IB]	.	.	.	x	x	.	.	.	.	.	265	O L
Bandit		[Ban]	.	.	x	x	x	x	x	.	.	.	988	O D
Barcelona		[Barc]	.	.	x	.	x	.	.	.	.	.	1792	L O P
Beast		[Bea]	.	.	.	x	x	.	.	.	.	.	429	O P L
BeBe		[BeBe]	.	.	.	x	x	.	.	.	.	.	1004	O P D
Beeper	(2)	[Beep]	.	.	x	.	x	.	.	.	.	.	482	O P D
Best Wishes		[BWish]	.	.	.	x	x	x	x	.	.	.	1024	O P D
Beta		[Bet]	.	.	.	.	x	.	.	.	.	.	1117	L O P
Black Monday	(3)	[BMon]	.	.	x	x	x	x	x	.	.	.	1055	L O P D
Bljec	(8)	[Blj]	.	.	.	x	x	.	.	.	.	.	369	O P
Blood	(2)	[Blood]	.	.	.	x	x	.	.	.	.	.	418	L O P
Bloody!		[Bloody]	.	x	x	.	.	.	.	x	.	x	N/A	B O
Blood-2		[Blood]	.	.	.	.	x	.	.	.	.	.	427	O P D
Bob		[Bob]	.	.	x	x	x	.	.	.	.	.	718	O P L
Boys	(3)	[Boys]	.	.	x	x	x	.	.	.	.	.	500	O D
Brothers		[Bro]	x	.	x	.	x	x	x	.	.	.	2045	L O P
Burger	(28)	[Burger]	.	.	.	x	x	x	.	.	.	.	Felülír	
Burghofer		[Bgh]	.	.	x	x	x	.	.	.	.	.	525	L O P

MEGNEVEZÉS			MÓD-SZER			FERTŐZÉS HELYE								
Név	Változatok száma	Rövidített névkód	Lopakodó technika	Önmagát titkosítja	Memóriába installálódik	COMMAND.COM	.COM állományok	.EXE állományok	Overlay állományok	Floppy bootszektora	Merevlemez bootszektora	Partíciós tábla	A fertőzött program méretnövekedése	KÁROKOZÁS MÓDJA
Busted			.	.	.	x	x	.	.	.	.	.	Felülír	O P L
CADKill		[CK]	.	.	x	x	x	x	x	.	.	.	1163	O P D
Cancer		[Pix]	.	.	.	.	x	.	.	.	.	.	1480	O P D
Cannabis	(2)	[CB]	.	?	x	.	.	.	x	.	.	.	N/A	B L O
Cara		[Cara]	.	.	x	x	x	.	.	.	.	.	1024	F L O P
Carioca	(6)	[Carioca]	.	.	x	.	x	.	.	.	.	.	951	O P
Cascade/170x	(14)	[170x]	.	x	x	.	x	.	.	.	.	.	1701	O P
Casino		[Casino]	.	.	x	x	x	.	.	.	.	.	Nincs	O P L
Casper	(2)	[Casper]	.	x	.	x	x	.	.	.	.	.	1200	L O P D
Caz		[Caz]	.	.	x	x	x	x	x	.	.	.	1204	L O P
CB-1530		[1530]	.	.	.	x	x	x	x	.	.	.	1530	L O P
CD		[CD]	.	x	x	.	x	x	x	.	.	.	2161	O L D P
Chaos		[GenB]	.	.	x	.	.	.	.	x	x	.	N/A	B O D F
Cheeba	(2)	[CHB]	.	x	x	x	x	x	x	.	.	.	1683	L O P
Chemist		[Chm]	.	.	x	x	x	.	.	.	.	.	650	O P L
Christmas Tree		[XA1]	.	x	.	.	x	.	.	.	.	.	1539	F O P L
Christmas Violator		[Vienna]	.	.	.	x	x	.	.	.			Nincs	O P D
Cinderella		[Cind]	.	.	x	x	x	.	.	.	.	.	390	O P L
Color		[Col]	.	.	x	x	x	.	.	.	.	.	802	O P D
Copyright		[1193]	.	.	x	x	x	.	.	.	.	.	1193	L O P
Cop-Mpl		[COP]	.	.	.	x	x	x	.	.	.	.	1113	L O P
Cossiga		[Cos]	.	.	x	.	.	x	x	.	.	.	899	O P L
Cracker Jack		[CRJ]	.	.	.	.	x	.	.	.	.	.	Vált.	L O P
Crash		[Crash]	.	.	.	.	.	.	.	.	.	.		(Megj.)
Crazy Eddie		[Crazy]	.	.	x	?	x	x	.	.	.	x	Vált.	F L O P
Crazy Imp		[Imp]	x	.	x	x	x	.	.	.	.	.	1445	O P L
Cree4per		[Cre]	.	.	x	x	x	.	.	.	.	.	475	O P L

MEGNEVEZÉS			MÓD-SZER			FERTŐZÉS HELYE								
Név	Változatok száma	Rövidített névkód	Lopakodó technika	Önmagát titkosítja	Memóriába installálódik	COMMAND.COM	.COM állományok	.EXE állományok	Overlay állományok	Floppy bootszektora	Merevlemez bootszektora	Partíciós tábla	A fertőzött program méretnövekedése	KÁROKOZÁS MÓDJA
Crew-2480		[2480]	.	.	.	x	x	.	.	.	.	.	2480	L O P
CRF		[CRF]	.	.	.	x	x	.	.	.	.	.	270	O P
CSL	(2)	[CSL]	.	.	x	x	x	.	.	.	.	.	457	L O P
Curse Boot		[Curse]*	.	.	x	.	.	.	.	x	x	.	N/A	B O
Dada		[Dd]	.	.	x	.	.	x	x	.	.	.	1363	O P D
Damage		[Alf]	.	.	x	x	x	x	x	.	.	.	1063	O D P
Dark Avenger	(11)	[Dav]	.	.	x	x	x	x	x	.	.	.	1800	O P L
Darth Vader	(6)	[512]	.	.	x	x	x	.	.	.	.	.	Vált.	O L P
Datacrime II-B		[Crime-2B]	.	x	.	x	x	x	.	.	.	.	1917	P F
Datacrime-2		[Crime-2]	.	x	.	.	x	x	.	.	.	.	1514	P F
Datacrime/1168	(3)	[Crime]	.	x	.	.	x	.	.	.	.	.	1280	P F
DataLock		[Data]	.	.	x	x	x	x	x	.	.	.	920	O P
Day10		[D10]	.	.	.	x	x	.	.	.	.	.	674	F L O P
DBASE		[Dbase]	.	.	x	.	x	.	.	.	.	.	1864	D O P
Dedicated		[Dame]*	x	x	x	x	x	.	.	.	.	.	Vált.	O P L
Define		[Def]	.	.	.	x	x	x	.	.	.	.	Felülír	L O P
Deicide		[Dei]	.	.	.	.	x	.	.	.	.	.	Felülír	F L O P
Demolition		[Dmo]	.	.	x	x	x	.	.	.	.	.	1585	L O P
Demon	(5)	[Dem]	.	.	.	x	x	.	.	.	.	.	Felülír	F L O P
Den Zuk	(5)	[GenB]	.	.	x	.	.	.	.	x	.	.	N/A	O B
Destructor		[Dest]	.	.	x	x	x	x	x	.	.	.	1150	O P
Devil's Dance	(2)	[Dance]	.	.	x	.	x	.	.	.	.	.	941	D O P L
Dir		[Dir]	x	.	x	x	x	.	.	.	.	.	691	O P D
Dir-2/CD 1x	(3)	[D2]	x	x	x	x	x	x	x	.	.	.	1024	O L D P
Disk Killer	(4)	[Killer]	.	.	x	.	.	.	.	x	x	.	N/A	BOPDF
DM	(3)	[DM]	.	.	x	x	x	.	.	.	.	.	400	L O P
Dodo		[Dod]	.	.	x	x	.	.	.	.	.	.	408	O P L

MEGNEVEZÉS			MÓD-SZER			FERTŐZÉS HELYE								
Név	Változatok száma	Rövidített névkód	Lopakodó technika	Önmagát titkosítja	Memóriába installálódik	COMMAND.COM	.COM állományok	.EXE állományok	Overlay állományok	Floppy bootszektora	Merevlemez bootszektora	Partíciós tábla	A fertőzött program méretnövekedése	KÁROKOZÁS MÓDJA
Do Nothing		[Nothing]	.	.	x	.	x	.	.	.	.	.	608	P
Doodle	(14)	[Doodle]	.	.	x	.	x	x	.	.	.	.	2885	O P
Doom II		[Dm2]	.	.	x	.	x	x	.	.	.	.	2504	O P D L
Dot Killer		[Dot]	.	.	x	x	x	.	.	.	.	.	944	O P
Dutch		[Dt]	.	.	x	x	x	x	x	.	.	.	555	D O P
D-Tiny	(4)	[D-T]	.	.	x	x	x	x	.	.	.	.	124	L O P
EDV	(2)	[EDV]	x	.	x	.	.	.	.	x	x	x	N/A	B O
Einstein		[Ein]	.	.	x	.	.	x	.	.	.	.	878	L O P
Eliza		[El]	.	.	.	x	x	.	.	.	.	.	1193	L O P
EMF		[EMF]	.	.	.	x	x	.	.	.	.	.	404	O P L
Empire	(3)	[Emp]	.	x	x	.	.	.	.	x	x	.	N/A	O P
Enemy		[Enm]	.	.	x	x	x	x	x	.	.	.	1285	O P D
Enigma		[Enigma]	.	x	x	.	.	x	x	.	.	.	1755	O P
Error		[Arma]	.	.	.	.	.	x	x	.	.	.	628	O P
ETC		[ETC]	.	.	x	x	x	.	.	.	.	.	572	O D L P
Exterminator		[M45]	.	.	x	x	x	x	.	.	.	.	451	O L D
E-92		[E92]	.	.	x	x	x	.	.	.	.	.	728	O D L
Farcus		[Farc]	.	.	x	.	.	.	.	x	x	x	N/A	B O P L
Father Christmas		[VHP]	.	.	.	x	x	.	.	.	.	.	1881	O P
Fear		[Dame]*	.	x	x	x	x	.	.	.	.	.	Vált.	O P L
Feist		[Fst]	.	.	x	x	x	x	x	.	.	.	670	O P L
Fellowship	(4)	[Fellow]	.	.	x	.	.	x	.	.	.	.	1022	O P D L
FichV2		[Fv2]	.	.	x	x	x	.	.	.	.	.	Nincs	O P L
Filler		[Filler]	x	.	x	.	.	.	.	x	.	x	N/A	B F L O
Fingers		[Fing]	.	.	x	x	x	x	x	.	.	.	1322	O P D
Fish	(2)	[Fish]	x	x	x	x	x	x	x	.	.	.	3584	O P L
Flash		[Flash]	.	.	x	x	x	x	.	.	.	.	688	O P D L

MEGNEVEZÉS			MÓD-SZER			FERTŐZÉS HELYE								
Név	Változatok száma	Rövidített névkód	Lopakodó technika	Önmagát titkosítja	Memóriába installálódik	COMMAND.COM	.COM állományok	.EXE állományok	Overlay állományok	Floppy bootszektora	Merevlemez bootszektora	Partíciós tábla	A fertőzött program méretnövekedése	KÁROKOZÁS MÓDJA
Flip	(5)	[Flip]	.	x	x	x	x	x	x	.	.	.	2343	O P D L
Form	(4)	[Form]	.	.	x	.	.	.	.	x	x	.	N/A	B O D
Frere Jacques		[Mule]	.	.	x	.	x	x	x	.	.	.	1811	O P
Friday 13th COM		[Fri13]	.	.	.	.	x	.	.	.	.	.	512	P
Frogs		[Frogs]	.	.	x	x	x	.	.	.	.	.	1500	O P
Fu Manchu	(4)	[Fu]	.	.	x	.	x	x	x	.	.	.	2086	O P
F-Word		[FW]	.	.	x	x	x	.	.	.	.	.	417	O P D
Generic Boot		[GenB]	.	.	x	.	.	.	.	x	x	.	N/A	B L O
Generic MBR		[GenP]	?	.	x	.	.	.	.	.	.	x	Megj.	F L O
Gergana	(9)	[Gerg]	.	.	.	x	x	.	.	.	.	.	Vált.	L O P
Get Password 1		[Jeru]	.	.	x	.	x	x	x	.	.	.	1914	O P L
Ghost Boot		[Ghost]	.	.	x	.	.	.	.	x	x	.	N/A	B O
Ghost COM		[Ghost]	.	.	.	.	x	.	.	.	.	.	2351	B P
Goblin		[CRJ]	.	.	x	x	x	.	.	.	.	.	1951	O P L
Gosia		[Gs]	.	.	x	x	x	.	.	.	.	.	466	L O P
Gotcha	(4)	[Gtc]	.	.	x	x	x	x	x	.	.	.	806	O P L
Got-you		[GY]	.	.	.	.	.	x	.	.	.	.	3052	L O P
Grapje		[Gr]	.	.	.	x	x	.	.	.	.	.	1039	L O P
Greemlin		[Arf]	x	.	x	x	x	x	x	.	.	.	1146	O P L D
Growing Block		[Grb]	.	.	x	x	x	x	x	.	.	.	1446	O P L D
Guppy		[Guppy]	.	.	x	x	x	.	.	.	.	.	152	O P
Haifa		[Hf]	x	x	x	x	x	x	x	.	.	.	2351	L O P
Halloechen		[Hal]	.	.	x	x	x	x	x	.	.	.	2011	L O P
Halloween		[HW]	.	.	.	x	x	x	.	.	.	.	10000	L O P
Happy N. Y.		[HNY]	.	.	x	x	x	x	x	.	.	.	1865	O P
Happy		[Happy]	.	.	.	x	x	.	.	.	.	.	453	O P
Hary		[Hary]	.	.	x	x	x	x	.	.	.	.	997	O L P

MEGNEVEZÉS			MÓD-SZER			FERTŐZÉS HELYE								
Név	Változatok száma	Rövidített névkód	Lopakodó technika	Önmagát titkosítja	Memóriába installálódik	COMMAND.COM	.COM állományok	.EXE állományok	Overlay állományok	Floppy bootszektora	Merevlemez bootszektora	Partíciós tábla	A fertőzött program méretnövekedése	KÁROKOZÁS MÓDJA
Hastings		[Hst]	.	.	.	.	x	.	.	.	.	.	N/A	O L
Hero	(2)	[Hero]	.	.	x	x	x	x	x	.	.	.	506	O L P
Hero-394		[HrB]	.	.	x	.	.	x	.	.	.	.	394	L O P
Hitchcock		[Hitc]	.	.	.	x	x	.	.	.	.	.	1121	O P
Holland Girl	(6)	[Sylvia]	.	.	.	.	x	.	.	.	.	.	1332	P
Holo/Holocaust	(3)	[Hl]	x	.	x	x	x	.	.	.	.	.	3784	O P L D
Horse Boot		[DRP]	.	.	x	x	x	.	.	x	x	.	N/A	B P
Horse	(7)	[Hrs]	.	.	x	x	x	x	x	.	.	.	1154	O P L
HS		[HS]	.	.	x	x	x	x	x	.	.	.	4103	O P L
Hungarian		[Hng]	.	.	x	x	x	x	x	.	.	.	695	O L
Hybrid		[Hyb]	.	.	.	x	x	.	.	.	.	.	1306	O P L
Hydra	(12)	[Hyd]	.	.	.	x	x	.	.	.	.	.	Vált.	L O P
Hymn	(3)	[Hymn]	.	.	x	x	x	x	x	.	.	.	642	O P D
H-2		[H-2]	.	.	x	x	x	x	x	.	.	.	1962	O P L
Icelandic II		[Ice-3]	.	.	x	.	.	x	.	.	.	.	661	O P
Icelandic	(3)	[Ice]	.	.	x	.	.	x	.	.	.	.	642	O P
Icelandic-3		[Ice-3]	.	.	x	.	.	x	.	.	.	.	853	O P
IKV528		[I528]	.	.	.	x	x	.	.	.	.	.	528	O P
Incom		[Inc]	.	.	.	.	x	.	.	.	.	.	648	O P
Infinity		[Inf]	.	.	.	x	x	.	.	.	.	.	732	O P
Invader	(8)	[Invader]	.	x	x	.	x	x	x	x	x	.	4096	B L O P D
Invol		[Inl]	.	.	.	.	.	x	x	.	.	.	1413	O P L D
Iraqi Warrior		[Lisbon]	.	.	.	x	x	.	.	.	.	.	777	O P L D
Israeli Boot		[Iboot]	.	.	x	.	.	.	.	x	.	.	N/A	B O
Italian Pest	(3)	[Murphy]	.	.	x	.	x	.	.	.	.	.	1910	L O P
ItaVir	(3)	[Ita]	.	.	.	.	.	x	.	.	.	.	3880	O P L B
I-B	(5)	[IB]	.	.	.	x	x	.	.	.	.	.	Vált.	F L O P

MEGNEVEZÉS			MÓD-SZER			FERTŐZÉS HELYE								
Név	Változatok száma	Rövidített névkód	Lopakodó technika	Önmagát titkosítja	Memóriába installálódik	COMMAND.COM	.COM állományok	.EXE állományok	Overlay állományok	Floppy bootszektora	Merevlemez bootszektora	Partíciós tábla	A fertőzött program méretnövekedése	KÁROKOZÁS MÓDJA
Japan		[C-J]	.	.	x	x	x	x	.	.	.	.	600	O P
Jeff	(3)	[Jeff]	.	.	.	x	x	.	.	.	.	.	828	O P D F
Jerk	(2)	[Jrk]	.	.	.	x	x	x	.	.	.	.	1077	L O P
Jerusalem	(48)	[Jeru]	.	.	x	.	x	x	x	.	.	.	1808	O P
JoJo	(3)	[JoJo]	.	.	x	.	x	.	.	.	.	.	1701	O P
Joke		[JK]	.	.	.	.	x	.	.	.	.	.	Nincs	
Joker	(3)	[Joke]	.	.	x	x	x	.	.	.	.	.	Nincs	O P
Joshi	(4)	[Joshi]	x	.	x	.	.	.	.	x	x	x	N/A	B O D
July 13th		[J13]	.	x	.	.	.	x	.	.	.	.	1201	O P D L
June 16th		[June16]	.	.	.	x	x	.	.	.	.	.	1726	F O P L
Justice		[Justice]	.	.	x	x	x	.	.	.	.	.	1242	O P
JW2	(2)	[Jab]	.	.	x	x	x	x	.	.	.	.	1812	L O P
K		[K]	.	.	x	x	x	x	x	.	.	.	4928	O P L
Kalah		[Kl]	.	.	x	x	x	.	.	.	.	.	390	O P L D
Kamikaze		[Kami]	.	.	.	.	.	x	.	.	.	.	Felülír	
Karin		[Kar]	.	.	.	x	x	.	.	.	.	.	1090	L O P
Kemerov	(3)	[Keme]	.	.	.	x	x	.	.	.	.	.	257	L O P
Kemerov	(5)	[Keme]	.	.	x	x	x	.	.	.	.	.	Vált.	O L P D
Kennedy	(4)	[Tiny]	.	.	x	.	x	.	.	.	.	.	308	O P
Keypress	(4)	[Key]	.	.	x	x	x	x	.	.	.	.	1232	O P D
Kiev		[Kiev]	.	.	.	x	x	.	.	.	.	.	483	L O P
Kiev-1		[K1]	.	.	.	x	x	x	.	.	.	.		
Klaeren		[Kla]	.	x	x	x	x	x	x	.	.	.	981	O P L D
Korea	(4)	[Korea]	.	.	.	.	.	.	.	x	x	.	N/A	B O
Kukaturbo		[Kakt]	.	.	x	x	x	.	.	.	.	.		Felülír
KU-448		[KU]	.	.	.	x	x	.	.	.	.	.	448	L O P
Label		[Label]		.	.	x	x	x	.	.	.	.	.	Felülír

MEGNEVEZÉS			MÓD-SZER			FERTŐZÉS HELYE								
Név	Változatok száma	Rövidített névkód	Lopakodó technika	Önmagát titkosítja	Memóriába installálódik	COMMAND.COM	.COM állományok	.EXE állományok	Overlay állományok	Floppy bootszektora	Merevlemez bootszektora	Particiós tábla	A fertőzött program méretnövekedése	KÁROKOZÁS MÓDJA
Lazy		[Lazy]	.	.	x	x	x	.	.	.	.	.	720	O P
LCV		[LCV]	.	.	.	.	x	.	.	.	.	.		Nincs
Leapfrog	(3)	[Leap]	.	.	x	x	x	.	.	.	.	.	516	O P D
Leech		[Leech]	x	x	x	x	x	.	.	.	.	.	934	O P L D
Lehigh	(2)	[Lehigh]	.	.	x	x	.	.	.	.	.	.	N/A	P F
Leprosy	(7)	[Vip]	.	.	x	x	x	x	x	.	.	.	Felülír	
Leprosy-3	(4)	[Lep3]	.	.	.	x	x	x	.	.	.	.	Felülír	L O P
Leprosy-B		[Vip]	.	.	.	x	x	x	.	.	.	.	Felülír	
Lib1172	(2)	[1186]	.	.	x	x	x	.	.	.	.	.	1172	L O P
Liberty	(13)	[Liberty]	.	.	x	x	x	x	x	.	.	.	2862	O P
Lisbon	(2)	[VHP]	.	.	.	.	x	.	.	.	.	.	648	P
Little Pieces		[LPC]	.	.	x	.	x	x	.	.	.	.	1374	O P
Loa Duong		[Loa]	.	.	x	.	.	.	.	x	x	x	N/A	B O P L
Love Child	(3)	[LC]	.	.	x	x	x	.	.	.	.	.	488	O D
Lozinsky	(4)	[Loz]	.	.	.	x	x	.	.	.	.	.	1023	O P D
Lucifer		[Alf]	x	.	x	x	x	x	x	.	.	.	1086	O P D L
Macedonia		[Mce]	.	.	x	.	x	.	.	.	.	.	400	L O P
Malage		[Mlg]	.	.	x	x	x	x	x	x	x	x	2626	O P L
Maltese Amoeba		[Irs]	.	x	x	x	x	x	x	.	.	.	2505	O P L
Mannequin		[Mn]	.	.	x	x	x	x	x	.	.	.	778	O P L D
Manoal		[Mno]	.	.	x	x	x	.	.	.	.	.	957	L P
Manta		[Mant]	.	.	.	x	x	.	.	.	.	.	1077	L O P
Marauder		[Mar]	.	.	.	x	x	.	.	.	.	.	860	O P L
Mardi Bros.	(3)	[Mardi]	.	.	x	.	.	.	.	x	x	.	N/A	B O
Mface		[Mfc]	.	.	x	x	x	.	.	.	.	.	1441	O P L
MG	(4)	[MG]	.	.	x	x	x	.	.	.	.	.	500	L O P
MGTU	(4)	[MGTU]	.	.	.	x	x	.	.	.	.	.	273	O P D

MEGNEVEZÉS			MÓD-SZER			FERTŐZÉS HELYE								
Név	Változatok száma	Rövidített névkód	Lopakodó technika	Önmagát titkosítja	Memóriába installálódik	COMMAND.COM	.COM állományok	.EXE állományok	Overlay állományok	Floppy bootszektora	Merevlemez bootszektora	Partíciós tábla	A fertőzött program méretnövekedése	KÁROKOZÁS MÓDJA
Michelangelo		[Mich]	.	.	x	.	.	.	.	x	x	x	N/A	B O
Microbes		[Micro]*	.	.	x	.	.	.	.	x	x	.	N/A	B O D
Miky		[Miky]	.	.	x	x	x	x	x	.	.	.	2350	O P L
Mini	(4)	[M45]	.	.	.	x	x	.	.	.	.	.	Vált.	O P
Mir	(2)	[DAV]	.	.	x	x	x	x	x	.	.	.	1745	O P L
Mirror	(2)	[Mirror]	.	.	x	.	.	x	.	.	.	.	928	O P
MIX1	(4)	[Ice]	.	.	x	.	.	x	.	.	.	.	1618	O P
Mix2		[MX2]	.	.	x	x	x	x	x	.	.	.	2280	O P
Moctezuma		[MC]	.	.	x	x	x	x	x	.	.	.	2208	L O P
Mono		[Mo]	.	.	x	x	x	.	.	.	.	.	1063	L O P
Monxla	(3)	[VHP]	.	.	.	x	x	.	.	.	.	.	939	O P
Monxla-B		[VHP]	.	.	.	x	x	.	.	.	.	.	535	O P L
Mosquito		[Mosq]	.	x	x	.	.	x	x	.	.	.	1028	O D P
MPC		[MPC]	.	.	x	.	.	x	x	.	.	.	689	O P L
MPS 1.1		[M11]	.	.	.	x	x	.	.	.	.	.	469	L O P
MPS 3.1	(3)	[MPS]	.	.	.	x	x	.	.	.	.	.	640	L O P
MSTU		[MSTU]	.	.	.	x	x	x	.	.	.	.	531	L O P
Mule	(2)	[Mule]	.	x	x	x	x	.	.	.	.	.	4171	O P D
Multi		[M-123]	.	.	.	x	x	.	.	.	.	.	123	L O P
Mummy		[Mum]	.	x	x	.	.	x	x	.	.	.	1374	L
Munich		[Mun]	.	.	.	x	x	.	.	.	.	.	Nincs	O P
Murphy	(6)	[Murphy]	.	.	x	x	x	x	x	.	.	.	1277	O P
Music Bug	(11)	[MBug]	.	.	x	.	.	.	.	x	.	x	N/A	B O
Mutant	(8)	[Mut]	.	.	.	x	x	.	.	.	.	.	123	L O P
Mutation Engine		[Dame]*	x	x	x	x	x	.	.	.	.	.	Vált.	
M-128		[M128]	.	.	x	x	x	.	.	.	.	.	128	L O P
Necrophilia		[Nec]	.	.	x	x	x	.	.	.	.	.	Vált.	O P L D

MEGNEVEZÉS			MÓD-SZER			FERTŐZÉS HELYE								
Név	Változatok száma	Rövidített névkód	Lopakodó technika	Önmagát titkosítja	Memóriába installálódik	COMMAND.COM	.COM állományok	.EXE állományok	Overlay állományok	Floppy bootszektora	Merevlemez bootszektora	Particiós tábla	A fertőzött program méretnövekedése	KÁROKOZÁS MÓDJA
New Sunday		[Su2]	.	.	x	.	x	x	x	.	.	.	1636	O P L D
Newcom		[Alf]	.	.	x	x	x	.	.	.	.	.	3045	O P L
New-1701		[1701]	.	.	x	x	x	.	.	.	.	.	1701	L O P
Nina		[Nina]	.	.	x	x	x	.	.	.	.	.	256	O P D
Nines Compliment		[Nns]	.	.	x	x	x	.	.	.	.	.	705	O P L
Nobock		[Nbk]	.	.	.	.	x	.	.	.	.	.	440	L O P
Nomenclature	(4)	[Nom]	.	.	x	x	x	x	x	.	.	.	1024	O P D
NOP		[NOP]*	.	.	x	.	.	.	.	x	.	x	N/A	O B L
No-Int		[Stoned]	x	.	x	.	.	.	.	x	.	x	N/A	O B L
Off Stealth		[SVC50]	x	.	x	x	x	x	x	.	.	.	1689	O P D
Ohio		[Ohio]	.	.	x	.	.	.	.	x	.	.	N/A	B O
Ontario		[Ont]	.	x	x	x	x	x	.	.	.	.	Vált.	O P D
Oropax	(5)	[Oro]	.	.	x	.	x	.	.	.	.	.	2773	P O
P1	(7)	[P1r]	.	x	x	.	x	.	.	.	.	.	Vált.	O P D L
P529		[529]	.	.	x	x	x	.	.	.	.	.	529	O P D
Padded		[Pad]	.	.	.	x	x	.	.	.	.	.	2589	O P L
Pakistani Brain	(8)	[Brain]	.	.	x	.	.	.	.	x	.	.	N/A	B
Parasite		[Par]	.	.	.	.	x	.	.	.	.	.	Nincs	
Paris		[Paris]	.	.	.	x	x	x	x	.	.	.	4909	O P D L
Parity		[Parity]	.	.	.	x	x	.	.	.	.	.	441	O P D
PathHunt		[Ph]	.	.	.	.	x	x	.	.	.	.	1231	D L O P
Patient		[Pt]	.	.	x	.	x	x	x	.	.	.	1504	L O P
Payday		[Jeru]	.	.	x	.	x	x	x	.	.	.	1808	P
PC Flu		[802]	.	.	x	x	x	.	.	.	.	.	802	L O P
PCV		[PCV]	x	.	x	.	x	x	.	.	.	.	1904	L O P
Pentagon		[Pentagon]*	.	.	.	.	.	.	.	x	.	.	N/A	B
Perfume	(2)	[Fume]	.	.	.	.	x	.	.	.	.	.	765	P

MEGNEVEZÉS			MÓD-SZER			FERTŐZÉS HELYE								
Név	Változatok száma	Rövidített névkód	Lopakodó technika	Önmagát titkosítja	Memóriába installálódik	COMMAND.COM	.COM állományok	.EXE állományok	Overlay állományok	Floppy bootszektora	Merevlemez bootszektora	Particiós tábla	A fertőzött program méretnövekedése	KÁROKOZÁS MÓDJA
Pest	(8)	[Murphy]	.	.	x	x	x	x	x	.	.	.	1910	O P L
Phantom		[Phant]	.	.	x	x	x	.	.	.	.	.	2253	O P
Pig		[Pig]	.	.	x	x	x	.	.	.	.	.	407	O P L
Ping Pong-B	(7)	[Ping]	.	.	x	.	.	.	.	x	x	.	N/A	O B
Pirate		[Pir]	.	.	.	x	x	.	.	.	.	.	Felülír	L O P
Pixel	(5)	[Pix]	.	.	.	x	x	.	.	.	.	.	779	O P
Plague	(3)	[Plague]	.	.	.	.	x	x	.	.	.	.	Felülír	
Plastique	(9)	[Plq]	.	.	x	x	x	x	x	.	.	.	3012	O P D
Platinum		[Plt]	.	x	.	.	.	x	x	.	.	.	1489	O P L D
Plov		[Plov]	.	.	x	x	x	x	x	.	.	.	1000	L O P
Poem		[Pm]	.	.	x	x	x	.	.	.	.	.	1825	F L O P
Pogue		[Dame]*	.	x	x	.	x	.	.	.	.	.	Vált.	L O P
Polimer		[Polimer]	.	.	.	x	x	.	.	.	.	.	512	O P D
Polish 217		[P-217]	.	.	.	x	x	.	.	.	.	.	217	O P D
Polish-2		[Pol-2]	.	.	x	x	x	.	.	.	.	.	512	O P D
Possessed	(6)	[Poss]	.	.	x	x	x	x	x	.	.	.	2443	L O P
Pregnant		[Prg]	.	.	x	x	x	.	.	.	.	.	1199	L O P
Print Screen	(2)	[PrtScr]*	.	.	x	.	.	.	.	x	x	.	N/A	B O D
Prism		[Flip]	.	.	x	x	x	x	x	x	.	x	2153	B F L O P
Psycho		[Psc]	.	.	.	.	x	.	.	.	.	.	N/A	O
QMU		[QML]	.	.	x	x	x	.	.	.	.	x	1513	F L O P
QP3		[QP3]	.	.	x	x	x	x	x	.	.	.	1028	L O P
Quiet		[Qt]	.	.	x	x	x	.	.	.	.	.	2063	O P
Rage		[Rag]	.	.	.	x	x	.	.	.	.	.	575	L O P
Ram		[Ram]	.	.	x	.	x	x	x	.	.	.	Vált.	L O P
Raubkopi		[Raub]	.	.	.	x	x	x	.	.	.	.	Vált.	L O P
RedX	(2)	[Redx]	.	.	.	x	x	.	.	.	.	.	796	O P

MEGNEVEZÉS			MÓD-SZER			FERTŐZÉS HELYE								
Név	Változatok száma	Rövidített névkód	Lopakodó technika	Önmagát titkosítja	Memóriába installálódik	COMMAND.COM	.COM állományok	.EXE állományok	Overlay állományok	Floppy bootszektora	Merevlemez bootszektora	Partíciós tábla	A fertőzött program méretnövekedése	KÁROKOZÁS MÓDJA
Relzfu		[233]	.	.	x	x	x	.	.	.	.	.	233	O P L
Reset		[RST]	.	.	.	x	x	.	.	.	.	.	440	O P
RMIT		[RMIT]	.	.	.	x	x	x	.	.	.	.	Felülír	L O P
RNA		[RNA]	.	.	.	x	x	x	x	.	.	.	7296	O P L
RPVS		[453]	.	.	x	x	x	.	.	.	.	.	453	O P
R-10		[R10]	.	.	x	x	x	.	.	.	.	.	500	O P
R-11		[R-11]	x	.	x	x	x	.	.	.	.	.	700	O L D
Saddam		[Saddam]	.	.	x	x	x	.	.	.	.	.	919	O P D L
Saturday 14th	(3)	[Arma]	.	.	x	.	x	x	x	.	.	.	685	F O P L
SBC		[SBC]	.	.	x	.	x	x	x	.	.	.	Nincs	L O P
Scott's Valley		[2133]	.	x	x	.	x	x	x	.	.	.	2133	L O P D
Scream 2		[Sc2]	.	x	x	x	x	x	x	.	.	.	1324	O P L
Screaming Fist		[Scr]	.	.	x	x	x	x	x	.	.	.	711	O P L
SCT		[SCT]	.	.	.	.	x	.	.	.	.	.	Nincs	
Semtex		[Set]	.	.	x	x	x	.	.	.	.	.	1000	L O P
Sentinel	(3)	[Sent]	.	.	x	x	x	x	x	.	.	.	4625	L O P D
Sentinel-X		[BCV]	.	.	x	x	x	x	x	.	.	.	4625	L O P D
Sh		[Sh]	.	.	.	x	x	x	x	.	.	.	Felülír	L O P
Shadow	(3)	[Sha]	.	.	.	x	x	.	.	.	.	.	723	O P
Shake	(2)	[Shake]	.	.	x	.	x	.	.	.	.	.	476	O P
Simulati		[Sim]	.	.	.	.	x	.	.	.	.	.	1257	L O P
Sis	(2)	[Sis]	.	.	x	x	x	x	x	.	.	.	2380	O P L
Skism		[Jeru]	.	.	x	.	x	x	x	.	.	.	1815	O P
Slayer		[Slay]	.	.	x	.	x	x	x	.	.	.	5120	O P L D
Slow	(5)	[Slow]	.	x	x	.	x	x	x	.	.	.	1721	O P L
Small-38		[M45]	.	.	.	.	x	.	.	.	.	.	38	O P L
Smily		[Sml]	.	.	x	x	x	.	.	.	.	.	1987	O P L

MEGNEVEZÉS			MÓD-SZER			FERTŐZÉS HELYE								
Név	Változatok száma	Rövidített névkód	Lopakodó technika	Önmagát titkosítja	Memóriába installálódik	COMMAND.COM	.COM állományok	.EXE állományok	Overlay állományok	Floppy bootszektora	Merevlemez bootszektora	Partíciós tábla	A fertőzött program méretnövekedése	KÁROKOZÁS MÓDJA
Socha		[SCH]	.	.	.	.	x	.	.	.	.	.	Nincs	
Solano	(4)	[Sub]	.	.	x	.	x	.	.	.	.	.	2000	O P L
Something		[658]	.	.	x	x	x	.	.	.	.	.	658	L O P
Sorry	(3)	[Sorry]	.	.	x	x	x	.	.	.	.	.	731	O P
Sov	(3)	[Sov]	.	.	.	x	x	.	.	.	.	.	545	L O P
Spanish April Fool		[D28]	.	.	x	.	.	x	x	.	.	.	1400	O L P
Spanish		[Spain]	.	.	x	x	x	x	x	.	.	.	2930	O P L D
Spanz		[Spz]	.	.	x	x	x	.	.	.	.	.	663	O D
Spar		[Spar]	.	.	x	x	x	x	.	.	.	.	1255	O P
Spyer	(3)	[Spyer]	.	.	x	.	x	x	x	.	.	.	1181	O P
Squawk		[Sqa]	.	.	x	x	x	x	x	.	.	.	852	O P L
Squeaker		[Sqe]	.	.	x	x	x	x	x	.	.	.	1091	L O P
Staf		[Staf]	.	.	x	x	x	.	.	.	.	.	2083	O P L
Star Dot	(4)	[Sdot]	.	.	x	.	x	.	.	.	.	.	Nincs	O P L
Stardot-801	(3)	[I-F]	.	.	.	x	x	x	.	.	.	.	604	D F L O P
Stink		[Sti]	.	.	.	.	x	.	.	.	.	.	1254	L O P
Stoned	(26)	[Stoned]	.	.	x	.	.	.	.	x	.	x	N/A	O B L
Stone-90		[VHP]	.	.	.	x	x	.	.	.	.	.	961	O P
Striker		[STR]	.	.	x	x	x	.	.	.	.	.	461	D O P F
Subliminal	(3)	[Sub]	.	.	x	x	x	.	.	.	.	.	1496	O P
Sunday	(6)	[Sunday]	.	.	x	.	x	x	x	.	.	.	1636	O P
Sunday-2		[Su2]	.	.	x	x	x	x	x	.	.	.	2877	L O P
Suriv 402		[S-4]	.	.	x	x	x	.	.	.	.	.	897	L O P
Suriv A	(2)	[SurivA]	.	.	x	.	x	.	.	.	.	.	897	O P
Surrender		[Sur]	.	.	x	x	x	x	x	.	.	.	513	O P L
SVC 5.0/6.0	(2)	[SVC50]	x	x	x	x	x	x	x	.	.	x	3103	B L O P
Sverdlov	(2)	[Sv]	.	.	x	x	x	x	x	.	.	.	1962	O P

MEGNEVEZÉS			MÓD-SZER			FERTŐZÉS HELYE								
Név	Változatok száma	Rövidített névkód	Lopakodó technika	Önmagát titkosítja	Memóriába installálódik	COMMAND.COM	.COM állományok	.EXE állományok	Overlay állományok	Floppy bootszektora	Merevlemez bootszektora	Partíciós tábla	A fertőzött program méretnövekedése	KÁROKOZÁS MÓDJA
SVir	(4)	[Svir]	.	.	.	.	.	x	.	.	.	.	512	L O P
Swap Boot		[Iboot]*	.	.	x	.	.	.	.	x	.	.	N/A	B
Swiss 143		[S143]	.	.	.	x	x	.	.	.	.	.	143	O P D
SX		[SX]	.	.	x	x	x	.	.	.	.	.	800	L O P
Sylvia		[Sylvia]	.	.	x	.	x	.	.	.	.	.	1332	L O P
Sys		[Sys]	x	x	x	x	x	x	x	.	.	.	N/A	O P D
Syslock/3551		[Syslock]	.	x	.	.	x	x	.	.	.	.	3551	P D
S-847		[Pix]	.	.	x	.	x	.	.	.	.	.	850	O P
Taiwan	(11)	[Taiwan]	.	.	.	.	x	.	.	.	.	.	708	P
Taiwan3		[T3]	.	.	x	x	x	x	x	.	.	.	2905	O P D L
Taiwan4		[T4]	.	.	x	x	x	x	x	.	.	.	2576	O P D
Telecom Boot		[Tele]*	.	x	x	.	.	.	.	.	x	x	N/A	B P
Telecom File		[Tele]	.	x	x	.	x	.	.	.	.	.	3700	B P O D
Tequila		[Teq]	x	x	x	.	.	x	.	.	.	x	2468	O P F L
Terror	(3)	[Ter]	.	.	x	x	x	x	x	.	.	.	1085	O P F
Tester		[TV]	.	.	x	x	x	.	.	.	.	.	1000	O P
Timid		[Tmd]	.	.	.	x	x	.	.	.	.	.	306	L O P
Tiny 133		[T133]	.	.	.	x	x	.	.	.	.	.	133	O P
Tiny	(31)	[Tiny]	.	.	.	x	x	.	.	.	.	.	163	O P
Tokyo		[Tokyo]	.	.	x	.	.	x	.	.	.	.	1258	L O P
Tony		[Tn]	.	.	.	x	x	.	.	.	.	.	200	L O P
Topo		[Topo]	.	.	x	.	x	.	.	.	.	.	1542	L O P
Traceback	(3)	[3066]	.	.	x	.	x	x	.	.	.	.	3066	P
Traveller		[Trv]	.	.	x	x	x	x	.	.	.	.	1220	L O P
Troi		[Troi]	.	.	x	x	x	.	.	.	.	.	322	O P L
Tuesday	(2)	[Alf]	.	.	x	.	x	x	x	.	.	.	1163	O P L D
Tumen V0.5		[Tum5]	.	.	x	x	x	.	.	.	.	.	1663	O P L D

MEGNEVEZÉS			MÓD-SZER			FERTŐZÉS HELYE								
Név	Változatok száma	Rövidített névkód	Lopakodó technika	Önmagát titkosítja	Memóriába installálódik	COMMAND.COM	.COM állományok	.EXE állományok	Overlay állományok	Floppy bootszektora	Merevlemez bootszektora	Partíciós tábla	A fertőzött program méretnövekedése	KÁROKOZÁS MÓDJA
Tumen V2.0		[Tum2]	.	.	x	x	x	.	.	.	.	.	1092	O P L D
Turbo	(2)	[Pol-2]	.	.	x	x	x	.	.	.	.	.	448	L O P
Twin-351		[Twin]	x	.	x	.	x	x	.	.	.	.	351	L O P
Typo Boot	(2)	[TBoot]	.	.	x	.	.	.	.	x	x	.	N/A	O B
Typo/Fumble/712	(2)	[712]	.	.	x	.	x	.	.	.	.	.	867	O P
Ucender		[Uce]	.	.	x	x	x	x	x	.	.	.	1783	O P L
USSR 1049		[Alf]	.	.	x	x	x	x	.	.	.	.	1049	O P L
USSR 2144	(8)	[U2144]	.	x	x	x	x	x	x	.	.	.	2144	L O P D
USSR 256	(5)	[U256]	.	x	.	x	x	.	.	.	.	.	256	P D
USSR 257		[U257]	.	x	.	x	x	.	.	.	.	.	257	P D
USSR 3103		[SVC]	x	x	x	x	x	x	x	.	.	x	3103	B L O P
USSR 311		[U311]	.	.	.	.	x	.	.	.	.	.	321	O P
USSR 394		[U394]	.	x	.	x	x	.	.	.	.	.	394	P D
USSR 492		[U492]	.	.	.	.	x	.	.	.	.	.	492	O P
USSR 516	(4)	[Leap]	.	.	x	x	x	.	.	.	.	.	516	O P
USSR 600		[U600]	.	x	.	x	x	.	.	.	.	.	600	P D
USSR 696		[U696]	.	x	.	.	x	.	.	.	.	.	696	P D
USSR 707		[U707]	.	x	.	x	x	.	.	.	.	.	707	P D
USSR 711		[U711]	.	x	.	.	x	.	.	.	.	.	711	P D
USSR 830		[U830]	.	.	x	x	x	.	.	.	.	.	830	O P
USSR 948		[U948]	.	x	.	.	x	x	x	.	.	.	948	O P D
USSR	(11)	[USSR]	.	x	.	.	.	x	.	.	.	.	575	O P
V1028		[QP2]	.	.	x	x	x	x	x	.	.	.	1028	O P L
V125		[M128]	.	.	x	x	x	.	.	.	.	.	125	P
V1463		[1452]	.	.	.	x	x	.	.	.	.	.	1463	O P
V2000	(3)	[2000]	.	.	x	x	x	x	x	.	.	.	2000	O P L
V2100	(5)	[2100]	.	.	x	.	x	x	.	.	.	.	2100	O P D L

MEGNEVEZÉS			MÓD-SZER			FERTŐZÉS HELYE								
Név	Változatok száma	Rövidített névkód	Lopakodó technika	Önmagát titkosítja	Memóriába installálódik	COMMAND.COM	.COM állományok	.EXE állományok	Overlay állományok	Floppy bootszektora	Merevlemez bootszektora	Particiós tábla	A fertőzött program méretnövekedése	KÁROKOZÁS MÓDJA
V270X		[268P]	.	.	.	x	x	.	.	.	.	.	270	O P L D
V299		[V299]	.	.	.	.	x	.	.	.	.	.	299	O P D
V2P2		[v2p2]	.	x	.	.	x	.	.	.	.	.	Vált.	L O P
V2P6		[V2P6]	.	x	.	.	x	.	.	.	.	.	Vált.	L O P
V400	(5)	[MCE]	.	.	x	.	x	.	.	.	.	.	Vált.	O P D
V483		[B483]	.	.	x	x	x	.	.	.	.	.	483	O P
V5		[V-5]	.	.	.	x	x	x	.	.	.	.	547	O D
V800	(3)	[V800]	x	x	x	.	x	.	.	.	.	.	800	O P L
V801		[V801]	.	.	x	x	x	x	x	.	.	.	801	O P L
V82		[V82]	.	x	.	.	.	x	x	x	x	x	2000	O P L
V961		[V961]	.	.	x	x	x	.	.	.	.	.	961	O P
Vacsina	(19)	[Vacs]	.	.	x	.	x	x	x	.	.	.	1206	O P
Vcomm	(5)	[Vcomm]	.	.	.	.	.	x	.	.	.	.	1074	O P L
VHP	(7)	[VHP]	.	.	.	x	x	.	.	.	.	.	Vált.	L O P
Victor	(2)	[Victor]	.	.	x	x	x	x	x	.	.	.	2458	P D L
Vienna/648	(49)	[Lisbon]	.	.	.	.	x	.	.	.	.	.	648	P
Violator	(5)	[Vienna]	.	.	.	x	x	.	.	.	.	.	1055	O P D
Viper		[Vip]	.	.	.	x	x	x	.	.	.	.	Felülír	L O P
Virus-101		[101]	.	x	x	x	x	x	x	x	.	.	2560	P
Virus-90		[90]	.	.	x	.	x	.	.	.	.	.	857	P
Voronezh	(2)	[Vor]	.	x	x	x	x	x	x	.	.	.	1600	O P D
VP		[VP]	.	.	.	x	x	.	.	.	.	.	913	L O P
Vriest		[Vrst]	.	.	x	x	x	.	.	.	.	.	1280	L O P
VTS		[VTS]	.	.	.	.	x	.	.	.	.	.	Nincs	
V-Label		[Label]	.	.	x	x	x	x	.	.	.	.	Felülír	L O P
W13	(4)	[W13]	.	.	.	.	x	.	.	.	.	.	532	O P
Warrior 2		[war2]	.	.	.	.	x	.	.	.	.	.	Nincs	

MEGNEVEZÉS			MÓD-SZER			FERTŐZÉS HELYE								
Név	Változatok száma	Rövidített névkód	Lopakodó technika	Önmagát titkosítja	Memóriába installálódik	COMMAND.COM	.COM állományok	.EXE állományok	Overlay állományok	Floppy bootszektora	Merevlemez bootszektora	Partíciós tábla	A fertőzött program méretnövekedése	KÁROKOZÁS MÓDJA
Warrior		[War]	.	.	x	.	.	x	.	.	.	.	1024	O P D
Whale	(34)	[Whale]	x	x	x	x	x	x	x	.	.	.	9216	L O P D
Wisconsin	(3)	[Wisc]	.	x	.	x	x	.	.	.	.	.	825	O P D
Wolfman	(3)	[Wolf]	.	.	x	x	x	x	.	.	.	.	2064	O P
Wonder		[Wond]	.	.	.	.	x	x	.	.	.	.	Felülír	L O P
Wordswap	(4)	[Ws]	.	.	x	x	x	x	.	.	.	.	Vált.	D F L O P
WWT	(3)	[WWT]	.	.	.	x	x	.	.	.	.	.	Vált.	L O P
Xabaras		[Xab]	.	.	.	.	.	x	.	.	.	.	Felülír	L O P
Xuxa		[xu]	.	.	x	x	x	.	.	.	.	.	1413	O P L
Yale/Alameda	(3)	[Alameda]	.	.	x	.	.	.	.	x	.	.	N/A	B
Yankee-2		[Enigma]	.	.	.	.	x	x	.	.	.	.	1961	O P
Yap		[Yap]	.	x	x	x	x	.	.	.	.	.	6258	L O P
Zaragosa		[Zar]	.	.	x	x	x	x	x	.	.	.	1159	L O P
Zero Bug/1536		[Zero]	.	.	x	.	x	.	.	.	.	.	1536	O P
ZeroHunt		[Hunt]	x	x	x	.	x	.	.	.	.	.	N/A	O P D
ZK900		[Z900]	.	.	x	x	x	x	.	.	.	.	900	L O P
ZRK	(3)	[ZRK]	.	.	x	x	x	x	x	.	.	.	2968	O L P
# 1		[N1]	.	.	x	x	x	.	.	.	.	.	11240	O L P

Irodalomjegyzék

1. Adney, William A. – Kavanagh, Douglas E.: The data bandits. In: Byte, 1989. 1. 167-270. p.
2. Alaplap mikroszámítógép magazin mágneslemez melléklettel. A „Vírusőrjárat" rovatban rendszeresen közöl cikkeket a vírusokról. Publ.: Cédrus Informatikai Rt., Budapest. (A továbbiakban: Alaplap.)
3. Auf der Knie. In: Der Spiegel, 1988, 11. 7. 294. p.
4. Bayerische Hackerpost. München. (A bajor számítógépbetörők szakmai fóruma.)
5. Bombenstimmung. In: Computer Live, 11/1990. Összeállítás. Kivonatosan közli a Computer Panoráma 1991. januári száma.
6. Börstler, Torsten – Fischer, Christoph: Sabotage vorprogrammiert! Computer-Viren bedrohen Datenbestände. In: CAK Nr. 8. 1989. okt. 44-53. p.
7. Brown, Richard: Interrupt list rel. 91. 1. 5. Szövegállomány. Via HomeBase BBS, USA 1991.
8. Brunnstein, Klaus: Blindes Vertrauen in den Computer. Unterschätztes Risiko. In: Bild der Wissenschaft, 2/1988. 96. p.
9. Brunnstein, Klaus: Mythen und Fakten über Computer-Viren. In: Chip, 1989. 3. 50-56. p.
10. Brunnstein, Klaus: PC-Viren. Dichtung und Wahrheit. In: Computer Magazin, 1989. 9. 47-49. p.
11. Brunnstein, Klaus: Risiken der Informationsverarbeitung. In: Computer Magazin, 1989, 1-2. 31-35. p.
12. Brunnstein, Klaus: Viren-Telex mit Virus-Katalog. Ein monatlicher Informationsbrief für Datensicherheit, 1989-1990. Ed.: Vogel Verlag, Würzburg.
13. Brunnstein, Klaus: Über Viren, Würmer und andere seltsame Geister in Computersystemen — Ein kleines Informatik-Bestiarium. In: Angewandte Informatik, 1987. 10. 397. p.
14. Brunnstein, Klaus: Zur Klassifikation von Computer-Viren. Der Computer Virus Katalog. In:Tagungsband der 19. GI-Jahrestagung.
15. Brunnstein, Klaus – Fischer-Hübner, S.; Swimmer M.: Classification of Computer Anomalies Security Conference, New York 1991.
16. Brunnstein, Klaus – Fischer-Hübner, S.; Swimmer M.: Concepts of an Expert System for Virus Detection. In: IFIP TC11 Security Conference, 1991
17. Brunnstein, Klaus – Fischer-Hübner, S.: Risk Analysis of Trusted Computer Systems In: IFIP TC11 Security Conference, 1990 Helsinki
18. Bunge: Die jüngsten Prüfungsergebnisse des Bundesrechnungshofes zur

Datensicherheit. In: 14. DAFTA Tagung in Köln. Gesellschaft für Datenschutz und Datensicherheit e. V. 1990 november.
19. Burger, Ralph: Das groe Computer-Viren Buch. Ed.: Data Becker GmbH, Düsseldorf–Wien, 1987. (Későbbi kiadásait részben átírták, aktualizálták.)
20. Burger, Ralph: Das groe PC Viren Schutzpaket. Ed.: Data Becker GmbH, Düsseldorf–Wien, 1989.
21. Buruzs Tamás: A számítógépes vírusok természetrajza. Szakdolgozat 1991/S-3. Ed.: Kandó Kálmán Villamosipari Műszaki Főiskola, Budapest. A szakdolgozat a benne lévő teljes víruskód (Potyogós) miatt csak szakmai kutatás céljára hozzáférhető, zárt anyag!
22. Buruzs Tamás: Rezidens Virus Killer (RVK). Dokumentációs állományok.
23. Buruzs Tamás: Self Protection Systetms (SPS). Dokumentációs állományok.
24. Cohen, Fred: „Computer Viruses". Dissertation. University of Southern California. Ed.: USC, 1985.
25. Cohen, Fred: Computer Viruses: Theory and Experiments. Ed.: University of Southern California, 8/1984. Reprint in Computer & Security, 6/1984.
26. Cohen, Fred: Models of Practical Defenses against Computer-Viruses. In: Computer & Security, 2/1989.
27. Computerworld-Számítástechnika. Rendszeresen közölt a vírusokra vonatkozó információkat és előrejelzéseket. Publ.: IDG Lapkiadó Kft., Budapest. (A továbbiakban: CWI, illetve IDG.)
28. Cremer, Dorothea – Pohl, Harmuth: Zur Computerkriminalität im 5. StÄG der DDR und 2. WiKG der Bundesrepublik aus der Sicht der Informationstechnik 1.– 2. In: Datenschutz und Datensicherung 1990/10. 493-497. p. és 1990/11. 551-558. p.
29. Datenschleuder. Hamburg. (A Chaos hackercsoport folyóirata.) Ed.: Chaos, Hamburg.
30. Dierstein, Rüdiger: Anmerkungen zur Rechtslage. Programm-manipulationen — Trojanische Pferde, Viren und ihre Bekämpfung. Ed.: Carls-Cranz-Gesellschaft e.V. Oberpfaffenhofen 1991 April.
31. Dierstein, Rüdiger: Computer-Viren In: DFVLR Institutsbericht, IB 582/6, 1986 Juli.
32. Dierstein, Rüdiger: Computer-Viren 1. In: KES, 1985. 03. 77-86. p.
33. Dierstein, Rüdiger: Computer-Viren 2. In: KES, 1985. 04. 125-135. p.
34. Dierstein, Rüdiger: Computer-Viren 1. In: Output, Nr. 1986/8. 33-40. p.
35. Dierstein, Rüdiger: Computer-Viren 2. In: Output, Nr. 1986/10. 43-47. p.
36. Dierstein, Rüdiger: Computer-Viren — Was man jetzt darüber wissen mu. In: PM Computerheft 1989. März-Apr. 16-21. p.
37. Dierstein, Rüdiger: Computer Virus. In: Conference Proceedings of the Scuricom 86, 4th Worldwide Congress on Computer and Communications Security and Protection, Paris, 1986. Febr.
38. Dierstein, R.: Das Israel Virus. In: KES, 2/1988.
39. Dierstein, Rüdiger: Die neue Gefahr — Computer Viren In: KES, Zeitschrift für Kommunikations- und EDV-Sicherheit, (továbbiakban: KES), 3/85-4/85, Peter Hohl Verlag, Ingelheim.

40. Dierstein, Rüdiger: Programm-Manipulation-Computer. Viren und deren Bekämpfung. In: Recht der Datenverarbeitung RDV, Heft 3. 1989. 101. p.
41. Fisher, Christoph: Grundlagen der Virenbekämpfung In: PC Woche, 1991/10 (1). 4-16. p.
42. Fisher, Christoph: Tarnkappaviren sind nicht unentdeckbar. In: Datenschutz Berater, 1991/3, 1-4. pp 14.(3)
43. Die Hackerbibel. Vol. 1.-2. (Német hacker-kiadvány.) Ed.: Chaos, Hamburg.
44. Ducan, R. (compiled): The MS-DOS Encyclopedia. Ed: Microsoft Press, Redmond, Washington, 1988.
45. Elmer-DeWin, P.: Invasion of the Data Snatchers! In: Time, 26/9/1988. 62. p.
46. Experimente mit Computer-Viren. A KES 2/87. száma idézi a Die Datenschleuder underground lapot. (No.18. 2/1987.)
47. Fites, P.; Johnston, P.; Kratz, M.: The Computer Virus Crisis. Ed.: Van Nostrand Reinhold, N.Y. 1989.
48. Flu Shot+ ver.1.5 User manual. Ed.: Software Concepts Design, N.Y. 1989.
49. Frost, David: The Complete Computer Virus Handbook. Ed.: Price Waterhouse, 1988.
50. Greenberg, R.M.: Know the Viral Enemy. In: Byte, 6/1989. 275. p.
51. Günter, Frhr. von Gravenreuth: Computer Viren, Datenspione, Crasher und Cracker. In: Neue Zeitschrift für Strafrecht, Heft. 5. 1989. 201-248. p.
52. Günter, Frhr. von Gravenreuth: Rechtliche Beurteilung von Computer Viren: GI Fachgespräch, Okt. 1989. Springer Verlag, Tagungsband der 19. GI-Jahrestagung. 1989. Band 1. 619-628. p.
53. Hirst, Joe: List of known PC viruses. Publ.: British Computer Virus Research Center, Brighton/Essex, 1989.
54. Hoppenrath, D.: Computerviren: Problem oder Psychose. In: Computer Persönlich, 3/1989. 45. p.
55. Hoppenrath, D.: Impfung via Software. In: Computer Persönlich, 3/1989. 48. p.
56. Hoppenrath, D.: Kranke Programme. In: PC-Magazin, 35/1988. 20. p.
57. Hozzászólás vírusügyben. In: CWI, 1988. 25. szám.
58. Goodwin, Jim: Virus Information Summary List. In: VSUM9003.ZIP 1990-02-18 from Homebase/CVIA Bulletin Board BBS, USA.
59. Kane, Pamela: V.I.R.U.S. Protection. Vital information resources under siege. Foreword by Dvorak, John C. Ed.: Batham Books New York, 1989. & Dr. Panda Utilities by Andy Hopkins from Paralex Ltd. New York.
60. Kastenmüller, S.: Erkennen von Computer-Viren. In: KES 4/1988.
61. Kis János: A tiltott gyümölcs mindig kívánatos. In: Alaplap, 1990. 9. szám, 38. p.
62. Kis János: Egy veszélylehetőség realitássá vált. Virtank.doc, a Prgdoki 2.11...2.13 verzióihoz adott összefoglaló dokumentációs állomány. Szamizdatként Budapesten, Kecskeméten. 1988-1989.

63. Kis János: Hogyan kell vírust írni? In: Delta-Impulzus, 1989. 9. szám, (V. 6.), 40. p.
64. Kis János: Modern trójai háború. In: Delta-Impulzus, 1989. 8. szám, (IV. 22.), 24. p.
65. Kötél Gyula: A programfejlesztés módszertani kérdései a katonai információfeldolgozási rendszerek fejlesztésében. Egyetemi doktori értekezés. Ed.: Zrínyi Miklós Katonai Akadémia 287/6/88 nyt. sz, Budapest. 1990. (Kutatási célra hozzáférhető.)
66. Küzdelem a számítógépes vírusok ellen. Steve, R. – White David – M. Chess Cheng – Jimmy Kuo tanulmánya az IBM részére In: Floppy.Lap mágneslemez folyóirat. Cédrus Rt. 1991/1.-2.-3. Kis János utószavával. A fordítás alapjául szolgáló szöveg az IBM kutatási jelentések sorozatában jelent meg: Report Number RC 14405 1989 IBM Los Angeles Scientific Center Los Angeles, CA
67. Labor, Zeitschrift für Word Processing. (Víruscikkek, adatátvitel.) Technikai szamizdat. Ed.: Labor c/o Glaser, D-2000 Hamburg 50, Hospital Str. 61.
68. Másolás? Védelem? (A hónap témája. Összeállítás.) In: Alaplap, 1991. 1. szám.
69. McAfee, John: Scanxx.DOC, Cleanxx.DOC, Netscan.DOC, Vshieldxx.DOC, Mdisk.doc, Virlist.txt szoftver-dokumentációs állományok. 1988-1991.
70. McAfee, John: The virus cure. In: Datamation, 1989. 02. 15. 29-40. p.
71. Mosich, Donna: Norton Antivirus User Manual 1.0.1 Ed.: Szmatec Corp. USA Cupertino CA. 199O és a program dokumentációs állományai.
72. MS-DOS-Viren erkennen und bekämpfen. Chip Special, No. 82005/90003 1. Aufl. Ed.: Vogel Verlag, Würzburg, 1990.
73. Mutopf, Günther: Drei Schritte zur Heilung. In: Chip, 11/1989. Ed.: Vogel Verlag, Würzburg, 1989.
74. Mutopf, Günther (comp.): Trojanische Pferde, Viren und Würmer. Eine ernstzunehmende Gefahr für PC-Anwender. Ed.: PerComp Verlag GmbH, Hamburg, 1989.
75. Mutopf, Günther: Wenn die Programme auf der Platte Amok laufen. Serie In: Die Computerwoche, 5/1990, 34. p., 6/1990, 26. p., 7/1990. 30.p.
76. Péntek 13-a! Vírusölő program. In: CWI, 1989. 36. szám.
77. Rablók és pandúrok. In: CWI, 1989. 6. szám.
78. Roberts, R.: Computer Viruses. Ed.: Compute! Books, Greensboro, NC, 1988.
79. Rubenking, N.J.: Infection Protection. In: PC Magazine, 4/1989. 193. p.
80. Schöneburg, E.: Computer Centre Risk Analysis by Expert Systems. In: Dornier Post 1/1987. Dornier GmbH, Friedrichshafen.
81. Schöneburg, E.: Computer-Viren — Eine aktuelle Bedrohung für Computer-Systeme. In: Dornier Post, 1/1987. Dornier GmbH, Friedrichshafen.
82. Schöneburg, E.: Computer-Viren und Trojanische Pferde. Gefährliche Softwareangriffe an Computersysteme. In: Neue Zürcher Zeitung, 1987. 9. 29.

83. Schöneburg, Eberhard – Heinzmann, Frank – Namyslik, Frank: Computer-Viren. Gefahren und Schutzmöglichkeiten. Ed.: Markt und Technik Verlag, Haar bei München, 1989.
84. Schöneburg, Eberhard – Heinzmann, Frank – Namyslik, Frank: Virus Power Pack (Programm und Buch). Ed.: Markt und Technik Verlag, Haar bei München, 1989.
85. Shapira, Eli – Sherman, Yuval: Turbo Anti Virus Toolkit *Tntvirus* ver. 6.80A dokumentációs állománya és felhasználói kézikönyve. Ed.: Carmel Software, Haifa, 1990.
86. Shapira, Eli – Sherman, Yuval: Turbo Anti Virus Toolkit *Tntvirus* ver. 6.71B demó verzió dokumentációs állomány. Ed.: Carmel Software, Haifa, 1990.
87. Skulason, Fridrik: F-Prot antivírus programcsomag dokumentációs állományai. Ed.: Reykjavik, 1991 febr.
88. Small business Innovation Research Program. Ed.: US Defense Dept, Washington DC. 1990. (A 45. oldaltól víruspályázat: Computer Virus and Electronic Counter Measures)
89. Sperber, J.: Virusfieber. In: Microcomputer Zeitschrift, 7/1988. 74. p.
90. Számítógépvírusok, avagy ki fél a cyberpunkoktól? In: CWI, 1989. 31. szám.
91. Szegedi Imre: Harc az adatgyilkosok ellen. In: Alaplap. 1990. 8. szám, 32. p.
92. Szegedi Imre: Megindult a hazai vírustenyésztés? In: Alaplap, 1990. 10. szám, 36. p.
93. Szegedi Imre: Személyi számítógépes vírusok elterjedésének veszélyei és az ellenük való védekezés a Magyar Honvédségben. Első magyar víruskönyv. (Doktori értekezés.) Magyar Honvédség, Zrínyi Miklós Katonai Akadémia 587/4/90, Budapest, 1990. (A benne közölt teljes víruskódok miatt nem publikálható anyag.)
94. Szegedi Imre: Szisztematikus doktorálás. In: Alaplap, 1990. 9. szám 36. p.
95. Technical Notes on AIDS DISK Trojan Mail Information. In: AIDSTECH. ZIP, 1989-12-23. From: Homebase/CVIA Bulletin Board BBS, USA.
96. Terjed a vírusjárvány az Egyesült Államokban. In: CWI, 1989. 22. szám.
97. Tűzre, vízre, adatokra vigyázzatok. In: CWI, 1989. 34. szám.
98. Újabb gyógyszer a Péntek 13-a ellen. In: CWI, 1989. 40. szám.
99. Veldman, Frans: A TBSCAN és a TBSCANX szekvenciális víruskereső programok leírásai: TBSCAN.DOC (1990 12. 15) és TBSCANX.DOC (1991. 04. 02) Thunderbyte BBS.
100. Verborgener Befehl — Bericht Cohens Arbeit. In: Der Spiegel, 4/1987.
101. Védőoltás vírus ellen. In: CWI, 1989. 22. szám.
102. Vírusok. In: CWI, 1988. 13. szám.
103. Vírusvadászat. (A hónap témája. Összeállítás.) In: Alaplap, 1991. 8. szám.
104. Woehlebier, H.: Der Weihnachtsbaum, der um die Welt ging. In: KES, 1/1988.

Víruskeresés

Tartalomjegyzék

A könyv szerzői a következő címeken érhetők el:

Szegedi Imre
Safe Kft
1134 Budapest, XIII., Gidófalvy u. 31.
Telefon: 140-7681
Telefon/Fax: 183-3267

Kis János
Chip szerkesztőség
1300 Budapest III., Lajos u. 160-162.
Telefon/Fax: 168-6266
Lakás: 1027 Budapest II., Margit körút 24.
Telefon: 116-8896 és (06) 60-16-162
BBS: VirNET Budapest, Tel.: 115-4402, 0–24 h, 9600 BPS, 8N1, MNP5

Az Alaplap Könyvek sorozat kötetei beszerezhetők:

Cédrus Kiadó Kft, Alaplap szerkesztőség
1441 Budapest VIII., Reguly Antal u. 8.
Telefon/Fax: 133-1839

256,- FT

Az Alaplap Könyvek sorozat kötetei

1. Farmosi István—Kis János—Szegedi Imre: Víruslélektan
2. Nagy Gábor: Tömör gyönyör
3. Kis János—Szegedi Imre: Új víruslélektan
4. Kis János—Szegedi Imre: Vírushatározó
5. Számítástechnikai alaplexikon I. (Jodál Endre: Általános fogalmak)

A SZÁMÍTÁSTECHNIKAI ALAPLEXIKON tervezett köteteinek fő témakörei

I. Általános fogalmak
II. Adatkommunikáció
III. Gazdaság, pénzügy, kereskedelem
IV. Ipari számítástechnika
V. Eszközök és gyártási technológiák
VI. Mesterséges intelligencia
VII. Négynyelvű szótár