

Farmosi István – Kis János – Szegedi Imre

Vírusrélektan



ALAPLAP KÖNYVEK



FARMOSI ISTVÁN—KIS JÁNOS—SZEGEDI IMRE

VÍRUSLÉLEKTAN

CÉDRUS

Szerkesztette: FAKLEN PÁL

© Farmosi István - Kis János - Szegedi Imre, 1990

Felelős kiadó: Sebestyén Ilona

Felelős szerkesztő: Németh István

Borítóterv: Zátonyi Tibor

Cédrus Informatikai Részvénytársaság

Felelős vezető: Vékony Tamás

Szedés: Compu-Typo Kft.

Nyomtatás: Policoop Nyomda

Felelős vezető: Szabó István

ISBN 963 02 8675 0

ELÖLJÁRÓBAN

avagy

AD USUM DAUPHINI

A francia királyságban volt először hivatalosan szokás — és eme dicstelen gyakorlat napjainkig elterjedt szerte e földgolyó bison —, hogy az egyetemes kultúra kincseiből, a világirodalom alapmunkáiból, a klasszikusokból külön kiadásokat készítettek a trónörökös számára, megfosztva azokat érzelmefelkavaró vagy bűnösnek tartott tartalmuktól. Az így átírt, elferdített, megszélesített műveket nevezték azután nemes egyszerűséggel a trónörökös (azaz a dauphin) használatára készített műveknek, latinosan „ad usum dauphini”-nak. Nos, ez a módszer nemcsak a diktatúrák gyakorlata. Üzleti, gyártási titokra hivatkozva, (vagy az egyszerű „csak” indoklással) sem a számítógépgyártók, sem a programkészítők, sem pedig a kereskedők nem publikálták az összes fontos tényt az általuk forgalomba hozott számítástechnikai rendszerekről. Igyekeztek a felhasználót maximálisan kiszolgáltatott helyzetbe hozni, hogy megtarthassák saját hatalmukat.

A titok mindig izgatta az emberek fantáziáját. Fiatalok — nevezzük nevén a gyermeket: hackerek, azaz számítógépes betörők és programfeltörők — szórakozásból vagy éppen az ismeretlen és tiltott gyümölcs vonzásának engedve egyre jobban megfejtették a számítástechnikai rendszerek féltett titkait. Munkájuk eredményeképpen kezdett megtörni a varázs, és a maga meztelenségében jelent meg a sokáig misztikus ködbe burkolt számítástechnika. A szakma és a szakirodalom hivatalos része azonban minderről nem nagyon vett tudomást. A valóban használható „éles információk” vagy szájhagyomány útján, vagy pedig szűk belső körnek szóló kiadványokban terjedtek. Nem véletlen, hogy nagy népszerűsége tettek szert azok a programok, amelyeken sokszor mindössze ennyi állt: „IBM INTERNAL ONLY”, azaz eredetileg csak az IBM cég belső használatára készült, de onnan mégis kiszivárgott program. Eddig a kiadók sem igen versengtek — az őskorszak Peter Nortonját kivéve —, hogy a szélesebb szakközönségnek is hozzáférhetővé tegyék ezeket a csak zárt körben vagy egyáltalán nem közölt titkokat. Ideje már, hogy megtörjön e hallgatás. Akkor is, ha ez egyes „kiválasztottak” érdekeit sérti. A felhasználóknak is alaposabban meg kell ismerkedniük a rájuk leselkedő veszedelmek természetrajzával. Könyvünk az informatikai

társadalmakat fenyegető egyik kártevőről, a számítógépek programvírusairól szól. Egy olyan, egyre táguló szakterületről és programozástechnikáról, amelynek létezését egyesek még kétségbe is vonták, mások pedig komolytalanul tartották az ezzel a kérdéssel való foglalkozást. „Nem kell pánikot kelteni” — mondták.

Korábban a szakmabeliek sikerrel akadályozták meg ilyen vagy amolyan indokokra hivatkozva Ralph Burger Nagy víruskönyvének magyar kiadását. Csak a már megszűnt Delta-Impulzusban, később a CWI Számítástechnikában és a Mikroszámítógép Magazinban, majd a magyarul is megjelenő Chip nyugatnémet számítógépes folyóirat magyar kiadásában, valamint 1990 nyarától a Cédrus Rt. kiadásában megjelenő Alaplap számítástechnikai folyóiratban találkozhattak rendszeresen ilyen témában aktuális információkkal.

A Hamburgi Egyetem Vírustesztelő Központjában (Virus Test Centrum Universität Hamburg) van Európa egyik legnagyobb, nem nyilvános vírusadatbankja. Ők nem járulnak hozzá a forráskódok publikálásához, hiszen sokan éppen ezek felhasználásával írtak új, az eddigieknél is durvább vírusokat. Mi is követjük ezt az elvet könyvünkben. Célunk a veszélyre és annak elhárítására felhívni a magyar számítógép-használók figyelmét. Munkánkban saját kutatásainkra támaszkodunk, de néhány esetben felhasználjuk a hamburgi kutatók információit is. Hasonlóan sokat segítettek az amerikai McAfee Inc. publikációi, valamint az izraeli-amerikai Carmel Software dokumentációi és programjai is.

Köszönetünket nyilvánítjuk a BBS-ek fenntartóinak szerte a világon, hogy összeállíthattuk ezt az anyagot. Különösen sokat használtunk fel dr. Solomon's, valamint Patricia M. Hoffmann dokumentációjából, amely John McAfee Virnet rendszerében szerepelt. Az adatbiztonsággal és a számítógépes terrorizmus elhárításával foglalkozó csoportok rendszeres publikációikkal és adatszolgáltatásukkal szintén hatásosan segítik a nemzetközi fellépést az adatgyilkosok ellen. Közülük a legfrekvenciáltabb helyen talán Yasrael Radaí csoportja tevékenykedik a Héber Egyetemen, Izraelben. Hollandiában Jan Terpstra, az NSZK-ban pedig a Hamburgi Egyetem Vírustesztelő Központja publikál rendszeresen adatokat a programvírusokról.

Közben a sok új kiadás ellenére Ralph Burger könyve is túlhaladottá vált, így a szerzők szükségesnek látták, hogy eredeti művet hozzanak létre, amelyet a programozástechnikában járatlan felhasználó éppen olyan eredményesen tud használni, mint a programozó, akinek meg kell védenie rendszerét

a vírusprogramok támadásától vagy éppen programozótársai „piszkos trükkjeitől”. E könyvünk tartalmazza az egyik szerzőnek, Szegedi Imrének a számítógépvírusokról készített akadémiai doktori disszertációjának azon fejezeteit is, amelyek közérdeklődésre tarthatnak számot.

A vírustechnológia alapjában a „piszkos trükkök” közé tartozik, éppúgy, mint a programok élettartamát, másolhatóságát korlátozó eljárások. És az emberek nem mind „Grál-lovagok”, mindig vannak köztük ártó szándékúak, akiktől meg kell(ene) védeni a társadalmat. A tudás hatalom, s annál kisebb a vele való visszaélés veszélye, minél szélesebb körben megismerik a korábbi titkokat. Az emberek józanságában és etikai érzékében bízva invitáljuk az olvasót a számítástechnika egyik rejtett boszorkánykonyhájába.

A szerzők ezúton is köszönetet szeretnének mondani a sok névtelen felhasználónak, akik segítettek megismerni azokat a programokat is — sokszor állásukkal játszva, főnökeik kifejezett tilalma ellenére —, amelyeket hazai és külhoni fejlesztő laboratóriumokban főztek ki a bevétel növelésére, vagy amelyek a „nagy magyar szoftverkommuna” csatornáin keresztül jutottak el Magyarországra. Szerencsére vannak tisztességes emberek a „piszkos trükkök” hazai kutatólaboratóriumai környékén is. Ők lelkiismeretük parancsának engedelmeskedve, sok esetben még forráskódok kiszolgáltatásával is segítettek elkerülni azokat a víruskárokat, amelyek ezen információk nélkül feltétlenül bekövetkeztek volna. Sokan használnak így jogtisztán, de mindenféle másolásvédelem és egyéb trükk nélküli programokat Magyarországon, amelyeknek máshonnan történő beszerzésére nincs lehetőség. Bármennyire szeretnénk is leírni ezeknek a cégeknek és programjaiknak a nevét, hallgatnunk kell róluk, hacsak sajátos hazai jogrendünk folytán nem akarjuk pénzünket és időnket a hosszadalmas és biztos pervesztéssel kecsegtető bírósági eljárásra pazarolni. Mert sajnos nemcsak hasznos programok, hanem büntető másolásvédelmek, terrorisztikus célú vírusok is készülnek a hazai és külhoni műhelyekben. Hosszabb távon azonban Magyarország sem szigetelheti el magát a számítástechnika világában és az üzleti életben külföldön végbemelő folyamatoktól. A tapasztalat egyre inkább igazolja, hogy a tisztesség, a bizalom — no meg a megfelelő jogi garancia — üzletileg mind a forgalmazóknak, mind a felhasználóknak kifizetődik.

Sajnos, sok forgalmazó Nyugat-Európában egyfajta „vadkeletnek” tekinti Magyarországot. A hazai forgalmazók rémhíreinek és félretájékoztatásának eredményeképpen maguk is követik a magyar forgalmazóknál látottakat. De

ellenpéldákat is hozhatnánk. A védelem nélkül forgalomba került Quattro új verziójának vagy a PcTools eredeti változatának üzleti sikere megmutatta, hogy lehet Magyarországon kifizetődő üzleteket tisztességesen is kötni. Az így megvett szoftvereket ugyanis általában nem adják tovább megvásárlóik, hanem becsületbeli ügynek tekintik a szerződés betartását... Olyannyira, hogy a Norton Commander 3.0 verziójából a hazai forgalmazás megkezdése után három hónappal is képtelenek voltunk tesztpéldányt szerezni. Ennek ellenére nem haragszunk rájuk! Valami elkezdődött...

Bár könyvünkben az IBM-kompatibilisnak mondott gépek programvírusaival foglalkozunk, az abban elmondottak jó része — főleg az általános terjedési elvekről és részben a védekezési stratégiáról leírtak — érvényesek más rendszerkörnyezetre is. A C-64-es gépeknek éppúgy megvan a maguk vírusstényészete, mint a nagygépes operációs rendszereknek.

Magyarországot a nagygépes vírusok pusztítása eddig messze elkerülte, de erre nem nagyon lehetünk büszkék, mert ezt csapnivaló adatátviteli rendszerünknek és telefonhálózatunknak köszönhetjük. A gépek sokfélesége és elszigeteltsége ez esetben előnyt jelentett, de ez remélhetőleg már nem tart sokáig... A politikai változásokkal együtt megnyílt annak a lehetősége, hogy a korábbiaknál nagyobb teljesítményű berendezések kerüljenek be teljesen legálisan az országba. Rövidesen megjelennek a DEC VAX gépei, hasonlóképpen várható az IBM AS400 gépeinek elterjedése. Itt még egyelőre nincsenek vírusok. Nagyon sok múlik azon, hogy a forgalmazók a különben igen drága berendezésekhez képesek lesznek-e megfizethető áron megfelelő szoftvereket is biztosítani. Mert ha nem, akkor a szoftverkommuna ezekre a nagy berendezésekre is kialakul, annak minden veszélyével együtt. A gépek méretéből és hálózati kiépítéséből következően az okozott kár azonban itt jóval nagyobb lesz.

Nem szabad a homokba dugni a fejünket, inkább fel kell készülni szakmailag és etikailag is az új korszakra. Ehhez természetesen hozzátartozik a megfelelő törvények megalkotása és elfogadása. A forgalmazóknak viszont az eddigi árkartellt feladva, tisztességes áron, tisztességes szoftvereket kell forgalmazniuk, hogy ne legyen érdemes szoftvert lopni... és szoftvert megadatokat tönkretenni.

Budapest, 1990. szeptember

Farmosi István, Kis János, Szegedi Imre

JÓTÉKONY KÖD MELY „ÁPOL S ELTAKAR”

Jelenleg a számítógépet használók mindennapos gondja a vírusprogramok elleni védekezés. Mégis a hallgatás fala veszi körül az egész témakört. Mi szeretnénk megtörni ezt a csendet.

Minél alacsonyabb az alkalmazástechnika kultúrája, annál jobban be lehet csapni a felhasználót. Ilyen környezetben még olyan nagyvállalatok, szoftverházak is képesek megélni, amelyek a tisztességtelenséget a cég üzletpolitikájának rangjára emelik. Nagy értékű szoftverrendszerekbe beépítenek például olyan időzítő rutinokat, amelyek hatására a szoftver a garanciális idő letelte után nem sokkal tönkremegy. Mások másolásvédelem ürügyén teszik tönkre a felhasználó gépét, adatait.

Korábban a Clippert gyártó és értékesítő híres amerikai cég a legelső programverziókat úgy forgalmazta, hogy azok bizonyos számú futtatás után megölték magukat, s ha a gépen véletlenül volt vele fordított adatbáziskezelő rendszer, akkor azt is. Ebbe majdnem belebuktak, és így a később forgalomba került programverziók már korrektül működtek. Magyarországon később a forgalmazó maga próbálta meg másolásvédelemmel ellátni a Clipper hazai változatát. A felhasználók kinevették, és inkább a védelem nélküli kalózpéldányokat kezdték használni. Végül Magyarországon is az eredeti, védelem nélküli szoftvercsomag került forgalomba...

Még jócskán van mit tenni itthon azért, hogy a számítástechnikában is jogállamiság legyen. Ehhez mindenekelőtt meg kellene változnia a jogi szabályozásnak, szigorúan megbüntetve a számítógépes programokkal kárt okozókat, korlátozva az erőfölénnyel való visszaélés lehetőségét. Példaként lebeghet szemünk előtt az USA szabályozása, amely a számítógépek vírusainak tenyésztését és terjesztését — a számítógépes programokkal való károkozást — továbbá az adatlopást bűncselekménynek tekinti (data crime), és elég szigorúan bünteti. Programozástechnikai kérdésekben a hallgatás fala azonban még ott is áll, bár helyenként már omladozik.

A számítógépes programok és adathálózatok feltörésével foglalkozó fiata-

lok — a hackerek — korábban e szakma fenegyerekeinek számítottak. Céljuk az önfitogtatás, a károkozás volt. Napjainkra egyre több ilyen tehetséges hacker döbben rá: az informatikai társadalmakban tudásuk olyan fegyverré is válhat, mint az orvosé, a mikrobiológusé vagy az atomtudósé.

A nyugatnémet és amerikai hackerek nagy része, bár szorgosan folytatja egyes adathálózatok feltörését, kialakított egy sajátos etikai kódexet. Eszerint nem módosítják a megtalált adatokat, csak a maguk céljaira használják fel a „kapott” üzleti információkat... Ha pedig egy érzékenyebb rendszerbe hatolnak be, akkor jelzik az üzemeltetőnek, hogy valami hiba van védelmi szisztémájukkal. Aki számítógépes programokat ír, ugyanúgy hibázik, mint mások, néha pedig lustasága is nagy úr.

Londonban 1989-ben rendeztek egy adatbiztonsággal foglalkozó konferenciát. A CWI-Számítástechnika (a továbbiakban CWI) 1989/49. számában megjelent tudósítás szerint az ottani szakemberek bíralták a kormány halogató taktikáját, amellyel késlelteti a számítógépes kalózkodásnak, az adatok és gépek megrongálásának büntetését célzó törvény életbeléptetését. „A Lordok Háza még mindig úgy véli, hogy az effajta kalózkodás nem több rosszindulatú viccnél, ami legfeljebb némi anyagi hátrányt okoz” — jelentette ki az egyik alsóházi tag. A személyi jogok védelméről szóló törvénytervezetet egyébként még 1988 tavaszán tárgyalta első olvasatban az angol kormány, a büntető szankciókra vonatkozó ajánlásokat pedig 1989 novemberében az angol törvényhozás jogi bizottsága. Az október végén közzétett szöveg három informatikai bűncselekményt különböztet meg, amelyekkel nem érdektelen megismerkednünk:

— Alapbüntetésként három hónapig terjedő szabadságvesztés kiszabását javasolja minden olyan esetben, ha valaki engedély nélkül hatol be egy információs rendszerbe. A büntett jogi meghatározásánál a magánlaksértést tekintették analóg helyzetnek.

— Azok a számítógépes kalózkodók, akik saját tisztességtelen céljaik érdekében avatkoznak be egy rendszer működésébe — mindegy, hogy ezt milyen módon teszik —, öt esztendeig tartó maximális büntetéssel sújthatók.

— Ugyancsak ötesztendei börtönnel büntethetnék meg azokat is, akik számítógépvírus segítségével rongálnak meg vagy semmisítenek meg valamilyen informatikai rendszert, illetőleg abban tárolt adatokat.

Ha ehhez hasonló törvények Magyarországon is lennének, vajon az egyes számítástechnikai cégek vezetői és munkatársai közül hányan kerülhetnének be valamelyik állami műintézetbe kényszerű vendégeskedésre?

Az említetteknél jóval szigorúbb Svédországban a jelenleg is érvényben lévő jogi szabályozás. Itt a büntetési tétel felső határa az életfogytig terjedő fegyház.

Az adatrendszerek megzavarása néha emberéletet is követel. Az USA-ban valaki behatolt egy kórházi gyógyszerár számítógépes rendszerébe, és az ennek következtében túladagolt gyógyszer egy ember halálát okozta. Jóval többen halhattak volna meg Franciaországban, ahol egy gyógyszergyár központi számítógépében információkat módosítottak, kifejezetten terrorista szándékkal.

A magyar jogrendszer még nem készült fel ilyen informatikai kihívásokra. Sokáig egyes személyek — sőt neves szoftverforgalmazó cégek — azt is megakadályozták, hogy valóban részletes információk jelenjenek meg a számítógépes vírusprogramokról. Érveik sorában hivatalosan az állt az első helyen: mi lenne, ha mindenki elkezdene vírusokat írni. De a háttérben az a félsz bujkált, hogy saját trükkjeik is lelepleződhetnének és extraprofitjuk csökkenne. Korszerű jogrendszerben nem tartható fenn az információnak ez a monopóliuma. Az általánosságok mellett konkrétumokról is kell írni, hogy minden számítógép-alkalmazó megismerkedhessen az őt is fenyegető láthatatlan veszedelemmel, és tenni tudjon valamit ellene.

A másik hivatalos indoklás ez volt: ezekkel az ismeretekkel visszaélhetnek a terroristák, inkább ne terjesszük azokat. „Amiről nem beszélünk, az nem létezik.”

A számítógép legértékesebb részét az adatok jelentik. Ezek lehetnek táblázatok, szerkesztett szövegek, saját programok, nagyobb adatbázisok, vagy esetleg ott lehet a cég teljes könyvelése. Az adatok értéke mellett eltörpülhet a hardver és a szoftver értéke. Sajnálatos módon ezeket az adatokat nem csupán a műszaki vagy programhibából eredő megsérülés veszélye fenyegeti. Egyes emberek szántszándékkal ezeknek az adatoknak és programoknak a megsemmisítésére készítene (erkölcsileg nagyon alacsony, programozói tudásban elég magas színvonalon állva) sajátos programokat.

Korábban azt hirdettük, hogy a számítógépvírusok és más kártevő szoft-

verek Magyarországon nem fejthetik ki tevékenységüket. Most pedig már nemcsak a külföldön elterjedt vírusprogramok ütötték fel fejüket, hanem saját, „hazai tenyésztésű” vírusváltozatok és trójai programok is felbukkantak. Legtöbbjük önbíráskodási céllal, másolásvédelem ürügyén.

Az egészségügyi járványtani számításokkal foglalkozók már az ötvenes években felfigyeltek arra, hogy egy fertőző gócból kiinduló járvány terjedése nagyon jól modellezhető. Amennyiben ráadásul egy gyógyíthatatlan kórrol van szó, akkor a megfertőzhető népesség mintegy kétharmadának kihalása után a fertőzés önmagától már nem terjed tovább, majd teljesen megszűnik. Ezt a teóriát a középkor nagy pestisjárványai a gyakorlatban igazolták. S lám: hasonló törvényszerűségek vonatkoznak a vírusprogramok terjedésére is. A számítógépvírus az élő anyag működőképes modellje!

E tárgyban az első komoly publikáció egy ilyen járvány matematikával foglalkozó szakember tollából látott napvilágot még 1957-ben! (N. T. J. Bailey: *The Mathematical Theory of Epidemics*. Ed.: Hafner 1957.) Természetesen senki sem hitt a szerzőnek, tanulmánya eltűnt a hasonlóan száraz anyagok süllyesztőjében. Maga a programvírus, illetve vírusprogram fogalom is csak később bukkant fel a szakmai publikációkban, 1974-ben. (A két elnevezés sokáig mindenféle jelentésbeli különbség nélkül, vegyesen volt használatos. Az utóbbi időben már kezd kialakulni, hogy a vírusprogram az átfogóbb kategória, a programvírus pedig azon belül a programokat megtámadó vírusféléket jelöli, elhatárolva például boot-vírusoktól. — A szerk.) Az ACM-nek *Use of Virus Functions to Provide a Virtual APL Interpreter under User Control* című tanulmányában találhattunk rá először erre a meghatározásra, egy B. Gunn nevű szerző munkájában. A következő publikáció már 1982-ben jelent meg, a *The Worm Programs — Early Experience with a Distributed Computation* című, ma már beszerezhetetlen tanulmánykötet.

Európában a Dortmundi Egyetemen az NSZK-ban J. Kraus foglalkozott ugyanezzel a témakörrel 1980-81-ben. A kutatás ekkor még a legteljesebb titoktartás mellett folyt. Egyes katonai körök úgy látták, hogy a vírusprogramok alkalmasak egyes érzékeny technológiák és szoftverek le- és ellopásának megakadályozására és az ellenséges hatalmak számítógéprendszerének totális megbénítására. A bomba 1984-ben robbant az NSZK-ban: A *Der Spiegel* hírmagazin (Verborgener Befehl — Bericht über Cohens Arbeit,

1984. 47. szám) egy rövid cikkben számolt be az önreprodukáló programok létéről, felhíván a figyelmet a számítógépes technikai kultúrára leselkedő veszélyekre is. Ezután már nem lehetett letagadni létüket.

Milyen különös véletlen! Magyarországon is akkor bukkant fel az első vírusprogram, igaz, még Commodore 64-es gépen. Ennek hordozója néhány népszerű játékprogram volt. Terjesztője pedig egy, a gépek javításával foglalkozó „szakember”, aki ezzel a piszkos trükkkel ért el magának nagyobb forgalmat, könnyű kereseti lehetőséget. Programvírusa ugyanis olyan külső pályára vitte a lemezmeghajtó olvasófejét, ahonnan csak kézzel, a lemezeység szétszedésével lehetett visszavezényelni. Mellesleg Magyarországon ezt a vírust használták először másolásvédelemre egy kereskedelmi forgalomban árusított Commodore könyvelőprogramban.

Az információt egy idő után már nem lehetett visszatartani. Botorság volt azt hinni, hogy a szakirodalom kirekesztésével nem terjed tovább ennek az új programozási lehetőségnek az ismeretanyaga. A témával konkrétan foglalkozó elméleti publikációk sorát egy amerikai kutató, Friedrich Cohen *Computer Viruses, Theory and Experiment* (University of Southern California, 1983) című tanulmányában alkalmazta a gyakorlatban. Ő végzett először valós kísérleteket az egyetem VAX 11/750 típusú gépén UNIX multitasking operációs rendszerkörnyezetben, amit megismételt egy VMS-VM/370 operációs rendszerű hálózati rendszerkörnyezetben is. Az eredmény több mint megdöbbentő volt.

A multitask (többfelhasználós) környezetben a vírus elindítása után gyakorlatilag nulla időpillanatban mind a 33 rendszerállományt és az adminisztrátor programállományát megfertőzte, majd az elindítás utáni 18. másodpercben a négy felhasználó állományai is fertőzöttek voltak. A hálózatos rendszerben a századik másodpercben vált teljessé a fertőzés. Hangsúlyozni kell azonban, hogy ezek a rendszerek annak idején semmilyen külön beépített védelemmel sem rendelkeztek a vírusok ellen. Ennek azonban akkor még nem sokan mérték fel a veszélyeit. Megjelentek a vírusprogramot kibocsátó, mint az illegális programmásolókat megbüntető — önbíráskodó — másolásvédelmi programrendszerek, ugyanakkor a fiatalok is „jó tréfának” tekintették a hálózatok vírusokkal történő megfertőzését.

Az első, valóban a gyakorlatban használható, nem elméletieskedő publi-

káció a nyugatnémet számítógép-betörők — a hackerek — lapjában jelent meg (Bayerische Hackerpost, Adalbertstr. 41/B, D-8000 München 40). Ez a kiadvány a világ azon kevés technikai „szamizdatjai” közé tartozik, amelynek ismerete elengedhetetlen a számítógéprendszerek biztonságtechnikájával foglalkozó szakemberek számára. Mellesleg a titkosszolgálatoknak kedvenc olvasmányai közé tartozik. (Egy véletlen folytán annak idején magam is hozzájutottam, s így kezdtem el ezekkel a kérdésekkel foglalkozni. K.J.) Hasonlóan érdekes információkat lehet szerezni még egy Nyugat-Németországban megjelenő hacker-kiadványból, a Chaos Computer Club viszonylag rendszeresen megjelenő periodikájából. Ez adta közre az első teljes és valóban futtatható vírus forráskódot, 1986. évi 12. számában. (B. Fix Virus-source Rush-Hour, ed.: Chaos Computer Club e.V. D-2000 Hamburg 20, Schwenkenstr. 85, Datenschleuder.)

1989 februárjától Magyarországon is végigsöpört a vírusjárvány. Az első, valóban komolyan károkozásra képes vírusprogram — hála az előzetes felvilágosító munkának és a szabadsoftverként is terjesztett vírusölő programoknak — viszonylag kevés kárt okozott. Ez a rendszer folyamatos újraindítását okozó, úgynevezett Reset vagy Reboot vírus volt.

Ennél már többet pusztított a Péntek 13-a vírus, 1989 őszén, amelynek első példányaait a Szovjetunióból programmal együtt, floppyn hurcolták be egy magyar bányavállalat számítóközpontjába, ahonnan az továbbterjedt. Az eredeti változat a Postánál, valamint a Budapesti Műszaki Egyetem számítógépes rendszerében programok és adatok végleges elvesztését és a rendszer leállását okozta, de a helyzet még mindig nem volt annyira katasztrofális.

A vírusoknak is megvan a maguk sorsa. Maga a szovjet vírusváltozat egy izraeli eredetű vírusnak, az Israeli #2-nek, másik nevén Jerusalem-B-nek „megpatkolt verziója”. Az eredeti onnan kapta a nevét, hogy a palesztinok az izraeli Hebrew University (Jerusalem) számítógép-hálózatába juttatták be 1987 decemberében, azzal a céllal, hogy azon a napon, amikor péntek 13-ára esik, törölje az állományokat, amelyeket megfertőzött.

Ezt a vírust a Szovjetunióban teljesen visszafejtették, majd némileg módosítva újrafordították. Sajnos egyre több Magyarországon készült átirása is megjelent, amelyet a hagyományos killerek és detektorok nem érzékelnek. Így például felbukkant egy olyan változat is, amely az elkövetkezendő első

keddre, azaz 1990. május elsejére volt programozva, hogy elpusztítsa a fertőzött adatállományokat.

A vírusprogramok ellen — mint korábban hozott példáink is bemutatták — a világ minden jogszerűsége törekvő országában hivatalosan fellépnek. Vagy az adatvédelmi törvény keretében (mint az USA-ban), vagy a polgári törvénykönyvben a károkozással kapcsolatosan (mint az NSZK-ban), vagy pedig a terrorizmus elleni harccal és az állambiztonsággal kapcsolatosan (mint például Izraelben) büntetik ezeknek a vírusoknak az íróit és tudatos terjesztőit. Az Amerikai Egyesült Államokban például a szigor odáig megy, hogy az államigazgatásban, a hadseregben nem alkalmazható egyetlen olyan program sem, amely bármiféle másolásvédelemmel van ellátva. Majdnem minden USA tagállamban megtiltják az ilyen programok kereskedelmi forgalomba bocsátását is.

A törvényi szankciók az európai országok nagy részében sajnos nem hatékonyak, és a jogszabályok is kétértelműek, ezért rendelkezéseik egyelőre még kijátszhatók. A szaklapokban nem is egy másolásvédelmi eszköz (program és hardverlock) hirdetését olvashatjuk. És ha hirdetnek ilyen programokat, akkor valószínűleg vevő is akad rá. Súlyosbítja a helyzetet, hogy a kevésbé vagy egyáltalán nem hozzáértő vevőnek bebeszélük: a másolásvédelem kifejezetten vírusvédelmet szolgál, vagy éppenséggel azt akadályozza meg, hogy eltulajdonítsák az ő drága pénzen megvásárolt programját. Sajnos a CAD-CAM szoftverek forgalmazói is ilyen trükkökkel élnek, pedig ott különösen fontos lenne a gyors telepíthetőség, a megbízhatóság, s hogy a felhasználó a programot saját vállalatának határain belül úgy használhassa, ahogy az munkájához a legmegfelelőbb.

Vannak nem károkozó, tisztességes programlopás-védelmi eljárások is. Ilyen például, hogy a programot „beégetett” sorszámmal, valamint a felhasználó nevére szóló dedikációval látják el, s így nyomon követhető az illegálisan forgalmazott példányok eredete.

Még egy kérdést kell előre tisztázni. A másolásvédelem fogalmát sokan összekeverik — nem egy esetben tudatosan! — a hozzáférési jogok, illetve a szelektív hozzáférés biztosításával, pedig két különböző dologról van szó.

A másolásvédelem célja a program futásképesységének megakadályozása vagy tönkretétele, abban az esetben, ha a programot nem a forgalmazó által

készített eredeti lemezről indítják (kulcslemezes futtatás), illetőleg ha nem építenek a gépbe vagy nem csatlakoztatnak a géphez szintén az eladó által rendelkezésre bocsátott, nem szabványos hardvereszközt (kulcskártyát, illetőleg hardverlock-ot). Amennyiben nem talál a program megfelelő környezetet, jó esetben csak „öngyilkos” lesz, rossz esetben aránytalanul nagy kárt is okoz a felhasználónak, mintegy önkényesen megbüntetve őt az illegális másolásért. Rafináltabb módszerek alkalmazása esetén ez a rutin később, egy látszólag zavartalan működési periódus után aktivizálódik, ezáltal a kártétel még nagyobb lesz. Ha a lappangási idő alatt nem szabadít ki magából szaporodásképes károkozót, akkor „trójai funkcióban” működik, ha pedig kiszabadít, akkor vírusprogramként lép akcióba. Mindenképpen illetéktelen beavatkozás a felhasználó munkájába. Senki sem venne olyan kalapácsot, amely csak egy bizonyos üzem, bizonyos színűre festett szobájában, egy meghatározott gyári számú munkaasztalon, az eladó által rendelkezésre bocsátott és sorszámozott satuban megfogott munkadarabhoz lenne használható, s ha ezen feltételek valamelyike hiányozna, akkor a kalapács felrobbanna, elpusztítva az üzemet és használóját egyaránt... (Hogy azért ez túlzás? Igen, de csak egy kis túlzás!)

A másolásvédelemmel ellentétben a hozzáférés-védelem a számítástechnika egyik legtermészetesebb eszköze. Azt határozza meg, hogy milyen jogkörű felhasználó mely adatállományokat vagy azok mely részeit és milyen jogosítvánnyal, beavatkozási lehetőséggel (írás, olvasás, írás és olvasás, keresés, másolás stb.) használhatja. Ezt vagy az adathálózat biztosítja a hálózati vagy normál operációs rendszer alapszolgáltatásaként (pl. Novell, UNIX), vagy pedig szoftveres titkosítással oldják meg. Ilyen titkosítás esetén csak a kulcsszó (szavak) ismeretében végezhetők meghatározott műveletek a meghatározott állományokban, de amennyiben nem tudjuk a kulcsot, és illetéktelenül próbálkozunk belenézni a számunkra nem hozzáférhetővé tett „aktákba”, kárt akkor sem okozunk, a rendszer nem semmisít meg állományokat, legfeljebb megtevesztő információkkal traktál bennünket.

Például a PKARC—PKXARC—PKPAK—PKZIP programrendszerek rossz jelszó megadásakor „szemetet” csomagolnak ki magukból, vagy pedig hibaiüzenettel utalnak arra, hogy az állomány sérült. Ez utóbbit a megfelelő kulcsszónál természetesen nem teszi. Kárt viszont soha nem okoz...

A tisztességes forgalmazás az előfeltétele annak, hogy a felhasználók is tisztességesek legyenek. Minden programnak van egy adott ára — ez az úgynevezett lopáshatár — amelyet a nyugati országokban nagyon jól behatároltak. Ez arányban áll annak a személynek a jövedelmével, munkabérével, akinek a munkáját a program helyettesíteni hivatott. Ugyanakkor az oktatási intézmények nem termelő célra ennek az üzleti forgalmi árnak a töredékeért kapnak jogos példányokat, vagy például a szaksajtó képviselői, a szaklapok szerkesztősei is kaphatnak ingyenes, de jogosított és működő — azaz nem demonstrációra lebutított — szoftvereket. Ilyesmi Magyarországon ritkaságszámba megy, nyugati cégek készségesebben adnak tesztpéldányokat.

Hazánkban a vírusok járványszerű terjedése 1990-ben felgyorsult. Ennek több oka is van. Egyes forgalmazók például egy-egy program néhány eladott példányával szeretnének meggazdagodni. Így a főkönyvi rendszerek tucatjaiban találhatunk olyan másolásvédelemnek álcázott időzített aknákat, amelyek a forgalmazók bevételeit növelik, s teremtenek számukra folyamatos piacot. S ezek a programok sok esetben a megadott idő letelte után maguk is vírussá válnak, megrongálják az adatállományokat, sőt egy részük terjedni is képes.

Ismét számolnunk kell ugyanazzal a jelenséggel, amivel a Commodore 64 megjelenésekor találkoztunk, hogy a javításra szoruló gépek számát mesterségesen is növelni lehet. Találkoztunk olyan vírusirtó programmal is, mely ugyan levette a vírust, de biztos ami biztos alapon feltett egy olyan másikat, amelyik ellen nem volt hatásos. Így csinált piacot az újabb programverzióknak... Most pedig esély van arra is, hogy egyesek maguk írnak olyan vírust, melyet aztán komoly tarifáért kiirtanak.

Nem véletlen, hogy Nyugat-Európában a számítógépvírusok elleni programokat vagy önköltségi áron, vagy ingyenesen biztosították a felhasználóknak. Ez a jótékony irányzat azonban megszűnni látszik. A piacon kapható termékek egyre nagyobb hányada alapszik az emberek félelmének megvámolásán. Ezek a programok, bár jók, de nagyon drágák. Szerencsére az olcsó közprogramok, a freeware-ek, shareware-ek között is találhatunk valóban jó programokat. Ezeknek a komoly szellemi befektetést tartalmazó szoftvereknek az ára csak töredéke a hasonló tudású kereskedelmi szoftverekének. A nagy forgalmazó cégek is támogatják fejlesztési és reklámpénzeikből ezeket

a törekvéseket, saját érdekükben. Erre különösen akkor figyelhetünk fel, amikor náluk is felüti a fejét valamilyen alattomos vírusjárvány.

A vírusirtó szoftverek olyanok, mint az elsősegély. Egy adott problémát oldanak meg. Viszont a hangsúlynak a fertőzés megelőzésén kellene lennie. Az erre a célra forgalmazott szoftverek árából legalább a fejlesztési költségeknek és a témával foglalkozók bérének, közterheinek meg kell térülniük. Így sajnos a szabad szoftverek mellett egyre inkább számolni kell az igen drága vírusmegelőző védelmi programrendszerek elterjedésével is.

EGY KIS TIPOLÓGIA

Milyen is egy vírusprogram? Semmiképpen sem olyan, mint az élő szervezet, azaz nem látható mikroszkóp alatt, mint egy baktérium. (Bár volt egy orvosnő, aki miután megjelent Magyarországon az első ilyen víruscikk, felhívta a szerkesztőséget és kérte: mutassunk már neki egy ilyen vírust mikroszkóp alatt!)

A vírusprogramokra nagyon találó meghatározást adott Buruzs Tamás, a Kandó Kálmán Villamos Műszaki Főiskola informatika szakos hallgatója, amikor az MTESZ egyik rendezvényén Éltető Lászlóval, a másolásvédelmek ismert szerzőjével folytatott vitájában a következőket mondta: „A vírusprogram intelligencia és mesterséges értelem, de erkölcs és érzelem nélkül. Intelligenciáját a programozójától kapta, és annyira lehet erkölcstelen, amennyire a program írója is az. Már ma is lehetséges olyan programot írni, amely belátható időn belül tönkretetheti egy teljes számítógép-generáció működését. Például egy vagy két esztendőn belül lehetetlenné tehető, hogy valaki MS-DOS alatt futó programot alkalmazzon. A vírusprogram valójában az élő anyag működését utánzó életképes modell. Olyan, mint a biológiai fegyver, mert miután kiengedték a laboratóriumból, még maga az alkotója is elveszíti az ellenőrzést felette.”

Szerencsére vírusfejlesztő készlettel kereskedelmi forgalomban még nem jelentkezett egyik gyártó sem. Viszont információink vannak arról, hogy nem kereskedelmi forgalomban Magyarországon már létezik olyan fejlesztő rendszer, melynek kutatómunkálatai „programmásolás-védelem fejlesztés” fedőnéven mintegy másfél esztendeje folynak. Ennek eredményeképpen jelennek meg az önbíráskodó másolásvédelmek a hazai piacon.

Könyvünk egyik célja, hogy leleplezzük a vírusírók által használt programozástechnikai trükköket, s bemutassuk azt az eszköztárat, amelynek segítségével még egy ismeretlen vírus ellen is viszonylag rövid idő alatt megírható a specifikus killer (azaz a vírusprogramot kitakarító és az eredeti állományt a lehetőségekhez képest eredeti formájában visszaállító), illetve a detektor

(azaz a vírus jelenlétét, a vírus által végzett rendszerműveleteket érzékelő) program. Az elsődleges cél a felhasználók adatainak védelme!

Elmúlt már az az idő, amikor egy-egy vírus ellen írt programmal le lehetett tarolni a magyar piacot. A felhasználó nagyobb biztonságra vágyik, és azt részesíti előnyben, amelyik a károk megelőzésére komplex védelmet tud nyújtani. A világon ma még nem sok cég szakosodott erre a feladatra, s azok is folyamatos információ- és programcserét folytatnak egymással. Most folyik annak a rendszernek a kidolgozása, amely szigorú garanciák mellett teszi lehetővé a vírusok cseréjét. Vírusok elleni programot könyvből ugyanis nem lehet írni, mert szükséges hozzá magának a vírusnak a birtoklása és visszafejtése. A garancia pedig azért kell, mert túl nagy a kísértés arra, hogy miután valaki kidolgozta az ellenanyagot a vírus ellen, utána kiszabadítsa azt a „palackból”, hogy ezzel saját vírusellenes programjának keresletét növelje.

A számítógépes vírusokat, a kárt okozó programokat igyekszünk leleplezni, mielőtt azok még kárt okozhatnának. A számítógépes vírusprogramok kidolgozásának az volt az egyik célja, hogy a felhasználót bosszantsa és megakadályozza a program vagy a számítógép rendeltetésszerű használatában. Tehát, hogy romboljon, kárt okozzon. A vírusok ott szaporodnak a legjobban, ahol egy számítógépet egymástól függetlenül többen használnak: egyetemeken, iskolákban, számítástechnikai klubokban. Ha ilyen helyekről kerül elő egy vírusprogram, az általában még nem jelenti azt, hogy ott is fejlesztették ki. Nagy szoftverforgalmuk miatt ezek a számítógéplaborok sajátos „légyfogóként” működnek, és az itt felbukkanó vírusok mintegy előre jelzik az országos járványokat is.

A számítógépes vírusprogramok a biológiai vírusokhoz hasonlóan az egészséges szervezetet (programot, gépet) megtámadva szaporodnak. A számítógép operációs rendszerét felhasználva fertőzik meg a programokat, ritkábban magát a gépet, a hardvert. Néhány vírus az üres floppylemezt fertőzi meg — ezek az úgynevezett boot-vírusok —, így elősegítik a szoftvercserével történő terjedést. Olyan „ördögi kóddal” fertőzik meg a programokat, amelyek más számítógépen is reprodukálni tudják önmagukat. A hordozó programot — miként a biológiai hadviselés szakirodalmában — vektornak nevezik a szakírók.

A hordozó program ügyes megválasztásától függ, hogy a fertőzés milyen

nagy adatállományban és programállományban lép fel egyidejűleg. Vegyünk például egy olyan programot, amely egyszerűen és gyorsan készít másolatot lemezünkről. Ez nyilvánvalóan egy olyan szoftver, amelyet mindenki másolni fog, különösen akkor, ha szabad szoftverként került a piacra. Csábító lehetőség beleépíteni egy olyan vírusprogramot, amely például 100 másolás után aktivizálódik. De ha a programozó nem tudja megoldani a másolás figyelését — ami programozástechnikailag valóban nehéz feladat —, akkor választhatja például azt, hogy a vírus egy év lappangási idő alatt nem csinál semmit. Addig pedig, amíg életre nem kel, csak terjednie, észrevétlenül szaporodnia kell, azaz bemásolnia magát más programokba. Amikorra kellőképpen elterjedt, mintegy varázsütésre megindul a károkozás! A pokolgép robban. Ha a felhasználó még a terjedési szakaszban észreveszi a vírus jelenlétét, akkor megakadályozhatja a pusztítást.

A vírusok általában a COMMAND.COM, az IBMBIO.COM és az IBMSYS.COM (illetve .SYS) programokat fertőzik meg az MS-DOS™, valamint az IBM PC-DOS™ operációs rendszerek esetén, mivel ezek minden DOS rendszerlemezen megtalálhatók. Az UNIX™, a XENIX™ operációs rendszer, valamint a NOVELL™ hálózati szoftverekkel már nehezebb a vírusok dolga, mert ezek a rendszerek részben védettek a külső, illetéktelen programmódosítások ellen. De ezek is kicselezhetőek. Az operációs és hálózati rendszerállományok méretének figyelése minden esetben célszerű. Természetesen ha már bejutott a vírus, az a programok elindításával azonnal tovább is terjedhet.

Az egyes önreprodukáló és kártékony programokat különbözőképpen nevezi a szakirodalom. Célszerű tisztázni, mit minek nevezzünk, hogy ugyanazt értsük rajta mindannyian.

Programférgek (worms)

Olyan programok, amelyek nem szaporodnak, hanem belépve egy rendszerbe keresztülrágják magukat annak védelmi mechanizmusán. Feladatuk legtöbbször az, hogy behatoljon az operációs rendszer magjába — a kernelbe —, és onnan kihozzanak bizonyos információkat, például jelszótáblákat. Ennek elvégzése után általában csendesen kimúlnak.

Trójai programok

Kissé körülményesen „trójai faló típusú programoknak” is nevezik őket. A lényege: ezek a programok csak álcázásra szolgálnak. Mást tesznek, mint amit ígérnek. Például megveszünk egy könyvelői vagy DTP programrendszert, s egy év és néhány nap elteltével gépünket bekapcsolva azt vesszük észre, hogy programunk is, adatállományunk is tönkrement. Tessék megvenni az új verziót!

Bár az ilyen programot a vírusok egyik alfajaként tisztelik, az általában nem viselkedik „tisztességes” vírushoz illően. Legtöbbször ugyanis aktivizálódása után azonnal „üt”, olyannyira, hogy nincs is ideje szaporodásra, legfeljebb a gépen belül. Hogy valójában miért sorolják sokan mégis ebbe a kategóriába? Egyszerűen azért, mert programmásolás útján terjed, hordozójuk legtöbbször valamelyik program valamelyik változata. Amikor pedig az egész kiderül, forgalmazója programhibásnak vagy másolásvédettnek nevezi. Ezek az üzleti csibészségek — az USA-t kivéve — a bíróságok előtt ma még általában büntetlenek maradnak. Mire ugyanis az igazságszolgáltatás lomha gépezete működésbe lép, eltűnnek a bizonyítékok. S a gyanús programok forráskódjának kiadására a világon szinte sehol sem kötelezhető senki sem.

Trójai program lehet akár egy diagnosztikai program vagy egy játék, amit kifejezetten károkozási szándékból készítettek. Például mialatt lefut egy számítógépes pornó-show, tönkremegy a merevlemez.

Nem trójai program, bár hasonlóképpen viselkedik az a szoftver, amelyben valamilyen súlyos hibát felejtett benne programozója. Ilyen a Norton Disk Doctor első kiadása (NDD.EXE a Norton Advanced Utilities programcsomagból), amelynél programozási hiba miatt, amikor nem DOS rendszerrel, hanem például a Disk Manager szoftverrel formáztuk merevlemezünket, akkor az NDD a C: partíció kivételével mindent tönkretesz. Ránéz, közli, hogy hibás — ugyanis nem DOS —, és sajnos kérdés nélkül „helyreállítja”, tönkreteszi. Az újabb verzióknál cselekvés előtt kérdez, mert ezt a hibát kijavították. Szintén nem trójai program az a program, amellyel az operációs rendszer feje felett átnyúlva kárt is lehet okozni. Ez ilyenkor a mi hibánk. Például ha valaki megfelelő ismeretek nélkül belekotor a FAT-ba, azaz az állományelhelyezkedési táblába (file allocation table), és kárt okoz, az ma-

gára vessen! A programokba csak olyan helyeken turkáljunk bele, ahol értjük is, mi történik, amikor valamit megváltoztatunk!

Vírusprogramok

A gyakorlatban vírusprogramoknak azokat a programrendszereket nevezzük, amelyek önmagukat reprodukálni képesek. Más szoftverek megfertőzésével, esetleg formázott floppyval vagy éppenséggel magával a géppel terjednek (hardvervírusok). Továbbító közeg lehet számukra a számítógépes adatátviteli hálózat is. A fertőzés, a támadási felület, a károkozás és a terjedés módja szerint ezeket tovább osztályozzák a mindent beskatulyázni kész szakemberek. Ha már az ember megteremtette adatbázis-kezelő rendszereit, fel is szeretné tölteni azokat. Próbáljunk meg most mi is belenézni ezekbe a fiókokba. Vegyük sorra, milyen típusú vírusok keseríthetik meg életünket.

1. Memóriaszemét vagy „kuka-vírusok”.

Teleszemetelve a memóriát lehetelenné tehetik egy másik program futását. Más kárt nem okoznak, csak egy kis rendszerleállást... akár néhány száz gépen. Általában nem rongálják meg a rendszerben lévő adatokat, s a jóindulatúbbak nem is másolják be magukat más programokba. Írójuk inkább szakmai tudásának fitogtatásával igyekezett másoknak gutaütést okozni, bármiféle materiális romboló szándék nélkül.

Hasonlóképpen írható úgynevezett „kiszolgáltató” vírus is. Ezzel elsősorban a számítástechnikai adatvédelmi rendszereket lehet kijátszani. Mert tegyük fel, írunk egy vírusprogramot, amely hozzákapcsolódik a Novell billentyűzetkezelő rutinjához, esetleg a bejelentkezést adminisztráló LOGIN.COM-hoz. Azért oda, mert ezeket mindenkinek használnia kell. Ezek után a beültetett „poloska” megfigyeli, melyik felhasználó jelentkezik be supervisorként, azaz teljes jogú rendszergondnokként és milyen jelszóval. Az elvesztett jelszót a vírus kódolva lerakja egy olyan állományba, amelyhez mi is hozzáférünk. Innen már csak le kell kérdezni valamilyen másik programmal, s a jelszó ismeretében azt csinálunk e rendszerrel, amit akarunk.

Némileg nagyobb felkészültséggel ezt a viccet meg lehet csinálni úgy is, hogy a nyilvános kommunikációs hálózaton keresztül, például a telefonvonal gateway-n, azaz külső csatlakozáson keresztül juttatjuk be házi „kémün-

ket". Egy ilyen tréfa eredményeként sikerült 1989-ben megbénítania egy amerikai diáknak az USA Arpanet félkatonai tudományos adathálózatát. Itt nem is annyira a program főrutinjának a megírása a nehéz feladat, hiszen csak foglalni kell a memóriát, mindig újra bemásolva a már addig bemásolt szemetet a meglévő mellé. Ilyen stratégia esetén nincs olyan memória, amely egyszer ne telne be! A nagyobb akadályt az adatvédelem kicselezése jelenti, hiszen ezek a rendszerek kívülről nem fogadnak végrehajtható programokat. Ilyen behatolást ezért inkább csak programférgékkel lehet megoldani.

2. A programkódot módosító vírusok

A legismertebb és leggyakoribb víruscsalád. Az eredeti programmal sohasem találkozunk, hacsak magunk nem írunk ilyet. Viszont az általa módosított programmal könnyen köthetünk nem kívánatos ismeretséget. Igaz, ez a kód már magát a vírust is tartalmazza. Tágabb értelemben ide sorolhatjuk a floppy és a merevlemez formátumát megzavaró „vendégeket” is. Szintén nagyon sok altípusa létezik, támadáspontja és terjedési módja szerint.

Veszélyességük miatt ezekkel fogunk könyvünkben legtöbbet foglalkozni, hiszen a szoftvermásolás és az adatátvitel során főképpen ezek a vírusok terjednek. Ebben a csoportban tarják számon a szakemberek az etikátlan másolásvédelmet, valamint egyes hasznos, a vírusok ellen használható szoftvertípusokat is. Megjegyzendő, hogy a másolásvédelemként alkalmazott vírus jellegű programok egy része nem szaporodik, csak a kijelölt célprogramot fertőzi meg a „védelem felrakásának” nevezett folyamat során.

3. Hardvervírusok

Az eddig említett vírusok fertőzési forrása maga is program. Ez adatátviteli csatornán vagy floppyn kerülhet a rendszerbe. Arra kevesen gondolnak, hogy fertőzési forrás lehet maga a hardver is, pontosabban az abban gyárilag vagy egyéb úton eltárolt szoftver, melyet angol szakmai műszóval firmware-nek neveznek.

A régi PC-kben és XT-kben nagyon kevés olyan rejtett zug volt, ahova egy ilyen csapdát be lehetett volna építeni. Ki kellett volna cserélni vagy a gép ROM BIOS-át, vagy pedig a lemez meghajtó kontrollerének a ROM-ját. Az AT volt az első olyan gép, amely szinte tálcán kínálta a vírusnak a lehetőséget.

Az óra IC-nek vannak olyan nem publikált EEPROM regiszterei, ahova beírható egy meglehetősen rövid, de üzemképes víruskód. Azért hallunk viszonylag ritkán ezekről, mert egy-egy gyártó cég — főleg Nyugat-Európában — nem engedheti meg magának, hogy fertőzött terméket bocsásson ki. Komolyabb hardvervírust szinte kizárólag csak a gyártó helyezhet el egy rendszerben. Újabb lehetőséget kínált ilyen hardvervírusnak a felhasználókhoz való becsempészésére a másolásvédelem új irányzata. A hardverkulcsos szoftverek esetében a géphez csatolandó „fekete doboz” már elég komoly memóriával rendelkezik a hardver által terjesztett vírus célbajuttatásához. Erre sajnos az USA-ban már voltak próbálkozások, nem is sikertelenül.

A COCOM-mal kapcsolatos egyik kongresszusi vitában hangzott el, hogy a szuperszámítógépek és programok olyan védelemmel vannak ellátva, amelyek megakadályozzák e gépeknek ismeretlen helyen való működtetését. Egyes amerikai nagygépekről, szuperszámítógépekről és programvédelmi kártyákról már köztudomású volt, hogy műhold segítségével le lehet kérdezni működési helyüket, és a feladatot is, amin éppen dolgoznak. Ugyanakkor ezek a gépek ilyen műholdparancsokkal tönkre is tehetők. A hardverlock is hasonló lehetőségeket kínál. Az informatikai társadalmakban egyre több adat, vezérlés összpontosul ezekre a géprendszerekre, a felhasználó pedig ki van téve terroristáknak, hatalmukkal manipuláló erőknek, vagy a forgalmazók zsarolásának.

Hogy ilyen rendszerek vannak, az tény. A nemzetközi bankátutalási rendszerben például az egyes terminálok „utolsó utáni óra” típusú védelemként központi utasítással tönkretételők. Az egyes IC-gyártók nagy anyagi eszközökkel folytatnak kutatásokat a korlátozott élettartamú félvezetők, illetve a kibonthatatlan áramköri tokozások kifejlesztésére. Egy jelenleg Németországban élő magyar fizikusnak, Teleki Péternek több országban elfogadott, elméleti jelentőségű szabadalmi bejelentése van, ebben felvázolja a nyomtatott áramköri lapka élettartamát korlátozó eljárásokat, illetve megteremti annak elméleti lehetőségét, hogy az idő függvényében egy bizonyos IC-lapka felszínén kialakított áramkör egy másik, ettől teljesen eltérő áramkörre alakuljon át. Például ha megveszünk egy ROM kártyát, az abban lévő információ jól beállítható idő letelte után eltűnik, és helyét például a szoftver újbóli megvásárlására felszólító rendszerüzenet veheti át...

Bár nem vírus, de ebben a témakörben feltétlenül említésre érdemes a hardverbe beépített és a szoftverben felejtett programhiba, a „bogár” (bug). Leggyakrabban az új processzorok első sorozataiban találhatók. Az ok egyértelműen a sietség, amellyel az új terméket piacra szerették volna dobni. Furcsa dolog, de tény, hogy az Intel 8085-ös, a 80386-os processzorok első sorozataiba hibás mikroprogramot égettek be, s a processzor bizonyos lebegőpontos aritmetikai műveleteknél hibázott. Úgy látszik, a sietség azonos hibákat szül, mert hasonló gondok miatt késlekedett az Intel 80486-os termékének a sorozatgyártása. A gyártók határidőre elkészültek az új konstrukciókkal, mégis csak késéssel, 1990 tavaszán indulhatott a nagyobb sorozatok kibocsátása.

4. Hardvermódosító vírusok

Bár hardvervírusoknak nevezik általában ezeket a vírusokat is, inkább a vírusprogramok speciális nemzedékének tekinthetők. Jobb kifejezés hiányában hardvermódosító vírusoknak nevezzük őket. Az elektronikai szakmérnökök körében tartotta magát az a tévhit, hogy pusztán programokkal nem tehető tönkre egy áramkör vagy nem válhat ócskvassá egy egész berendezés. Az élet rácaffolt erre. Az egyre intelligensebb építőelemeknek egyre több a sebezhető pontjuk, hiszen a gyártás tipizált, és sok áramkörüi lapkáról csak a mikroprogramok beégetése során dől el, hogy valójában milyen feladatokra szánják azokat. S amit egyszer beégettek — tehát nem az áramkörbe „huzaloztak be” —, azt megfelelő technológiával bármikor módosítani is lehet. Csak papír és ceruza, no meg némi szaktudás kell egy ilyen program kifejlesztéséhez. Mit is tesznek ezek a programok?

Szórványosan Magyarországon is felbukkantak a 80386-os processzor mikroprogramját módosító vírusprogramok. Ezek a processzorban a gyártás során betöltött, elektromosan írható és törölhető regiszterekben található mikroprogramokat írják át. Az ehhez szükséges utasításokat a gyártók természetesen nem publikálták, de voltak ügyes programozók, akik kiderítették ennek módját.

Hasonló ötlettel működik az a hatását szövegszerkesztőkön keresztül kifejtő hardvervírus, amelyet a Sierra Software cég Larry nevű játékprogramjai terjesztenek. Ennek első példányairól 1988 decemberében, karácsony első

napján az osztrák tévéhíradóból szerezhett tudomást a világ. A szoftver egyes kalózváltozatai(?) terjesztettek egy olyan vírust, amely először megfertőzte a gépekben lévő rezidens programokat, például a Sidekicket vagy a Norton Commandert. Ha utána behívtak egy szövegszerkesztőt, akkor átmászott abba. Érdekes módon csak a magas szintű programnyelveken írtakat, például az MS-Word-öt szerette, míg az Assemblerben írtakat (Personal Editor, Norton Editor) nem bántotta. S ha azután nyomtatni szeretett volna vele a gyanútlan felhasználó, akkor valami érthetetlen zagyvalékot kapott Epson printerén. Ugyanis ez a program — ha hinni lehet a híradásoknak, mert szerencsére messze elkerülte gépeinket — egy kissé megkeverte a nyomtató EEPROM-ját.

Ahhoz, hogy megértsük a dolgot, tudni kell: a nyomtatók nagy részét üres EEPROM-mal szerelik össze, és kiszállításkor a gyártó azokat a karakterkészleteket tölti be, amelyeket a vevő kér. S ráadásul vannak olyan olcsó és drága típusok az Epson gyártmányai között, amelyek csak a nyomtató EEPROM tartalmában különböznek. Ez a vírus nem azonos a könyvünkben MIX néven regisztrálttal. Az ugyanis csakis szoftveres úton zagyválja hihetelenül össze a kinyomtatott szöveget.

A továbbiakban főleg a programkódot módosító vírusok lélektanával, az ellenük való védekezéssel, a szükséges elővigyázatossági rendszabályokkal, ismert vírusok lelkiéletével szeretnénk foglalkozni. Megismertetni mindenkit azokkal a veszélyekkel, amelyekkel számolnia kell bármily kis számítástechnikai rendszer üzemeltetése során is. Aki pedig nem szereti a száraz programlistákat, utálja az Assamblert, a vírusprogramok visszafejtésének és analízisének szinte egyedüli eszközét, az se tegye le a kiadványt! Ígérjük, hogy a listák átugrásával is érthető lesz a leíró rész mindenki számára, aki alapfokon már ismeri a számítástechnikai fogalmakat.

EGY PÁNIK TÖRTÉNETE: PÉNTEK 13

Ha péntek 13-ára esik, a babona szerint az szerencsétlen nap. A magyar — és általában az európai — számítástechnikában 1989 októberében valóban kellemetlen volt ez a nap. A második számítógépes bűnözési hullám egyik oszlopos tagja, a Péntek 13 vírus ekkor Magyarországon is rombolt. Bár hivatalos vélemények szerint csak jelentéktelen károkat okozott, e sorok íróinak mint hivatásos vírusvadászoknak alkalmuk volt követni a történeteket, és a kárt nagyobbak látták. Így talán indokolt, hogy az időrendi sorrendet felrúgva először ezzel a vírusprogrammal foglalkozzunk. Aktivizálódása után egy héttel már látszott, mekkora kellemetlenséget okozott:

— A Magyar Posta pénzügyi számítógépes helyi hálózataiban több rendszer leállt.

— A Budapesti Műszaki Egyetem több helyi hálózatában — amelyek Novell alapú rendszerek — ezen a napon sok állomány eltűnt, illetőleg hálózatlan állapotba került.

— Megelőzőként több számítóközpontban ezen a napon nem dolgoztak. Ezzel, bár elkerülték a rongálást, magát a kórokozót nem semmisítették meg.

— Az APEH (aki nem ismerné: az Adó- és Pénzügyi Ellenőrzési Hivatal) cáfolta, hogy nála adatok semmisültek volna meg. Igaz, ekkor még a DOS alapú PC-kkel csak adatrögzítést végeztek, az adatbázis Siemens nagygépeken volt más cégeknél, amelyeket ez a fertőzés nem érintett. Mindenesetre elfogadták, ha valaki ezen a napon a vírusveszélyre tekintettel átállította gépének belső óráját.

— A Magyar Rádió a Péntek 13 vírus aktivizálódásának reggelén szakértők bevonásával tájékoztatta az érintett szakmai köröket. Felhívták a figyelmet, hogy ez a vírus csak az MS-DOS™ és az IBM-DOS™ operációs rendszerű gépeket veszélyezteti. Azon a napon ennek ellenére sok telefon futott be a Commodore™-64 tulajdonosoktól is.

— A CWI is előre felhívta a figyelmet a veszélyre, és a védekezéshez egy vírusmentesítő program teljes Assembler listáját közölte. Később kiderült,

hogy ez a szoftver bizonyos szélsőséges esetekben, ha a vírus éppen paragrafushatárra épült be, nem volt képes az állományok teljes körű visszaállítására. Ezt a programot a Műszertechnika Kisszövetkezet egy segédprogrammal kiegészítve ingyenesen a felhasználók rendelkezésére bocsátotta. Mintegy 1500 felhasználó kapta meg tőlük akkor ezt a programot. Hasonló feladatokra ekkor már megjelentek pénzért árusított programok is. Közülük minőségével tűnt ki a CS & Egér álnévre hallgató szerzőpáros (Leitold Ferenc és Tábor Csaba) CHKVir programjának első kereskedelmi verziója.

Ide tartozik, hogy elmondjuk: ekkor találtak egymásra a jelenleg újra az Ázsió Microtrade támogatásával működő vírusirtó csoport tagjai. A csoport magját ennek a könyvnek a szerzői alkották. Kínosan ügyeltünk szakmai és etikai függetlenségünkre, ezért utána a legalkalmasabb működési kereteket több helyen is keresgeltük (Új Hullám, Szolinfo Kft.), mígnem 1990 őszére létrehoztuk az Ázsió-Viki csoportot. Közben újabb tagok is beléptek, mert munkánk sajnos egyre több lett. A Péntek 13 vírus dühöngésének évében kibocsátottuk a Prgdoki 2.11E angol, majd magyar nyelvű verzióját, amelyet a vészhelyzetre való tekintettel az Ázsió támogatásával ingyen osztottunk a Orgtechnik kiállításon. Sajnos a bétatesztes verzió elkészítése során ugyanabba a hibába estünk, mint a CWI-s program szerzője. A program nem volt képes korrekten eltávolítani a vírust, ha az paragrafushatárra esett. Ezt a verziót Kecskemét környékén hoztuk forgalomba. Az Orgtechnik kiállításra azonban már elkészítettük a korrigált végleges verziót, s forgalomba hoztunk egy segédprogramot a korábbi hiba kiküszöbölésére. Mintegy 2000 felhasználóhoz jutott el a program ezen a csatornán.

Ezek után néhány szót magáról a vírusról, amely akkora idegességet okozott a felhasználók körében.

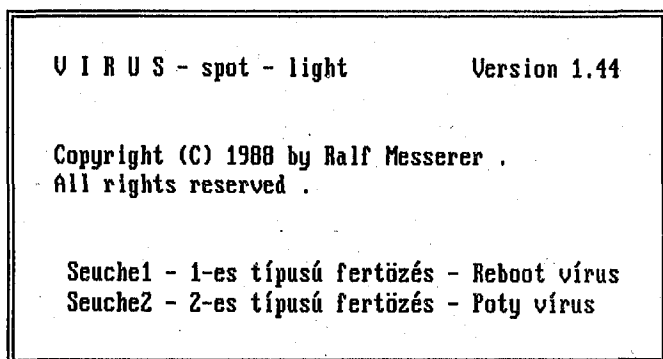
Születésének dátuma a szakirodalmi adatok szerint 1987 decembere. Ekkor fedezték fel a Jeruzsálemi Héber Egyetem (Hebrew University of Jerusalem, Israel) számítógépes hálózatában. A fertőzést szerencsére nem sokkal annak megtörténte után diagnosztizálták, és viszonylag rövid idő alatt sikerült elhárítani. Akkor a legközelebbi Péntek 13-a éppen arra az évfordulóra esett, amikor a palesztínok elkezdtek harcolni az izraeliek ellen, így a vírusakció valószínűleg a kor technikai színvonalának megfelelő merényletkísérlet volt.

A szakemberektől az eredeti változat a Jerusalem-A, az Izraeli Vírus #1, a

Péntek 13, illetve az 1813-as vírus nevet kapta. Ezeken a neveken hivatkoznak rá ma is a szakkönyvek.

Amikor ez a vírus megérkezett Magyarországra, az már nem az eredeti volt, hanem annak a Szovjetunióban átírt változata. Feltételezhető, hogy rajtunk és az NDK-n keresztül jutott el utána Nyugatra is. Fertőzési tünetei és aktivizálódási feltételei hasonlóak a nemzetközileg ismert standard víruséhoz, de azért vannak eltérések.

Megjegyzendő, hogy nagy késéssel felbukkant ennek a vírusnak egy „megpatkolt” verziója is. A vírusazonosítót írták át, hogy a hagyományos technológiára épülő detektorok ne ismerhessék fel, valamint némi humorral a dátumot kedd 1-jére tették, mert 1990-ben az első dátum, amely ennek a feltételnek megfelelt, május elseje, a munka ünnepe volt...



A VIRUS-spot-light víruskereső program bejelentkezője

GYAKORLATI VIROLÓGIA

A Kedd elseje kapcsán kerültünk szembe azzal a problémával, hogyan készüljünk fel a detektor programok és a vírusirtó szoftverek írásakor az ilyen egyszerű, de nagy hatású „piszkos trükkökre”. Ekkor jutottunk arra a következtetésre, hogy nemcsak a vírust azonosító bájtsorozatot kell figyelni, hanem meg kell találni a programnak azt a fő rutinját, amely nem írható át anélkül, hogy a vírus működése ne károsodna. Illetve ha ezt valaki átírja, azzal egy gyökeresen új vírust hoz létre. Tehát ezt a rutint — a vírusmagot, azaz kernelt — szintén figyelni kell. A Prgdoki v3.02 már ennek a felismerésnek a jegyében született, nem a szabványos és megszokott módon ismeri fel a Péntek 13 vírust, hanem a dátumtól függetlenül irtja az átírt verziókat is.

A legnagyobb probléma az, hogyan takarítsuk ki a vírusokat az állományokból. Sajnos a felülíró vírusok beépülése esetén nem sokat tehetünk, hiszen nem mentik el azokat az információkat, amelyek az eredeti állapot helyreállításához szükségesek. Ilyenkor csak egy korábbi mentés visszatöltése segít, meg a fertőzött állományok teljes törlése.

A legkézenfekvőbb a vírusspecifikus irtás, amely egyben a legjobb eredményt adja. Hátránya, hogy minden egyes vírusváltozatot vissza kell fejteni a forráskódig, majd megírni a megfelelő detektort és irtó programot. Éppen ezért csak azok a szoftverek használhatóak eredménnyel, amelyek ugyanabban a víruskörnyezetben születtek. Standard nyugati vírusellenes programoktól tehát csak a standard nyugati vírusokkal szemben várhatunk megbízható fellépést, a hazai kártevőket többnyire csak speciális hazai vírusölőkkel lehet kitakarítani.

A másik lehetőség a megelőzés. Egy rendszert annyira zárttá kell tenni, hogy megakadályozhassa a vírusok belépését a gépbe vagy a hálózatba. Az is kézenfekvő megoldás, ha a vírusok illegális funkcióhívását figyeljük valamilyen szoftverrel. Általában a hozzáférés-védelmi rendszerek — mint az egyik legkomplexebb, a magyar gyártmányú Dataplan Hi-Sec — rendel-

keznek ilyen lehetőséggel. A megoldás a tárrezidens védelmi programok használata. Számolni kell viszont azzal, hogy ahol tiszta célra használják fel ezeket a lehetőségeket, ott jó pár szoftverünk nem fog vele együtt működni. Általában a komplexebb rendszerek figyelik az érzékeny állományok megváltozását, és minden jelzésnek ki kell vizsgálni az okát.

A vírusirtó programok írásához nagyfokú vírus- és rendszerismeret kell. Ráadásul több út is áll előttük. Az egyik, ami a felhasználó szemszögéből a leggyorsabb és legeredményesebb: olyan fejlesztési feltételek kialakítása, hogy a vírus felfedezése után nagyon rövid idővel, a mintapéldány birtokában megírható legyen a specifikus ellenszer. Vírusirtó csoportunk is ezt az utat követi. Ha egy ismert vírus átiratáról van szó, akár hat-nyolc óra alatt is elő tudjuk állítani az ellenszert. Teljesen új technológián alapuló vírusok esetében ez néhány nap. Bizonyos átirások előre sejtethetők — például az azonosító és a dátum átirása —, így azok eleve beleépíthetők a programba. Ezért képes a szoftver regisztrálni és kiírtani például a Péntek 13 különböző dátumra beállított variánsait. Ez a szoftver nagy kezdeti ráfordítás után gyors eredményt és korrekten helyreállított állományokat produkál, de csakis azokat a vírusokat ismeri fel, amelyekre megtanították, ezért a standard vírusdetektorokkal, például a Scan-nel, a Patyomkinnal s esetleg a FluShot+-szal kombinálva ad megfelelő biztonságot.

Egyre erősödött az igény a különböző védelmi elvek integrálására. Ennek jegyében született a Sysdoki, amely a külföldi komplex védelmi rendszerek — például az izraeli Turbo Antivirus Toolkit — nyomdokain elindulva, de annak hiányosságait kiküszöbölve, az eddig bevált módszereket integrálva elhárítja a fertőzést, illetve megakadályozza annak megtörténtét.

Más utat járva, a BME két vírusirtója, Leitold Ferenc és Tábor Csaba azt szeretné elérni, hogy szoftvereik ne csak a konkrét vírusokat, hanem a vírusfunkciókat is regisztrálják. Nemcsak konkrét vírusazonosítókat keresnek, hanem a programkód elemzésével szoftverük igyekszik megtalálni az illegális funkciót hordozó rutinokat is.

A DataPlan Kisszövetkezet Hi-Sec hozzáférés-védelmi rendszere is nagy biztonságot nyújt. Ez azonban állapotvédelem, a rendszernek azt az állapotát védi, amelyet a konfigurálás során megadtak. Az állapotinformáció természetesen folyamatosan változtatható, a szükségletnek megfelelően. Részben

azt akadályozza meg, hogy ismeretlen eredetű program jusson a rendszerbe, részben a felhasználó kontrolljához kapcsolja a programállományok átírását, a direkt lemezírást, a rezidens programok jelenlétét. Ha kilépése után egy program rezidens részt hagy hátra, akkor a számítógép riasztó jelzést ad.

Tudományos kutatás is folyik, amely az öntanuló vírusvédelmi rendszerek kialakítását tűzi ki célul. Izraelben és az Egyesült Államokban viszont egyre inkább fel szeretnék készíteni a jövőendő operációs rendszereket az adatok biztonsága elleni merényletek kivédésére. Az ilyen elven létrehozott operációs rendszerek már immunisak lennének a vírusok támadásaival szemben. Amíg a DOS vagy az azt követő operációs rendszer mindezt nem tudja, addig is kell valami külön „őrség”, amely átveszi a rendszerből még hiányzó funkció ellátását. Erre kiválóan alkalmas a Buruzs Tamás és ifj. Zsadányi Pál programozók által kifejlesztett SPS (self protection system), amely a futtatható programokat megtoldja egy önvédelmi rutinnal, s ezáltal azok mindig reagálnak a jelentkező vírusok módosítási, beavatkozási kísérleteire. Azért célszerű az operációs rendszer állományait így felvértetni, mert azok eltűrik ezt a beavatkozást. A McAfee-féle új Scan program, az 1990 augusztusában forgalomba hozott és 4.55V66-B verziószámot viselő változat már rendelkezik ilyen, az egyes állományok után kapcsolható azonosítót kibocsátó és leszedő funkcióval.

```
SERUM - Hilft gegen Computerviren - Vers.4  
(C) 1988 by Michael The PC-Guru Fitz & Heinz Veit  
Switch to interesting drive.  
SERUM2 C opt.Logfile for checking complete drive,  
SERUM2 R opt.Logfile for healing complete drive,  
SERUM2 D drive:[pathname]\*.COM  
for healing a single file  
SERUM2 M Build Restore-file for dead .COM
```

A Serum2 víruskereső szabadszoftver bejelentkezője

Felismerni és ártalmatlanná tenni

Ahhoz, hogy eredményesen tudjunk védekezni a fellépő kór ellen, tisztában kell lennünk azzal, hogy melyek a betegség kezdeti tünetei. Minél korábban felfedezzük a vírust, annál nagyobb a valószínűsége, hogy nem szenvednek kárt programjaink, adataink. Természetesen a megelőző rendszabályok betartása alapvető szempont, de tévedés lenne azt hinni, hogy csak eredeti gyári szoftvereket használva nincs mitől tartanunk.

A másolásvédelemmel ellátott programok esetében fennáll az a veszély, hogy valamilyen tisztességtelen funkciót is beleépítettek programozóik. Különösen érvényes ez a szoftveres másolásvédelmekre. Kisebb a veszély, ha védelem nélküli eredeti programot használunk. Az USA-ban végzett piaci megfigyelések szerint a védelem nélküli kereskedelmi szoftver a legbiztonságosabb, különösen akkor, ha az egy (ott) ismert szoftverház terméke. De nem engedhetik meg maguknak a stikliket a kisebb cégek sem. A szabad-szoftverek használatakor viszont éppen az amerikai eredetűeknél kell nagyon vigyázni programjaink épségére. Elektronikus adatbankokból lehívott programok kevésbé veszélyesek, mert az ilyen szervezetek csak tesztelt, vírusmentes programokat forgalmaznak.

Nyugat-Európában felemás helyzet alakult ki. A legtöbb felhasználó védelem nélküli, „szürke” amerikai példányokat használ. Feltéve, ha jó neki az angol nyelvű kópia. Ha viszont ragaszkodik a német nyelvű verzióhoz, akkor „átvakarja” az eredeti szöveget, vagy pedig szakemberekkel leszedeti a másolásvédelemet. Általában ezek a példányok jutnak el Magyarországra. Ennek ellenére — vagy talán éppen ezért? — az egyedi kópiaszámmal ellátott és a szám nélküli szoftverek forgalmazása is felfutóban van. Német nyelvterületen általában nem okoz problémát az eredeti amerikai kópia legális beszerzése. S bár igen komisz másolásvédelmek is előfordulnak, nem ez a jellemző. Amerikából importált szokásként néhány cég megpróbál védelemként hardverlock-ot alkalmazni. Nem népszerű, s a felhasználók egyre határozottabban fellépnek azért, hogy a valóban jó programokat korlátozás nélkül használhatóvá tegyék.

Egyre több fertőzés fordul elő viszonylag olcsó, eredeti gyári szoftverrel. Magyarországot is elérte, és 1990 augusztusában már javában működött a Bootkiller vírus, amely egy sorozat Disk Manager v3.30-as eredeti program-

lemezzel jött be. Tudunk olyan Péntek 13 fertőzésről is, amely egy tajvani kéziszkennerhez adott vezérlő szoftverrel érkezett be egyik tudományos intézetünkbe. Az importáló cégek természetesen tagadják, hogy az általuk szállított szoftver fertőzött volt, s mindenért a felhasználót okolják.

Vegyük sorra a vírus jelenlétére utaló tüneteket:

— A számítógép sebessége csökkenhet, mert ha aktivizálódása után a vírus rezidenssé válik, akkor minden program indításánál újra végrehajtódik. Ez különösen akkor szembetűnő, ha egyszerre több rezidens részt tartalmazó vírust sikerült „begyűjtenünk”.

— Minél előrehaladottabb a vírusfertőzés, annál lassúbb lesz a számítógépünk, a merevlemezen pedig rohamosan fogy a szabad terület. Az illegális lemezműveletek — a vírus írása a lemezre — tovább lassítja a gépet.

— A vírusok a fertőzés során hozzáépülnek az adott programokhoz, megnövelve azok eredeti méretét, ezzel is foglalva a lemezen a helyet. Ezért nem árt, ha rendszeresen ellenőrizzük egyes érzékeny állományaink méretét. Erre a DOS DIR parancsa az új technikát alkalmazó vírusok megjelenése miatt már nem alkalmas, de léteznek megfelelő új segédprogramok.

— Korábban kifogástalanul működő programjaink egyszerre csak nem futnak. Ha újra installáljuk azokat, akkor elindulnak, de csak rövid ideig tartják magukat.

— Egyes programok futásakor — amelyeket korábban hibaüzenet nélkül tudtunk használni — hibaüzeneteket kapunk, illetőleg a BIOS közli velünk, hogy nem képes a programot betölteni a memóriába, mert túl nagy.

— Egyre több lesz az olvasási hiba. Esetleg megnő a rossz clusterek mennyisége a lemezen. Ez a tünet a boot-vírusra jellemző.

— Egyre több lesz a floppy formázásakor a probléma. Különösen akkor, ha például 1,2 Mbájtos meghajtóval 360 kbájtos floppyt szeretnénk formázni. A floppy formázásakor gyanús jel, ha a DOS CHKDSK parancsa 5 k-nál kisebb rossz szektort jelez. Különösen akkor, ha két egymás után formázott gyári floppynál ez az érték ugyanaz, vagy annak többszöröse, ami a boot-vírus fertőzésének biztos jele. Fontos tudni, hogy a boot-vírussal fertőzött üres floppy is terjeszti a kórt.

— Amennyiben valamilyen segédprogrammal megnézzük lemezünk boot-szektorát, annak a végén szöveges rendszerüzeneteket kell találni (angol,

német vagy éppen más nyelven). Utána az ASCII karakterek látszólagos felsorolása következik. Amennyiben itt tömör kód vagy nem odaillő szöveg található, akkor boot-vírussal fertőzöttünk vagyunk. Megjegyzendő, hogy egyes intelligens vírusok képesek becsapni közismert segédprogramjainkat, és látszólag érintetlen boot-szektorra mutatnak! (Csellel az elmentett ép boot-rekordra irányítva programunkat!) A magyar eredetű Töltőgető vírus egy másik trükköt dobott be. Csak a boot programrészét cseréli le, a szöveges részt érintetlenül hagyja! Szerzője bizonyítottan olvasta korábbi publikációinkat, ezért találta ki ezt a megoldást.

— Ha korábban kifogástalanul futó programunk valami furcsa dolgot művel, például nem végez mentést, logikátlanul sort emel a képernyőn stb., akkor fennáll a vírusfertőzés gyanúja.

— A programmal írásvédetté tett merevlemez vagy a „leragasztott” floppy csak részleges biztosítékot nyújt az ellen, hogy a programvírus beleírjon. Vannak közöttük olyanok — például az Eddie —, amelyek az INT 13 megkerülésével, közvetlenül vezérlik az általuk ismert kontrollereket. Ezek ellen az ilyen írásvédelem hatástalan! Egyike a DOS nem publikált lehetőségeinek. A „szakemberek” szerint ez lehetetlen, valójában nem az, mert csak egyetlen jelzőbitet kell felülbírálni. Néhány eredeti IBM diagnosztikai program él, az egyik ismert hazai programrendszer másolásvédelme pedig — hasonlóan az Eddie vírushoz — alaposan vissza is él ezzel a lehetőséggel.

— Mindenképpen gyanúra ad okot, ha egy leragasztott floppyról szeretnénk programot beolvasni, de az ismert program azt reklamálja, hogy floppynk írásvédett. Ez csak a régi, primitívebb vírusokra igaz, mert a fejlettebbek már úgy kezelik a DOS kritikus hibaüzenetét, hogy észre sem vesszük!

Néhány óvintézkedés

1. Programjainkról gyakran csináljunk biztonsági (backup) mentést, lehetőleg nem DOS-verziótól függő programmal. Ilyen például a Fastback, a PC-Backup vagy a Norton Backup program. Minél gyakrabban mentünk, annál jobb. Fordítsunk különös figyelemet új, nem tesztelt szoftvereink első futtatására.

2. A rendszer konfigurációs információit tartsuk állandó megfigyelés alatt.

Ha egy számítógépet több személy használ, akkor természetesen csak egy személy ellenőrizze állandóan a konfigurációs információkat, és csak ő vihessen fel új programokat a számítógép merevlemezére.

3. Új programjainkat először elkülönítve futtassuk, lehetőleg olyan gépen, ahol nincsenek pótolhatatlan információk.

4. Másolásvédezt programot — amennyiben lehetőségünk van rá — ne használjunk! Ha jogi okokból — no meg azért, mert Magyarországon nincs más szerzési lehetőség — erre mégis rákányszerülünk, akkor használjunk helyette védelem nélküli és alaposan letesztelt „szürke” példányt. Ha frissen szedtük vagy szedtük le a védelmet egy szoftverről, akkor használata előtt alaposan teszteljük le olyan gépen, amelyen nincsenek kényes, pótolhatatlan anyagok, mert sok esetben a védelem első, viszonylag könnyen leszedhetőnek látszó szintje alatt további szinteken, késleltetve működésbe lépő pokolgépek rejtőzhetnek. Különösen a magyar és a nyugat-európai szoftverek veszélyesek ebből a szempontból!

5. Legyen áttekintésünk szerzési forrásainkról, mindig tudnunk kell, hogy melyik programot kitől vettük vagy szereztük. A programot csak akkor másoljuk fel a fontos információkat tartalmazó merevlemezre, ha meggyőződünk megbízható működéséről és a vírusellenes vizsgálatokat is elvégeztük. Nagyon hasznos a néhány hetes üzemszerű próba, sok-sok programindítással. Nagy programrendszereknél az AT belső óráját az ilyen próbák során többször is állítsuk előre, legalább két évvel!

6. Ne vegyünk korlátozottan installálható, kulcslemez, vagy szoftveres másolásvédelemmel ellátott programot. Ha nem kapunk nekünk megfelelőt, akkor inkább magunk írássunk saját céljainkra védelem nélküli programot. Megrendelt programnál ragaszkodjunk a forráskód átadásához! Igaz, ez néha drágább megoldás, de feltétlenül megtérül az üzembiztonságban, az adatvédelemben.

7. A programnak a merevlemezre való installálásakor az alábbi lépéseket tegyük meg:

— Mielőtt a programjainkat merevlemezre másolnánk, előbb próbáljuk ki floppylemezről — feltéve, hogy futnak floppyról és elérnek rajta!

— Mielőtt a floppylemezről a programot elindítanánk, merevlemezeinket a Dprotect, Lock, HDSEntry vagy más hasonló programmal (DPROTECT

C:) tegyük írásvédetté. A Dprotect program rezidens marad.

— A CHK4BOMB nevű programmal — ez egy viszonylag elterjedt szabadszoftver (freeware) — ellenőrizzük az adott program üzeneteit és a közvetlen szektorírást. A harddisk számára veszélyesek lehetnek a ROM BIOS-on keresztül történő közvetlen szektorírások vagy az alacsony szintű lemezműveletek, különösen akkor, ha utánuk nem következik a FAT aktualizálása.

— Az általunk ismert vírusdetektorokkal, vírusölő programokkal ellenőrizzük le új lemezünk tartalmát. Nem árt, ha a boot-szektor is megvizsgáljuk! Ne feledjük, a detektorok és ellenőrző programok csak azokat a vírusokat ismerik fel, amelyekre programozók felkészítették őket.

— Indítsuk újra a rendszert, hogy a rezidens Dprotect eltűnjön a tárból, és ezután másoljuk fel új programunkat a harddiskre.

8. Állandóan figyeljük a rejtett (hidden) fájlok számát. Egyes programok, mint például az AutoCAD, amennyiben szabálytalanul lépünk ki, ilyeneket nagy tömegben produkálnak. De ezek nem vírusok! A főkönyvtárat is ellenőrizzük ebből a célból, mert ha oda pakol valamit, annak már hatása lehet egész számítógépes rendszerünkre. Ha ezek az állományok gyarapodnak, ha méretük változik, az gyanúra ad okot.

9. Legalább a vírusellenőrző programjainkat tartalmazó floppylemezt tegyük írásvédetté, s legyen belőle több kópia. Mindig csak az egyiket használjuk. Hasonlóképpen járunk el a DOS-sal és a merevlemez kezelő programokkal is (pl. Disk Manager). Ezzel elérjük, hogy ha mégis beüt a mennykő, van vírusmentes programunk a rendszer újraélesztéséhez. Nem árt, ha programjainkról először mindig másolatot készítünk, és azt installáljuk, azzal dolgozunk, az eredetit pedig biztos helyen őrizzuk.

A vírusirtó programok most „számháborúval” versengenek, hogy melyik hányféle vírust tud kiirtani vagy detektálni. Gondoljunk azonban arra, hogy a legtöbb vírust felismerő és kiirtó programrendszer sem ér sokat, ha éppen azzal az egy vírussal vagy helyi vírusváltozattal nem tud mit kezdeni, amelyik az Ön gépét támadta meg. A vírusvadász cégeknek ezért minden új vírus gyors felderítése fontos, olyannyira, hogy ha valaki számukra addig ismeretlen vírussal kopogtat be hozzájuk, annak általában ingyen átadják vírusirtó programjaikat és már az új kórokozó felderítésére is alkalmasá tett detektort.

Ne kerüljenek ilyen helyzetbe, de ha mégis, akkor legalább éljenek ezzel a lehetőséggel!

Elsősegély

Mit kell tenni akkor, ha rendszerünk minden előzetes óvatosság ellenére vírusos lett?

— A legfontosabb: ne barkácsoljunk! Ha felismerjük a kór okát, és van ellene megfelelő killerünk, akkor futtassuk le a gépen és összes(!) program-
lemezünkön. Ha így sem tudunk segíteni, akkor hívjunk szakembert. Ahhoz, hogy munkáját megkönnyítsük, előtte használjuk a Scan vírusdetektor legfrissebb változatát. (Ezt a programot Magyarországon szabad szoftverként terjesztik.) Gondosan jegyezzük fel, mely állományokra mit írt ki, és utána könyvünk mellékelt dokumentációs táblázata alapján vagy a Scan programokhoz adott, McAfee-féle VIRLIST.TXT állomány segítségével azonosítani tudjuk, milyen vírusról van szó.

— Formázzunk a vírusos rendszerrel egy rendszerlemez. Tegyük rá néhány rendszerállományt és vírusgyanús programot. Ezzel konzerválni tudjuk a vírust a későbbi vizsgálatok számára.

— A szakértők megérkezéséig a rendszert ezután már ne használjuk.

SZÁMHÁBORÚ ÉS VAKLÁRMA

HOGYAN HASZNÁLJUK A SCAN CSALÁDOT?

A közelmúltban jutott el hozzánk egy Magyarországon ismeretlen keleti szoftveres cég terméke, amely 149-féle vírust tud irtani... De valóban annyit, vagy csak reklámból írták rá ezt a számot? Rögtön kiderül.

A vírusok többségének van .COM és .EXE állományokba beépülő kódja. Tehát ha ezeket különállóaknak tekintjük, akkor egy vírusból máris kettő lesz, mert a két változat irtása természetesen más algoritmust igényel. De folytassuk tovább. Az egyes vírusok kódjában a kezdő vírusgyártó kisiparosjelöltek átírják a karakteres azonosítókat. Például a Disk Killernek, valamint a Stoned/Marijuanának is van ilyen magyarul beszélő változata. Ha valakinek nincs gátlása, ezeket is külön vírusoknak tüntetheti fel, annak ellenére, hogy ha jó a felismerő algoritmus, az eredeti eljárással is irtani lehet őket. Tehát nem külön vírusok, hanem csak változatok. Azután vannak vírusok, amelyeknek a kódjába nyúltak bele, például a magyar Kedd 1 csak a Péntek 13 B változatának további variánsa. Most ez újfajta vírus vagy ugyanaz? S végül vannak olyan „leszármazott” vírusok, amelyeknek eredeti kódját alaposan átírták. Ezeket viszont már jogosan tekinthetjük önálló változatoknak.

S ha ezek után a forgalmazó elhatározza, hogy minden vírus minden változatát külön típusnak veszi, akkor a korábbi mintegy 10 helyett ugyanaz a program rögtön 22 eltérő vírust tud irtani, anélkül hogy közben akár egyetlen bitet is átírtak volna benne. És még csak nem is hazudik senki. Ez a számháborúsdí azonban nem okoz különösebb gondot.

Több zavar forrása a vírusdetektorok okozta vakriadó, amely nyugtalanítja a felhasználót, esetleg fölös kiadást is okoz neki. Ilyesmi főleg azokkal a szoftverekkel fordul elő, amelyeket még a víruskorszak hajnalán írtak vagy pedig éppen a mostani számháború jegyében a szakkönyvekben található vírusazonosítók felhasználásával. Sajnos a komoly szakemberek is kénytelenek bekapcsolódni a számháborúba. Már McAfee is azt írja dokumentációjában új Scan verziójáról, hogy 253 programvírust detektál. A verziószámában azonban csak a tisztességesen elkülöníthető fősoportokat jelöli meg,

jelenleg 66-ot. Hasonló bűvészmutatványokkal találkozhatunk az izraeli Turbo Anti Virus Toolkit dokumentációjában, de több magyar szoftverírónál is.

Ha egy vírusjelző vakriadót jelez, annak legtöbbször az az oka, hogy a vizsgált program tartalmazza a vírus azonosítóját. Ezek általában első generációs vírusdetektorok, mint a Prgdoki v.2.xxE sorozata, az osztrák Ikarus program rezidens és főmodulja, a Look nevű víruskereső, hogy csak a legismertebbeket említsük. Komolyabb a gond akkor, amikor jónak tartott szoftver téved, s ráadásul gyári programlemez „gyanúsít meg” vírussal. Ez történt 1990 júniusában, nem kis pánikot okozva egyik tervezővállalatunknál. Itt a CHKSeq hazai szabadszoftverként forgalmazott víruskereső a (c) Brain vírust jelezte egy építészeti tervezőrendszer kulcslemezén. De csak vaklárma volt.

S itt meg kell állni egy pillantra. Érdemes-e hazai programot írni könyvek-ből és más szakirodalomból összeszedett vírusazonosítók felhasználásával, vagy jobb átvenni egy olyan szoftvert, amely már bevált és ingyenes standard programként használják szerte a világon? Nem inkább a birtokunkban lévő magyar specialitások biztos detektálására és irtására kellene koncentrálni erőinket? Az így írt programok a standard programokkal együtt alkalmazva nagyobb biztonságot adnak, mint a számháború jegyében hevenyészve megírt programok. Ha viszont megnézzük a CeBIT-en bemutatott vírusellenes programokat, hamar kiderül: a jövő a komplex védelmi rendszereké, az egyetlen termékbe integrált megelőző, kereső, irtó és helyreállító program-rendszereké.

A helyreállító algoritmusok területén úgy látszik, Magyarország eredményes kutatásokat folytat. A Prgdokit felváltó Sysdoki is ennek a koncepciónak a jegyében született. Remélhetőleg nemcsak vírusírásban, hanem a vírusellenes küzdelemben is „nagyhatalom” leszünk, felzárkózva Izrael és az USA mellé. Jobb lenne, ha ilyesmivel, nem pedig vírusírással állítanánk ki erkölcsi bizonyítványt a magyar számítástechnikáról. Sajnos úgy látszik, hogy ennek a szaklapokban többször is megismételt kérdésnek nincs nagy fogatja. Már legalább négy eredeti magyar fejlesztésű vírussal „gazdagodott” a számítástechnika.

A Scan vírusdetektor

Magyarországon az alapszoftverek közé tartoznak ezek az USA-ban szabadszoftverként terjesztett programok. A Scan-t az adatbiztonsággal foglalkozó McAfee Associates készíti és terjeszti. A Scan nem képes a hálózatos közegben való futásra. Erre csak a nem szabadszoftverként forgalmazott párja, a NetScan alkalmas.

A Scan a korábbi Pkarc helyett most a Pkzip programmal tömörített formában kerül a felhasználókhoz. Az állomány kibontás után mindig tartalmaz egy VIRLIST.TXT szövegállományt a detektálható vírusok rövid táblázatával, valamint egy Validate nevű programot, amellyel ellenőrizni lehet az állomány sértetlenségét. A Validate algoritmusát — bár a vírusírás megnehezítésére szakmai körökön kívül nem publikálják — szabványként fogadták el sok országban. Azokat a CRC-értékeket tartalmazza ennek a programnak a dokumentációja, amelyeket ellenőrizni szeretnének vele. Lényegében egy speciális módon képzett ellenőrző összeget, azaz CRC-t vizsgál. Mivel ezek a szoftverek széles körben elterjedtek, de a felhasználókhoz általában leírás nélkül kerülnek, érdemes összefoglalni használatuk módját.

A McAfee-féle teszterek közül legelterjedtebb a SCAN.EXE program, jelenlegi legújabb változata a Version 4.5V66-B. Az első (tizedesponos) szám a szoftververzió jelzése, a V betű utáni szám pedig azt mutatja, hogy hány vírusfőcsoportot tud azonosítani. Ezt a változatot már felkészítették a kelet-európai vírusokkal való találkozásra. Nagy biztonsággal felismeri a barkácsolt változatokat is, például a Yankee Doodle, a Péntek 13, a Vacsina-B variánsait, de sajnos még nem azonosítja az eredeti kelet-európai vírusokat, a Töltögetőt, a Turbo Kukacot, a Kukacot és egyes Vacsina-átiratokat.

A Scan65 verzió soha nem készült el. Helyette egy kárt okozó trójai változat került forgalomba. Éppen ezért a dokumentációk alapján mindig ellenőriznünk kell a Validate segédprogrammal. Magyarországon a 45-ös jelzésű verziót írták át trójajává, illetve vírushordozóvá. A Yankee Doodle hazai átiratát illetve a V2000 vírust kapcsolták hozzá titokzatos kezek. Néha a számot is átfírták 99-re vagy másikká, az eredetinél nagyobb kétjegyű számra.

Elindításakor a Scan program előbb öntesztelést végez. Ha bármilyen változtatást vagy sérülést tapasztal, azonnal leáll. Elsősorban diagnosztikára, másodsorban gyorssegélyre, a fertőzött állományok törlésére való. A szoftver

terjesztői is kéri, hogy mindenki a legfrissebb változatot igyekezzen használni. Az amerikai vírusellenes programok közül ez az egyetlen, amely a mi környezetünkben is elfogadható védelmet nyújt. 213 vírusváltozatot detektál 90 %-os biztonsággal. A korábbi változatok számos hibáját kiküszöbölték benne. Egy viszont benne maradt: ha egy víruskeresőben a kódnak éppen az a része van bináris formában, amelyre ő is keres, akkor hamis riadójelzést ad. Ezt teszi a Prgdoki 2.11E verziójánál és az azzal forgalmazott összes segédprogramnál, valamint az osztrák Ikarus programrendszer VU.EXE nevű programjánál is.

A Scan programot — a 4.5V66-B verziószámától kezdve — a következőképpen kell használni:

SCAN d1: ... d10: /NLZ /M /D /A /E .xxx /NOMEM /MANY /AV /RV /CV

(d1: d2: ... dn: az összes logikai és fizikai meghajtó felsorolása, ahol az ellenőrzést végre kívánjuk hajtani),

/ után adjuk meg a nem kötelezően alkalmazandó opciókat. Ezeknek a kapcsolóknak a jelentése a következő:

/NLZ — Ne vizsgálja a tömörített LZ.EXE állományok belsejét. A Scan új funkciója az USA-ban ismert, nálunk pedig várhatóan megjelenő újabb tömörítő programmal, az LZ.EXE-vel készített állományokban a kipakolás nélküli víruskeresés. A nálunk megszokott többi tömörítő program állományaiban csak a Shez 5.3 vagy afeletti verzióival és ezzel a Scan programmal együttesen lehet víruskeresést végezni.

/D — Írja felül és törölje a fertőzött állományokat. Ilyenkor mindig kérdez. Ha törölni akarunk, akkor a kérdésre az Y, különben pedig az N betűt kell leütni. Hexa C3-mal azaz CR kóddal előbb felülírja az állományt, azután törli. Utólagos visszaállítására nincsen mód! A Scan család a boot-vírusokat nem tudja törölni, csak detektálni.

/M — Vizsgálja meg a memóriát az összes általa ismert vírusra. Rendszerindításra a 640 kbájtnyi memória átvizsgálása a gép sebességétől függően 1-2 percig is eltarthat. Ha a memóriában például megleli a Dark Avenger-t, akkor riaszt, és felszólít arra, hogy tiszta floppyról behívott rendszerrel indítsunk újra. Nem árt tudni, hogy ha Disk Manager-rel vagy Hardprep-pel, esetleg egyéb ilyen segédprogrammal formáztuk lemezünket, akkor azok

meghajtójának, valamint a megfelelő CONFIG.SYS állománynak is rajta kell lennie a tartalék indítólemezen. Ne használjuk ezt az opciót, ha a rendelkezésünkre álló rezidens Scan, azaz a Scanres verziószámában V42 vagy annál kisebb szám szerepel, mert az hamis riasztást eredményez.

/A — Minden állományt vizsgáljon meg.

/E .xxx .yyy — A vizsgálandó overlay állományok kiterjesztését kell itt megadni, ha azok eltérnek a hagyományos megjelöléstől. Ha nem adunk meg kiterjesztést, akkor csak a következőkre vizsgál: OVL, OVG, OV1, OV2, OVR, SYS, BIN és PIF. Ha megadunk kiterjesztést, azt a következőképpen tegyük: SCAN C:/E .ABC .XYZ .123

/NOMEM — Hagyja ki a memóriatesztet.

/MANY — Több floppyt vizsgáljon meg egymás után, az újabb floppy vizsgálatára az Y, a vizsgáldás befejezésére pedig az N billentyűvel utasíthatjuk a programot.

/AV — Ellenőrző kódot fűz a megadott állományok végéhez. Nem minden program tűri ezt a beavatkozást!

/RV — Leszedi az ellenőrző kódot a megadott állományokról.

/CV — Ellenőrzi, hogy az ellenőrző kódhoz képest változott-e valami az egyes állományokban. A Scan jelenlegi verziója mintegy 3 perc alatt néz végig egy 16 MHz-es AT-n 1000 állományt egy közepes gyorsaságú winchesteren. Ha ezt az opciót használjuk, mintegy 255-300 %-kal csökken a sebesség.

Lehetséges egyetlen alkönyvtár vagy egy konkrét állomány ellenőrzése is a következő módon: SCAN C:\DIRECT\PROGRAM.EXE

Abban az esetben, ha a rendszer nem standard boot-szektorrt használ (régebbi Zenith PC, Hewlett Packard PC-k), a Scan ezt felfedezi és figyelmeztető jelzést, hamis riadójelet ad. Ilyenkor a boot és a partíciós tábla megváltozására figyelmeztet. Erre a hamis riadójelzésre nem kell figyelni.

Ha más programmal akarjuk kapcsolni a Scan-t, akkor a következő DOS errorlevel értékeket adja vissza futás után:

- 0 — Normális befejezés, vírust nem talált.
- 1 — Normális befejezés, egy vagy több vírust talált.
- 2 — Nem szabályos befejezés (error).

A program Kelet-Európában szabadszoftver. Az USA-ban magánszemélyek ingyen használhatják, intézményektől névleges regisztrációs díjat (25 USD) kérnek, amelynek fejében az új változatot elküldik a megrendelőknek. Magyarországon az Ázsio-Viki adatátviteli vonalon kapja a legfrissebb verziót, és az onnan beszerezhető.

A rezidens Scanres program

A program neve SCANRES.EXE, verziószáma V59. Mintegy 95 %-os biztonsággal képes detektálni 73 nagy vírustörzs változatait, beleértve a kelet-európai átírásokat. Sajnos jó pár mamut programrendszer nem tűri meg a tárban, így az összeférhetőséget egyedileg kell kipróbálni. A Clipperezett programokkal a legtöbb esetben jól megfér. A program ugyanazokat a vírusokat ismeri fel, mint a megfelelő verziójú normál Scan. A Scanres-nek a boot lemezegység gyökérkönyvtárában kell lennie. Nevének begépelésével vagy az AUTOEXEC.BAT-ba való beírásával indítható.

A Scanres tárban maradó része 19 kb-ajttal csökkenti az operatív memória méretét. Mintegy négy másodperc alatt elhelyezkedik a tárban és nem csökkenti a gép sebességét sem. Amennyiben fertőzött programot indítunk, nem engedi futni. Közli velünk a fertőzés tényét, majd felhívja figyelmünket arra, hogy a pontos azonosítás érdekében futtassuk le a normál Scan programot is. A fertőzött program futtatási kísérlete után a DOS-ba tér vissza, kárt sem okoz, de vírust nem tud irtani.

A hálózati NetScan

Nem szabadszoftver! Ennek ellenére, ha nem is a legfrissebb verzióhoz, de hozzájutnak a magyar felhasználók, tehát érdemes megismerkedni alkalmazásával. Ugyanazokat a vírustörzskeket detektálja, mint a neki megfelelő Scan, viszont hálózati üzemre is felkészítették, és nem okoz zavarokat a hálózat működésében. Ajánlatos, hogy a supervisor használja. Ez a hatáskör, azaz minden állománynak és könyvtárnak olvasási és írási joggal történő elérése a program hálózati futtatásához kötelező! Egy kiterjedt hálózat alapos ellenőrzése az /A opcióval akár fél óráig is eltarthat.

Ha egy állományt a hálózatban más is használ, akkor hibaiüzenetet kapunk. Ugyanúgy egyes speciális Novell attribútummal rendelkező állományoknál

is jelez (például a NET\$.OS esetében), s ekkor tovább kell léptetni a programot, hogy hagyja ki annak az állománynak a vizsgálatát.

Használata: NETSCAN d1: d2: ... dn: [/M /D /A /NOMEM]

Ahol d1: ... dn: az összes olyan meghajtó meghatározása, ahol vizsgálunk. Ezek között lehetnek logikai meghajtók is!

Opciói:

/D — Fertőzött állományok törlése. (Supervisor jog olvasásra és írásra kötelező!)

/M — Memóriateszt az ismert vírusok rezidens részeire.

/A — Minden állomány vizsgálata.

/NOMEM — Memóriateszt kihagyása.

Az opciókra hasonlóképpen viselkedik, mint a normál Scan, és inkompatibilitásai is ugyanazok. Lehetséges egyetlen állomány vagy könyvtár vizsgálata is. Ezt a következőképpen adjuk meg:

NETSCAN L:\DIRECT\PROGRAM.EXE

Ha valami miatt mégsem tudna olvasni egy állományt — pl. Novell esetében —, akkor kérdésére az Ignore választ, azaz az I betűt leütve kell kihagyatni azt az állományt. Ez a Novell egyes rendszerállományai esetében fordulhat elő. Más esetekben ilyen megállások után a Fail válasznak megfelelő F betűvel lökhetjük tovább az ellenőrzés folyamatát.

VShield — a pajzsos őr

McAfee vírusellenes programcsomagjának rezidens tagja. A Scanres-nél jobb termék. Magyarországon szabadszoftver, az USA-ban magánosok ingyen, hivatalos szervek pedig regisztrációs díjért használhatják.

Számozásának logikája azonos a megfelelő Scan programokéval. A jelenleg érvényes verzió jelzése 2.0V64. Képes 111 főcsoportot és összesen 182 változatot detektálni. A felismerés biztonsága mintegy 95 %.

A program felismeri a verziószámban meghatározott főcsoportokba tartozó vírusos állományokat, és nem engedi a víruskódot lefutni. A <CTRL><ALT> melegendítés során bent marad a memóriában, és megakadályozza, hogy fertőzött floppyról rendszert indíthassunk.

A program elindítása után betöltődik az egész rendszer, majd ellenőrzi a boot-szektor, a partíciós táblát, a FAT-ot, valamint a rejtett rend-

szerállományokat és a COMMAND.COM-ot, végül saját magát is. Utána, ha a /SWAP opciót alkalmazzuk, egy rezidens része bent marad a memóriában (mintegy 3 kb-ot), amely probléma esetén behívja lemezről a program többi részét mint overlay állományt. A /SWAP paraméter nélkül 25 kb-nyi helyet foglal el a rezidens része a tárban. A programok indítása során 4 másodperc kell arra, hogy végigfusson rajta, a rendszer újraindításánál pedig 6 másodperc. Ilyenkor tehát azt látjuk, hogy a megszokottnál hosszabb ideig töltődik a programunk. A /SWAP paraméter használata esetén ehhez még 600 msec időt kell hozzáadni. Egyébként nem módosítja a gép sebességét és a programok futásidejét.

Nem minden programmal fér össze a memóriában. Így ezeket ki kell próbálni. Amennyiben minden általunk használt programmal képes együttműködni, akkor a következőképpen kell használnunk:

Az AUTOEXEC.BAT állományt ki kell egészíteni a következő parancssorral. (Természetesen az opciókat akkor használjuk, ha kell. A program akár hagyományosan parancssorból, akár pedig más .BAT állományból elindítható!)

VSHIELD [/SWAP[pathname] /F[pathname] /NB /NOMEM]

/SWAP — Nem kötelező paraméter. Ha megadjuk, akkor a VSHIELD az operációs rendszerbe integrálódik, de csak a rezidens modulja. Ha mellé path-ot is megadjuk, akkor oda teszi a maga által létrehozott speciális overlay állományt, az úgynevezett SWAP fájlt. Alapértelmezése: oda teszi, ahol a főprogramja található. Ha használjuk e kapcsolót, a rezidens rész kisebb lesz, mint 3 kb-ot! Például:

VSHIELD /SWAP

VSHIELD /SWAP D:\KAKADU

/F paramétert kell az előbbi pontban megadottak szerint használni, ha az általunk használt DOS verzió 2.0 vagy régebbi. Funkciójában kiegészíti a /SWAP paramétert az annak alkalmazásához hiányzó DOS funkciókkal.

Például: VSHIELD /SWAP /F C:\

(Csak DOS 2.0 vagy régebbi verzió használata esetén!)

/NB — Ezt akkor kell megadni a VShieldnél, ha nem akarjuk, hogy a rendszer újraindulása során ellenőrizze a boot-szektor. Néha használata vagy éppen mellőzése okozza, hogy összeakad a többi rezidens programmal.

/NOMEM — akkor alkalmazzuk, ha nem akarjuk a memóriában a VShieldet használni az éppen behívott programok ellenőrzésére, azaz csak bootvédelmet kívánunk. A két opció együttes alkalmazásakor csak a rejtett állományokat és a COMMAND.COM-ot ellenőrzi.

VSHIELD /NB /NOMEM

A VSHIELD.EXE helye kötelezően a bootoló merevlemez főkönyvtárában van! Ha vírust talál, akkor kiírja a képernyőre, hogy mit és melyik állományban talált, a fertőzött program futását pedig a víruskód lefutása előtt megakadályozza.

A memóriából eltávolítható a /REMOVE opcióval történő ismételt behívással. Néhány esetben, a SWAP módot követően eltávolítása nem mindig sikerül, ha több egyéb rezidens programot is használtunk. Ilyenkor erre rendszerüzenet hívja fel a figyelmet, és újra kell indítani a <RESET> gombbal a rendszert. Például: VSHIELD /REMOVE

Hamis riadót adhat, ha a memóriában más vírusdetektor rezidens program is van.

Nem fér össze a program a PcTools PC-Cache programjával és sok más programrendszerrel sem. Clipperezett adatbáziskezelők viszont jól tűrik.

Ha más programmal akarjuk kapcsolni a VSHIELD-et, a következő DOS errorlevel értékeket adja vissza futás után:

- 0 — Normális befejezés, vírust nem talált.
- 1 — Normális befejezés, egy vagy több vírust talált.
- 2 — DOS vagy program rendszerhiba (system error).

Egy gyorssegély: a CleanUp Virus Remover

A McAfee Associates víruseltávolító programjainak különböző verziói használatosak Magyarországon. Jelenleg főleg a 3.1V59 jelzésű használatos. Kevésbé terjedt viszont el, mint a hozzá tartozó detektorok, aminek oka viszonylag egyszerű.

A Scan programcsalád egy-két kivétellel nagyon jól detektálja a magyar vírusátiratokat, ugyanakkor viszonylag gyakran hibázik, s ennek során tönkreteszi a különben még megmenthető állományokat is. Nagyobb részben az USA-ban előforduló vírusváltozatokat ismeri, s mivel az itthoni változatok víruskódhossza sok esetben eltérő, ezért az a szakasz, amit a vírusirtó kívág,

vagy túl rövid, vagy túl hosszú, s ezáltal tönkreteszi a vírustól megtisztítandó állományt.

Nagyon sok esetben tehát ez sem tesz mást, mint a Scan program a /D opcióval: törli a fertőzött állományokat. Ennek ellenére nem árt megismerkedni működésével, hiszen sok esetben — a klasszikus vírusok esetében — kihúzhat bennünket a bajból. De használata során ne feledjük: lehet, hogy elveszítjük állományaink egy részét, ezért használata csak végszükség esetén ajánlható.

A program integritásvédelemmel rendelkezik. Ha valaki módosítja, vagy netalán átírja, akkor nem fut, hanem üzenettel figyelmeztet bennünket a beavatkozásra. A program neve: CLEAN.EXE. A következő vírusok standard nemzetközi verzióit képes irtani (a magyar átírásokat hibásan kezeli):

Alabama, Alameda, Ashar, Dark Avenger, Disk Killer, Jerusalem-A, Jerusalem-B, Jerusalem-E, Pakistani Brain, Payday, Ping Pong, Ping Pong-B, Stoned, Sunday, Suriv03, 1260, 1701, 1704, 4096.

Az általa irtott többi vírus esetében sokszor töröl. A Scan sorozat ismertett tagjai a meglelt vírus teljes neve mellett közlik a McAfee által bevezetett nemzetközi nyilvántartásra is alkalmas vírusazonosító kódot. (A vírusazonosító kódokat és azok feloldását e könyv mellékletében közöljük.) Ezt kell megadni a programnak az alábbi szintaktika szerint:

CLEAN d1: d2: ... dn: [vírusID] /A /MANY

ahol

dn: — Annak a meghajtónak a jelzése, ahol takarítani akarunk.

[vírusID] — A kitakarítani szánt vírus azonosítója, amelyet vagy a Scan programok leírásából, vagy pedig a könyv mellékletében található táblázatból olvashatunk ki. Az írásmód is lényeges! A kódot szögletes zárójelek közé kell foglalni, s egyszerre csak egy vírusra végezhető el a mentesítés.

/A — Az összes állományt (nemcsak a .COM és .EXE kiterjesztésűeket) végignézi.

/MANY — Több floppy tisztításakor azonos meghajtóra ismételt. Ez csak floppymeghajtóra adható meg opciónak! Példáink:

CLEAN C: D: [Jeru]

a C: és a D: meghajtóról a .COM és .EXE állományokból a Jerusalem vírus eltávolítását kérjük.

CLEAN C:\TEMP [Dav] /A

Pucolja ki a C: meghajtó TEMP alkönyvtárából a Dark Avenger vírust (név keresztreferenciát szintén e mű végén találhatunk), mégpedig úgy, hogy minden állományt megvizsgál.

A HTScan programozható rekurzív víruskereső program.

A programot 1990.06.05. dátummal látták el, ami új fejlesztésre utal, szerzőként pedig Harry Thijssent jegyzik. Hasonló a szabad memóriai igénye mint a Scan sorozat tagjainak. Minimálisan 256 kb-át szükséges a futásához. A merevlemez vagy floppy egész területén vírusazonosító karaktersorozatok keres, igen nagy sebességgel. Ezeket egy szövegszerkesztővel editálható ASCII állományból veszi, amelynek neve: HTScan.Dat vagy VirScan.Dat

A HTScan programot igen sok azonosító string befogadására tervezték. A vírusazonosítók száma maximálisan 4000 lehet. A fejlesztő dokumentációja szerint a vírusazonosító stringek száma nem befolyásolja a program futási idejét. A tesztek alapján nincs lényeges futási időkülönbség 1 és 100 vírusazonosítóra történő ellenőrzés esetén. A HTScan a vírusazonosítókat tartalmazó fájlt minden futtatás előtt külön fájlból olvassa be. A vírusazonosító állományok tartalmát a felhasználó tetszőlegesen módosíthatja, illetve új vírus esetén tovább bővítheti. Ezzel a módszerrel biztosították a víruskereső program programozhatóságát. A program elindítása után a HTSCAN.DAT fájlt keresi az aktuális könyvtárban. Ha ilyen nevű állományt nem talál, akkor a VIRSCAN.DAT állományt keresi. Ezek egyikének feltétlenül léteznie kell, vagy helyette más nevű állományt is kijelölhetünk szignatúrafájlként.

A program használata:

HTScan <path> [<path>...] [opciók...]

Opciók:

/A — Az összes fájl ellenőrzése az összes vírusra.

/D — A fertőzött fájl törlése/átnevezése. (Mielőtt a HTScan program törölné/átnevezné az állományokat, kijelzi azt.)

/I — A program copyright információjának megjelenítése.

/R — A fertőzött állományok átnevezése. Átnevezés előtt rákérdez.

/N — Nem ellenőrzi az alkönyvtárakat.

/O[=]<log.file> — A vírusellenőrzés eredményét a megadott fájlba leteszi.

/S — A boot-szektor átlépése. (Hálózati használatkor.)

/V[=]<sign.list> — A megadott fájlt használja vírusazonosító szignatúra állományként.

/X — Több floppylemez ellenőrzése.

Programkilépési kódok:

0 — Nem volt vírus.

1 — Egy vagy több vírus volt.

1 — Hibás programfuttatás.

A vírusazonosító fájl (HTSCAN.DAT, VIRSCAN.DAT) programozása:

Vírus neve:

Bármilyen 1-től 80 karakterig terjedő ASCII karaktersorozat.

A vírusazonosító string fájl hatásköre:

PART, BOOT, SYS, COM, EXE, OVL, BIN, PIF kiterjesztés bármelyike vagy akár mindegyike felsorolva, szóközzel elválasztva. Értelmezésük:

PART — Partíciós tábla, csak merevlemezre

MAIN — A partíciós tábla szinonímája

BOOT — Boot-szektor

SYS — *.SYS fájlok

COM — *.COM fájlok

EXE — *.EXE fájlok

OVL — *.OVL fájlok

OV* — Overlay fájlok

BIN — *.BIN fájlok

PIF — *.PIF fájlok

Vírus-szignatúrák leírásának szabályai

A vírus-szignatúrák tetszőleges összefüggő hexadecimális számok lehetnek. A vírusazonosító minimális hossza 8, maximális hossza pedig 80 karakter lehet. Az első karakter után a ?, * helyettesítő karakterek használata megengedett.

? — A kérdőjel helyén bármilyen érték, fél bájt érték is lehet.

*x — A következő x bájt értékét a program figyelmen kívül hagyja az ellenőrzés során. Az x felvehet értéket hexa 1 és hexa F között.

A „*x” értékkel megadott bájt után, a következő bájt ismét tartalmazhat „*x”-et, de nem tartalmazhat ?-et. A maszkolt vírusazonosító string hossza nem lehet nagyobb, mint 128 bájt.

Lehetőség van a vírusban elhelyezett szöveg keresésére is. A keresendő szöveget dupla kérdőjelek között kell elhelyezni. Mellékletünkben ilyen szabályok szerint közöljük jó pár vírus azonosító karaktersorozatát.

Az Ázsió-Vikin keresztül forgalmazott, önköltségi áron terjesztett példányokhoz havonta bocsátunk ki a magyar vírusokkal is aktualizált és tesztelt szignatúraállományokat, amelyek a magyar vírusfajtákkal és mutánsokkal együtt több mint 180 vírus felismerésére alkalmasak. A VIRSCAN.DAT állományt a következő Magyarországon előforduló vírusazonosítókkal bővítettük ki:

Yankee Doodle 2932, Yankee Doodle 2941, Turbo Kukac 9.9, Victor/Ivan, 1260, Vaccina v05, Vaccina v16, Vaccina v24, Filler/Töltögető, Polimer.

HTScan scans for:

19 Boot-Record viruses

0 viruses in Partition-Table

19 viruses in Boot-Sector

80 file viruses

total 99 viruses

Signature file name: VirScan.Dat

C:\KEDIT\KEZIK.TXT 1 time infected with: Fu Manchu A Virus

C:\KK\U10A\UIR09.TXT 1 time infected with: Fu Manchu A Virus

C:\KK\U11\KESZ\UIR09.TXT 1 time infected with: Fu Manchu A Virus

C:\KK\U9\USUM9003\UIRUSSUM.DOC 1 time infected with: Fu Manchu A Virus

4 file(s)/boot-record(s) infected

0 Partition-Table(s) scanned.

1 Boot-Sector(s) scanned.

1069 file(s) scanned.

Karakteres kereséskor a HTScan olyan állományban is vírust jelez, (mint itt például könyvünk kéziratában), amelybe vírus fizikailag be sem épülhet

AIDS TÁJÉKOZTATÓ LEMEZ

avagy

EGY INFORMATIKAI MERÉNYLET TRÓJAI MÓDRA

1990 elején a számítógépes rendszerek elleni különös merényletről kaptunk híreket. 1989 decemberében, néhány napos eltéréssel több ezer „informatikai bombát” postáztak mágneslemezen. A küldemény az „AIDS Information Disk” volt, s a címzetteknek mint AIDS szakértői segédeszközt kínálták. A CW Communication, a szétküldési címlista jóhiszemű szolgáltatója csak utólag tudta meg, milyen akciónak tették részesévé, akkor viszont azonnal vállalták egy szakértő, Jim Bates munkájának finanszírozását, hogy minél előbb kidolgozzák az ellenanyagot. Azóta Magyarországon is megvan a megfelelő killer, sőt sikerült hozzájutni Jim Bates forrásértékű, szinte bájtisztító dokumentációjához, aminek alapján könyvünknek ezt a sok szempontból tanulságos fejezetét megírtuk.

Történetünk valahol Panamában kezdődik. Olyan, mint egy sci-fi, de sajnos valóság. Az informatikai merényletet kivitelezése profi munkára vall. AIDS-kutatással foglalkozó intézetek kaptak egy mágneslemezt postán. Ezek legtöbbször Angliában és Panamában adták fel. A kísértőlevél szerint egy AIDS szakértői rendszer demonstrációs változata van a lemezen. Ez azonban csak az álcázás, a „faló” volt. Ez a trójai program akkor sem veszélyes a felhasználónak, ha merevlemez nélküli gépben floppyról futtatják. Hogy megismerhessük a valódi veszélyt, tisztán kell látni, hogyan „élesíti be” magát ez a rendszer.

Miután a „Trojan AIDS”-nek is nevezett program installálta magát és kényelmesen elhelyezkedett a merevlemez méhében (az egyszerű felhasználó számára elérhetetlenül), a program figyelőállásba helyezkedik. Az első fázisban egy számlálórutinnal azt figyeli, hányadik alkalommal indítjuk újra a rendszert. Amikor letelt a számunkra engedélyezett 90 újraindítás, aktivizálódik a második, a romboló rutin: egy sajátos algoritmus alapján titkosítja az állományokat és a könyvtárakat a merevlemezen, hihetetlen káoszt okozva.

Ha a program befurakodott a merevlemezre és nincs megfelelő killerünk,

a kezdeti időben adatainkat egy ügyes fogással még hiánytalanul visszanyerhetjük. Ha ugyanis NEM a fertőzött merevlemezről indítunk rendszert, akkor nem aktivizálódik a vírusrutin. Ekkor adatainkat zavartalanul kimenthetjük, utána pedig a merevlemezen alacsony szintű formázást kell végezni. Az így letisztított lemezre már installálhatunk egy tiszta rendszert, s végül visszatölthetjük adatainkat.

Általános érvényű óvintézkedés, hogy amikor megveszünk egy programot, mindig két másolatot készítsünk róla, amelyek közül az egyiket használjuk, míg az eredetit és a másik másolatot mint könyvtári példányt elzárjuk. Vírusok támadása vagy bármilyen más állománypusztulás esetén így mindig van honnan hibátlanul visszatölteni a gépbe programjainkat. Bár így egy kicsit több floppyt fogunk felhasználni, de megéri. Másolásvédtett szoftvert már csak ezért sem szabad vásárolnunk. A demólemezeket és az újonnan vásárolt vagy szerzett szoftvereket először olyan gépen kell futtatni, amelyen nincsenek kulcsfontosságú adatok, s csak a sikeres vizsga után engedjük azokat az „éles” számítástechnikai rendszerbe. A boot-vírusok esetében adatmentő lehet a tiszta tartalék DOS rendszer, hiszen legalább az adatállományokat ki tudjuk másolni a merevlemezről.

A Trojan AIDS vírusra visszatérve, említettük, hogy terjesztője egy demó szoftver. Generáló rendszere is érdekes, mert a programozástechnikában szokatlan megoldásokat tartalmaz. A programot egy installációs rutin teszi fel a gépre. Kihasználja, hogy a könyvtárak és a futtatható programok neve a képernyőn számunkra láthatatlan karakter vagy DOS terminátor jel is lehet, ha azt ügyesen alkalmazzák. A magukat Cyborg-nak nevező „vállalkozás” tagjai az ALT 255-ös karaktert nevezték ki erre a célra. Most lássuk a folyamatot!

1./ Az installáló program létrehoz egy rejtett AUTOEXEC.BAT állományt, ami maga is szokatlan. Hát még a tartalma!

```
CD \<ALT255>
REM<ALT255>
```

Az eredeti AUTOEXEC.BAT állományt átnevezi a program AUTO.BAT-ra.

2./ A program létrehoz egy rejtett <ALT255> karakterrel megnevezett alkönyvtárat, benne egy REM<ALT255>.EXE nevű programmal.

Amikor ezt a rendszert indítjuk, akkor a program csendesen számolja a rendszerindításokat. A következő fázisba, mint a bevezetőben említettük, csak 90 indítás után lép át a program.

Gondoljunk arra, hogy a rendszer által használt <ALT255> karakter, az úgynevezett „hi space” a standard DOS eljárásban állománynév-terminátor, a név végének és a kiterjesztés kezdetének a jele, így önmagában hagyományosan sem állománynévként, sem pedig könyvtárnévként nem használható. Itt mégis használják.

Ezek a rejtett alkönyvtárak persze törölhetők, és ezáltal meg tudjuk bénítani a programot, de ilyenkor még nem biztos az eredmény, ezért néhány hónapon át ellenőrzéseket szükséges végezni a lemezen, nagyon figyelve minden szokatlanra, rejtett állományra és alkönyvtárra. Ezt azonban csak az első időszakban lehet megtenni!

A rejtvényekből néhány már megfejtve

Először is, maga a floppylemez nem tartalmazza a vírust, így nincs is mit keresni rajta. Amikor az installáló program elindítja a számlálót, létrehoz egy látszólag véletlen számot a rendszerindítások számából, majd aktivizálódik a trójai program, és szétroncsolja az adatokat, valamint a programokat a merevlemezen. A rendőrségi nyomozócsoporthoz adatai szerint ezt a trójai programot tartalmazó floppyt legalább 7000 cégnek küldték el 1989 decemberében és 1990 januárjában. A címlista forrásaként felhasználták a CW Communications céget, ami egy magazinok és újságok címlistáit készítő és címkéket nyomtató vállalkozás. A vállalkozók fizetnek a címjegyzék összeállításáért, kinyomtatásáért és a küldemények postázásáért. Nos, az elkövető szervezet is fizetett ezért a listáért 158.000 dollárt a Chase Manhattan Bankon keresztül a PC Business World tekintélyes szaklap sajtószolgálatára hivatkozva, annak nevében. Többek között azoknak a listáját kérték, akik annak idején jelen voltak a WHO 1988-as stockholmi AIDS-konferenciáján.

A címlisták és a címkék annak és rendje módja szerint elkészültek. A cég el is küldte azokat a megrendelőnek, és pedig a Bond Streetre Londonba, egy Ketema and Associates cég részére. A megrendelés indoka az volt, hogy ez

a vállalkozás Nigériából származó kereskedelmi szoftvercsomagokat szeretne postázni. Így azután az USA-tól Svédorszáig, az NSZK-tól valószínűleg Magyarorszáig mindenhová eljutottak ezek a veszélyes postai küldemények.

Már vannak becslések az okozott károkról is. 1989 decemberében a Londoni Tőzsdén, az új-zélandi, ausztráliai bankokban, valamint a brit Honvédelmi Minisztériumban ez a trójai lemez nagy rombolásokat okozott. Hasonló károkról érkezett jelentés a skandináv AIDS-kutatási centrumként is üzemelő stockholmi Roalagstull kórházból is, ahol a nyilvántartás adatainak nagy része megsemmisült. Ők indították el a vírusriadót is. Több tucat lemez érkezett a WHO genfi központjába is, különböző kutatók nevére. Franciaországban a küldemények legtöbbit a WHO párizsi központjának adatrendszerében pusztítottak. Az Európában azonosított küldemények közös vonása, hogy azokon a PC Cyborg panamai cég szerepelt feladóként 1989. december 8. és 12. közötti bélyegzéssel, London SW1, SW7, W1 körzeteinek postahivatalaiból. Sok ellentmondó hír kering ennek a trójai programnak a terjedéséről, természetéről és az általa okozott károkról. Mindenesetre szakszerűen, nagy tudással előkészített terrorista akcióról volt szó.

Eddig senkinek sem sikerült visszafejtenie a kódot. Az installációs lemezen két, összesen mintegy 320 kilobájtos állomány tartalmazza a programrendszert, INSTALL.EXE és AIDS.EXE nevű állományok formájában. A vizsgálatok szerint az egész rendszert Assamblerral megspékelt Quick BASIC programnyelven írták. A programrendszer csak installálás után tud működni.

A trójai funkciók nyomkövetése hihetetlenül nehéz, mert az eddig elmondottak csak a kezdetet jelentik. Utána a program sok lépésben építi fel végleges struktúráját, egyéb rejtett és irracionális nevekkal számos furcsa alkönyvtárat és állományt hozva létre. A szükség nagy erőfeszítésekre sarkallta a károk méréséklésében érdekelt szakembereket. Megpróbáltak programozási eljárásokat kidolgozni a folyamat követésére, mert a trójai programrendszer DOS-SHELL rutinokkal és magukat sokszor átiró és módosító segédprogramokkal teszi teljesen követhetetlenné a folyamatot.

A továbbiakban az eddig feltártak alapján ismertetjük a rendszernek a működését mint a számítógépes terrorizmus egyik „gyöngyszemét”. Természetesen nem forráskód szinten, csak annyira, hogy megérthessük: sok olyan

hely van egy gépen, ahova el lehet dugni egyet s mást.

Nyomdatechnikai okokból, illetve a nem láthatók láthatóvá tétele érdekében a programrendszer működésének ismertetése során néhány számítógépes karakter helyett más jelzést fogunk alkalmazni a könyvtári struktúrák jelzésére, mégpedig az alábbiakat:

– az ALT 255 (vagy másképpen HEX FF) karakter helyett, amely a monitoron szóköznek mutatkozik, valójában DOS karakterként funkcionál.

@ – az aláhúzás karakter (ALT 95 vagy másképpen HEX 5F) helyett.

s – a szóköz karakter helyett az állomány- és alkönyvtárnévben.

A kiindulási pontot a küldeményekből érintetlenül megszerzett eredeti lemezek jelentették, ezekből sikerült néhány dolgot visszafejteni. Létkérdés ugyanis, hogy megtanuljuk, mit csinál a program a brutális erő képviselő szoftverbomba bekapcsolásáig, és mit lehet tenni az aktivizálódás megelőzésére akkor, amikor a rendszer már beépült a merevlemez struktúrájába.

Installálás és aktivizálódás

A trójai vírus eddig mindegyik elkapott program esetében 90 rendszerindítás után következett be, de csak akkor, ha az INSTALL program szabályosan lefutott. Ez megegyezik a dr. Solomon's által észlelt két eddigi példával. Ami viszont eltérő és érthetetlen, hogyan biztosítja a program a hamis ellenőrzést (dozen verify), mielőtt a kód akár egyszer is végrehajtott volna. Mert az bizonyított, hogy ezt még a program aktivizálódása előtt, azaz az első rendszerindítás előtt megteszi! Vajon miért aktivizálódik számos kópia esetében a figyelmeztetés, előre felhíva a figyelmet a károkozásra, mielőtt még visszafordíthatatlanul elindulna a destruktív rendszer? Talán hiba van az install vagy a számláló rutinban? Esetleg több verziót bocsátottak ki? Mindezek a kérdések még válaszra várnak.

A folyamat teljes lefutásához egy normál AT gépen mintegy 90 másodperc szükséges. A teljes installációs folyamat alatt a a képernyőn egy referencia-

szám látható. A leírás szerint ha regisztrálja a programot, ez lesz a referencia-száma. Amikor a a program destruktív folyamata beindul, akkor ismételten megmutatja a monitoron a referenciaszámot, világos utalással a számmal kapcsolatos összefüggésekre. Esetleg titkosítási és dekódolási folyamat során van szükség erre a betű-szám kombinációra? Például ilyen 12 jegyű referenciaszám volt az egyik példányon: A9738-1655603. Ez nem hozott létre share-lemezt. Egy másik vizsgált példány kódja A935759-1048985, ez pedig létrehozott ilyen lemezt.

Amikor a küldeményt gyanútlan tulajdonosa megkapja és behelyezi a gépébe, először is el kell indítania az installálási folyamatot. Ekkor jön létre a már korábban is említett 255-ös ASCII karakter (azaz szóköz) nevű rejtett alkönyvtára, mégpedig a C: merevlemezegység gyökérkönyvtárából nyílóan. Az eredeti AUTOEXEC.BAT állományt átmásolja egy AUTO.BAT nevű állományba. Ennek az első sorába elhelyez egy megjegyzést:

```
REM Use this file in place of AUTOEXEC.BAT for  
convenience
```

Azaz „az AUTOEXEC.BAT helyett egyszerűbb, ha ezt a állományt használja”. S itt van az első csavar. (Úgyanis a program ezen álcázó állomány mellett létrehoz egy hidden (azaz rejtett) AUTOEXEC.BAT állományt is, ami ténylegesen végrehajtásra kerül:

```
echo off  
C:  
cd\#  
rem# PLEASE USE THE auto.bat FILE INSTEAD OF  
autoexec.bat FOR CONVENIENCE  
auto.bat
```

A CD után, még ha a felhasználó meg is leli ezt az állományt, egy olyan karaktert talál, ami nem jelenik meg a monitorján. Így valójában ez az ártalmatlannak tűnő program a következőket hajtja végre:

Belép a rejtett, a szóköz (space) karaktert mint elnevezést viselő alkönyv-

tárba, és ott végrehajtja a REM#.EXE állomány futtatását. Ennek az a feladata, hogy visszaszámoljon a beállított rendszerindításokból, s a számláló nulla állásánál indítsa a tönkretétel második fázisát. S amikor a véletlen számláló eléri a nullát, kitakarítja a merevlemezt, mégpedig alaposan. Ez már a vég, de előtte még sok minden történik. Mintha valaki vagy valakik itt akarnák kiélni szadizmusukat. Az eredeti AUTOEXEC.BAT végrehajtódik, miután a program megfelelő része lefutott. Hiába keressük hagyományos módon, mert Hidden, System, Read-only attribútumot kapott.

Létrehoz egy meglehetősen szokatlan könyvtári struktúrát is a C: meghajtó főkönyvtárából kiindulva. Ha említett jelölésrendszerünket használjuk, akkor ez így néz ki:

```
C:\###s###
```

```
C:\###s###\##s####
```

```
C:\###s###\##s####\#####s##
```

```
C:\###s###\##s####\#####s##\ERROR IN THE
```

Az Error nevű nem rejtett könyvtár, de jól el van dugva szem elől. Utána építi fel saját állományait is, amelyek hasonlóan ötletesen vannak elnevezve:

```
@.ss@
```

```
@.s@
```

```
@.s@@
```

```
@@@.ss@
```

```
@@@@.s@@
```

Ezekből képződnek azok az összekutyult nagyméretű állományok, amelyek majd teljesen megtöltik a merevlemezt, amikor a pokolgép „felrobban”. Az installálás során először megvizsgálja, hogy nem írásvédett rendszerrel van-e dolga. Az A: meghajtón létrehoz egy TESTZZT.P állományt, amit utána eltüntet. Egyszerű ötlet, de működik! Ha a floppy írásvédett, akkor nem működik a rendszer.

Aktivizálódás

Kilencven újraindítás után a monitor képernyőjének közepén a következő angol nyelvű üzenet jelenik meg:

„The software lease for this computer has expired. If you wish to use this computer, you must renew the software lease. For further information turn on the printer and press Return.”

„A szoftverbérleti szerződés erre a számítógépre lejárt. Amennyiben még szeretné használni ezt a számítógépet, meg kell újítania a bérleti szerződést. További információkért kapcsolja be a nyomtatót és nyomja meg a Return billentyűt.”

Amennyiben a felhasználó eleget tesz az utasításnak, akkor printere a következő, szintén angol nyelvű dokumentumot írja ki:

„If you are reading this message, then your software lease from PC Cyborg Corporation has expired. Renew the software lease before using this computer again. Warning: do not attempt to use this computer until you have renewed your software lease. Use the information below for renewal.

Dear Customer!

It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive: - a renewal software package with easy-to-follow, complete instructions; - an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A9738-1655603-

The price of 365 user applications is US\$189. The price of a lease for the lifetime of your hard disk is US\$378. You must enclose a bankers draft, cashier's check or international money order payable to PC CYBORG CORPORATION for the full amount of \$189 or \$378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.”

„Ha Ön ezt az üzenetet olvassa, akkor szoftverének bérlete a PC Cyborg Corporationnél lejárt. Újítsa meg szoftverbérletét, mielőtt számítógépét ismét használná. Figyelmeztetés: ne is próbálkozzon a számítógép használatával mindaddig, amíg bérletét meg nem újította. Használja a megújításhoz alábbi információinkat:

Kedves Ügyfelünk!

Itt az ideje, hogy kifizesse a bérleti díjat a PC Cyborg Corporationnek. Töltsse ki a SZÁMLÁT és csatolja befizetését az Önnek megfelelő bérleti konstrukcióra. Ha nem a kinyomtatott SZÁMLÁT használja, akkor minden levelezésében hivatkozzon a lent közölt referenciaszámra. Válaszul megküldjük Önnek: — megújított szoftvercsomagunkat, könnyen követhető, komplett leírással; — önmagát automatikusan installáló lemezünket, melyet percek alatt bárki használni tud.

Fontos referenciaszámok: A9738-1655603-

A 365 felhasználói alkalmazás ára 189 dollár. Merevlemezének teljes élettartamára szóló bérleti díj 378 dollár. Megrendelése mellé csatolnia kell a PC CYBORG CORPORATION részére szóló bankátutalást, csekket vagy egyéb nemzetközi fizetőeszközt, a 189, illetve 378 dolláros teljes összegre vonatkozóan. Tüntesse fel a nevet, a céget, a címet, a várost, az államot, az országot, az irányítószámot. Megrendelését küldje az alábbi címre: PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.”

Miután ezt a levelet a gép kinyomtatta, a következő üzenetet jeleníti meg a monitoron:

„Please wait thirty minutes during this operation. Do not turn off the computer since this will damage your system. You will be given instruction later. A flashing hard disk access light means WAIT!!!!!”

„Kérem, várjon harminc percet, amíg tart ez a művelet. Ne kapcsolja ki a számítógépét, mert az tönkreteszi a rendszerét, károsodik. Később újabb utasításokat fog kapni. A merevlemez kijelzőjén villogó fény azt jelenti, VÁRJON!!!!!”

Ez az üzenet mintegy óra hosszát marad a képernyőn, fél óráig pedig a merevlemez nagy intenzitással dolgozik.

Felbukkant ennek a trójai programrendszernek egy másik verziója is, amely tovább variálja a felhasználó és a gép kínzását.

Ha újra akarjuk indítani a gépet a <CTRL><ALT> billentyűkkel, akkor a gép hangszórója a rendőrségi sziréna hangját hallatja, a monitorra pedig kiírja az alábbi üzenetet:

„Sorry for the long delay ... still processing ... please wait.”

„Elnézést a hosszú várakozásért ... tart a feldolgozás ... kérem, várjon.”

Az újraindítási kísérlet során nemcsak a rendőrsziréna hangját hallatja a rendszer, hanem egy újabb üzenettel is meglep bennünket:

WARNING — if you interrupt the program you will destroy the files on drive C.

FIGYELMEZTETÉS — ha megszakítja a programot, tönkreteszi állományait a C: meghajtón.

Hosszabb idő eltelte után — pl. 40 perc volt 20 Mbájtos XT-n, 4,77 MHz órajellel — a megjelenő angol nyelvű üzenet felszólítja a felhasználót, hogy tegyen be egy formázott üres lemezt. Az <ENTER> gomb lenyomása után a lemezre generál egy SHARE.EXE nevű programot, valamint a teszt során egy MMM247HU.CPA nevű állományt. Ez utóbbi neve a tapasztalatok szerint kópiánként változik! Utána ismét üzenet nekünk:

„The SHARE DISKETTE in drive A is now ready for use. Please remove it. Take it to another computer. Turn on that computer in the usual way. After the computer has been booted, insert the SHARE DISKETTE into its drive A. Then at the C prompt type A:SHARE and then press ENTER. A short routine will follow on that computer. Afterwards, return the diskette to this computer.”

„A TARTALÉKLEMEZ az A: meghajtóban használatra készen. Vegye ki. Vigye át egy másik számítógéphez. Kapcsolja be azt a szokásos módon. Rendszerindítás után tegye be a TARTALÉKLEMEZT az A: meghajtóba. A

C bejelentkezőhöz írja be, hogy A:SHARE és nyomja le az Enter billentyűt. Egy rövid rutin következik azon a gépen. Utána hozza vissza a lemezt ehhez a számítógéphez.”

Ha a gyanútlan felhasználó mindezt megteszi, tönkretette a másik gépet is. Ezzel installálja ugyanis a lemezt felismerhetetlenül összekeverő trójai programot. Ha újra beteszi a gépbe ugyanezt a lemezt, akkor egy új tartalékmezt követel a gép, mert különben törli az adatokat...

Rövid idővel utána összeáll a rendszer, és attól a pillanattól kezdve a gép használhatatlanná válik. Innen már a forgalomban lévő két trójai verzió ugyanúgy működik. Amint dr. Solomon's sejtette, eltérően működő, de azonos eredményre vezető verziókat postáztak a számítógépes terroristák.

A trójai program elleni védőprogramot író Jim Bates, valamint a szétküldés alapjául szolgáló címlistát összeállító PC Business World szerkesztője, Mike Magee 1989. december 20-án a fentiekről számítógépes körlevelében tájékoztatta az elektronikus levelesládák használóit.

A következmények

Amikor vége a merevlemez megmunkálásának, a főkönyvtárban egy új állomány jön létre a C: meghajtón, a CYBORG.DOC. Ebben az állományban megismétlik a kinyomtatott levélben található utasításokat a program „regisztráltatására”. Azon a lemezen 0 bájtos szabad helyet találunk azután, amikor a tartalomjegyzéket szeretnénk kilistázni. A DOS operációs rendszerre ráül egy sajátos héj rutin, a shell, ami ezután megakadályozza, hogy rendeltetésszerűen használjuk a gépet. Ezt a rutint CYBORG.EXE-nek nevezik, és természetesen hidden read-only attribútumai vannak, hogy a normál listázás során ne lehessen észrevenni. Ez azután nem enged semmilyen DOS funkciót meghívni vagy futtatni, helyette csökönyösen egyetlen rendszerüzenetet ismétel:

„WARNING: You risk destroying all of the files on drive C. The lease for a key software package has expired. Renew the lease before you attempt any further file manipulations or other use of this computer. Do not ignore this message.”

„FIGYELMEZTETÉS: Ön a C: meghajtón lévő összes állomány tönkretételét kockáztatja. Egy kulcsfontosságú szoftvercsomag bérlete lejárt. Előbb újítsa meg a bérletet, mielőtt megkísérelné, hogy további fájlműveleteket végezzen vagy más módon használja ezt a számítógépet. Ne hagyja figyelmen kívül ezt az üzenetet.”

Ha mégis akarunk más műveletet végezni, akkor a számítógép illegális utasításra vagy fájlnévre hivatkozó rendszerüzenettel nem hajtja végre. Ha pedig kikapcsoljuk a gépet, és egy tiszta rendszerlemezről indítunk, akkor azt látjuk, hogy az egész merevlemezen egyetlen állomány, a CYBORG.DOC jelentkezik, és 0 bájt szabad hely maradt. Természetesen minden korábbi állomány rajta van a lemezen, de titkosítva, átkódolva és hidden attribútummal. A kísérletek során megfertőztek egy 20 Mbájtos merevlemezt. 90 rendszerindítást végezve elindították a trójai programot, majd miután az elvégezte a fentebb említett műveleteket, a hidden attribútum levételével listázhatóvá tették a tartalomjegyzéket. Az eredmény magáért beszél:

Volume in drive C has no label

Directory of C:\

#UCU#R	AK	10071	13-07-85	1:43p
#UC@R&	AK	27760	3-07-85	1:43p
COMMAND	COM	23717	13-07-85	1:43p
#1!8_68@	AU	587	3-19-89	9:11a
6#1N	AK	32	2-27-89	12:33p
KF{0U	AK	853	13-12-89	4:07p
}G6R	AG	98	1-04-80	12:01a
AUTOEXEC	BAT	108	1-04-80	12:01a
AUTOEXEC	BAK	17	1-04-80	12:01a
}#@&	AU	172562	8-07-89	10:40a
&_}1	AU	46912	12-07-89	11:58a
!}	AU	7294	3-01-87	4:00p
1G	AU	102383	3-01-87	4:00p
H8C	AU	146188	1-04-80	12:11a

CYBORG	DOC	1326	1-04-80	12:05a
CYBORG	EXE	642	1-04-80	12:05a
AUTO	BAT	117	1-04-80	12:06a
17 File(s)		0 bytes free		

Ezekhez még számos rejtett alkönyvtár is hozzáadódik. Azokban egy indexelt szekvenciális adatbázis részeit találhatjuk, amelynek mezőit a 20h-val töltötték fel. Ez az adatbázis foglalja el a lemez szabad területeit. Amennyiben a rendszer tápfeszültségét kikapcsoljuk, a merevlemez már nem bootol. Ha az AUTOEXEC.BAT állományt akár csak egyszer is végrehajtotta a rendszer, a <CTRL><ALT> billentyűkombinációval történt minden újraindítás után kiadott DIR parancs vagy DOS utasítás végrehajtásakor láthatóvá válik a figyelmeztetés. Amennyiben a Norton Utilities vagy más segédprogram segítségével belenézünk a CYBORG.EXE állományba, a következő érdekes jelenséggel állunk szemben. Ezt a szöveget az 560 offset címen találjuk az állományban:

```
<false end-file-marker> <The Norton Utilities cannot read  
this file because the FAT has been locked> BORG EXE
```

És kódot természetesen nem találunk semmilyen megszokott segédprogrammal. Amennyiben direkt szektorolvasással próbálkozunk, rájöhethetünk a trükkre, hogy a CYBORG.EXE programkód egyes részleteit szétszórva a legkülönbözőbb offset címeken találhatjuk meg. A rendszer bennünket megelőzve a szövegeket és a merevlemez teljes könyvtári struktúráját alaposan átkódolta. Az előbbieken bemutatott 20 Mbájtos merevlemez korrekt főkönyvtári listája a következő volt:

```
Volume in drive C has no label  
Directory of C:\  
IBMBIO COM 10071 13-07-85 1:43p  
IBMDOS COM 27760 3-07-85 1:43p  
COMMAND COM 23717 13-07-85 1:43p  
INFECTED EXE 587 3-19-89 9:11a
```

TINY	COM	32	2-27-89	12:33p
W13_B	COM	853	13-12-89	4:07p
AUTO	BAT	98	1-04-80	12:01a
AUTOEXEC	BAT	108	1-04-80	12:01a
AUTOEXEC	BAK	17	1-04-80	12:01a
AIDS	EXE	172562	8-07-89	10:40a
SCAN	EXE	46912	12-07-89	11:58a
FA	EXE	7294	3-01-87	4:00p
NU	EXE	102383	3-01-87	4:00p
REM	EXE	146188	1-04-80	12:11a
14 File(s) 15872000 bytes free				

A kódolás során megállapítható volt, hogy a titkosítás és a megfejtés során az egyes betűket vonalak vagy egyéb jelek jelentik. A rendszer két kódtáblát alkalmazott. Az egyik a fájlkiterjesztéseket titkosította a következő táblázat alapján:

Eredeti	Kódolt	Eredeti	Kódolt
Nincs kiterj.	AB	APP	AC
BAK	AD	BAS	AF
BAT	AG	CAT	AH
CMP	AI	CNF	AJ
COM	AK	DAT	AL
DB	AM	DBF	AN
DCT	AO	DEM	AP
DIR	AQ	DOC	AR
DVC	AS	DYN	AT
EXE	AU	FIL	AV
FNT	AW	FRM	AX
GLY	AZ	HLP	BA
INP	BC	LBR	BD
LOC	BF	INI	BB
MDF	BG	?MF	BH

MNU	BI	MSG	BJ
NDX	BK	OUT	BL
OVL	BM	OVR	BN
PGM	BO	PIF	BP
PRD	BQ	PRG	BR
PRN	BS	SCR	BU
SET	BV	SK	BW
REC	BX	ST	BX
STY	BY	SYS	BZ
TBL	CA	TXT	CB
WK1	CC	WK2	CD
WKS	CE	XLT	CF
XQT	CG	ZBA	CH
DRV	CI	LRN	CJ
CAL	CK	FON	CL
SPL	CM	MAC	CN
TST	CO	LGO	CP
GRB	CQ	GRA	CR
DTA	CS	\$\$\$	CT
VC	CU	TMP	CV
PAS	CW	OBJ	CX
MAP	CY	LST	CZ
LIB	DA	ASM	DB
BLD	DC	COB	DD
COD	DE	FOR	DF
FMT	DG	DIF	DH
DRW	DI	FLB	DJ
PIC	DK	PAT	DL
VFN	DM	GEM	DN
REN	DO	IMG	DP
RSC	DQ	MEM	DR

Az egyes állományok tartalmát szintén igen ötletesen egy másik kódtáblát használva tünteti el:

Eredeti	Kódolt	Eredeti	Kódolt
!	F	#	I
\$	' (apostrophe)	%)
&	S	' (apostrophe)	G
(#)	7
- (minus)	9	0 (zero)	_(underscore)
1	N	2	- (minus)
3	\$	4	{
5	}	6	T
7	&	8	E
9	0 (zero)	@	D
A	K	B	(
C	M	D	J
E	5	F	1
G	U	H	R
I	Z	J	4
K	W	L	@
M	8	N	Y
O (letter O)	V	P	L
Q	H	R	O (letter O)
S	!	T	6
U	B	V	X
W	%	X	P
Y	2	Z	Q
^ (caret)	~ (tilde)	_(underscore)	C
{	3	}	A
~ (tilde)	^ (caret)		

A rendszer adatait és a rendszerállományokat érintetlenül hagyja, és nem is kódolja át. A partíciós tábla és a boot-szektor érintetlen marad. Így a bevezetőben említett feltételezés, hogy a rendszerből valamilyen boot-vírus

válik le, sok-sok winchester tönkretétele után sem igazolódott be. A rendszerállományokra viszont ráépül egy sajátos héj, ami vezérli a disznóságokat, és a felhasználó a jelenlegi eszközeivel nem tud ennek a sajátos operációs rendszernek a mélyére hatolni. A rendszerállományokat és egyéb fontos rendszerelemeket egy titkosított alkönyvtárban rejti el, ahová a FAT-ban lévő belépési pontot is elkódolja. A kapuőr és a rendszer karmestere a CYBORG.EXE állomány, ami programozástechnikai csúcsteljesítmény. 1990 februárjában ennyi vált ismertté e példátlan programcsomagról. Eddig egyetlen használható ellenprogram készült, az amerikai Jim Bates által írt Clearaid, amely az Ázsio-Vikinél szükség esetén hozzáférhető. Ezzel vissza lehet állítani a rendszer eredeti állapotát.

Dr. Solomon's jelezte — és mi is bemutattuk —, hogy a rendszer létrehoz egy SHARE.EXE nevű állományt, amelynek futtatásával eredeti formában 30 szabad újraindítást engedélyez, mielőtt tönkretenné a merevlemez adatállományát, amennyiben az instrukcióknak megfelelően cselekedtek. Megjegyzendő, hogy más forrásokból származó Cyborg lemezek a próbák során nem hozták létre sem a SHARE állományt, sem pedig a hozzájuk tartozó dokumentációt. Úgy tűnik, a SHARE-t létrehozó példányokat az USA-ban, a többi pedig Európában terjesztették. Mind a mai napig semmi hír magukról a merénylőkről. Ők, a számítástechnika történetének első sikeres terrorista akcióját kifundálók, boszorkánykonyhájukban esetleg újabb trükkökön törnek a fejüket. Reméljük, hogy nem így van. Ilyen programozói zsenialitással értelmes feladatok megoldásában igazán nagyszerűt — és hasznosat — produkálhatnának.

A célba vett áldozatok egyértelműen az AIDS-kutatással foglalkozó intézmények voltak. Így Magyarország sem áll kívül a veszélyeztetettek körén, mert itt is működnek AIDS-kutatással foglalkozó, nemzetközi konferenciákon részt vevő intézmények. Így ha kapnak programlemezeket, az olyan gépen, amelyen éles adatok vannak, még véletlenül se indítsák el! Erre a célra megéri egy különálló, hálózatba nem kapcsolt tesztelő gépet tartani.

Végezetül, mit tanácsol Jim Bates, ha valaki ilyen programrendszerrel találkozok:

1. Először tiszta rendszerlemezről indítsuk el a gépet.
2. Valamilyen segédprogrammal szedjük le a Hidden és System attribútu-

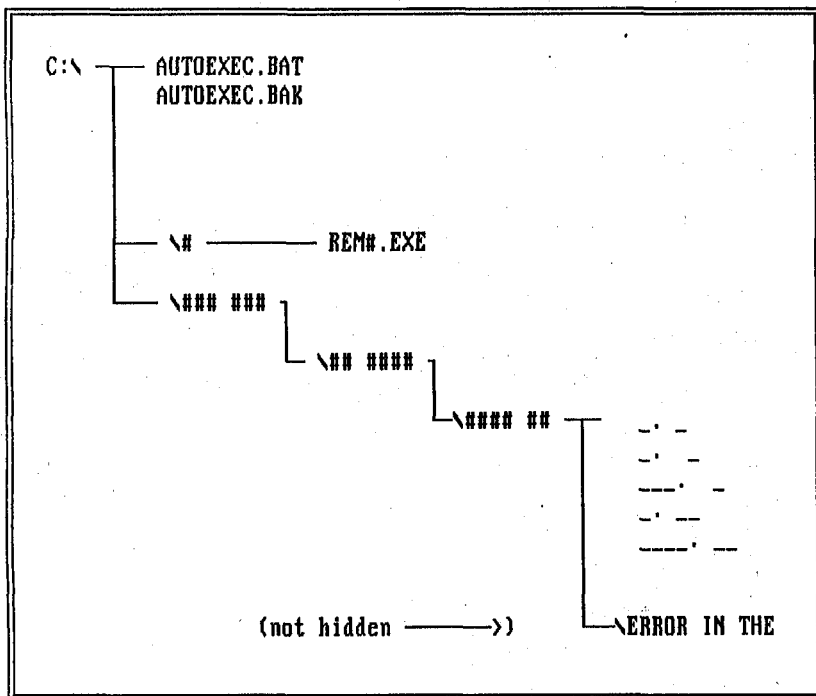
mot a rejtélyes állományokról és könyvtárakról.

3. A fejezetben említett összes állományt törölni kell, beleértve az AUTO-EXEC.BAT-ot is.

4. A Trojan AIDS esetében vissza kell nevezni az AUTO.BAT-ot AUTO-EXEC.BAT-ra.

5. Normálisan újra kell indítani a gépet.

Hogy mindezt miért írtuk le ilyen részletesen? Vannak jelei, hogy mások is próbálkoznak ilyen terrorista célú trójai programok írásával. S ha már ismerjük egy ilyennek a „lelkületét”, nem esünk pánikba, ha véletlenül becsap a mennykő.



Az AIDS Information Disk trójai program könyvtárstruktúrája

NEM CSODASZEREK

Sokan azt hiszik, ha valamilyen programvírus elleni programmal végigfésülik saját floppylemezeiket és a gépek merevlemezét, akkor náluk már nem történhet semmilyen baleset, védve érzik magukat a programvírusok támadásaival szemben. Hazánkban kézen-közön sok vírusdetektor forog, így érdemes alaposabban megvizsgálni a legelterjedtebb programokat. Használjuk-e őket, és ha igen, akkor mire alkalmasak ezek a szoftverek?

E programok két nagy csoportját különböztethetjük meg: a szabadon terjeszthető és felhasználható közprogramokat — azaz többnyire sharewareket —, valamint a kereskedelmi forgalomban kapható jogvédett programokat. Ez utóbbiakat általában másolásvédelemmel is ellátják, így viszonylag kevés példány kerül belőlük tényleges használatba. A védelem nélküliek viszont rohamosan terjednek, természetesen minden leírás nélkül. Ha tisztes-séges a forgalmazó, ha megfelelő kiegészítő szolgáltatásokkal és elérhető áron adja védelem nélküli programját, akkor az illegális másolatok nem okoznak neki számottevő kárt, hanem inkább reklámot csinálnak neki. A szabad szoftverek még népszerűbbek. Éppen ezért beszereztünk és teszteltünk néhány hazánkban elterjedt vagy elterjeszteni szándékozott (Turbo Anti Virus Toolkit) programot, hogy a származási országban nyilván jól alkalmazható program mennyire válik be a magyar viszonyok között.

Tesztünkbe a csak Nyugaton beszerezhető termékeken kívül beválogattuk a Cédrus Rt. SolarSoft programkönyvtárában kapható olcsó szoftvereket és a magyar szoftverkommuna csatornáin keringő, tisztázatlan eredetű példányokat is.

Ikarus

Az osztrák piacon jó hírnévnek örvendő az Ikarus vírusmegelőző programcsomag. Sikertült megszerezni annak 1.6-os verzióját. A program a disztributív lemezen sok demonstrációs állományt, valamint két fő programot a VU.EXE segédprogramot, valamint a tárrezidens védelmet adó

GUARD.COM-ot tartalmazza. Bár a program Ausztriában elég drága (mintegy 1500 schilling), különböző változatait Magyarországon is elterjedten alkalmazzák.

A programcsomaghoz mellékelt demonstrációs és oktató programokból sok érdekességet lehet megtudni a számítógép belső világáról. Először lássuk a fő programot, a VU.EXE-t. A programcsomag nem rendelkezik másolás-védelemmel. Igaz, önmagát sem védi meg, mert a hozzánk jutott másolatról egy potyogós vírust kellett leszedni. A program komoly hibája, hogy nem kódolva tartalmazza a vírusazonosítókat. Így például a Scan hamis hibajelzésként az 1701/1704 vírus jelenlétét érzékeli, pedig csak az azonosító szekvenciát látja!

Az általunk tesztelt 1.6 verzió bejelentkezéskor német menüt kínál fel:

Viren suchen	(Víruskeresés)
Programme entseuchen	(Vírusirtás)
Speicherbelegung	(Tárfoglalás)
GUARD installieren	(A GUARD program installálása)
Information	(Információ)
Ende Virus-Utilities	(Kilépés a vírusellenes programokból)

A programot aktív vírusokkal tesztelve kiderült, melyiket ismeri fel kifogástalanul. Meglepetésünkre felismerte a Kedd 1 magyar vírusátírást is, és korrekten kiírtotta. Amikor a vírust felismerte és kitakarította, akkor az állományokat is korrekten állította helyre. A két folytonos rendszerhívást okozó vírusverziót külön vírusnak vette. Zavaró, hogy ezeknek a vírusoknak nem a nemzetközileg ismert neveit használja, hanem az 1701-et Virus #1-nek, az 1704-et pedig Virus #2-nek nevezi. Rendszerüzenetei is értelemszerűen német nyelvjűek:

1701.COM ist mit Virus #2 infiziert.
1704.COM ist mit Virus #3 infiziert.
KEDD1.COM trägt Jerusalem Virus.
PENTEK13.COM trägt Jerusalem Virus.
REBOOT.COM ist mit Virus #1 infiziert.

PENT13MU.EXE trágst Jerusalem Virus.

Magyarországon már túlhaladott, hiszen nem ismer fel és így nem irt ki olyan elterjedt vírusokat és változatokat, mint a Yankee Doodle, az Eddie/Dark Avenger, az Ivan/Victor v1.00 vagy a Vacsina-B.

A GUARD.COM 1.5-ös verzióját találhatjuk a programcsomagban. Nagyon jól sikerült program, egyetlen hibája, hogy nagyon nagy a tárban maradó része, 8000 bájt. A 13-21 megszakítókat veszi el, és saját magán átszűrve adja vissza. Védi a boot-szektor, a formázást megakadályozza. Ezen kívül egy sajátos filozófia alapján védi a .COM és .EXE állományokat. Ez a logikus megokolás úgy szól, hogy egy .EXE vagy egy .COM program nem fr bele egy másik .EXE vagy .COM állományba, ezért ha ilyen történik, az értelemszerűen illegális művelet.

A Magyarországon előforduló vírusok közül a következők ellen nyújt védelmet: 1701/Cascade, 1704/Cascade, Jerusalem-B, Eddie/Dark Avenger, Vienna-B/Reboot, Ivan/Victor v1.00.

Erőssége, hogy megóv az Ivan/Victor fertőzése ellen. Ez az egyetlen olyan „szabadon” hozzáférhető szoftver, ami Magyarországon nem kereskedelmi program és ezt tudja, bár a fertőzést megszüntetni nem képes. Viszont nem véd meg a Yankee Doodle és a Vacsina-B vírusok támadásától.

A programot elindítva aktivizáljuk. Lehetőség van arra is, hogy letiltsuk képernyőüzeneteit, vagy a védelmet csak egyetlen lemez meghajtóra kérjük. Nem ad teljes körű védelmet, ezért ma már korszerűtlen termék. A szoftvert az Ikarus Software GmbH (A-5700 Zell am See, Franz-Josef-Str. 7) készítette és forgalmazza.

Dr. Solomon's Antivirus Toolkit v2.2 (1989)

Nyugat-Európában, de főként az USA-ban szinte csodaszerként emlegetik a Dr. Solomon's Antivirus Toolkit vírusfertőzés-elhárító programrendszert, így nagy várakozással fogtunk neki a tesztnek, hogy megtudjuk, mennyire alkalmazhatóak ennek a programrendszernek az elemei a hazai körülmények között.

A FINDVIRU.EXE a programcsomagban a diagnosztikát végzi. Segítség-

gével azonosítani lehet az esetleges behatolót. A dokumentáció szerint a következő — magukat az egyes állományokhoz hozzáfűző — fájlvírusokat ismeri fel:

Ismert elnevezése (és hossza):

— (405)

Vienna, Vienna-B/Reboot (648)

Datacrime (1168)

1701/Cascade/Poty #1 (1701)

1704/Cascade/Poty #2 (1704)

Jerusalem-B/Péntek 13 (1813)

Traceback (3066)

Ezzel szemben Magyarországon a következő vírusok fordultak elő a tesztünk idején, 1990 májusában:

648/Reboot #1

Vienna-B/Reboot #2

1701/Cascade/Poty #1

1704/Cascade/Poty #2

Jerusalem-B/Péntek 13

Yankee Doodle/Music, 5 órai tea

Ivan/Victor v1.00

A vizsgálat során ezekkel fertőzött tesztállományokat alkalmaztunk. A Magyarországon előforduló vírusok közül a felsorolt két utolsó program kivételével mindegyiket megtalálta. Nagy biztonsággal felismeri a Péntek 13 magyarországi mutánsát, a Kedd 1-jét is. Sajnos nem mindig jól diagnosztizál, csak a karakteres azonosítókat keresi, így vaklármát is okoz, például az Ikarus v1.6, Prgdoki v2.11E, a Guard (az Ikarus programrendszer tárrezidens modulja) esetében. Ezekben a programokban ugyanis nincs kódolva a keresési minta.

Nem ismeri fel az utóbbi időben Magyarországon elterjedt, „népszerű” vírusokat: Eddie/Dark Avenger, Ivan/Victor v1.00, Yankee Doodle, Vaccina-

B (A vírus magyar átiratának hossza nem egyezik meg a nyugati víruskatalógusokban megadottal!). Természetesen az ezekkel fertőzött állományokra is azt írja ki, hogy "is ok", tehát a felhasználókat tévesen informálja. Tesztjének eredményét a nyomtatóra is kiküldi. Kérdés után megvizsgálja a boot-szektor is. A következő boot-vírusokat keresi, s azokat ki is tudja irtani a programcsomag egyéb programjai (zárójelben) segítségével: Brain (UnBrain program), Italian/Bouncing Ball (UnItal program), Pentagon, Yale/Alameda, Stoned.

A Magyarországon eddig előfordult boot-vírusok esetében kicsit jobb az arány, mert a négy leggyakoribb közül hármat képes detektálni, de a legelterjedtebb Disk Killer ellen sajnos hatástalan! Ugyancsak komoly probléma, hogy nem tud mit kezdeni a DOS 4.xx verziójának boot-szektorával. Ez már a program eredeti amerikai felhasználói környezetében is nagy fogyatékoságnak számít. Az ellenőrzés során — ha a felhasználó kéri — beoltja a floppylemez boot-szektorát a következő vírusok ellen: Brain, Italian, Stoned (az InocBrain, InocItal, InocStone programokat hajtja végre). A vizsgálat eredményét szintén nyomtatóra küldi.

INOC1813.EXE — A megadott lemezen beolt minden (COM, EXE) fájlt a Jerusalem (Péntek 13) vírus ellen. Minden állomány után a következő vírusazonosító 5 bájtot írja oda: MsDos. Így a vírus — a beoltási filozófia értelmében — nem működik. Ugyanakkor az egyszerűbb víruskeresők vírusosnak jelzik az állományt, noha nem az. Ráadásul a magyar mutáns esetében, ahol más az azonosító, ez szintén nem működik. A magyar vírus azonosítója ugyanis MsDns.

INOC648.EXE — Beolt a Reboot vírus ellen. A fájl összehasonlításánál minden fájl megegyezik az eredetivel bájtszinten. Kiírja azt is, hogy az EXE állományok is be vannak oltva. A Reboot vírus csak COM állományokat fertőz meg. Nem sikerült arra rájönni, mit is csinál valójában.

INOC1168.EXE — Ugyanaz a helyzet, mint az INOC648-nál.

INOCINT.COM — Beoltja az Int 21h-t (DOS function call), és akkor 864

bájt rezidens marad. Az újabb vírusok nem használják ezt a megszakítást, és ezért „sétágaloppban” úgy fertőznek, ahogy akarnak. Az utóbbi idők vírusai közül erre képes a Reboot, az Ivan, az Eddie, valamint a Yankee Doodle... Ha olyan programot indítunk, amely a 1701-1704/Cascade vagy a Jerusalem vírussal fertőzött, akkor a PC lemerevedik, és csak a hard reset vagy a főkapcsoló képes bele életet lehelni. Ez komoly hiba, mert teljes dBase állományok veszhetnek el amiatt, hogy nem lehet őket szabályosan lezárni! A lemerevedés előtt még utolsó erejével egy rendszerüzenetet ír ki, például:

„WARNING — something just asked if 1813 virus was present!!! This is a characteristic of 1813 trying to infect. The computer will stop IMMEDIATELY — please make a note of the program that you tried to run, and call for assistance.”

„Figyelem! — Valami éppen rákérdezett, hogy jelen van-e az 1813-as vírus!!! Ez annak a jele, hogy a 1813-as megpróbál fertőzni. A számítógép AZONNAL le fog állni — jegyezze meg, hogy melyik programot akarta futtatni és hívjon segítséget.”

Ennek a megoldásnak a károkozó hatása — ha dBase adatokkal dolgozunk — felér egy jól megírt víruséval. Csak annyi a szerény kérdésünk, hogy miért nem lehet a háttérben memóriarezidensen kezelni ezeket a vírusokat, rendszerleállítás nélkül. A magyar RVK első verziói (1.40-ig), csakúgy, mint az osztrák Guard-Ikarus rendszer, ezt a legtöbb esetben kifogástalanul megoldották! Talán a nagyobb cirkusz kedvéért?

INOCBRAI.EXE — Beoltja a floppy boot-szektorát a Brain vírus ellen. Az alábbi hexa szekvenciát teszi be a floppy boot-szektorának bájtjaira:

Bájt:	Hexa:
4.	34
5.	12
39.	FC
41.	1F
42.	3B

INOCITAL.EXE — Beoltja a floppylemezt az olasz pingpongozó vírus (Bouncing Ball) ellen. Csak floppy esetében működik! A következő hexa szekvenciát helyezi el a floppylemez boot-szektorában:

Bájt:	Hexa:
39.	E0
41.	08
42.	1A
508.	57
509.	13

INOCSTON.EXE — Beoltja a floppylemezt a Stoned vírus ellen. A következő négy hexa értéket teszi be a floppy boot-szektorának első négy bájtjára:

Bájt:	Hexa:
1.	EA
2.	05
3.	00
4.	C0

Ez a Stoned vírusnak is az első négy bájtja, és valószínűleg ezért nem megy már rá a floppylemezre. További eltérések a boot-szektorban:

Bájt:	Hexa:
39.	F8
41.	14
42.	04

Így a floppylemez nem lehet vírushordozó, tehát a vírus nem is kerülhet rá a számítógép merevlemezére. Ebben az esetben kivételesen jó megoldást alkalmaztak!

KILLBAD.EXE — A boot-vírusok által bejelölt hibás szektorokat felsza-

badítja. Floppyn kifogástalanul működik, viszont winchesteren már nem. Ilyen nagy cég, — bármennyire utálja is a DOS 4.xx verzióit (amiben e sorok írója mélységesen egytért vele, K.J.) — nem teheti meg, hogy nem vesz róla tudomást.

A merevlemez tesztet DOS 4.xx BIGDOS partíciós lemezen végeztük el (FAT-16), ami azt jelenti hogy a DOS 3.xx verzió 32 Mbájtos korlátját túllépő DOS partíciót használtunk. Ezt nem ismeri fel, és az alábbi hibaüzenetet írja ki:

~ Encountered DOS error 2:7 while reading the FAT sectors

(DOS hiba 2:7 a FAT-szektorok olvasásakor.)

NOFLOPPY.COM — Floppy hozzáférés korlátozása az INT 13 megszakításon keresztül.

0 = read/write permit

1 = write prohibit

2 = read and write prohibit

0 = olvasás/írás engedélyezése (Ez a normál állapot.)

1 = írás letiltása (Vagyis a floppyról csak olvasni lehet.)

2 = olvasás és írás letiltása (Nem lehet a floppyhoz hozzáférni.)

A program jól működik, csak éppen értelme, használhatósága a nem szakember számára kétséges.

NOHARD.COM — a merevlemezhez történő hozzáférést korlátozza.

0 = read/write permit

1 = write prohibit

2 = read and write prohibit

0 = olvasás/írás engedélyezése (Ez a normál állapot.)

1 = írás letiltása (Vagyis a floppyról csak olvasni lehet.)

2 = olvasás és írás letiltása (Nem lehet a floppyhoz hozzáférni.)

A Reboot vírus egyszerűen megkerüli és úgy dolgozik a winchesterrel, mintha ez a program ott sem lenne!

PEEKA.EXE — Felhossa a megadott lemez megadott szektorát a monitorra. Használata igen kényelmetlen, profi számítógépes tudás kell ahhoz, hogy felhozhassa a merevlemez adott szektorát a képernyőre. A laikus felhasználó pedig mit tud tenni? Ismernie kellene a BIOS hívásokat ahhoz, hogy valamit egyáltalán kezdhesen a program paraméterezésével.

Például: Az INT 13 paraméterezése úgy történik, hogy az első floppy 0, a második floppy 1, a merevlemez pedig Hex 80, vagyis Dec 128. Ha ezen túljutott, akkor már csak azt kell tudnia, hogy a lemezek fejei 0-tól és nem 1-től számozódnak, a szektorok pedig 1-től kezdődő számok. Arról nem is szólva, honnan tudja az egyszerű felhasználó, hogy a normál merevlemezen 17 szektor van, az RLL lemezen pedig 25... Ez a program szakmán kívüli felhasználó számára kezelhetetlen! A szakmabeliek viszont valami egyszerűbben kezelhetőt használnak, hiszen akad belőle éppen elég.

UNDELETE.COM — Törölt állományok visszaállítása. Beszámozza az állományokat, és utána egyenként erre a számra történő hivatkozással meg kell adni az állományok nevét. (Az első után már nem is látható, hogy melyik milyen számú.) Ha végrehajtottuk a visszaállítást, a rendszer lefagy. Nem profi munka, teljesen használhatatlan program! Sokkal jobb a Norton QU (Quick Udelete) vagy a PC Tools Undelete funkciója. E műfajban a legtöbbet eddig a PC Tools 6.0 Undelete segédprogramja nyújtotta, hiszen az a törölt állományok visszaállítását egy egyszerű DOS művelet kezelhetőségi szintjére egyszerűsítette.

UNBRAIN.EXE — A Brain vírust megöli. Ez a vírus Magyarországon 1990 augusztus végén bukkant fel.

UNITAL.EXE — A Magyarországon is elterjedt olasz pingpongozó boot vírust (Bouncing Ball) megöli. A Bootkill v1.02, v1.03 is tudja ezt.

WATSON.EXE — Ez a program a Sherlock programmal együtt használatos. Elindítása után az aktuális könyvtárban létrehozza a LIST.SLF nevű állományt, amely a megadott merevlemez könyvtáraiban található EXE, COM, SYS állományok listáját tartalmazza. Ezt az állományt ki kell másolni floppyra, s ez lesz a Sherlock program INPUT állománya, amely nélkül az el sem indul. Bonyolult egy megoldás!

SHERLOCK.EXE — A Sherlock program az A: meghajtóban lévő floppylemezen megkeresi a LIST.SLF nevű állományt, majd az itt található állományokra egy ellenőrző összeget hoz létre, és az eredményt a CHECK.SFP állományban floppyra tárolja. Kimenteti a boot-szektor ellenőrző adatait is.

HOLMES.EXE — A harmadik lépésben a Sherlock program által létrehozott és floppylemezre kimentett CHECK.SFP állomány tartalmát hasonlítja össze a megadott merevlemez tartalmával. Ha eltérés van az ellenőrző összegnél, akkor szirénázik, és a felhasználóra bízta, hogy mit csináljon... Ezt a magyar programok közül a Hemingway Kft. által forgalmazott VIRTEST.EXE egyetlen programmal, kevés cirkusszal is eredményesen megoldja. Hasonlóan egyszerű megoldású a Prgdoki utóda, a Sysdoki, ahol viszont ez egy nagyobb rendszer részfunkciója. Egyes állományokra McAfee Vali-date segédprogramja alkalmazható változásellenőrzésként.

TRYOUT.EXE — Demó program. Megfertőzi a floppylemez boot-szektorát... Kifejezetten tisztességtelen, reklám céljaira használja a vírus technológiát! Az elmentett floppy boot-szektorának helyére reklámszöveget operál.

QCV.EXE — Tárolja az EXE, COM, SYS fájlok aktuális méretét, ha vírusosak, akkor azzal együtt. A következő ellenőrzés során kiírja, hogy melyik fájlnak tér el a mérete. Ha egy állományról letakarítottuk a vírust, akkor annak méretváltozását is kijelzi. Jól használható, gyors információt ad a rendszerről.

ZAP.COM — Az adott állományt feltölti „Z” betűvel.

Összességében megállapítható, hogy e programcsomagnak nagyobb a

reklámja, mint a tudása. A nálunk általánosan elterjedt vírusok közül több is képes őt kijátszani. Más esetekben a hazai piacon kapható programok az adott feladatra egyenértékűek, de inkább jobbak. A teszt során az volt az érzésünk, hogy két programra való ötletből írtak egy egész lemezt kitöltő mamutrendszert, amelynek egyes tagjai nehezen kezelhetőek, mások pedig kifejezetten haszontalanok.

Reklám céljából pedig floppyra fizikailag is író vírusdemót készíteni — amely élesben használja az eljárást, s nemcsak szimulálja — súlyos etikai vétség. A lemezen található programdokumentáció kifejezetten gyenge, viszont a TROJAN.DOC állomány a korábbi verziókhoz hasonlóan forrásértékű az USA vírushelyzetére nézve.

Turbo Anti Virus Toolkit

Magyarországon a vírustalanítás érdekében néhány felhasználó — az egymásra sokszor acsarkodó csoportok láttán — a külföld felé fordul. Különösen egy-egy jelentős külföldi szakkiallítás után (mint az IFABO és a CeBIT) terjed itthon is sok kiválóan megszerkesztett demó szoftver. Így juthatott el egyre több felhasználóhoz az izraeli Carmel Software Engineering cég Turbo Anti Virus Toolkit (TAV vagy TNT) programjának demonstrációs változata, amely nem irt, csak detektál.

Az általunk tesztelt példány másolásvédett volt. Egyszerre csak egy installálást, összesen pedig nyolcvan install-uninstall lehetőséget engedélyezett. Szerencsére a teszthez sikerült megoldani, hogy ugyanazt a lemezt korlátlan számban installálhassuk. Erre szükség is volt, mivel a program a kipróbálás során többször is tönkrement.

Kissé szokatlan volt a másolásvédelem, s amikor az okáról érdeklődtünk, a következő derült ki. A forgalmazó más izraeli szoftvertermékeket is forgalmaz nálunk és a többi kelet-európai országban. A magyar forgalmazóktól hallott rémtörténetek hatására döntött úgy, hogy Magyarországon másolásvédelemmel ellátott példányokat forgalmaz. Hasonlóképpen teszi ezt Ausztriában is, abból a megfontolásból, hogy itt vásárolnak a magyar importáló cégek. A többi nyugati piacon a szoftvert mindenféle másolásvédelem nélkül forgalmazzák.

A programot floppyról vagy merevlemezről használhatjuk, de a védelem

következtében a szolgáltatást éppen akkor nem vehetjük igénybe, amikor a legnagyobb szükség lenne rá, mert például a vírus kiirtotta a merevlemez állományainak nagy részét. A védelem a HIDDEN SYSTEM READ ONLY alkönyvtárba, amelynek neve <ALT255> karaktereket is tartalmaz, letesz egy nulla bájtos és egy változó hosszúságú SYS állományt, hasonló attribútummal. Így egy lemezkatasztrófa esetén akkor sem működik a program, ha ez megsérül. A teszt során egyszer nálunk is tönkrement a Disk Managerrel formázott merevlemez partíció. Ha csak egyszer lehetett volna installálni, akkor a szoftver elveszett volna.

Most nézzük meg alaposan magát a programrendszert a magyar vírusvilág körülményei között!

1990-ben a bécsi IFABO-n a bemutatták a TNT 5.98-as változatát. Magyarországra a CeBIT '90 után kerültek be az első demó-példányok a TNTVir67-ből. A vírusölő program (számolási manőverekkel, amiről korábban már részletesen szóltunk) a kiírás szerint 95 vírust képes hatástalanítani. A demó és az eredeti program között az a különbség, hogy az egyes verziókat feltételes fordítási opcióval készítették el. A demó verzió csak a readme állományban leírt vírusok keresésére alkalmas, a vírusok kiölésére nem. Sajnos vakriasztást is ad, aminek komoly anyagi kihatásai is lehetnek. A felhasználóktól értesültünk arról, hogy már a TNTVir74 demó verzió is az országba érkezett. Az egyik felhasználó nem tudta 200.000 forintos termékét eladni, mivel a TNTVir74 a programjában az AIDS Information Disk vírusát jelezte. (Természetesen nem volt ott!!)

Mindez számunkra igen meglepő volt, de ugyanez a demó program a Basrun, Klavgen és más 1984-es programokban is AIDS vírust mutatott ki, holott az nem vírus, hanem trójai programrendszer, és nem is a programokba épül be. Sőt olyan szoftverekben is talált AIDS vírust, amelyek már a vírus keletkezése előtt a piacon voltak. E mögött vagy trehány programozás, vagy pedig a kereskedelem és a piac tudatos manipulálásának szándéka rejlik. Mindenesetre ezt követően magyar környezetben előforduló vírusokon teszteltük a TNTVírus v6.80 LAN teljes vírusölő programot. A teszteket MS-DOS 4.01 operációs rendszer alatt, IBM AT névtelen klón gépen, valamint MS-DOS 3.30 operációs rendszer alatt végeztük. Előzetesen annyit kell leszögezni, hogy mind a monokróm IBM klón gépen, mind pedig az EGA

monitoron a kép kezelésével nem volt probléma, automatikusan felismerte a monitor típusát. A szoftver nagyon lassan állt fel, amit bécsi kollégánk a védelem nélküli példányon nem tapasztalt.

A programcsomag az alábbi részekből áll:

TNTVIRUS.EXE — vírusölő program, másolásvédett.

TSAFE.EXE — rezidens vírusvédelmi program, nem másolásvédett.

BOOTSAFE.EXE — partíció táblát, boot-szektor ellenőrző program, nem védett.

A TNTVirus vírusölő programot az izraeli Codesafe másolás elleni védelemmel látták el. Hogy a másolásvédelem milyen trükköket rejt még magában, azt nem tudjuk. Egy biztos, hogy ügyes programozók 2 óra alatt megfejtették és hatástalanították a védelmet, s ez a védelem nélküli példány egész Európában elterjedt. A programot DOS 4.01 operációs rendszerrel, 40 Mbájt merevlemezkapacitással és a Magyarországon előforduló vírusokkal teszteltük. Indítás után a program leellenőrzi a védelmet, majd ezt követően dekódolja magát. Az emiatt igen lassú bejelentkezés után kiválaszthatjuk, hogy melyik lemezegységen akarjuk elvégezni a vírusellenőrzést. A vírusellenőrzési menüben a következő opciók közül választhatunk:

- Víruskeresés
- Vírusölés
- Vírusölés és immunizálás

A program víruskereső rutinja egy felhasználói Turbo Pascal programban tévesen jelezte az 1260 elnevezésű vírust (lásd a CWI 1990/27. számában megjelent Vaklárma című cikket). A Magyarországon előforduló Yankee Doodle vírusokat úgy írja ki, hogy közben a megtisztítandó állományt tönkreteszi! Valószínűleg nem ez a Yankee Doodle változat állt a fejlesztők rendelkezésére. A magyar eredetű átiratot fel sem ismerte. A töltőgető boot-vírust szintén nem tudja azonosítani, az 1701/Cascade vírus magyar átiratát pedig rosszul szedi le, és ezzel tönkreteszi magát a fertőzött programot is.

A felhasználók a vírustalanítás hibáit csak utólag veszik észre, amikor

működésképtelenné vált programjaikat használni szeretnék. Az ilyen véletlenül (vagy néha tudatosan) kárt okozó vírusirtó programokat a szakmában szintén trójai programoknak nevezik. Ebben az esetben is csak programozási hibáról van szó, nem pedig szándékos károkozásról.

Az egyes programoknak vírusokkal szembeni immunissá tételére az Immunize program szolgál. Az Immunize az egyes programokba az 5 bájt hosszú MsDos sztringet írja be. Ez a módszer a Jerusalemből (Péntek 13) vírus ellen nyújt védelmet, a többi vírus vidáman megfertőzi az egyes állományokat. Ennél a megelőző rendszabályok is jóval hatásosabbak! A programnak ez a menüje nagyon gyengének bizonyult.

A következő menüpont — amely a dokumentáció szerint 100 %-os program-helyreállítást biztosít — szintén gyengécske. Mit takar ez a művelet? Egyszerűen a DOS copy parancsának megfelelően kimásolja az állományokat floppylemezre. Ha ugyanezt a merevlemezre kérjük, akkor az IMAGES.TAV alkönyvtárba Hidden, System, Read Only attribútummal másolatot készít az állományokról. Ez annyit jelent, hogy 20 Mbájt programterület helyreállításához 40 Mbájt hely kell. Ha az egyes programok vírusosak lesznek, akkor a program innen visszamásolja a kópiát.

Nem érdemes részletezni, hogy ez milyen nevetséges megoldás. A felhasználót megtéveszti és nem is hatásos. A Carmel Software Engineering szerint ezzel a visszamásolós módszerrel még az ismeretlen vírusok által megtámadott állományok is helyreállíthatók. A megoldás azonban nem megnyugtató. Az első vírusgenerációk ugyanis még azt az állományt fertőzték meg, amelyiket éppen elindították, az újabb vírusok azonban keresnek maguknak más fertőzhető állományokat is, tekintet nélkül azok attribútumára. Így előfordulhat, hogy a vírus a már elmentett állományokra is rátelepszik, és akkor a program ezeket hozza vissza. Mindemellett a Backup menü DOS 4.xx alatt néhány esetben rosszul is közölte a könyvtárak tartalmát, pedig a 3.30-as DOS-sal jól működött. Megítélésünk szerint a programot a DOS 4.xx verziójával nem tesztelték le. Időnként a DOS 3.30 alatt is előbukkan egy rejtélyes hibaüzenet: Incorrect Window, valamint egy szám. Erre a dokumentációban nincs utalás. Utána a rendszer lefagy, és csak a Reset gomb segít.

Végül még annyit a TNTVirus programról, hogy a Victor v1.0 vírust kiszámíthatatlan esetekben rosszul távolítja el.

A TSafe általános célú rezidens vírusvédelmi program. Ugyanúgy, mint a TNTVirus programot, Turbo C-ben írták. Ez az oka annak, hogy 27 kb-ot foglal el a memóriából. Nagyon kevés olyan felhasználó van, aki megengedheti magának, hogy ilyen hosszú rezidens programot beültessen a memóriába! A program működése a rövid használat alatt korrektnek tűnt. A demó és a teljes verziójú programrendszer is ugyanazt a rezidens programot használja, tehát már a demóval is hozzájuthatunk. Nagyobb programrendszerek mellé még abban az esetben sem fér be, ha van EMS-ünk. A Ventura mindegyik verziójával összeférhetetlen. Hasonlóképpen nem szíveli a Lotus 1-2-3 újabb verzióit!

A Bootsafe boot-szektor és partíciós tábla elmentő és visszaállító program. Elindítása után a főkönyvtárba CBOOT.TAV néven elmenti a boot-szektor és a partíciós táblát. Ez a funkció megegyezik az általunk több mint fél éve forgalmazott CHKBoot, CHKPart nevű programok funkciójával. A Bootsafe program sem kezeli a 4.xx DOS-t. Érthetelen, hogy miért nem DOS 3.xx és 4.xx kompatibilis funkciót használnak. Ha a programot 4.xx DOS alatt elindítjuk, akkor a következő hibaüzenetet kapjuk vissza:

Disk Error

Cause: Disk Read Error

Press any key

Ha a TNTVirus programból sikerült valahogy kicsikarni, hogy mentse el a boot-szektor és a partíciós táblát, akkor a Bootsafe program már azt írja ki, hogy a boot-szektor és partíciós tábla rendben van. Ez persze nem igaz, mert a CBOOT.TAV 1024 bájt hosszú állomány második fele üres és nem tartalmazza a boot-szektor. Hasonlóképpen sikerült a teszt során kiirtani a Disk Managerrel formázott lemez nem DOS partícióit is. A program kijelenti, hogy változás történt a partíciós táblában, és azután „kiigazítja”. Az eredmény: újra kell formázni azt a partíciót! Ez egy ilyen szoftvertől megengedhetetlen!

A TNTVirus program vírus elleni önvédelmi rendszert nem tartalmaz. A programot a 4096 vírussal megfertőztük, majd ezt követően megpróbáltuk elindítani. Sajnos a vírusölő program fertőzött állapotban nem indul. Mivel

a TNTVírus programvédelemmel van ellátva, nem lehet tudni, hogy a védelem ebben az esetben hogyan működik. Úgy reagál rá, mintha valaki a programot piszkálta volna, vagy csak nem érzékeli a vírust? Mindenesetre helyreállítani már magát a programot sem lehet. Sajnos a másolásvédelemmel ellátott programoknál a vírusfertőzés okozta károk következményeit nem lehet kiszámítani.

A Turbo Anti Virus program ára körülbelül 27 ezer forint. 1990 nyarán 10 példány volt belőle Magyarországon. A demó verzió ingyenes, víruskereső funkciója jó. Vakriasztásai miatt csak mint másodlagos víruskereső programot célszerű használni. A teljes programot megvétele nem javasoljuk, mert nem ismeri fel a magyar vírusokat.

Szabadszoftverek

Az egyik ismert program **SV** névre hallgat. Indítása a program nevének és a vizsgálni kívánt meghajtó betűjelének begépelésével történik. A hazánkban elterjedt verzió **VIRUS-spot-light** néven jelentkezik be, verziószáma 1.44. Üzenetei német nyelvűek. Szerzője Ralf Messerer, 1988-ban írta. A program a Potyogós **COMMAND.COM** (Seuche2 azaz 2-es típusú fertőzés rendszerüzenettel), valamint a rendszer újraindítását okozó vírust (Seuche1) ismeri fel, mint első típusú fertőzést. Semmilyen egyéb vírust nem képes detektálni. Ugyanakkor ezeknél a vírusoknál is csődöt mond abban az esetben, ha egymás után több fertőzte meg a programot. Ma már korszerűtlen és a hatásos vírusfelderítésre alkalmatlan, ennek ellenére nagyon sokan használják Magyarországon.

A másik ilyen „őskövület” a **Serum2** program két változata, a version 2 és a version 4. Rendszerüzenetei vegyesen német és angol nyelvűek. A két egymás után megjelent verzió használata azonos. Ha opció nélkül indítjuk el, akkor megkapjuk a vegyes német-angol nyelvű segítséget. A C opcióval a teljes lemez ellenőrzését, az R opcióval a teljes lemez gyógyítását kérhetjük, míg a D opcióval egy adott állományban kérhetünk írtást. Az M opció használatakor a még érintetlen állományokból kivesz mintegy 60-70 bájtnyi információt a későbbi helyreállítás céljából.

A program írójáról csak annyit tudunk, amennyit a rendszerüzenet elmond magáról: Michael, a „PC Guru”, valamint Fritz és Heinz Veit. Az egyik verzió

a rendszer újraindítását okozó vírust tudja irtani, míg a másik már a potyogós COMMAND.COM-ot is felismeri, igaz, ezt „Time Stamp” néven detektálja. Az ellenőrzések során mindkettő létrehoz egy SERUM.MIF nevű naplóállományt is. Csak az aktuális meghajtó ellenőrzésére képesek. Detektálni és irtani egyaránt lehet velük. Van bennük egy érdekes programozási hiba is: ha 1701 bájtól kisebb állományt kell helyreállítani, akkor a program „Runtime error 100 at 0000:0322” rendszerüzenettel leáll, de a helyreállítást hibátlanul elvégzi. Kombinált fertőzések esetén is megállja a helyét, csak az utolsónak rákapcsolódott vírust ismeri fel és takarítja ki.

A két programgeneráció ismerete egy érdekes következtetésre kínál alkalmat: a programok íróinak hazájában fordított volt a vírusok megjelenésének sorrendje, mint Magyarországon. Először a rendszerhívást okozó vírus lépett fel, s csak utána a potyogós. Ezeknek a programoknak közös sajátosságuk volt, hogy meglehetősen bután állították helyre az állományokat, nem ismerték fel a vegyes fertőzéseket, de kárt nem okoztak. Hasonlóan primitív a **Wirusdisk** program. Ez csakis a potyogós fertőzések felismerésére alkalmas. Komoly hibája, hogy egyértelműen tisztának jelzi a programot, ha nincs benne potyogós vírus, pedig attól más vírus még lapulhat benne...

A Cédrus Rt. SolarSoft programkönyvtárában található egy érdekes szovjet vírusellenes program, a **Doctor**. Az egyik szovjet akadémiai intézetben gyorssegélyként készült 1988-ban, szerzője Geraszimov. Csak a reboot típusú vírusok irtására alkalmas. Annyiszor kell futtatni, míg az összes program tiszta nem lesz. Vegyes fertőzéseket nem ismer fel. Hibakezelése sem valami tökéletes, mert ha 0 bájtos programra vagy olyanra fut rá, amelynek az elején az ugrócím hibás, akkor „Runtime error 100 at 0000:002XX” rendszerüzenettel leáll. Kárt nem okoz.

Ez utóbbi megállapítás nem vonatkozik egy lengyel szerzőnek, Jerzy Sobczykknak, a Varsói Műszaki Egyetem tanárának programjaira. Két szoftvere forog közkézen Magyarországon. A **Diag** vírusdetektor csak a rendszerhívást okozó vírust képes felismerni. Ez a program a SolarSoft programkönyvtár révén vált ismertté. A program üzenetei angol nyelvűek. Sok esetben saját magát is fertőzöttnek jelzi, holott nem az. Ugyanis a program nem képes megkülönböztetni, hogy a vírusról vagy pedig annak kódrésztételéről van csak szó. Ez utóbbit ugyanis, mint a felismeréshez szolgáló etalont

önmagában is tárolnia kell. Így persze hogy megtalálja!. Időnként — teljesen rapszodikusán — keres egy **VIR_KILL.#2** nevű állományt. Nem irt, csak detektál. Több bajt okozhat ugyanennek a szerzőnek egy másik programja, a **Cure** víruseltávolító. Ez felismeri a rendszerhívást okozó vírust, ki is irtja, csak éppen rosszul, mert túl sokat vág ki a fertőzött programból. Ekkorát nehéz tévedni. Lehet, hogy egy nálunk ismeretlen rendszerhívó vírusváltozat ellen írták?

Egy érdekes és hibás program a **Vaccine v1.1**. Eredetileg a program arra készült, hogy az IBM DOS rejtett és rendszerállományait figyelje. Az MS-DOS állományaira — eltérő hosszuk és nevük miatt — nem alkalmas. A program eddig minden futtatási környezetben teljesen irracionálisan, „vad” névvel alkönyvtárakat hozott létre. A programról gyanítható, hogy valamilyen trójai program, s nem vírusdetektor. A **CHK4Bomb** detektálása szerint közvetlen szektorírást végez, utána pedig nem aktualizálja a tartalomjegyzéket.

Végezetül érdemes az imént említett, általánosan használható detektorral, a SolarSoft programkönyvtár **CHK4Bomb** programjával foglalkozni. Nem vírusok ellen írták, hanem arra, hogy a kódot végigelemezve felhívja a figyelmet az illegális lemezműveletekre. Megvizsgálja, hogy a program végez-e direkt, a DOS megkerülésével végzett abszolút szektorírást, vagy végez-e egyes szektorokra, illetve a lemezre kiterjedő formázást, esetleg használ-e BIOS-rutinokat. Ezekben az esetekben ugyanis nagy a valószínűsége, hogy a program a könyvtár aktualizálása nélkül kiirtja adatainkat. A maga kategóriájában az egyik legjobb program! Ugyancsak a SolarSoft kínálatában bukkant fel az **Antibody** program. Ez a program indításakor /S opcióval lemezre menti a rendszerállományok, néhány kiválasztott program, valamint az AT CMOS konfigurációjának adatait. Ha paraméter nélkül indítjuk, akkor az elmentett adatokkal összehasonlítva figyelmeztet a változásokra. Szintén jól használható segédprogram.

A felhasználók érthető módon a szokásosnál alaposabban olvassák a vírusokról szóló információkat. Természetesen mi is ezt szoktuk tenni, és a gyakorlati tanácsokat rögtön ki is próbáljuk.

A CWI 1990/27. (július 5-i) számában Horváth Miklós több vírust bemutatott, köztük az 1260 néven ismerettest is. A cikkben leírtak szerint a

McAfee-féle Scan59 vírusdetektor felismeri azt. Próbaképpen a vírusadatbankunkban lévő, külföldről kapott 1260-ast a Scan59 programmal teszteltük, de az sajnos nem ismerte fel a vírust. Ez a vírus egyike azon új vírustípusnak, amely a titkosítási kulcsot mindig variálja, és minden fertőzés során egy kicsit megváltoztatja magát, ezért felismerése elég nehéz. A „stealth”, azaz lopakodó programozástechnikát alkalmazza. Ha a vírustestből vesszük a felismerési mintát, akkor szinte biztos, hogy kudarcot vallunk. Csak akkor tudjuk biztosan és megbízhatóan detektálni jelenlétét, ha meglettük a kezdő dekódoló algoritmus elejét, aminek majdnem mindig állandónak kell lennie. A publikált vírusazonosító sztringek alapján nem mindig lehet a vírust felismerni. Igazán korrekt detektort és vírusölő programot csak az tud a vírus ellen írni, akinek a vírus a birtokában van, és azt teljesen vissza is fejtette.

A nagyon általános víruskereső programok egy bizonyos szintig (és bizonyos működési elvig) jól működnek, amíg nem jön egy új vírus és egy új elv. A CWI idézett számában bemutatták a **Catchvir** szoftvervírusokat felfedező programot (5.950 Ft/pld). Sajnos kópia hiányában nem tudtuk azt tesztelni, de a cikkben leírtak alapján a Műszertechnika egykor forgalmazott FCH programjához hasonlóan működik. Az állományok hosszát, dátumát, attribútumát és CRC-jét tárolja. Ez az elv egy évvel ezelőtt, amikor még csak egy-két vírus volt elterjedőben, talán sikeres szoftver lehetett volna. Az újabb vírusok azonban újabb elveket is hoztak magukkal.

Ilyen szempontból az egyik legügyesebb, ezért csak nehezen felfedezhető — a **Catchvir** programmal pedig egyáltalán nem detektálható — a „4K hosszú” vírus. A vírus más nevei: 4096, Frodo, Hidding, Century, 100 Years. A vírus nemzetközileg elfogadott neve 4096, de a 100 éves név is jellemző rá, mivel a vírus a megfertőzött állomány dátumát 100 évvel megnöveli. (A DOS DIR parancsa csak az évszám két utolsó számjegyét írja ki.) Ez a vírus az egyik legkellemetlenebb. A .COM és .EXE mellett OV* és adatállományokat is megfertőz. A vírus aktivizálódása után nem csökkenti a BIOS által visszaadott memória méretét. A szokásos memóriavizsgáló programokkal (SMAP, SNOOP stb.) nem mutatható ki a memóriában. Először a COMSPEC-ben magadott COMMAND.COM parancsprocesszort fertőzi meg. A vírus annyira ügyes, hogy amikor a DOS DIR parancsával megnézzük a

katalógus tartalmát, a DOS az eredeti programhosszúságot mutatja meg. Ha valamilyen fájleditorral meg akarjuk nézni a fertőzött állományt, akkor a vírus a programnak az eredeti, úgynevezett header részét mutatja meg. Ez az oka annak, hogy a szabványos CRC-ellenőrző és víruskereső programok nem találják meg a vírust, mivel az a program eredeti állapotának megfelelő adatokat adja vissza az ellenőrző programoknak. Így semmilyen változást nem tapasztalunk. Csak a fizikai olvasással, a bájtok olvasás közbeni számolásával védhető ki ez az ügyes szoftvermanipuláció. Éppen ezért ezt a vírust nagyon kevés program találja meg az egyes állományokban. Ahhoz viszont, hogy bármilyen műveletet lehessen végezni, előbb ezt a vírust a memóriából kell kitakarítani, és ez nem is olyan egyszerű dolog.

CHKVIR FAST! Virus Check Utility Version 1.60 10-12-1988
Free program !!! by Cs & Egér Co.

If you have problem, call Cs & Egér Co. !

Address: Technical University of Budapest
Department of Electronical Technology
1111 Budapest, Goldmann Gy. square 3.
Computer laboratory in building U2 216.
Phone: Budapest, 66-40-11 / 27-52

Usage: CHKVIR directory

VIRUS v1.0 !!! - Poty vírus azonosítása.

VIRUS v2.0 !!! - Reboot típusú vírus azonosítása.

A CHKVir víruskereső szoftver (v.1.60) bejelentkezője

VÍRUSHATÁROZÓ

A rendszerezés ötletét Jim Goodwin hasonló munkájából merítettük, aki 1989 áprilisában állt elő egy hasonló, a BBS-eken keresztül terjesztett ALLVIRUS.LST című, akkor teljesnek tartott listával. Így az úttörő szerep az övé, s mi csak annyit tehetünk, hogy saját szerény tudásunkkal „megpatkoljuk” ezeket az eredeti anyagokat.

Ez a határozókönyv a szakirodalmi ismertetések és a közkézen forgó vírusdetektorokból és killerekből szerzett információk alapján tartalmazza azoknak a számítógépvírusoknak az adatait, amelyek különféle változatokban világszerte felbukkannak, így Magyarországon is bármikor előfordulhatnak. Annál is inkább, mert vannak emberek, akik egyénileg vagy csoportosan terjesztik, illetve átírják azokat, ezért a nemzetközileg ismert, úgynevezett standard vírusokon kívül számos helyi szörnyszülött létezik. Magyarország is „büszkélkedhet” ilyennel, magunkénak vallhatjuk a Péntek 13 vírus átírását, a Május elseje vagy más néven Kedd elseje vírust. Eredeti magyar fejlesztés a Polimer vírus és a Töltögető is.

A vírusok keletkezésének és garázdálkodásának fő helyszíne az utóbbi időben megváltozott, mert az USA-ban a szigorú adatvédelmi törvények miatt már nem kis kockázattal jár a vírusírás. Inkább az NSZK, Olaszország, valamint a Közel-Kelet a víruskészítés melegágya. Újdonságként megjelentek a bolgár, a szovjet és a magyar eredetű programvírusok, amelyek innen kerülnek be a világ programáramlásába.

A szakirodalmat és a BBS rendszerek üzeneteit tanulmányozva sajnálattal kellett megállapítani, hogy az elnevezések még nem egységesek. Végül arra a következtetésre jutottunk, hogy az eligazodást azzal segítjük legjobban, ha a John McAfee-féle Virscan programrendszer 4.5V66-B verziója által használt elnevezéseket alkalmazzuk. Ezeket a neveket a program is felismeri, az egyébként még használatos többi elnevezést pedig — akárcsak a természettudományokban — szinonimákként kezeljük. A könyv végén a keresés megkönnyítésére egy keresztreferencia-táblázatot is adunk.

Ami pedig az egyes vírusok leírásait illeti, szintén a biológiából vettük módszerünket, azaz a tipikus vírusokat igyekeztünk leírni, amelyeket már töviről hegyire tanulmányoztak a víruskutató és adatvédelmi központokban, és többnyire hozzánk is eljutottak. Egységes szempontok alapján próbálunk rámutatni az azonosított vírusok kódjának a felismerés szempontjából fontos részleteire. A jelenlegi lista az 1990. augusztusi állapotot tükrözi.

Vírusrendszertan

Először ismerkedjünk meg a felhasznált úrlap 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. A rendezésnél az angol ábécé betűrendjét vettük figyelembe.

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 boot-szektorba 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 esetben — az önmagukat titkosító vírusoknál a hossz változó lehet, ezért ilyenkor ennek az adatnak minimális a jelentősége. Végül az is előfordul, hogy egyszerűen nincs ilyen mérhető adat.

Kódtípusa: Az alábbi rövidítések segítségével megjelöljük a vírus viselkedésének főbb szabályait, hogy milyen állományokat fertőz és hogyan épül be a programba:

- A = Minden .COM és .EXE programállományt fertőz.
- B = Boot-vírus.
- C = Csak .COM programállományt fertőz.
- D = A DOS boot-szektorát fertőzi a merevlemezen.
- E = Csak .EXE programállományt fertőz.
- F = Csak (360 kbájtos) floppyra fertőz.
- K = COMMAND.COM-ot fertőz.
- M = Fertőzi a master boot-szektor (partíciós táblát) a merevlemezen.
- N = Nincs memóriarezidens része.
- O = Felülír állományokat.
- P = Parazita vírus.
- R = Van memóriarezidens része.
- T = Manipulálja a FAT-táblát.
- X = Manipulálja/fertőzi a partíciós táblát.

Megjegyzés: Szokatlan a magyar szakirodalomban a parazita vírus megjelölés. Az általunk eddig alkalmazott „appendelő” — az állományokhoz hozzáépülő és azok hosszát megnövelő — kifejezés csak akkor találó, ha a vírus az állomány végéhez kapcsolódik. Az állomány elé másolva magát (mint például a Magyarországon Péntek 13 néven ismert Jerusalem-B vírus a .COM állomány fertőzése esetén) vagy az állomány belsejébe épülve nem pontos az eddigi kifejezés, ezért vettük át az angol szakirodalomban használt „parasitic” megfelelőjét.

Azonosítása: Ebben a pontban kíséreljük meg összefoglalni, miként lehetséges az egyes programvírusokat azonosítani. Mi csak az MS-DOS™, illetve az IBM-DOS™ világának programvírusaival fogunk foglalkozni. Segédprogramként amerikai szabadszoftvereket ajánlunk szakirodalmi adatok alapján, tekintet nélkül arra, hogy azokat ismerik-e Magyarországon vagy Európában. Ennek szabványosítási oka van, ugyanis a szakirodalom ezeket a programokat tekinti etalonnak.

Az általunk hivatkozott standard programok listája:

- F-Prot — Fridrik Skulason's F-Prot detector/disinfector.
- 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.

Eltávolítása: Ebben a pontban igyekszünk tanácsot adni arra, hogyan szabaduljunk meg a kellemetlen vendégtől. Sajnos a nemzetközi standard programok a legtöbb esetben törlést ajánlanak, mint egyetlen segítséget. Ez érthető is, hiszen egy vírust sokkal könnyebb felismerni, mint úgy eltávolítani, hogy a megtámadott programállományok sértetlenül megmaradjanak. Egyes kereskedelmi szoftverek szerencsére már ez utóbbira is képesek.

Referencialista:

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

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

CHKVIR — A (CS) & Egér (Leitold Ferenc és Tábor Csaba, Budapesti Műszaki Egyetem) programsorozata. Korábbi változatai detektálták a Cascade és a reboot-vírusokat. Újabb — és már kereskedelmi szoftverként forgalmazott — változatai a dokumentáció szerint a vírusváltozatokkal együtt mintegy 50 vírust irtanak.

CHKSEQ — A (CS) & Egér (Leitold Ferenc és Tábor Csaba, Budapesti Műszaki Egyetem) szekvenciális víruskereső programja. Szabadszoftver. A szerzők igyekeztek a szakirodalomban fellelhető minden keresési szekvenciát, illetve vírusazonosítót beleépíteni. Előzetes detektálásra igen jó, viszont ha jelez, az nem mindig vírus. Sok vakriasztás fordulhat elő olyankor, amikor a keresés a szakirodalomban található és onnan kiemelt rövid szekvenciára támaszkodik, mint például a (c) Brain vírus esetében.

CLEANXX — 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 nem korrektül irtja, az állomány sok esetben tönkremehet. Csak végszükségben alkalmazzuk.

DOS COPY — A DOS operációs rendszer COPY parancsát nyugodtan használhatjuk arra, hogy a boot-vírussal fertőzött lemezeiről állományainkat lementsük. Ez a megoldás akkor hatásos, ha a boot-vírus rezidensen nem aktív. **NE HASZNÁLJUK AZONBAN A DISKCOPY, ILLETVE AZ XCOPY PARANCSONKAT ERRE A CÉLRA, MERT A FERTŐZÖTT BOOT-SZEKTORT IS ÁTVISSZÜK AZ ÚJ FLOPPYLEMEZRE!!**

DOS SYS — Ezt a DOS parancsot használjuk arra, hogy felülírjuk a fertőzött boot-szektor tartalmát a lemezen. Ebben az esetben egy írásvédővel leragasztott, a winchesteren lévő rendszerrel azonos rendszert tartalmazó floppylemezeiről kell a rendszert újraindítani, majd kiadni a megfelelő lemezre vonatkozó SYS parancsot és utána rendszert indítani.

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

EDDIKILL — A Dark Avenger vírushatást gyógyító program. Szegedi Imre és Farnosi István fejlesztői példánya. Széles körben elterjedt.

F-PROT — Fridrik Skulason's F-Prot detektor és gyógyító program.

KILLVAC — Vacsina-B vírust gyógyító program. Szegedi Imre és Farnosi István fejlesztői példánya.

M-1704 — Cascade/Cascade-B gyógyító program.

M-1704C — Cascade-C vírushatást gyógyító program.

M-3066 — Traceback vírushatást gyógyító program.

M-DAV — Dark Avenger vírushatást gyógyító program, valamint a fertőzés megelőzését is szolgálja azzal, hogy a lemez boot-szektorába felteszi a Dark Avenger azonosítóját.

M-JRUSLM — Jerusalem-B vírushatást gyógyító program.

M-VIENNA — Vienna, Vienna-B vírushatást gyógyító program. (A reboot-vírusok ellen hatásos.)

MDISK — MD boot-vírushatást gyógyító program. Természetesen a felhasználó DOS verziójának megfelelő típusú boot-szektorra kell akkor helyreállítani.

PRGDOKI — Szegedi Imre és Farnosi István programja a Magyarországon honos vírusok ellen. 2.11E verzióig szabadszoftver, onnan kezdve keres-

kedelmi termék. (A szabad verziónak több trójai jellegű illetéktelen átirása 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 Vaccina-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.

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

SYSDOKI — Szegedi Imre és Farmosi István újgenerációs vírusölő és megelőző programja. A korábbi verzióknak és ideiglenes killereknek megfelelő képességekkel rendelkezik, kibővítvé az izraeli és az amerikai vírusellenes együttműködés keretében kapott standard vírusok detektálásának és irtásának képességével. Komplex vírusvédelmi rendszer. Amennyiben előzetesen immunizálták vele a programokat, minden hagyományos módon támadó vírus ellen hatásos.

UNVIRUS — Yuval Rakavy (Izrael) vírushatározást 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 immúnanyagot beoltó vírusvédő szabadszoftvere.

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

VIR05 — A Yankee Doodle vírushatározást gyógyító 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. Itt még sok részletkérdés tisztázásra vár.

1

A vírus neve: AIDS.

Egyéb elnevezése: Hahaha, Taunt, VGA2CGA.

Hossza: Nincs rá adat.

Kódtípusa: ONC. Felülír, nem rezidens, a .COM állományokat fertőzi.

Azonosítása: Scan V40+, CHKSeq v.1.0.

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, a COM állományokat megfertőzni. Amikor a vírus 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 megrongált adatállomány, mivel a végrehajtható programok első 13 kb-átját felülírja, de nem menti el sehova. A vírus ebben a 13 kb-átban tárolja az AIDS felirat nagybetűit. Csak egy fertőzésmentes eredeti állomány visszatöltésére támaszkodhatunk.

Megjegyzés: Ez a vírus nem azonos az AIDS Information Disk/PC Cyborg trójai programjával. Az nem vírus, hanem programrendszer!

2

A vírus neve: Alabama.

Egyéb elnevezése: Eddig nincs.

Hossza: 1560 bájt.

Kódtípusa: PRET. Parazita, rezidens része van, .EXE állományokat fertőz, manipulálja a FAT-ot.

Azonosítása: Scan V43+, F-Prot, CHKSeq v.1.0, Sysdoki.

Eltávolítása: CleanUp, F-Prot, CHKVir v.4.01, Sysdoki vagy pedig a fertőzött állományok törlése.

Leírása: Az Alabama vírust először Jeruzsálemben, a Hebrew University (Izrael), 1989 októberében fedezte fel Yasrael Radai. A vírus első aktivizálódása 1989. október 13-án volt. Az Alabama vírus az .EXE állományokat fertőzi meg, fertőzési hossza 1560 bájt. A programvírus a fertőzést a rezidens részen keresztül hajtja végre. Amikor a programkód lefut, a memóriában elhelyezkedik a vírusnak egy 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 megszakításon keresztül közvetlen IN and OUT utasításokat használ. Amikor a vírus CTRL-ALT-DEL billentyűkombinációt észlel, egy látszólagos bootot hajt végre, hátrahagyva magát a RAM-ban. A vírus a memória végére építi be magát úgy, hogy a DOS és BIOS által meghatározott memória méretét nem csökkenti. Ezt a módszert több vírus is alkalmazza rezidenssé válása esetén. Ebben az esetben a vírus a memóriaellenőrző blokkon (MCB = memory controll block) keresztül lesz rezidens. Amikor a vírus már egy órája rezidens módon a tárban tartózkodik, egy villogó keretben megjeleníti a következő üzenetet a gép monitorán:

SOFTWARE COPIES PROHIBITED BY INTERNATIONAL LAW.....

Box 1055 Tuscumbia ALABAMA USA.

(A NEMZETKÖZI JOG ÁLTAL TILTOTT SZOFTVER
MÁSOLATOK..... Postafiók 1055 Tuscumbia 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: fogja és felcseréli egy nem fertőzött másik állomány

nevével. A szerencsétlen felhasználó pedig elgondolkodhat azon, hogy miért egy másik program fut le, mint amit ő elindított. Végül az egész rendszer szétzilálódik, tönkremegy. A fertőzés lassan, alattomosan történik. Az állományok felülírásában nagyon pedáns, „rendes teendőjeként” elvégzi azt minden pénteken. (A Jerusalemi vírus írójának ez a vírus adta az alapötletet az aktivizálódás feltételének kiválasztásához.)

Magyarországon az eredeti változat 1990 augusztusában tűnt fel.

3

A vírus neve: Alameda.

Egyéb elnevezése: Merritt, Peking, Seoul, Yale.

Hossza: Nincs rá adat.

Kódtípusa: BRF. Boot-vírus, rezidens része van, csak a floppy boot-szektorát fertőzi.

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

Eltávolítása: MDisk, CleanUp, F-Prot, CHKVir v.4.01, Sysdoki vagy a DOS SYS parancs 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 áttírt 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 kb-átos floppyra — de csakis arra — oly módon, hogy a memóriában maradó rész megfertőzi a boot-szektorát a rendszerlemezen és a többi floppyra. Programozástechnikailag érdekes feladat volt úgy megírni, hogy melegindításkor aktív módon a tárban maradjon és a DOS is üzemképesen betölthetessen. Az utóbbi időben Magyarországon is felbukkant a Vaccina-B vírus, amely hasonló elven működik.

A vírus elmenti a valódi boot-szektorát a track 39, sector 8, head 0 pozícióra. Az Alameda vírus eredeti verziója csak a 8086/8088-os processzorokkal ellátott gépeken futott, mert a kódhossz csökkentése érdekében direkt pro-

cesszorkódot alkalmazott a zseniális, terrorista hajlamú szerző. Az újonnan felbukkanó változatok már felismerik a 80286-os processzort is.

4

A vírus neve: Amstrad.

Egyéb elnevezése: Eddig még nem adtak neki.

Hossza: 847 bájt (valójában 850, mert a vírus végén 3 bájt 0 van).

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

Azonosítása: Scan V51+, F-Prot, CHKSeq v.1.0.

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

Leírása: Az Amstrad vírus megjelenését 1989 novemberében fedezte fel Jean Luz Portugáliában, azonban valószínűleg már korábban is jelen volt Spanyolországban és Portugáliában. Maga a vírus általános .COM fertőző, és bár nem memóriarezidens, nem fertőzi meg a COMMAND.COM-ot sem, mert akkor korán észrevehetnék tevékenységét.

A vírus az Amstrad számítógép-hamisítványokat jelzi. Nem okoz más kárt a rendszerben, mint azt, hogy megfertőzi az állományokat és kimutatja jelenlétét.

5

A vírus neve: Ashar.

Egyéb elnevezése: Shoe_Virus, UIUC Virus.

Hossza: Nincs rá adat.

Kódtípusa: BR. Rezidens része van, a boot-szektorra fertőzi.

Azonosítása: Scan V41+, F-Prot. CHKSeq v.1.0, Sysdoki.

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

Leírása: Az Ashar vírus a boot-szektorra fertőzi meg. A Brain vírus variációja vagy átirása. 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 meglehetősen hibás és szleng angolságú szöveg mondanivalóját kifejező fordítás. A cipő elnevezés nyilvánvaló gúnyos utalás a boot-vírus jellegre, miután a boot eredeti angol jelentése csizma — A szerk.)

Mindamellet a fenti rendszerüzenet sohasem jelenik meg a monitoron. A vírusazonosító sztring „ashar”, amelyet rendes 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-étől.

6

A vírus neve: Brain.

Egyéb elnevezése: Pakistani, Pakistani Brain.

Hossza: Nincs rá adat.

Kódtípusa: BR. Rezidens része van, a boot-szektorra fertőzi.

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

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

Leírása: A boot-vírusok egyik „mintadarabja”, nagyon sokat cikkeztek róla a lapok. A Brain vírus Pakisztánból, Lahore városából származik. A boot-rekordot fertőzi, felülírja saját kódjával, az eredetinek a 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 boot-szektorába helyezi el. Működése során a vírus először tárrezidens részét bocsátja ki magából, amely a RAM-ban 3–7 kb-ig terjedő részt foglal le magának. A Brain vírus igen ügyesen elrejtje 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 bootot elrakta. Így a gyanútlan felhasználó az eredeti bootot látja, a vírus pedig mintha ott sem lenne... Ez a megtévesztés az újabb lemezeditorokat már nem fenyegeti. Az átírások során a vírus egyes változataiból a felderítés megnehezítésére a vírusazonosítót hordozó „(c) Brain” szöveget távolították el.

Az eredeti Brain vírus csakis floppyt fertőz. Ez birizgálta néhány vírusíró szakmai hiúságát, és az eredeti vírust „továbbfejlesztették”. Többek között úgy, hogy a merevlemez is képes legyen megfertőzni. A 4.0 feletti MS-DOS™ és IBM-DOS™ operációs rendszerek esetében kissé más a lemezcímke-állomány szerkezete. A vírus viselkedését ebben a helyzetben még nem vizsgálták, tekintettel arra, hogy ezek a DOS-verziók alig terjednek a professzionális felhasználók között... Magyarországon is inkább fejlesztők dolgoznak a DOS 4.x verzióval.

A Brain vírus eddig ismert és felbukkant változatai:

- Brain-B/Hard Disk Brain/Houston Virus — ez a verzió már a merevlemez is megfertőzi.
- Brain-C — mint a Brain-B, de a „(c) Brain” lemezcímkét gondos kezek eltávolították.
- Clone Virus — Brain-C, amelybe visszaírták az eredeti copyright lemezcímkét.
- Clone-B — a Clone Virus alaposan átírt változata. Komoly károkat okozhat majd 1992. május 5-én, ugyanis akkor elpusztítja a FAT-ot!! Addig lapul és terjed.

Magyarországon eredeti (c) Brain fertőzés, valamint az Ashar verzió egyik átírata 1990 júliusában és augusztusában bukkant fel.

7

A vírus neve: Cascade.

Egyéb elnevezése: Fall, Falling Letters, 1701, 1704, Herbst, Poty #1, Poty #2, Potyogós COMMAND.COM, Austrian #2.

Hossza: 1701 vagy 1704 bájtt.

Kódtípusa: PRC. 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.

Eltávolítása: M-1704, CleanUp, F-Prot DXU2, Prgdoki, Serum, Serum2, Serum3, CHKVir v.4.01, Sysdoki.

Leírása: Magyarországon az első komoly vírusjárványt okozó program-vírus. Terjesztője egy hasznos segédprogram volt, amelybe trójai funkcióként ültették be. Az eredeti programnak az volt a célja, hogy a rendszerindításkor bekapcsolva maradó NUM LOCK gombot alaphelyzetbe visszaállítsa. Ez a vírus lehullatta a karaktereket a képernyő aljára. 1987 végén valaki a trójai programból megírta a csak .COM állományokat fertőző, memóriarezidens .COM vírust.

Az eredeti vírus hossza 1701 bájtos, és a fertőzés célpontjai az IBM PC-k klónjai voltak. Létezik egy olyan, 3 bájjal hosszabb változata, amely megvizsgálja, hogy a BIOS-ban van-e eredeti IBM copyright jelzés. Ha van, akkor fertőzés és egyéb bonyodalom nélkül kilép, a kód el sem indul. A vírus maga a vírusprogramok klasszikusa, sok programozástechnikai fogás itt jelentkezett először a vírustenyésztés „művészetében”. Ahhoz, hogy valaki egyáltalán elkezdjen a vírusok kitakarításával foglalkozni, mindenképpen itt kell kezdenie az ismerkedést. Sajnos a teljes, kellően dokumentált forráskódot a vírusíró nem publikálta. E könyv szerzőinek birtokában csak egy visszafejtett kód van. 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 indítja meg. Ebben szerepel többek között a gép és a monitor típusának vizsgálata. Az aktivizálódás attól is függ, hogy van-e belső óra a gépben.

A vírus aktiválja magát minden gépen, amelyikben CGA, EGA vagy VGA monitorkártya van. Néhány változata IBM PC/AT klónokon nem aktivizálódik, csak terjed. Potyogtató funkciója 1980—1988 közötti időszakban, azon belül is csak szeptember, október, november és december hónapokban működött. Ezen kívül — tehát napjainkban is — csak terjed. Mivel klasszikusnak számít, igen sok (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 néhány ellenőrzési pont — idő (timer), képernyőkezelő (videó) megszakítások — kezelését az operációs rendszertől. Mindebből még nem veszünk észre semmit, hiszen mindez nagyon gyorsan történik. A memóriában elbújva azután megkezdí tevékenységét. Először csak egy, később egyre több betű lepotyog a képernyőn, elrontva az ott lévő szövegeket, feliratokat, lehetetlenné téve így a munkát. A vírus egyes változatai a karakterek potyogtatása közben hangfektusokat is adnak. Egyetlen vírusos program is elegendő a teljes elszaporodáshoz! A külső (floppy), belső (merevlemez) adathordozókon és a helyi hálózatokon lévő állományokra egyaránt veszélyes! A kezdeti időben ártalmatlannak tartva sajnos sokan tudatosan terjesztették.

A Cascade vírusnak az utóbbi időben 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.

(Lásd még az 1704 Format vírus adatait is!)

8

A vírus neve: Cascade-B.

Egyéb elnevezése: Blackjack, 1704-B, Poty #2, 1704/Cascade, Black Jack 17+4=21.

Hossza: 1704 bájt.

Kódtípusa: PRC. Parazita, rezidens része van és saját magát is kiadósan 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 potyogtatós képernyőt valaki a rendszer újraindítását

eredményező rutinnal helyettesítette. Egyes változatai potyogtatnak is. Ami lényeges: a vírus aktivizálódása után egy véletlenszerű időpontban a rendszer rebootot csinál.

A következő változatát sikerült elkülöníteni: 1704-C — Azonos az 1704-B vírussal, azzal az eltéréssel, hogy minden esztendőben, december hónapban potyogtat. A megszokott detektorok kimutatják, de a mentésítés más eljárással történik.

9

A vírus neve: Chaos.

Egyéb elnevezése: Eddig még nincs.

Hossza: Nincs rá adat.

Kódtípusa: BR. Rezidens, a boot-szektor fertőzi.

Azonosítása: Scan V53+, CHKSeq v.1.0.

Eltávolítása: MDisk, CleanUp vagy a DOS SYS utasítás kiadása.

Leírása: Első észlelője James Berry volt Kentben (Anglia), 1989 decemberében. Ezután terjedt el. A Chaos mind a floppyn, mind pedig a merevlemezzen fertőzi a boot-szektor. Mint a boot-vírusoknak, ennek is van memóriarezidens része. Amikor a vírus megfertőzi a boot-szektor, felülírja az ott levő eredeti információt. Annak tartalmát a lemez másik helyére menti el, hogy a víruskód lefutása után betölthesse. A fertőzött boot-szektor vége üzenetet tartalmaz, ami szövegkereső programok segítségével megtalálható, amennyiben azok a boot szektorban is keresnek. (Például PC-Tools, Norton Utilities) Az üzenet:

Welcome to the New Dungeon

(Üdvözöllek az új vártoronyban)

Chaos

(Káosz)

Letz be cool guys

(Srácok, őrizzétek meg a hidegvéreteket)

A Chaos vírus már akkor rossznak jelzi a szektort, amikor az még olvasható. Aktivizálódásának feltételei ismeretlenek.

10

A vírus neve: Christmas.

Egyéb elnevezése: XA1.

Hossza: 1539 bájt.

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

Leírása: Április elsején a vírus tönkreteszi a FAT-ot. December 24. és január 1. között a vírus karácsonyfát rajzol a képernyőre, de akkor nem rombol.

11

A vírus neve: Dark Avenger.

Egyéb elnevezése: Black Avenger, Eddie.

Hossza: 1800 bájt.

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

Azonosítása: Scan V36+, F-Prot, CHKSeq v.1.0.

Eltávolítása: M-DAV, CleanUp, F-Prot, Prgdoki, Sysdoki.

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

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. 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 bájjal növekszik meg.

Dark Avenger fertőzés esetén egy írásvédett (leragasztott) vírusmentes floppy rendszerlemezzel 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 belemásolja saját darabjait és szöveges részét. Később a főkönyvtárt tartalmazó rész kivételével a merevlemezeken 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 részben sem azonos a Jerusalemi vírussal, bár hosszuk közel ugyanannyi.

A Dark Avenger vírus a következő szöveges üzenetet tartalmazza:

The Dark Avenger, copyright 1988, 1989

(A Sötét Bosszúálló, copyright 1988, 1989)

This program was written in the city of Sofia
(Ezt a programot Szófia városában írták)

Eddie lives..... Somewhere in Time!

(Eddie él.... Valahol az időben!)

A vírus aktivizálódása során először a COMMAND.COM-ot támadja meg. A DOS-tól gyakorlatilag a teljes vezérlést elveszi (timer, keyboard, videó, disk read/write, absolute disk read/write, TSR). Terjedésének gyorsasága miatt csak a vírusmegelőző programok bizonyulnak vele szemben hatásosnak. Ha az Eddie — Dark Avenger — vírus minden állományt megfertőzött, akkor szektoronként, azaz 512 bájtónként beépül az állományok közepébe, ezzel gyakorlatilag tönkretéve azokat. A vírus jelenléte gyakran okoz rendszerleállást, megmagyarázhatatlan géplefagyást. A tapasztalatok azt mutatják, hogy az eddig találtak közül ez az egyik legügyesebb és leggyorsabb vírus.

12

A vírus neve: Datacrime.

Egyéb elnevezése: 1280, Columbus Day.

Hossza: 1280 bájt.

Kódtípusa: PNC. Parazita, rezidens része nincsen. Titkosítja, azaz elkódolja magát. A .COM állományokat fertőzi meg.

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

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

Leírása: A vírust eredetileg Európában „fogták el”, nem sokkal azután, hogy 1989-es márciusi változata megjelent. A vírusprogram hozzáfűzi magát a .COM állományokhoz, azok hosszát 1280 bájttal megnövelve. Az első 3 bájtot az eredeti programban átírja, mert ide helyezi el azt az ugróutasítást, amely a program elindításakor a hordozóprogram végére, a víruskód elejére ugratja az operációs rendszert, hogy a víruskód lefuthasson. Ezt a 3 bájt-ot természetesen tárolja magában, mert arra szüksége van, hogy a gazdaprogram is zavartalanul lefuthasson. A vírusgyártásnak ez a klasszikus programozási fogása a legismertebb, már a Cascade típusú vírusoknál megjelent, azzal a különbséggel, hogy ott az eredeti ugrócím kódolva van.

A vírus terjedése során végigmegy az alkönyvtárakon .COM állományokat keresve. A COMMAND.COM-ot nem fertőzi meg a lebukás veszélyének

elkerülésére. Ugyancsak nem fertőzi meg azokat a .COM állományokat, amelyekben az állománynév hetedik betűje D. Előbb a merevlemez partíciót vizsgálja végig, és csak utána a floppymeghajtót. A vírus minden esztendőben október 12-ig terjed. Amikor elérkezik ez a dátum, akkor a monitoron a következő üzenetet jeleníti meg:

DATA CRIME VIRUS

RELEASED: 1 MARCH 1989

Ilyenkor alacsony szintű szektor- vagy cluster-formázást végez a merevlemezben. Nagyon valószínű, hogy a felhalmozódó hibás területek következtében a rendszer hamarosan összeomlik. Ennek a vírusnak másik megfigyelt változata abban tér el az alapverziótól, hogy nem terjed és nem fertőz állományokat április elseje után. Érdekes vírusprogramozási hibát derített ki az ismert számítógép-virológus, a Hollandiában dolgozó Jan Terpstra: ha a PC kontroller RLL vagy SCI típusú, vagy speciális AT-BIOS van a gépben, a vírus néhány esetben nem tudja az alacsony szintű formázást elvégezni.

13

A vírus neve: Datacrime II.

Egyéb elnevezése: 1514, Columbus Day.

Hossza: 1514 bájt.

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

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

Eltávolítása: AntiCrim, Scan /D, F-Prot.

Leírása: A Datacrime II az eredeti Datacrime vírus változata. Eltér az állományok mögé bemásolt hosszúságban. Az eredetivel ellentétben nemcsak a .COM, hanem az .EXE állományokba is belemászik. Titkosítási mechanizmusa azonos az eredeti verzióéval. Sajátossága, hogy hétfői napon nem formázza sem a merevlemez, sem a floppyt. Más napokon viszont igen...

14

A vírus neve: Datacrime IIB.

Egyéb elnevezése: 1917, Columbus Day.

Hossza: 1917 bájt.

Kódtípusa: PNAK. Nincs rezidens része. Átkódolva titkosítja magát, .COM és .EXE állományokat egyaránt megfertőz, beleértve a COM-MAND.COM-ot is.

Azonosítása: Scan V51+, F-Prot, CHKSeq v.1.0.

Eltávolítása: AntiCrim, Scan /D, F-Prot.

Leírása: A Datacrime IIB a Datacrime II vírus újabb változata, amelyet 1989 novemberében fedezett fel Hollandiában Jan Terpstra. Ez a vírus ugyanolyan, mint az eredeti Datacrime II, de titkosítási mechanizmusa eltérő, így mind a mentesítés, mind a felderítés mechanizmusa különböző.

15

A vírus neve: Datacrime-A vírus.

Egyéb elnevezése: 1168, Columbus Day.

Hossza: 1168 bájt.

Kódtípusa: PNE. Parazita, rezidens része van. Általános .COM-fertőző.

Azonosítása: Scan V51+, F-Prot, CHKSeq v.1.0.

Eltávolítása: AntiCrim, Scan /D, F-Prot.

Leírása: Az eredeti Datacrime vírus változata. Az eltérés a vírus hosszában van. A vírus a memória-ellenőrző blokkon keresztül válik rezidenssé. A vírus október 12-én a következő üzenetet jeleníti meg:

1 MARCH 1989, DATACRIME VIRUS

és közben újraformázza a merevlemez első sávját. Ez elegendő a teljes adatállomány elvesztéséhez.

16

A vírus neve: Datacrime-B.

Egyéb elnevezése: 1168, Columbus Day.

Hossza: 1168 bájt.

Kódtípusa: PNE. 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.

17

A vírus neve: DBASE.

Egyéb elnevezése: Még nincs.

Hossza: 1864 bájt.

Kódtípusa: PRC. Parazita, rezidens része van, .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 Ross Greenberg fedezte fel 1988-ban. A vírus fertőzi a .COM és az átfedő (overlay) állományokat. Érdekessége, hogy ezeken az általános sajátosságokon kívül kifejezetten vadászik a dBase .DBF állományaira. Innen kapta nevét is. Ha nyitott .DBF állományra lel, akkor abban véletlenszerűen áthelyezgeti, összekavárja a bájtokat, mérhetetlen kárt és káoszt okozva ezzel az adatokban. Lekönyveli, hogy milyen adatokat alakított át, és ezt az állományt, amely BUG.DAT névre hallgat, elhelyezi egy ugyanolyan nevű alkönyvtárban, mint az általa átirított .DBF állomány. A vírus ezeket a bájtokat visszatölti, amikor olvasásra megnyitják az állományokat. Így a kívülállónak úgy tűnik, mintha minden rendben lenne. Amikor pedig a BUG.DAT állomány létrehozása után eltelik 90 nap, a vírus tönkreteszi — felülírja — a FAT-táblát és a gyökérkönyvtár bejegyzéseit. A vírusokkal foglalkozó szakembernek az az érzése, hogy írója

ezt a programot eredetileg másolásvédelemnek találta ki. Miként azonban a seprű Goethe bűvészinásának kezében, itt a program kelt önálló és ellenőrizhetetlen életre. Valószínűleg azokat akarta megbüntetni, akik az USA-ban szokásos 90 napos áruvisszaküldési határidő után sem fizettek, de tovább használják a programot. Bizonyára az úgynevezett regisztrációs lemezen volt a leszedő program, amit a pénz beérkezése után kapott az ügyfél.

Amikor felismertük és azonosítottuk a vírust, a dBase programot törölni kell és tiszta kópiával pótolni. Azokat a .DBF állományokat mindenképpen elvesztjük, amelyeket a fertőzés ideje alatt hoztunk létre. A BUG.DAT alapján eddigi ismereteink szerint nem lehet helyreállítani a sérült állományokat.

18

A vírus neve: Den Zuk.

Egyéb elnevezése: Search, Venezuelan.

Hossza: Nincs rá adat.

Kódtípusa: BRF. Van rezidens része, csak a floppy boot-szektorát fertőzi meg.

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

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

Leírása: Kizárólag 360 kbájtos, 5 1/4" formátumú floppylemezekeken megfertőzi a boot-szektorát. Ha utána ilyen lemezről töltjük az operációs rendszert, akkor rezidens módon felmegy a tárbá. Ha ebben az esetben a rendszert a CTL-ALT-DEL gombokkal újraindítjuk, a vírus CGA, EGA, illetve VGA monitorokon karakteres 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 floppylemezt újraformázza. Azon a floppy-n, 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 klubban. A gépbetörők folyton betörnek.)

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 az Ohio vírus, amely hármuk közül a legerősebb, és akár a Den Zukkal, akár a Brinnel találkozik, mindegyiket törli és önmagát teszi fel a helyére.) A Den Zuk megírásában közreműködtek azok, akik az Ohio vírust készítették, amire a fentiekén kívül az is utal, hogy az „Y.C.1.E.R.P.” karaktersorozat mindkettőben előfordul.

19

A vírus neve: Devil's Dance.

Egyéb elnevezése: Mexican.

Hossza: 941 bájtt.

Kódtípusa: PRCT. 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 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 betölteni, lévén több mint 64 kbájttal hosszú. Amikor pedig egy fertőzött programot futtatunk és melegindítást csinálunk, akkor a tárban visszamaradó program-szegmens 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 gonoszkodó figurája a terroristák kedvencévé vált. (Lásd a Joker vírus leírását is.)

Ez a vírus romboló hatású. Aktivizálódásának feltétele a billentyűleütések meghatározott száma. Az első 2000 leütés után a vírus elkezd a színek csereberéjét a monitoron megjelenített szövegeknél. Ez a fertőzés első, kívülről is észrevehető jele. A következő, 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.

20

A vírus neve: Disk Killer.

Egyéb elnevezése: Computer Ogre, Disk Ogre, Ogre, Bootkiller.

Hossza: 3072 bájt.

Kódtípusa: BR. Rezidens része van, a boot-szektor támadja meg.

Azonosítása: Scan V39+, F-Prot, CHKSeq v.1.0, Bootkill, Sysdoki.

Eltávolítása: MDisk, CleanUp, CHKVir v.4.01, F-Prot, Bootkill, Sysdoki vagy DOS SYS.

Leírása: A Disk Killer vírus a boot-szektor megfertőzve saját elrejtőzéséhez kijelöl magának három nem használt blokkot a floppylemezen vagy a merevlemezen. Ezt a helyet a floppy a FAT-táblájában hibás blokkként jelöli meg, így azt nem tudják felülírni. Ráadásul a boot-szektor a saját ízlése szerint írja át. Amikor rendszert indítunk, betöltődik — mégpedig elsőként éppen ő — a memóriába. Lehetősége van arra, hogy megfertőzzön új lemezeket.

A merevlemezen elhelyezkedő vírus belső számlálója regisztrálja, hogy hány floppyt tudott megfertőzni, mert aktivizálódásának feltétele egy előre beállított érték elérése. Ha ez bekövetkezik, akkor elindul a destruktív folyamat, megjelenik a vírusra jellemző üzenet. Amíg üzenet, közben egy karakterrel véletlenszerűen keresztül-kasul felülírja az állományokat. Ilyenkor már csak a lemez újraformázása az egyetlen megoldás. A korábban floppyra elmentett állományainkból pedig rekonstruálhatjuk az eredeti állapotot... bár Murphy törvényei gyakran közbeszólnak.

Mivel a Disk Killer vírus fertőzése során lecseréli a megtámadott lemez boot-szektorát és rendszerindításkor az eredeti boot-szektor programja helyett először a víruskód töltődik be a memóriába, csak ezt követően érkezik el rendszerünk a DOS alapprogramjaihoz. Minden lemez boot-rekordja a lemezre jellemző információkat is tartalmazza, s ha olyan parancsokat használunk, amelyek végrehajtásához a boot-szektorban levő információkra van szükség — például CHKDSK, FORMAT —, akkor a vírus azonnal lecseréli önmagára a boot-szektor 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 boot-szektor lecserélve ezen a rejtett sávon bújik meg mindaddig, amíg nem aktivizálja 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.

(Lemezgyilkos — 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.)

A Disk Killer aktivizálódása után teljesen tönkreteszi a merevlemez tartalmát. Nullával feltölti a boot-szektorot, és ezzel elvesz a partíciós tábla információja is. ASCII karaktereket ír az állományelhelyezkedési táblába (FAT), és hexa E5 karakterrel felülírja a katalógusterület (directory) tartalmát. A vírus a merevlemezen nem jelöl be hibás szektorokat és nem épül be semmilyen állományba.

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 merevlemez gépeken és munkaállomásokon fertőz. A Novell hálózatban sem a server winchesterét, sem a többi munkaállomást nem fertőzi meg.

A vírus jelenlétéről sok hibás floppylemez-művelet és téves lemezfelismerés árulkodik. A vírust Magyarországon először egy Disk Manager v3.3 gyári programlemezen találtuk meg, és az valószínűleg az NSZK-ból került hozzánk.

21

A vírus neve: Do-Nothing.

Egyéb elnevezése: The Stupid Virus, 640K.

Hossza: 583 vagy 608 bájt.

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

Azonosítása: Scan V49+, F-Prot, CHKSeq v.1.0.

Eltávolítása: Scan /D vagy pedig F-Prot.

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 csak az aktuális könyvtár első bejegyzését. A többit békén hagyja. A vírus a memóriában a 9800:100h címre építi

be magát, és az egész 640 kb-át 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 kapta, mert a számítógépet megfosztja cselekvőképességétől. Nagyon nehezen vehető észre, mert más kárt nem okoz, és a felhasználó sokáig géphibára gyanakszik.

22

A vírus neve: Friday The 13th.

Egyéb elnevezése: COM Virus, Miami, Munich, South African, 512.Virus.

Hossza: 512 bájtt.

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

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

Eltávolítása: Scan /D, F-Prot, CHKVIR v4.01, Prgdoki3+, Sysdoki.

Leírása: Az eredeti Péntek 13 vírust először a Dél-Afrikai Unióban lelték meg, 1987-ben. Készítője terrorista 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 kivételt tesz a COMMAND.COM-mal, hogy nehezebben fedezhessék fel.

Amikor végrehajtotta programját, azaz megfertőzte az állományokat, ránéz a C: meghajtóra, hogy talál-e ott két COMMAND.COM-ot, illetve egyet az A: meghajtón. Ha megleli, akkor természetesen megfertőzi, legyen teljes 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 vírusnak ez a verziója kizárólag .COM állományokat fertőz meg. A fertőzés után az állománynak 64 kb-ajtnál kisebbnek kell lennie.

Elérkezvén péntek 13-a, ha ekkor a gazdaprogramot végrehajtatjuk a géppel, akkor az törli önmagát, mi pedig egy nem létező 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 PATH útvonalban.

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)

23

A vírus neve: Fu Manchu.

Egyéb elnevezése: 2080, 2086.

Hossza: 2086 bájt (.COM fájlhoz) vagy 2080 bájt (.EXE fájlhoz).

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

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

Eltávolítása: Scan /D, F-Prot.

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 véletlenszerűen eltelt idő után hatvan esetből egyszer a következő üzenettel hökkenti meg a gép használót:

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 melegstart (warm reboot) után a vírus mindezt ráadásul túléli a memóriában. 1989. augusztus 1. után a vírus a billentyűzet-pufferen keresztül egyes politikusok nevével fölszerszámozott megjegyzéseket áraszt a monitorra. Az üzeneteket a vírus kódolva tartalmazza! Néhány változata előszeretettel épül be átfedő (overlay), .SYS, valamint .BIN állományokba. Az USA-ban az irodalmi adatok szerint igen ritka, viszont Európában és a Közel-Keleten elég gyakori.

24

A vírus neve: Ghost Boot.

Egyéb elnevezése: Ghostballs.

Hossza: Nincs rá adat.

Kódtípusa: BR. Rezidens része nincs, a boot-szektor fertőzi meg.

Azonosítása: Scan V46+, F-Prot, CHKSeq v.1.0.

Eltávolítása: MDisk, CleanUp, F-Prot vagy a DOS SYS utasítás kiadása.

Leírása: Az egész kísérteties Ghost vírusházaspárt, azaz a boot és a .COM fertőző változatot Fridrik Skulason fedezte fel Grönlandon az Icelandic Universityn. A Ghost boot-vírus egyaránt rámegegy a floppy és a merevlemez boot-szektorára, 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 Boot-vírust, 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 megszüljön a boot-verziót. Így ha nem távolítottuk el a rendszerből, a .COM változat mindig újra és újra fertőzi boot-szektorunkat!

A vírus neve: Ghost COM.

Egyéb elnevezése: Ghostballs.

Hossza: 2351 bájt.

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

Azonosítása: Scan V46+, F-Prot, CHKSeq v.1.0.

Eltávolítása: MDisk vagy a DOS SYS parancs kiadása és az összes fertőzött .COM állomány törlése. A CleanUp és az F-Prot is kitakarítja.

Leírása: A Ghost kísértetcsalád női tagja. Hogy miért nőnemű egy vírus? Egyszerűen azért, mert szül. (Bővebben lásd a vírus boot változatánál, az előző leírásban.) A Ghost COM általános .COM állomány-fertőző. A folyamat során a megfertőzött állomány hossza 2351 bájjal megnő. A fertőzés tünetei hasonlóak a Ping Pong víruséhoz, véletlenszerűen károsítja a rendszert, vagy pedig egyszerűen csak fertőz. A Ghost COM vírus volt az első olyan ismert vírus, amely kétféle funkcióban is tud működni, fertőzve a .COM állományokat is, a lemez (floppy és merevlemez) boot-szektorait is. Miután a boot fertőzése megtörtént, már hagyományos vírusként viselkedik.

A vírus eltávolítása során figyelemmel kell arra lenni, hogy bár nincsen tárban maradó része, de aktív fertőző és boot-vírus. A mentésítés következő lépése, hogy az írásvédett DOS rendszerlemezről — amelynek természetesen garantáltan vírusmentesnek kell lennie — újraindítjuk a rendszert, majd vagy valamilyik segédprogrammal visszamentjük a korábban elmentett boot-szektor, vagy rendszerlemez esetében a SYS paranccsal visszateszük az eredeti rendszert. Jelenlegi ismereteink szerint az összes fertőzött .COM állományt törölni kell.

A vírus neve: Golden Gate.

Egyéb elnevezése: Mazatlan, 500 Virus.

Hossza: Nincs rá adat.

Kódtípusa: BR. Rezidens része van, a boot-szektorrt 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. A számlálót nullázza, amikor új floppyt vagy merevlemezt fertőzött meg, de ez a nullázás csak az új példány számlálójára terjed ki, a sajátja tovább fut. Amikor aktivizálódik, leformázza 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 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!

27

A vírus neve: Halloecken.

Egyéb elnevezése: Nem ismeretes.

Hossza: Nincs rá adat.

Kódtípusa: PA. Parazita, a .COM és az .EXE állományokat fertőzi meg.

Azonosítása: Scan V57+, CHKSeq v.1.0.

Eltávolítása: Scan /D vagy a fertőzött állományok törlése.

Leírása: A Halloecken vírust Christoff Fischer Nyugat-Németországban, az Universität Karlsruhe számítógépes rendszerében fedezte fel. Annak ellenére, hogy az NSZK-ban állítólag széles körben elterjedt, mindössze annyit tudunk róla, hogy .COM és .EXE állományokat fertőz. Hosszadatait még nem publikálták. Amikor fertőzött programállományt futtatunk, a billentyűről beadott karaktereket alaposan összezaggyválja, és nem tudunk értelmes szavakat beírni. Megjegyzendő, hogy ugyanezt produkálja néhány „magyar ékezetesre átalakított” PC is, ha eredeti angol programot futtatunk, és néhány német billentyűzet is. Ez nem vírus, hanem hozzánemértés vagy tudatos manipuláció következménye, inkompatibilis lett a kódkiállítás...

28

A vírus neve: Holland Girl.

Egyéb elnevezése: Sylvia, Netherlands Girl.

Hossza: 1332/1301 bájt.

Kódtípusa: PRC. Van rezidens része. Parazita, a .COM állományokat fertőzi.

Azonosítása: Scan V50+, F-Prot, CHKSeq v.1.0.

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

Leírása: Első felbukkanását Jan Terpstra jelentette Hollandiából. A vírus memóriarezidens, csakis a .COM állományokat fertőzi meg, kivéve a COM-MAND.COM-ot. A fertőzött állományok 1332/1301 bájjal 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.

29

A vírus neve: Icelandic.

Egyéb elnevezése: 656, One In Ten, Disk Crunching Virus.

Hossza: 656 bájt.

Kódtípusa: PRE. Van rezidens része, parazita, az .EXE állományokat fertőzi.

Azonosítása: Scan, 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 Virus”, azaz Lemezropogtató Vírus 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. Ennek hossza a 16 többszörösével változhat. (Ezt a DOS paragrafushatárai alakítják így.) A vírus jelzi magának, hogy beült egy állományba, ne jöjjön oda másik. Az erre szolgáló sorozat az állomány végén található bájt-csoport, mely hexadecimálisan: 4418,5F19.

Az Icelandic vírus a fertőzött program első futásakor átmásolja magát a szabad memória végére. Elrejtí magát a memóriát feltérképező programok elől. Amikor pedig a program utoljára ide akar írni, a rendszer összeomlik. Ha a vírust keressük, nem szabad arról megfélemedkezni, hogy az Int 13 hívó vektorát (hooked) jó pár olyan program is használhatja — teljesen legálisan —, amely nem fertőzött. Ha pedig a memóriateszt során az Int 13 nem jelentkezik hooked vektorként, azaz éppen nem használják, akkor a fertőzés minden tizedik programfuttatáskor bekövetkezik.

Ha a rendszerben csak egyetlen floppy van, vagy pedig egy 10 Mbájtnál kisebb 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.

30

A vírus neve: Icelandic-II.

Egyéb elnevezése: System Virus, One In Ten.

Hossza: 632 bájtt.

Kódtípusa: PRE. Parazita, rezidens része van, az .EXE állományokat fertőzi meg.

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

Eltávolítása: Scan /D, F-Prot.

Leírása: Az Icelandic-II átírt változata az eredeti Icelandic vírusnak. Először 1989 júliusában fogták el, ugyanott, mint 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 már bárki észreveheti, hogy valami történt az ő féltett szoftverével. Hasonlóképpen programozási hiba, hogy amikor a fertőzés céljából leveszi a 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. Van még egy feltételezés: ez egy korábbi program-

változat, csak később indították el, vagy később észlelték, mint ahogy a sorszám nélküli elsőt.

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.

31

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 fogták 1989 decemberében, mint társait. Írója valami sajátos logikával így ünnepelte a karácsonyt. Az Icelandic-III azonosító mezője (sztringje) az utolsó két „word” azaz 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. Szerkezetét kutatva 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. Az fertőzés során az egyes állományok hossza 853—868 bájt közötti hosszúsággal nő a paragrafushatárok miatt. Ha a programot véletlenül december 24-én futtatják, akkor a következő üzenetet írja ki a képernyőre:

Gledileg jól

(Boldog karácsonyt)

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: PRA. 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 fedezték 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 a megszakítások átirányításával eléri, hogy fél órával a vírusprogram lefutása után a rendszer sebessége tizedére csökken! 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 tizenharmadika 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 pedig csak a Péntek 13.

A következő 5 évben az alábbi hónapok 13. napja esik péntekre:

1991. szeptember, december.

1992. március, november.

1993. augusztus.

1994. május.

1995. január, október.

A vírusazonosító karaktersorozat: sUMsDos — amelynek még jó pár változata létezik az egész világon. (Sok jellemzőjét az ismétlések elkerülésére lásd különböző változatainál: Jerusalem B, New Jerusalem, Payday, Suriv 3.00.) Annyira jól sikerült az alapváltozat, hogy különböző verzióit boldogboldogtalan gyártja. Sokan éppen csak annyira változtatták meg, hogy a megszokott vírusdetektorok és killerek ne ismerjék fel. A Magyarországon Kedd 1-jére átírt változatának vírusazonosító mezője (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 csodálatos réteges fertőzés alakul ki, amelyet csak különleges technikákkal lehet gyorsan eltávolítani.

- Jerusalem-C — A Jerusalem B-vel azonos, de nem lassítja le a processzor működését. Magyarországon a Jerusalem B és C változata egyre szélesebb rendet vág a PC-k adatállományaiiban.

- 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 elseje. Majdnem annyira elterjedt, mint az eredeti Jerusalem-B. Nyugat-Európában és az USA-ban is felbukkant.

A Péntek 13 vírus eredeti dátuma 1987 utáni péntek 13-ára volt beállítva. A Kedd 1. vírusban a vírusazonosító kódot és a 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 5 évben az alábbi hónapok első napja esik keddre:

1991. január, október.

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 dátuma 1992.

33

A vírus neve: Jerusalem-B Destructive.

Egyéb elnevezése: Péntek 13, Jerusalem Mutant.

Hossza: 1813 bájt (.COM fájlban) és 1808—1823 bájt között (.EXE fájlban).

Kódtípusa: PRA. 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, JnVirus, Prgdoki, Sysdoki.

Leírása: Ez a vírus is a Jerusalem „víruscsalád” átfert változata. A vírus a negadott hosszánál +/- 256 bájttal rövidebben, illetve hosszabban épül be a programokba. Ha a vírus rövidebben épül be az állományokba, akkor felülírja az adott program utolsó 256 bájtját, ezzel lehetetlenné téve a program helyreállítását. A vírust Magyarországon először banki számítógépes rendszerben találták meg.

34

A vírus neve: JoJo.

Egyéb elnevezése: Nincs.

Hossza: 1701 bájt.

Kódtípusa: PRC. Parazita, rezidens része van és saját magát is kiadósan titkosítja, azaz átkódolja. A .COM állományokat fertőzi meg (a COMMAND.COM-ot is).

Leírása: A vírus minden 63800 bájt nál rövidebb .COM állományt (a COMMAND.COM-ot is beleértve) megfertőz. A vírus a memória-ellenőrző blokkon (MCB) keresztül, nem szabványos módon válik rezidenssé. A fertőzött lemezegységek első sávját a vírus véletlenszerűen felülírja. A JoJo vírus először Izraelben bukkant fel, valószínűleg terrorista szándékkal készült.

35

A vírus neve: Joker.

Egyéb elnevezése: Nem ismeretes.

Hossza: Nincs rá adat.

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

Azonosítása: Scan V57+, CHKSeq v.1.0.

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

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. Kedves terrorista hajlamú szerzőnk ugyanezt teszi a személyi számítógépek használóiival is. Csak először nevetünk rajta, amikor sírnánk, akkor már késő...

A Joker vírus válogatott marhaságokat tartalmazó üzeneteket küldözget. Ezeket szöveg formájában elhelyezi a fertőzött állományokban a vírus programkódjának elején, ha tehát ott ilyesmit olvashatunk, akkor „Joker barátunk” tette tiszteletét gépünkben. Ezek közül néhány csak rá jellemző, ezért a szövegkereső programokba is beépíthető.

Néhány jellegzetes üzenete:

Incorrect DOS version

(Nem megfelelő DOS verzió)

Invalid Volume ID Format failure

(Érvénytelen lemezcímke-azonosító. 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! Tegye el egy hamburgert az A: meghajtóba)

NO SMOKING, PLEASE!

Thanks.

(Kérem, ne dohányozzon! Köszönöm!)

Don't beat me!!

(Ne püfölgjön !!)

Don't drink and drive

(Ne igyon, ha vezet)

Another cup of cofee?

(Kér még egy csésze kávé?)

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.

36

A vírus neve: Kukac.

Egyéb elnevezése: @.

Hossza: 448 bájt.

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

Azonosítása: Sysdoki.

Eltávolítása: Sysdoki.

Leírása: Ez a vírus valószínűleg a Turbo kukac néven ismert vírus korábbi verziója, bár átírás is feltételezhető. Eredeti magyar fejlesztés. Célja a bosszantás. A .COM állományokat fertőzi meg. A vírusban a következő szöveg található:

Üdv minden nagytudásúnak ! Turbo @

37

A vírus neve: Lehigh.

Egyéb elnevezése: Nem ismeretes.

Hossza: Nincs rá adat.

Kódtípusa: ORKT. Felülírja az állományt, rezidens része van, a COMMAND.COM-ot fertőzi meg és manipulálja a FAT-táblát.

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

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 és 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 boot-szektorot. Eképpen az adatok elvesznek.

A Lehigh vírusnak létezik egy átírása, a Lehigh-2. Ez abban tér el az alapváltozattól, hogy a fertőzéseket számoló rutinja a RAM-ban működik, nem ír vissza a lemezre. Ha a számlálásban eléri tízet, akkor károsítja a boot-szektorot és a FAT adatait. Az adatok itt is elvesznek.

38

A vírus neve: Lisbon.

Egyéb elnevezése: DOS 62.

Hossza: 648 bájt.

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

Azonosítása: Scan V49+, F-Prot, CHKSeq v.1.0.

Eltávolítása: Scan /D, F-Prot.

Leírása: A Lisbon vírus a Vienna vírustörzs új hajtása. Ezt a változatot 1989 decemberében különítette el Jean Luz, Lisszabonban (Portugália) dolgozó adatbiztonsági szakember.

Maga a vírus igen egyszerű, a Vienna vírus kódjával való hasonlósága nagy, bár egy trükk azért van benne. Minden kódszóban az eredeti víruséhoz képest 1-2 bájjal el van tolva („shiftelve”) a kód, így az a hagyományos vírusdetektorok számára rejtve marad. Ezért nehéz a régebbi detektorokkal észlelni. A vírus minden 8. fertőzésnél pusztít. A megtámadott program 1-es szektorának első öt bájtját felülírja a következő szöveggel: @AIDS. Ezzel természetesen a program helyreállíthatatlanul tönkremegy!

39

A vírus neve: Machosoft.

Egyéb elnevezése: 3551.

Hossza: 3551 bájt (+ 0–15 bájt a paragrafushatár miatt).

Kódtípusa: PNC. 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 végignézi az aktuális könyvtárat a program futása alatt. Ha talál benne .COM állományokat, kinéz azokból egyet, és beleépítve saját kódját, megfertőzi azt. A kiválasztás a véletlen műve. A fertőzött állomány 3551 bájjal nő meg, ami szembetűnő változás. A fertőzés a VIRUS=OFF utasítással megállítható, amíg a COM-MAND.COM meg van fertőzve. A fenti utasítás 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 megszakítást használja, 20 szektort beolvasva a fertőzendő állományból. A fertőzés során a vírus a fájlokban található „MICROSOFT” copyrightot „MACHOSOFT”-ra cseréli le. Ezt a vírust gyakran összekeverik a hasonló hosszúságú Syslock vírussal. A vírus a DOS 4.xx verzió alatt inkorrekt módon működik!

40

A vírus neve: MIX/1.

Egyéb elnevezése: MIX1, Mixer 1.

Hossza: 1618 bájt.

Kódtípusa: PRE. 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: A terrorcélzattal készült vírusok sorában érdekes színfolt ez a kártevő. 1989. augusztus 21-én egyszerre bukkant fel számos szabad hozzáférésű izraeli elektronikus adatbankban, azaz BBS-ben. A vírus hozzáépül az állományokhoz. Ha egy fertőzött programot futtatunk, a memóriában a vírus 2048 bájtot foglal le a RAM-ből. A megtámadott állomány hossza minden fertőzés alkalmával 1615-1635 bájt közötti hosszal nő meg, az eredeti állomány paragrafushatárainak függvényében. A vírus nem támadja meg a 8 kb-ajtnál kisebb állományokat. A vírus egyszerű eszközökkel úgy azonosít-

ható, hogy a megfertőzött állományok utolsó négy bájtyát nézzük meg. Ha az állományba a vírus beépült, 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 pedig állandóan bekapcsolva marad, nem lehet kikapcsolni. A hatodik fertőzés után a bootoló rendszer 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 kbájtnál hosszabb állományokat fertőzik meg.

41

A vírus neve: New Jerusalem.

Egyéb elnevezése: Nincs.

Hossza: 1813 bájt (.COM-fertőzéskor) és 1808 bájt (.EXE-fájl esetén).

Kódtípusa: PRA. 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.

Eltávolítása: Saturday, CleanUp, CHKVir v.4.01, F-Prot, Prgdoki, Sysdoki.

Leírása: A New Jerusalem az eredeti Jerusalem vírus egyik változata. Az ismeretlen terroristák igen nagy tudással, éppen csak annyira változtatták meg az eredeti Jerusalem 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 pénteken, 13-án fejtik ki, ekkor törli az elindított programokat, függetlenül attól, hogy fertőzöttek voltak vagy nem. Más napokon csak terjed.

A vírus memóriarezidens, részben úgy viselkedik, mint az eredeti Jerusalem, de nemcsak azokat az állományokat képes megfertőzni. (Lásd még a rokonainál, a Jerusalem, Jerusalem B, Payday, Suriv 3.00 vírusoknál elmondottakat is!)

A vírus neve: Ohio.

Egyéb elnevezése: Nincs.

Hossza: Nem ismeretes.

Kódtípusa: BF. Rezidens része is van, csak a floppy boot-szektorát fertőzi meg.

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

Eltávolítása: MDisk, F-Prot, vagy pedig a DOS SYS parancs kiadása.

Leírása: Az Ohio vírus memóriarezidens résszel rendelkező, boot-szektorra fertőző vírus. Csak a 360 kb-ajos floppylemezekre tud felmászni. Az Ohio vírus 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. Felmerült az adatok elemzése során az is, hogy esetleg egy félresikerült, a (c) Brain vírus ellen vírustechnológiával védekező megoldással állunk szemben, vagy egy ilyen, eddig még nem ismert program átiratával.

Az Ohio vírusban a következő 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....

43

A vírus neve: Oropax.

Egyéb elnevezése: Music Virus, Musician.

Hossza: 2756–2806 bájt.

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

Azonosítása: Scan V53+, F-Prot, CHKSeq v.1.0.

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

Leírása: Az Oropax vírusról szakirodalmi információkkal rendelkezünk. Magyarországi jelenléte csak a tisztázatlan eredetű üzemzavarokból valószínűsíthető. A vírus véletlenszerűen aktivizálódik. Öt perccel az állomány megfertőzése után három eltérő hangot játszik le, hétperces időközönként ismételve azt. A magyarországi változat valószínűleg azonos az európai verzióval. Ez hat különböző hangot bocsát ki, szintén hétperces időközönként. (Megjegyzendő, hogy a Prgdoki különböző magyar kiadásában ezt a vírust azonosították — tévesen — az 5 PM Tee/Yankee Doodle vírussal.) Az Oropax 2756 és 2806 bájt közötti változó értékkel növeli a fertőzött állomány hosszát, úgy, hogy a megnövelt állományhosszúság osztható legyen 51-gyel.

44

A vírus neve: Payday.

Egyéb elnevezése: Nem ismeretes.

Hossza: 1808 bájt az .EXE és 1813 bájt a .COM megfertőzésekor.

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

Azonosítása: Scan V51+, F-Prot.

Eltávolítása: M-JRUSLM, UnVirus, Saturday, CleanUp, F-Prot.

Leírása: A Payday vírust az ismert holland vírusvadász, Jan Terpstra fogta meg 1989 decemberében. A vírus a Jerusalem-B átirata. 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. (Lásd még a rokon Jerusalem, Jerusalem B, New Jerusalem, Suriv 3.00 vírusokat.)

A vírus neve: Pentagon.

Egyéb elnevezése: Nem ismeretes.

Hossza: Nem ismeretes.

Kódtípusa: BRF. Rezidens része van, csak a floppy boot-szektorát fertőzi meg.

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

Eltávolítása: MDisk, CleanUp vagy pedig a DOS SYS parancs kiadása.

Leírása: A Pentagon vírus beleírja a normál MS-DOS 3.20 boot-szektorába az ott előforduló IBM helyett a következő karaktersorozatot: HAL. Ezen kívül még 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 beletnyomni a boot-szektorba, valamint az eredeti boot-szektor 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 kb-átos floppykat támadja meg. Megnézi azt is, hogy van-e rajta (c) Brain vírus. Ha rátalál, akkor eltávolítja és önmagával helyettesíti. Memóriarezidens része 5 kb-átnyi helyet foglal el a RAM-ban, és túléli a CTRL-ALT-DEL-t vagy a melegstartot is.

A vírus neve: Perfume.

Egyéb elnevezése: 765, 4711.

Hossza: 765 bájtt.

Kódtípusa: PNCK. Parazita, nincs rezidens része, .COM-fertőző. A COMMAND.COM-ot is megfertőzi.

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 hossza a vírus beépülése után 765 bájtal lesz hosszabb. A vírus érdekessége, hogy válaszol a felhasználó kérdésére. Ha vírusfertőzött program fut és a felhasználó begépel a 4711 karaktersorozatot, megtudhatja, hogy az egy német parfüm neve. A vírus innen kapta elnevezését. Ennek a vírusnak számos változata van. Többek között olyan, amelyik a kérdésre válaszolva felülírja azt különböző karakterekkel.

47

A vírus neve: Ping Pong.

Egyéb elnevezése: Bouncing Ball, Bouncing Dot, Italian, Vera Cruz.

Hossza: 1024 bájt.

Kódtípusa: BRF. Rezidens része is van, csak a floppylemez boot-szektorát fertőzi meg.

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

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 boot-szektorát fertőzi. Első felbukkanását 1988-ban jelezték. Az eredeti változat csakis floppyt támad meg.

A vírus aktivizálódása véletlenszerűen történik. Ekkor megjelenik egy erősebb pont, egy kis „pingponglabda” a monitor ernyőjén, s ott bolyong a jelek között. Ezt a jelenséget csak úgy tudjuk megszüntetni, hogy a gépet kikapcsoljuk. Ennek a verziónak más károsító hatását eddig nem tapasztaltuk, viszont sokan ezt az alapvírust kártékonyabb változatúvá dolgozták át.

48

A vírus neve: Ping Pong-B.

Egyéb elnevezése: Falling Letters, Boot, Pingpongozó vírus.

Hossza: 1024 bájt.

Kódtípusa: BR. Rezidens része van, a boot-szektorát fertőzi meg.

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

Eltávolítása: CleanUp, MDisk, CHKVir v.4.01, F-Prot, Bootkill 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 boot-vírus csak IBM PC/XT számítógépek merevlemezét fertőzi meg, ami arra enged következtetni, hogy a vírusok korábbi generációjához tartozik. A vírus fertőzése során 1024 bájt hibás szektort jegyez be a FAT-táblába floppy és merevlemez esetén is. A vírus nem írja felül a lemezegységen található információkat, hanem az első szabad területre épül be.

A vírus 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.

Ez a vírus valószínűsíthetően Olaszországból származik, Magyarországra pedig Csehszlovákián keresztül érkezett. A kiirtására alkalmas egyik legelső program szintén északi szomszédunkban készült.

A vírus neve: Polimer.

Egyéb elnevezése: Nem ismeretes.

Hossza: 512 bájt.

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

Azonosítása: Sysdoki.

Eltávolítása: Sysdoki. Törölni kell a fertőzött állományokat.

Leírása: 1990 nyarán jelent meg a Polimer kazettát 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 a következő szöveg jelenik meg egy pillanatra a képernyőn:

A le' jobb kazetta a POLIMER kazetta! Vegye ezt!

(Nem sajtóhiba! A „g” betű helyett aposztrófot gépelt be a vírusíró.)

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 Kiszövetkezethez!

50

A vírus neve: Pretoria.

Egyéb elnevezése: South Afrika, June 16.

Hossza: 879 bájt.

Kódtípusa: PNC. Parazita és nincs rezidens része. A .COM állományokat fertőzi meg. A COMMAND.COM-ot nem, az IBMDOS.COM és IB-MIO.COM állományokat viszont megfertőzi.

Leírása: Ha a vírus a DOS rendszerállományait megfertőzi, akkor a lemezzről nem lehet az operációs rendszert betölteni. A DOS rendszerállományok helyreállítása a DOS SYS parancsával lehetséges. Június 16-án a vírus a főkönyvtárban lévő összes állományt ZAPPED névre nevezi át.

51

A vírus neve: Saratoga.

Egyéb elnevezése: 642, One In Two.

Hossza: 642 bájt.

Kódtípusa: PRE. 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. 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.

52

A vírus neve: Saturday 14.

Egyéb elnevezése: Durban.

Hossza: 681 bájt (+ 0–15 bájt paragrafushatár-kiegészítés).

Kódtípusa: PRA. Parazita, rezidens része van, a .COM és az .EXE állományokba épül be.

Leírása: A vírus a rezidenssé válásához nem használja a DOS INT 21H, 27H megszakításait. A vírus az .EXE és a .COM állományokat fertőzi a COMMAND.COM kivételével. Nevének megfelelően akkor aktivizálódik, amikor a hónap 14. napja szombatra esik. Ekkor a lemezegység első 100 szektorát felülírja, ami a lemez teljes tartalmának elvesztését jelenti a boot-szektor, a FAT-tábla és a directory-terület információinak elpusztulása miatt. Nem helyreállítható.

53

A vírus neve: SF Vírus.

Egyéb elnevezése: Nincs.

Hossza: Nem ismeretes.

Kódtípusa: BRF. Rezidens része is van, csak a floppy boot-szektorát fertőzi meg.

Azonosítása: Scan (Alameda vírusként ismeri fel.)

Eltávolítása: MDisk, CleanUp, F-Prot vagy a DOS SYS parancs kiadása.

Leírása: Az SF Virus az Alameda vírusnak alaposan átírt verziója. A legfontosabb változtatás ott történt, hogy kicserélték az aktivizálódást irányító számláló beállítását, ezáltal 100 reprodukció után formázza a floppylemez. A fertőzés a CTRL-ALT-DEL melegstart hatására történik, és csak az 5 1/4"-os, 360 kbájtos floppykat fertőzi és formázza.

54

A vírus neve: Stoned.

Egyéb elnevezése: Hawaii, Marijuana, New Zealand, San Diego, Smithsonian.

Hossza: 512 bájt.

Kódtípusa: BMR. Boot-vírus, rezidens része van, floppyn a boot-szektorra fertőzi meg, merevlemezen pedig a partíciós táblát (a master boot-szektorra).

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

Eltávolítása: CleanUp, MDisk, CHKVir v.4.01, F-Prod, Bootkill, Sysdo-ki.

Leírása: A Stoned vírust először Új-Zélandon, Wellington városában észlelték, 1988 elején. Az eredeti vírusok csakis a 360 kbájtos, 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 két ilyen változatról tud a nemzetközi szakirodalom.

A vírus akkor válik memóriarezidenssé, amikor egy fertőzött floppyról indítanak rendszert. Ha rendszerlemez készítünk, ráteszi magát, de ha a memóriában van, akkor bármilyen hozzáférési műveletre, például egy tartalomjegyzék behívásakor is megteszi ezt. Nyolc rendszerindítás közül egy esetben a vírus a következő rendszerüzenettel lepi meg a gép használgóját:

Your computer is now stoned. Legalize Marijuana
(Az Ön számítógépe most ki van nyírva. Engedélyezzék a Marihuánát)

A Stoned volt 1990 februárjában az egyik legelterjedtebb vírus. Miután a floppy boot-szektorát fertőzte meg, a merevlemezen pedig a partíciós táblát cserélte le, kétféle fertőzési mechanizmussal működött. Kelet-Európában új elven terjedő vírusként jelent meg. Változatai legtöbbször csak annyiban különböznek egymástól, hogy a szöveg második mondata hiányzik (tehát az átiró nem követeli a marihuána szabad forgalmazását), vagy az üzenet töredékes, vagy pedig még tisztázatlan szerepű bináris kódot tartalmaz. A magyarországi változat megtámadja a merevlemezt is, és valószínűnek látszik, hogy az egyik átiró változatnak itthon „továbbfejlesztett” terméke.

A Stoned vírus fertőzése különösen 3 1/2"-os floppy esetén veszélyes, mivel ezeket a lemezeket teljesen használhatatlanná teszi. Az így megfertőzött floppy használata esetén ugyanis 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 lefűlése nehezebb a hagyományos vírusokénál. Vírusölő program használata nélkül a harddiszkről ez a vírus csak alacsony szintű (low level) formázással távolítható el. A vírus rezidens része 4 kb-át.

A Stoned vírus ismert változatai:

Stoned-B: majdnem azonos az eredetivel, csak annyiban tér el, hogy a merevlemez partíciós táblájába épül be. Ennek egyik alváltozata terjedt el Magyarországon, többféleképpen átiró szöveggel. Ha RLL kontrollert használunk, a vírus gyakran tönkreteszi a rendszert, mert ezt a kontrollert nem tudja korrekt módon kezelni.

Stoned-C: szintén majdnem azonos az eredeti Stoned vírussal, de a rendszerüzenetet valaki teljesen kitörölte belőle.

55

A vírus neve: Sunday.

Egyéb elnevezése: Nincs.

Hossza: 1636 bájt.

Kódtípusa: PRAT. Parazita, rezidens része van, a .COM, az .EXE és az átfedő (overlay) állományokat támadja meg, manipulálja a FAT-ot.

Azonosítása: Scan V49+, F-Prot.

Eltávolítása: CleanUp, Scan /D vagy F-Prot.

Leírása: A Sunday vírust egyszerre sokan fedezték fel az USA-ban, Seattle városában, Washington államban, 1989 novemberében. A vírus aktivizálódásának feltétele, hogy a gép belső óráján vasárnap legyen.

Today is Sunday! Why do you work so hard?

(Ma vasárnap van! Miért dolgozol ilyen keményen?)

All work and no play make you a dull boy!

(Ha mindig csak dolgozol, és soha nem játszol, unalmas fiú lesz belőled!)

Come on! Let's go out and have some fun!

(Gyere! Menjünk egy kicsit szórakozni!)

A Sunday vírus a Jerusalem vírus testvére. Kódja sok szempontból ahhoz hasonló. Károsító hatásáról eddig annyit tudunk, hogy néhány esetben megromítja a FAT-ot, és ezzel elvesznek az adatok.

56

A vírus neve: Suriv 1.01.

Egyéb elnevezése: April 1st, Israeli, Suriv01.

Hossza: 897 bájt.

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

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

Eltávolítása: Scan /D, F-Prot, UnVirus.

Leírása: A Suriv 1.01 memóriarezidens vírus az Izraelben felbukkant

vírusszalád legelső tagja. Később sokszor átírták. Ez a vírus 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.

57

A vírus neve: Suriv 2.01.

Egyéb elnevezése: April 1st-B, Israeli, Suriv02.

Hossza: 1488 bájtt.

Kódtípusa: PRE. Parazita, rezidens része van, az .EXE állományokat fertőzi meg.

Azonosítása: Scan, F-Prot, IBM Scan.

Eltávolítása: Scan /D, F-Prot, UnVirus.

Leírása: A Suriv 2.01 memóriarezidens résszel rendelkezik. Az .EXE állományokat fertőzi, ezzel mintegy pótolva korábbi változatának „mulasz-

tásait”. Április elsején aktivizálódik, ha akkor 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 aktivizálódásához 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. A vírus ebben az esetben csak egy állományt fertőz meg. Vírusazonosítója a kódban található: SURIV 2.01.

58

A vírus neve: Suriv 3.00.

Egyéb elnevezése: Israeli, Suriv03.

Hossza: 1813 bájt (.COM kiterjesztésű fájlok esetén) vagy pedig 1808 bájt (.EXE állományoknál).

Kódtípusa: PRA. Parazita, rezidens része van, .COM, .EXE, .SYS, .BIN, átfedő (overlay) állományokat fertőző programvírus.

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

El távolítása: Scan/D, CHKVir v.4.01, F-Prot, Prgdoki, Sysdoki, Unvirus.

Leírása: A SURIV sorozat szerzője egy .COM és .EXE állományokat egyaránt fertőző vírus önálló elkészítése helyett barkácsoláshoz fogott. A kiindulást a Jerusalem vírus adta. Mint látni fogjuk, még azt a fáradságot sem vette, hogy visszafejtse a kódot, ezért benne maradt az a programozási hiba, amelyik az eredetiben is benne volt.

A Jerusalem vírus azonosító karaktersorozata: sUMsDos. Ezt kicserélte a saját verziójelzésével: SURIV 3.00.

Itt jön a programozási hiba, ami bennmaradt. Ugyanis az eredeti Jerusalem pénteken, 13-án aktivizálódik. Ekkor törölnie kell a fertőzött állományokat. Abban az esetben viszont, ha a vírus már jelen van a rendszer memóriájában, vagy 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 a timermegsza-

kítás manipulálásával lassítja is a gépet. Miként a Jerusalem-B vírus, ez is fertőz átfedő (overlay), .COM, .EXE, .SYS, .BIN állományokat, viszont COMMAND.COM-ot nem.

59

A vírus neve: Swap.

Egyéb elnevezése: Falling Letters Boot, Israeli Boot.

Hossza: 740 bájt.

Kódtípusa: BRF. Rezidens része is van, a floppy boot-szektorát fertőzi meg.

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

Eltávolítása: MDisk, CleanUp, CHKVir v.4.01, F-Prot, vagy a DOS SYS parancs kiadása.

Leírása: A Swap vagy Israeli Boot-vírus első felbukkanását 1989 augusztusában jelentették. Csak floppykat támad meg. Rezidens része 2 kb-ot használ fel a RAM-ból erre a célra. A lemez fertőzésekor hibásként jelöl meg egy logikai egységet (clustert) a 39. sáv 6. és 7. szektorában, ahol elfér. A fejhez már nem ragaszkodik. Ha a lemez annyira tele van, hogy a fenti hely sem szabad, semmit sem ír felül, ezért a vírus nem 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 nem található meg. A Norton Utilities segítségével könnyen felismerhetjük a fertőzött floppykat, mert a boot-szektor végén normális esetben hibaüzeneteket találunk, ha viszont boot-vírus fertőzte meg, akkor itt tömör kód van.

A vírus neve: SysLock.

Egyéb elnevezése: 3551.

Hossza: 3551 bájt (+ 0–15 bájt a paragrafushatár miatt).

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

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

Eltávolítása: Scan /D, F-Prot.

Leírása: A SysLock vírus a programkódhoz kapcsolódó vírus, amely önmagát titkosítja. Nemcsak a rendszert és a .COM állományokat fertőzi, hanem az adatokat is tönkreteszi. Mivel nincs rezidens része, úgy fertőz, hogy a program futása alatt az aktuális könyvtárat végignézi. Ha talál benne .COM és .EXE állományokat, véletlenszerűen kiválaszt azokról egyet, és — beleépítve saját kódját — megfertőzi azt. 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 SysLock írója nagyon utálhatta a neves szoftvercéget, a Microsoftot, mert a vírus a károsítandó állományokat úgy választja ki, hogy az megkeresi bennük a Microsoft karaktersorozatot. A keresés során a nagy- és kisbetűk lehetséges kombinációira is figyelemmel van. Ezt utána a következő karaktersorozattal helyettesíti:

MACROSOFT

A SysLock vírus a gépben a környezeti (environment) változók között keresi a SYSLOCK-ot. Ha ennek értéke hexa 40-re van beállítva a következőképpen:

set SYSLOCK=@

akkor nem fertőz, és nem is okoz semmilyen kárt.

A SysLock ismert változata:

Macho-A: hasonlóképpen viselkedik, mint a SysLock vírus, azzal az eltéréssel, hogy a Microsoft karaktersorozatot a következővel helyettesíti: MACHOSOFT.

61

A vírus neve: Taiwan.

Egyéb elnevezése: Nincs.

Hossza: 743 bájt.

Kódtípusa: PNCK. Parazita, nem rezidens, a .COM állományokat — a COMMAND.COM-ot is beleértve — fertőzi meg.

Azonosítása: Scan V56+, F-Prot, CHKSeq v.1.0.

Eltávolítása: Scan /D vagy törölni a fertőzött állományokat.

Leírása: A Taiwan vírus először 1989 januárjában bukkant fel Tajvanban. Amikor a Taiwan vírus kódja végrehajtódik, három fertőzési kísérletet tesz. Először a C: meghajtó gyökérkönyvtárában kezdi. Amennyiben fertőzendő állományra lel, akkor kódjának első 743 bájttját a .COM állomány elejére teszi. A maradékot pedig (ami a kivett 743 bájtot már nem tartalmazza) áthelyezi a .COM állomány végére. A vírusban van egy súlyos programozási hiba: ha a .COM állomány 743 bájtnál rövidebb, akkor agyonvágja azt, ugyanis nem ellenőrzi a fertőzetlen program hosszát. Egy programnak legalább 1486 bájtnak kell lennie ahhoz, hogy a vírus jól beépülhessen. A Taiwan vírus romboló. Minden hónap nyolcadik napján a 0-logikai szektorból kiindulva a C: és a D: meghajtón abszolút szektorírással megformáz 160 szektort. A romboló hatás azért súlyos, mert ezzel agyoncsapja a főkönyvtárat és a FAT bejegyzéseit.

62

A vírus neve: Traceback.

Egyéb elnevezése: 3066.

Hossza: 3066 bájt.

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

Azonosítása: Scan, F-Prot, IBM Scan.

Eltavolítása: M-3066, VirClean, F-Prot vagy a fertőzött állományok törlése.

Leírása: Ha a Traceback vírus beépül a .COM és az .EXE állományokba, azok 3066 bájtal 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 keres további jelölteket, mégpedig az egész lemezen, a főkönyvtárból kiindulva. A keresési folyamat leáll, ha megtalálta új áldozatát, vagy pedig a lemezen már mindegyik állomány fertőzött lett.

A vírus neve rávilágít cselekedeteire. Először is a fertőzött állományokat megtalálhatjuk azon az elsődleges útvonalon, amelyet a PATH paranccsal állítottunk elő. Így nyomon lehet követni — visszafelé —, hogy a fertőzés honnan indult el. Innen a név: traceback, azaz „nyomkövetés visszafelé”. Másik jellegzetessége, hogy ha a vírus megfertőz egy másik kópiát ugyanabból a programból, mint amelyikből elindult a memóriába, akkor törli magát az eredeti hordozóból, és áttelepszik a másik példányba. Akkor azután lehet keresni!

A Traceback vírussal történt fertőzés első jele, hogy amennyiben a rendszerdátum 1988. december 28-a utáni, és a vírus beült a memóriába, a betűk elkezdnek potyogni. (Hasonlóképpen, mint a közismert Cascade/Potyogós vírus esetében.) Ez az állapot a fertőzés után egy óra elteltével bekövetkezik. Ha a billentyűzettel szeretnénk valamit begépelni, akkor a rendszer lemerevedik. Ez egy percig tart. 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.)

Egyéb elnevezése: 2930.

Hossza: 2930 bájt.

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

Azonosítása: Scan V41+, F-Prot.

Eltávolítása: Scan /D, F-Prot 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). Egyéb tulajdonságai hasonlóak.

64

A vírus neve: Turbo Kukac.

Egyéb elnevezése: Turbo @ v.9.9.

Hossza: 512 bájt.

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

Azonosítása: CHKSeq v.1.0.

Eltávolítása: CHKVir v.4.01, Sysdoki 1,0.

Leírása: Magyarországon elterjedőben lévő vírus. Ha aktív, akkor a Shift-Print Screen billentyűlenyomásra a „Turbo Kukac 9.9” szöveget írja ki. Képes bemászni a Novell hálózatok csak végrehajtható (Execute Only) típusú programjaiba is. Ez a vírus eddig csak nagyon szűk körben jelent meg néhány fejlesztő laboratóriumban. Magyar gyártmány, valamelyik egyetemi központban készült. Különböző szintekig visszafejtett forráskódjai is keríngenek, így új változatainak megjelenésétől is tartani lehet.

65

A vírus neve: Töltögető.

Egyéb elnevezése: Filler, Fill, Arc.

Hossza: Nincs rá adat.

Kódtípusa: BPRX. Rezidens résszel rendelkező, boot-szektorra fertőző, a partíciós táblát teszi tönkre. A „stealth” (lopakodó) technikát alkalmazza.

Azonosítása: Bootkill 1.04, Sysdoki.

Eltávolítása: Bootkill 1.04, Sysdoki.

Leírása: Aktivizálódásának feltétele, hogy a számítógép belső órája 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.

Ez a boot-szektor megtámadó vírus egyike a legintelligensebb vírusprogramoknak, amelyet valaha is írtak. Szerzője tisztességtelen szándékkal felhasználta benne mindazt a programozói tudást, ami a boot-vírusokról eddig napvilágra került. A vírus jelenléte a lemezen semmilyen megszokott eszközzel nem deríthető fel. Ha a memóriában van, akkor mindig az általa elraktározott sértetlen boot-szektor képét mutatja be, bármilyen segédprogrammal is kezdjük vizsgálni a lemezt. A (c) Brain vírus hagyományait követve védekezik a direkt lemezírással dolgozó segédprogramok ellen.

A Bootkill programcsomag eredetileg még azt tartalmazta, hogy a boot-vírus lecseréli a boot-szektor. Ismeretlen vírusok jelenlétéről éppen az árulkodik, hogy nem a megszokott szöveges rendszerüzenetet találjuk ebben a szektorban. Nos, a Töltögető az első olyan boot-vírus, amely miután a merevlemez fertőz, nem az egész partíciós táblát cseréli le, hanem annak csak a programját, s a rendszerüzeneteket változatlanul hagyja. A Bootkill program 1.04 verziója már nemcsak képes kiírtani ezt a vírust a memóriából, hanem a legtöbb esetben a merevlemez is helyreállítja a vírus „felrobbanása” után. Ha a Töltögető a Stoned vírussal kombináltan fertőzte meg lemezünket, akkor azt nem lehet egyszerűen helyreállítani, mert a két program „összedolgozva” eltünteti a partíciós tábla programját. A vírusmentesítő programnak ezt fel kell ismernie, és újra generálnia, amire csak a Sysdoki képes.

A vírus csak rendszerlemezre terjed, de ha a memóriában van, elegendő egy DIR parancs is a tiszta rendszerlemez megfertőzéséhez. A floppyn a partíciós táblában nem fér el, hiszen a programvírusokhoz viszonyítva hatalmas, több mint 4 kb-át a kód hossza. Ezért az eredeti boot-programot és testének nagy részét a 360 kb-ajos 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 merevlemez-es egységgel rendelkező gépen fejlesztették.

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 egyszerűen 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 Vaccina magyarországi eredetű (zenélő) átirataihoz, még a CTRL-ALT-DEL gombokkal történő rendszerindítás után is a tárban marad. Csak a főkapcsoló képes azt eltávolítani, no meg a megfelelő vírusölők...

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 és az most az országban közkézen forog. 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 Path Minder kódolójával rejtjelezte a kódot. A lemez maga is vírushordozó!! Elindítása épp ezért veszélyes. 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 fejlesztő még legalább három ettől eltérő változatot készített és engedett el. Elkészített egy formázásálló verziót is, de az nem bukkant fel, csak bizonyos részleteket tartalmaz róla a fejlesztőlemez.

66

A vírus neve: Typo Boot.

Egyéb elnevezése: Mistake.

Hossza: Nincs adat.

Kódtípusa: BR. Rezidens résszel rendelkező, boot-szektor fertőző vírus.

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

Eltávolítása: MDisk, F-Prot, Bootkill vagy pedig a DOS SYS parancs kiadása.

Leírása: A Typo boot-vírust először Yasrael Radai különítette el, 1989 júniusában, Izraelben. A vírus memóriarezidens része a rendszermemória végén 2 kbájtnyi helyet foglal el magának, amikor beépül az operatív tárba. A vírus meg szeretné reformálni a helyesírást. Nem Izraelben írták, mert a héber betűket nem ismeri. Ezért a héber vagy orosz karakterkészlet használatakor teljes zagyvaságot produkál. Viszont ha egy rendszert megfertőzött, akkor a DOS nyomtatási rutin vagy az arra épülő egyéb program használatakor minden karaktert kicserél annak kiejtett, azaz fonetikus képére. Hogy a hecc teljes legyen, a számokat is valami mással helyettesíti be. Csak a nyomtatási képet reformálja meg alaposan, az adatokat és a képernyőn megjelenő szövegeket nem bántja.

A Typo boot-vírus 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 detektorai és killerei erre is alkalmazhatóak!

67

A vírus neve: Typo COM.

Egyéb elnevezése: Fumble, 867.

Hossza: 867 bájt.

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

Azonosítása: Scan V48+, F-Prot.

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

Leírása: Brighton városában, 1989 novemberében találta meg Joe Hirst. A Typo COM vírus a Typo boot-vírus szülője. Létrehozza a boot-verziót, ugyanakkor minden karakterátírást ugyanúgy csinál a nyomtatón, mint a boot-verzió, 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.)

68

A vírus neve: Vacsina.

Egyéb elnevezése: Nincs.

Hossza: 1206 bájt.

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

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

Eltávolítása: Scan /D /A 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 a tárban marad. Amikor fertőzőskor beépül egy másik programba, azt „beep” hanggal is jelzi.

Valószínűsíthető, hogy „pandúrból lett rabló”: egy vírusellenes programnak, a francia Vaccine-nak vírussá átvírt változata. A Vaccine ugyanis a vírus technológiát 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.

69

A vírus neve: Vacsina-B.

Egyéb elnevezése: Zenélő, Forgószínpad, Yankee Doodle.

Hossza: 1765 bájt.

Kódtípusa: PRA. 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 egy sajátos átirata van terjedőben, amely valószínűleg „közvetlen import” az Egyesült Államokból, mert eddigi tömeges hazai előfordulásai szoros tengerentúli kapcsolatokkal rendelkező műszaki-tudományos számítóközpontjainkban voltak.

A vírus a 64 kb-ajtnál rövidebb .EXE állományokba épül be, de a .COM állományokat is fertőzi. A memória-ellenőrző blokk (MCB) közvetlen manipulálásával épül be a memóriába. Ha .EXE állományokat fertőz, akkor azokból .COM-ként futó, de változatlan nevű állományokat csinál. Ez megnehezíti a kitakarítását is. Van viszont benne egy programozási hiba. Nem veszi észre, ha a vírussal együtt az .EXE mérete meghaladja a .COM állomány lehetséges maximális méretét. A megfertőzés ilyenkor csak részben sikerül neki, a .COM állományt pedig azonnal tönkreteszi.

A már említett átirás annyiból állt, hogy az eredeti vírus „beep” hangjelzé-

sét valaki kicserélte a Yankee Doodle vírus által a hasonnevű nótát tartalmazó rutinnal. 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 is aktív marad.

A Vacsina vírus első magyarországi megjelenése után hamarosan kopogtattak nálunk a nemzetközileg ismert Vacsina-átiratok is:

- Vacsina v05 — 1217 bájt.
- Vacsina v16 — 1350 bájt.
- Vacsina v24 — 1760 bájt.

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

70

A vírus neve: Victor.

Egyéb elnevezése: Ivan, Iván a rettentő, Victor v.1.0.

Hossza: 2442 bájt.

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

Azonosítása: CHKSeq v.1.0, Prgdoki 3.02.

Eltávolítása: CHKVir v.4.01, Prgdoki 3.02, Sysdoki 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 egyre inkább terjed. Várhatóan Magyarország tranzitálja ezt a Nyugat-Európában eleddig ismeretlen vírust.

Első felfedezői nevezték el, a többi nevet pedig a károsult számítógép-alkalmazók adták neki. Önmagát a vírusrész is Victor-nak, azaz Győzőnek nevezi. A vírus eredetnyomozása eddig nem járt sikerrel. Valószínűsíthető mind a lengyel, mind a bolgár, mind pedig az orosz eredet. Annak nincs semmi jele, hogy esetleg Magyarországon készítették volna.

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 környezetében kíméletlenül tönkretesz minden programot. Felkészítették a Novell hálózattal való találkozásra is, ezért ha abba bekerül, a rendszer teljes összeomlását, megsemmisülését okozza. A Novell védelmi rendszere nem akadály a számára. A vírusban egy kicsit bőbeszédű rendszerüzenetet találunk, de ezt sohasem írja ki a képernyőre.

VICTOR V:1.0

The incredible high perfomance VIRUS.

Enchanced versions Aviable.

This program was imported from USSR.

Thanks to Ivan.

(A hihetetlenül nagy teljesítményű vírus. Fejlettebb verziók is kaphatók. A Szovjetunióból importált program. Köszönet Ivánnak. — Az angol szöveg „hibahelyesen” idézve. — A szerk.)

Magyarországon 1990. június közepén felbukkant egy másik változata. Ennek kódja teljesen azonos az eredetiével, csak ismeretlen kezek a rendszerüzenetet cserélték ki. A soha kiíratásra nem kerülő új szöveg:

Victor V1.0 The Incredible High Performance Virus

This is computermind killer.

For every user:WARNING!!!

Virus in BOX!

(Victor v1.0. A hihetetlenül nagy teljesítményű vírus. A komputeragygyilkosa. Figyelmeztetés minden felhasználónak! Vírus van a dobozban!)

A vírus neve: Vcomm.

Egyéb elnevezése: Vircomm.

Hossza: 637 bájt.

Kódtípusa: PRE. Parazita, de rezidens része is van, az .EXE állományokat fertőzi meg.

Azonosítása: F-Prot, CHKSeq v.1.0.

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 vírus, amely — talán éppen primitívsége miatt — gyorsan átlépte az országhatárokat, és Németországban is, az USA-ban is felbukkant. Lengyel eredetű. Az biztosnak tűnik, hogy 1989 decembere táján kezdett terjedni.

Egy fertőzött állományt elindítva az aktuális könyvtárban egy másik .EXE állományt is megfertőz. Amikor a Vcomm a fájl belsejébe (!) épül be, akkor annak hossza az 512 bájt többszörösével nő. Ha pedig a végéhez kapcsolja magát, akkor 637 bájtot tesz hozzá az .EXE állomány eredeti hosszához. A vírus memóriarezidens része figyelemmel kíséri, mikor akar írni a rendszer a lemezre, és az írás műveletét kicseréli olvasásra.

72

A vírus neve: Vienna.

Egyéb elnevezése: Austrian, Unesco, DOS-62, DOS-68, 1-in-8, 648, Vienna-A.

Hossza: 648 bájt.

Kódtípusa: PNC. Parazita, nincs rezidens része, a .COM állományokra specializálta magát.

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

Eltávolítása: M-Vienna, CleanUp, VirClean, CHKVir v.4.01, F-Prot, Prgdoki, Sysdoki.

Leírása: A Vienna vírust először 1988 áprilisában fogták meg Moszkvában, az UNESCO által a gyermekeknek tartott számítástechnikai szaktáborban. A program megfertőzi az útjába eső első .COM állományt, amikor futtatjuk. Minden nyolcadik fertőzés után egyszer melegindítást végez a rendszeren (warm reboot), mialatt a víruskód is végrehajtódik. A vírusban van egy programozástechnikai hiba is: számos .COM állomány megfertőzése után már nem hajlandó elindulni.

A vírus neve: Vienna-B.

Egyéb elnevezése: 62-B, Reboot #2, Rendszerhívó vírus.

Hossza: 648 bájt.

Kódtípusa: PNC. Parazita és 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 vírus egyik változata. Lényeges különbség a kettő között, hogy amikor saját maga melegindítást hajt végre, egyúttal törli azt a programállományt, amelyikből indították. A magyarországi tapasztalatok részben ellentmondanak a szakirodalomnak. Ez annak köszönhető, hogy a kódot néhányan kissé „átbarkácsolhatták”. Ennek ellenére hosszúsága nem változott, de a vírus irtásához szükséges információk is megegyeznek az átírt változatokban.

Az esetek egy részében lehetséges az állomány helyreállítása. Amikor az első öt bájt felülírása már bekövetkezett, speciális programozástechnikai megoldásokkal akkor állítható helyre a program, ha előtte egy olyan vírus fertőzte meg, amely — jóindulatú lévén —, elmentette az eredeti öt bájtot, mert szüksége volt rá...

A reboot (rendszerhívó) vírus kevésbé ügyesen megírt, néha mégis rosszindulatúbb vírusrutin, mint a potyogós! 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 ez két eltérő algoritmus alapján történhet:

1. A terjedési algoritmus működésbe lépésekor ráülteti magát az egyik programra, de nem feltétlenül arra, amelyikből hívták. A program futásán ezt gyakorlatilag nem lehet észrevenni.

2. A rombolási algoritmus elindulásakor pedig megsemmisíti (felülírja) a program első 5 bájtyát, 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!

74

A vírus neve: Virus-90.

Egyéb elnevezése: Nincs.

Hossza: 857 bájtt.

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

Azonosítása: Scan V53+, F-Prot, CHKSeq v.1.0.

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

Leírása: A Virus-90 Patrick Toulme által nevelési és oktatási célzattal készített és forráskódban is árusított program volt. 1989 decemberében kezdődött meg a forgalmazása az USA-ban, és 1990 januárjában már széles körben elterjedté vált. A szellem kiszabadult palackjából. Csak terjed, más nem csinál. Sajnos azonban hordozórutinként kezdi felhasználni más szerzők saját, immár valóban kártékony programjaikhoz.

75

A vírus neve: Virus101.

Egyéb elnevezése: Nincs.

Hossza: 2560 bájtt.

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

Azonosítása: Scan V57+.

Eltávolítása: Scan /D vagy törölni minden fertőzött állományt, ami egy-remegy...

Leírása: A Virus101 a "big brother", azaz a Virus-90 programvírusnak orwelli értelemben vett mindent figyelő „nagy testvére”. Szerzőjét ismerjük:

Patrick Toulme írta oktatási segédeszközként 1990 januárjában. A vírusnak van memóriarezidens része, a fertőzött állományokat figyeli, hogy hol vannak elrejtve. Amennyiben megfertőzött minden fertőzhető, akkor a boot-rekordba is beépül. A jelenleg ismert verzió kizárólag floppylemezt képes megfertőzni!

76

A vírus neve: V2000.

Egyéb elnevezése: Nincs.

Hossza: 2000 bájt.

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

Azonosítása: Scan V59+, CHKSeq v.1.0.

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

Leírása: A vírus a fertőzött program elindítása után rezidensen beköltözik a memóriába. Ezt követően megkeresi a COMMAND.COM-ot és megfertőzi azt. Ha ez megtörtént, akkor minden elindított vagy valamilyen hozzáfordulás céljából megnyitott (másolás stb.) .COM és .EXE állományt meg fog fertőzni. A vírus 2000 bájttal növeli meg az állományokat, de ezt a felhasználó nem látja a DOS DIR parancsával, mert a vírus a katalógusba az eredeti fájlhosszt írja vissza. A vírus nagyon agresszív, fertőzése rendszerösszeomlást, adatvesztést okoz és az operációs rendszer újbóli betöltését teszi lehetetlenné.

Valakinek — valószínűleg a Budapesti Műszaki Egyetemen — az az ötlete támadt, hogy egy vírust vírusdetektorhoz kapcsolva terjesszen. A vírushor-dozóvá átalakított program a SCAN57.EXE, a McAfee-féle víruskereső program átírt változata. Ez a program ilyen formában nem is létezett, az integritásvédelemmel még nem rendelkező 47-es verzió nagy leleménnyel elkészített átiratáról van szó. A programba a Virus 2000 bolgár eredetű programvírust ültették be a „tréfacsinálók”. (Jelenleg a McAfee-féle új programokból a 4.5V66-B jelű használható veszély nélkül.)

A Virus 2000 programvírus bolgár eredetű. Alig három hónappal azt követően, hogy az USA-ban felbukkant (1990 februárjában kapta meg az első

vírust a McAfee cég), hazánkban is megjelent. A .COM és .EXE állományokat fertőzi meg. A vírus az állományok után fűzi be magát. Benne szöveges azonosító található:

A vírus elején:

Only the Good die young.....

(Csak a jók halnak meg fiatalon.....)

A vírus végén:

(c) 1989 by Vesselin Bontchev

A vírus a floppyról kerülhet be a gépbe. Akkor fertőz, ha egy futtatható állományt olvasásra nyitott meg valamelyik másik program. Ez volt az értelme a Scan programra való ráépítésének is. Először a merevlemezen fertőz. 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 nem lehet azokat helyreállítani. Ha a memóriában aktív, akkor minden olyan állomány hosszából, amelyikbe beépült, levon 2000 bájtot. Így azokat a tartalomjegyzékekben eredeti hosszúságúaknak látjuk.

Mértékadó nyugati szakmai körök szerint nem valószínű, hogy a szerző Veszelin Boncsev lenne. Szerintük ő egy kiváló virológus programozó szakember, és éppen ellenségei akarták őt ezzel a módszerrel lejáratni. Ez a tények ismeretében hihető is.

77

A vírus neve: W13.

Egyéb elnevezése: Nincs.

Hossza: 534 bájt.

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

Azonosítása: F-Prot.

Eltávolítása: F-Prot vagy a fertőzött állomány törlése.

Leírása: A W13 vírus a .COM állományokat fertőzi, kivéve ha azok már

fertőzöttek. Nagyon silány munka. A programozási hibákat a szerző utólag igyekezett korrigálni. Lengyel eredetű program, ott is azonosították 1989 decemberében. Magyarországi felbukkanására is számítani lehet. Változatai:

- W13-A — 534 bájt hosszú eredeti változat, sok hibával.
- W13-B — 507 bájt hosszú javított kiadás.

Egyéb információink nincsenek róla, az eddigi változatok a gyenge minőség miatt nem terjedtek el.

78

A vírus neve: Yankee Doodle.

Egyéb elnevezése: Music, 5Pm tee.

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

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

Azonosítása: Scan V42+, F-Prot, CHKSeq v.1.0.

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

Leírása: Az eredeti Yankee Doodle vírust 1989. szeptember 30-án találta meg Alexander Holy, Bécsben, a North Atlantic Project számítógéprendszerben. A vírus a .COM és .EXE állományokba ül be. A fertőzött programok a vírus beépülése után általában 2899 bájttal lesznek hosszabbak. Az .EXE állományok esetében a paragrafushatárok miatt az állománynövekedés hossza eltérő.

Miután a vírus önmagát memóriarezidensként installálta, figyeli az órát. Amikor az eléri a 17:00 pm 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 valamegyik programozó honfitársunk beültette a Vacsina-B jelű vírustermékbe is.)

Az eredeti Yankee Doodle csak zenél, és azon kívül, hogy ezzel a képességgel felruházza a többi állományt is, nem tesz semmi ártalmat. A vírus átirít új változatai azonban már sokoldalúbbak, gonoszabbak. Például megke- resik és alaposan átírják a Ping Pong vírust, mégpedig úgy, hogy azok 100

fertőzés után öngyilkosságot kövessenek el. Csak találgatni lehet, vajon a szerző a másik vírus írójával azonos-e, vagy a konkurens bandából származott, vagy csak ismerte a Ping Pong szerzőjét...

Más változatai a Potyogós vírushoz hasonlóan karaktereket potyogtatnak a színes monitorokról, néha pedig a főkönyvtárban található és „A” betűvel kezdődő állományokat törlik (AUTOEXEC.BAT, ANSI.SYS stb.). Legáltalábbis a magyar tapasztalatok ezt mutatták. Részleges vagy teljes átírásokkal van dolgunk, ezeket azonban az ismert detektorok felismerik és a killerek gond nélkül kitakarítják. E lista elkészülte után, közvetlenül a könyv kinyomtatása előtt jelent meg azonban ennek a vírusnak egy jelentősen hosszabb magyar átírata, amelyet a hagyományos standard szoftverek nem irtanak ki. Szerencsére azonnal készültek rá ideiglenes killerek, és már ismeri a Sysdoki is.

A Yankee Doodle a vírusátiratokat készítő „kollégáink” körében népszerű alapanyag. Eddig három átírt változat terjedt el Magyarországon.

- Yankee Doodle 2885 bájt. (Ez megegyezik az eredeti McAfee hosszal.)
- Yankee Doodle 2932 bájt.
- Yankee Doodle 2941 bájt.

A nemzetközi vírusszakértők által 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 helyreállításnál tönkreteszik a fertőzött programot. A helyi vírusváltozatok ellen a helyben készült vírustalanítók mindig hatásosabbak és biztonságosabbak.

79

A vírus neve: Zero Bug.

Egyéb elnevezése: Palette, 1536.

Hossza: 1536 bájt.

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

Azonosítása: Viruscan V38+, F-Prot, CHKSeq v.1.0.

Eltávolítása: Scan /D, F-Prot 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 bájtal, 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 installálja magát rezidensen úgy, hogy önmagán átirányítja a 21h megszakítást. Miután a vírus megfertőzte a COMMAND.COM-ot vagy beült memóriarezidensen, megkezdí a .COM állományok fertőzését. Ebbe beletartoznak a COPY és az XCOPY parancs hatására keletkező állománymásolatok is. Végül is minden .COM állomány s természetesen az egész rendszer is fertőzött lesz.

Amennyiben a vírus által fertőzött COMMAND.COM töltődik be a gépbe, az elveszi a timer 1Ch megszakítót és önmagán átirányítja. Bizonyos idő elteltével megjelenik egy „holdarc jellegű” karakter, jelen esetben az ASCII 01 kódú, és körbeszaladva a monitor ernyőjén, jó étvággyal elfogyasztja a 0 számjegyeket... A vírus a jóindulatúak közé tartozik, mert nem töröl és nem is formáz semmit, kivéve ezt az utóbbi kicsiny ötletet. Kifejezetten „előnyös” a könyveléshez és az adónyilvántartáshoz... De nem ez az igazi megoldás.

80

A vírus neve: 405.

Egyéb elnevezése: Nem ismeretes.

Hossza: Nincs rá adat.

Kódtípusa: ONC. Felülíró, 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: A 405-ös nevet viselő vírus a felülíró típus képviselője. Csak a .COM állományokat fertőzi meg az aktuális könyvtárban. Az eredeti állomány 405 bájtnál kisebb mértékben nő, az eredeti vírushossz azonban mindig 405 bájt. A saját hosszúsága és a növekedés hossza közötti különbség az a

szakasz, amelyet helyrehozhatatlanul felülír az eredeti állományokban. A vírus folyamatosan felismeri a már fertőzött állományt, és azt újra meg újra megfertőzi. Egyelőre a szakirodalomban nincsenek részletesebb adatok ennek a sajátos vírusnak a működéséről.

81

A vírus neve: 1260.

Egyéb elnevezése: Nem ismeretes.

Hossza: 1260 bájt.

Kódtípusa: PNC. Parazita, nincs rezidens része, titkosítja magát, a .COM állományokat fertőzi.

Azonosítása: Scan V57+.

Eltávolítása: CleanUp V57+.

Leírása: Az 1260-as vírust először 1990 januárjában észlelték. A vírus nem ül be rezidensen a memóriába, ennek ellenére kifejezetten életképes, robbanásszerűen terjed. A fertőzés bekövetkezte után a .COM állomány hossza 1260 bájjal 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 átírja. Elsőként a DOS PATH által megadott könyvtárakban fertőzi meg a :COM állományokat, kivéve a COM-MAND.COM parancsprocesszort. A vírus kódolt formában épül be az egyes állományokba, és a kódoló rutint a felismerés megnehezítésére véletlenszerűen változtatja. A vírus a debugerek ellen néhány programozási trükköt is tartalmaz. Az 1260-os vírus lehetséges támadáspontjai a helyi hálózatok, beleértve az állományadagoló központi gépeket (file server) és a munkaállomásokat is. Ezekre a vírust kifejezetten felkészítették.

82

A vírus neve: 1704 Format.

Egyéb elnevezése: Formázó potyogós.

Hossza: 1704 bájt.

Kódtípusa: PRC. Parazita, rezidens része van, kódolja magát, a .COM állományt fertőzi.

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

Eltávolítása: M-1704, CleanUp, Scan/D, CHKSeq v.1.0, F-Prot, Prgdoki, Sysdoki.

Leírása: Teljesen azonos a Cascade vírussal, csak amikor aktivizálódik, egyúttal formázza is a lemezeket.

83

A vírus neve: 1720.

Egyéb elnevezése: Spanish II.

Hossza: 1720 bájt.

Kódtípusa: PRA. Parazita, rezidens része van, a .COM (COMMAND.COM kivételével) és az .EXE állományokat fertőzi meg.

Leírása: A vírus hossza 1720 bájt, amelynek utolsó 5 bájtja a =PSQR vírusazonosítót tartalmazza. 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.

84

A vírus neve: 2930.

Egyéb elnevezése: Spanish.

Hossza: 2930 bájt.

Kódtípusa: PRNA. Parazita, rezidens része van, a .COM (a COMMAND.COM-ot beleértve) 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. Visszafejtése folyamatban van.

A vírus neve: 4096.

Egyéb elnevezése: 100 year, 4k, Frodo, Century.

Hossza: 4096 bájt.

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

Azonosítása: Scan V53+, CHKSeq v.1.0, F-Prot, Sysdoki.

Eltávolítása: Scan /D, F-Prot, Sysdoki.

Leírása: A 4096-os vírust először 1990 januárjában észlelték. A vírus a tipikus programférgek családjába tartozik, lassú munkával okoz helyreállíthatatlan károkat az adatállományokban. Vizsgálata most van folyamatban a nagy víruskutató központokban. Az eddigi gyorsinformációk szerint a vírus a .COM és az .EXE állományokat fertőzi meg, ami után ezek hossza 4096 bájttal nő meg. A vírus rezidensen belül a memóriába. Jelenléte csak az állományok hosszának megnövekedéséből tűnik fel. A százéves elnevezést onnan kapta, hogy az évszámnak a DOS DIR által nem mutatott első két számjegyéhez 100-at hozzáad.

A 4096-os vírus megfertőzi a .COM, az .EXE és az átfedő (overlay) állományokat, következetesen 4096 bájttal megtoldva azok hosszát. Néha a vírus rezidensen ül a memóriában, és akkor a hossznövekedés nem látszik a könyvtári listában. Amikor így a memóriában üdül, akkor megfertőz minden végrehajtható állományt, ha megnyitják azokat, beleértve a másolást is a DOS COPY, illetve XCOPY paranccsal.

Ez a vírus egyaránt pusztítja az adat- 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 vírus 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 jelene szinte hihetetlenül hangzik: ha másolatot akarunk készíteni a fertőzött állományról — a vírus természetesen ott ül a memóriában —, a fertőzött állomány új másolata fertőzésmentes lesz! Ez kínálja azután a mentesítés abszurdnak tűnő alábbi eljárását is. Amikor a vírus

a memóriában van, minden fertőzött állományról készítünk egy másolatot floppyra a COPY parancs segítségével úgy, hogy a másolat nevében ne szerepeljen a programfájl megszokott kiterjesztése. Azaz ne használjunk .EXE, .COM, .SYS, .OVL kiterjesztéseket. Amikor ezzel elkészültünk, a rendszert a főkapcsolóval kikapcsoljuk, majd utána bekapcsolva egy tiszta, írásvédett floppyról indítsuk a rendszert úgy, hogy a vírus ne legyen jelen a memóriában. A rendszer bejelentkezése után a DOS DEL parancsával töröljük az összes futtatható állományt, majd az átkeresztelten lemásolt állományokat visszanevezzük eredeti nevükre és kiterjesztésükre.

Amikor kitakarítottuk a fertőzött állományokat, utána még sokat kell kínlódnunk a nagy mennyiségű keresztkapcsolt cluster miatt, mert ha azokat nem szüntetjük meg, a keresztkapcsolt állományok nagyon gyorsan károsodni fognak. Ez a vírus a „stealth”, azaz lopakodó programozási technikát alkalmazó vírusok családjának legelső tagja. Sajnos a benne alkalmazott eljárások terjedésével az új vírusok felfedezése és a fertőzött állományok megtisztítása egyre nehezebb lesz.

VÍRUSVILÁG MAGYARORSZÁGON

Könyvünk itt következő részében az 1990 közepéig Magyarországon előfordult és hozzánk eljutott vírusok „lelkiéletéről” szeretnénk egyet s más elmondani. Talán lesz némi átfedés a vírushatározóban leírtakkal is, de a téma jellegénél fogva ez szükségeszerű.

Bár visszafejtett assembler listák formájában birtokunkban van a legtöbb vírus teljes forráskódja, számos külföldi és itthoni számítástechnikai szakemberrel, de még pszichológussal is konzultálva úgy határoztunk, hogy ezeket most nem közöljük. Egyelőre barátkozzon meg mindenki a gondolat-tal: a vírusok köztünk vannak, meg kell ismerni őket. Ha már általánosan megszokott, természetes dolog lesz, hogy az informatikában is vannak veszélyes eszközök és anyagok, amelyek kezeléséhez a szakmai tudáson kívül szellemi érettség, morális érzék, felelősségtudat is szükséges, akkor másként lehet kezelni ezeket az információkat is.

Gondoljuk csak el: az iskolában kémiaórán milyen régóta tanítják, hogyan kell nitroglicerint készíteni, mégsem fogunk hozzá, hogy a konyhában ilyet kutyulva felrobbantsuk haragosunkat. Előbb-utóbb az informatikában is el kell jutnunk erre a szintre. Most viszont még csak egyes kódrészleteket ragadunk ki a vírusokból, hogy a programozásban járatos szakemberekkel érzékeltsük az itt alkalmazott érdekes és más területeken is gondolatébresztő ügyes megoldásokat. Miként a haditechnika a világon mindenütt az élenjáró technológiák közé tartozik, ezt a technikát a számítástechnikában a vírusprogramozás jelenti.

A közölt kódrészletek disassemblerrel (Sourcer 1.92 verziója, az amerikai V Communications Inc. programjával) készültek, csak az egyes címkeneveket írtuk át beszélő nevekre, no meg a kommentárok is tőlünk származnak. Arra mindenképpen alkalmasak, hogy az adott problémát szemléltessék. Az egyes azonosító szekvenciákat a programozástechnikában megszokott hexadecimális formában közöljük.

Kérjük, az se hagyja ki teljesen ezt a fejezetet, aki nem ért a programozás-

technikához. Csak a rövid listákon kell átugornia, de a magyarázó szöveg — ígérjük — érthető lesz a csupán számítástechnikai alpműveltséggel rendelkezők számára is. Ez a fejezet bizonyára nem készült volna el ilyen alapos-sággal, ha Szegedi Imre nem éppen a programvírusokból írja hadtudományi doktori disszertációját. A disszertációjában általa elmondottak sok helyen visszaköszönnek közös munkánkban, s különösen ilyen „melléktermék” ez a könyvfejezet.

Egy kis karakterológia...

Mielőtt belemerülnénk a vírusok lelkivilágába, csoportosítsuk először őket hatásuk szerint, hiszen minden vírus valamilyen család része. Legcélszerűbb, ha a rendszerezés fő szempontjának azt tekintjük, hogy a vírusok a számítógépnek és az operációs rendszernek mely pontját támadják.

Jó tudni például, hogy vannak nem vírus természetű bosszantó programcskák, amelyek egyik-másik vírus működését szimulálják, vagy csak jópofáskodnak. Kárt nem okoznak és nem is szaporodnak, csupán a felhasználók idegeit rongálják, főleg azokat, akik nem tudják, milyen ellenféllel is állnak szemben. Ezeket a programokat mi is használjuk oktató munkánk során a vírusjelenségek szimulálására.

CRBX — A képernyő tartalmát jobbról balra eltoló rezidens vírusszimulátor.

DRAIN — Víz „kicsurgatása” a számítógépből és a lemezegységek felpörgetése. (Joker szimulátor.)

FACE — 50-100 „röhögő pofa” zavarja és lassítja a munkát, összekeverve a képernyő tartalmát.

GOBBLE — 1-60 perces időközönként beletöröl a képernyőtartalomba. Az osztrák Ikarus vírusellenes program oktatóprogramja.

SOUND — 1-60 perces időközönként ijesztő hangeffektust ad.

Már egyáltalán nem ártalmatlanok az állományok méretét megnövelő, úgynevezett appendelő vírusok. Ezek lehetnek .COM, .EXE vagy egyéb programállományt megfertőzők. A megfertőzött állománytól függően épülnek be a programba, akár úgy is, hogy a paragrafushatároktól függően változó hosszal növelik annak méretét. Fejezetünkben az alábbi appendelő vírusok lelkivilágát vesszük ki. Sajnos a Magyarországon előforduló változatok és

vírusok száma 1990. februártól júniusig jelentősen megnőtt. Íme, ahogy időrendi sorrendben megjelentek hazánkban az egyes állományokba beépülő, úgynevezett fájl- vagy parazita-vírusok:

1741 Cascade	/ Poty #1
1744 Cascade	/ Poty #2
Vienna	/ Reboot #1
Vienna-B	/ Reboot #2
Jerusalem-B	/ Péntek 13
Jerusalem Mutant	/ Kedd 1
Dark Avenger	/ Eddie
Yankee Doodle	/ Music
Ivan/Victor v.1.00	/ Iván

A sort folytathatnánk tovább, 1990. szeptemberében a mutánsokkal együtt mintegy 60 vírus él és virul országunkban.

A lemezeken a DOS egy program jellegű bevezető részt, úgynevezett boot-szektorhoz létre a formázás (inicializálás) során. Ide is beépülhetnek a speciális boot-vírusok. Ezek érdekessége, hogy formázott, de különben üres lemez is hordozhatja a fertőzést. Szerencsére kevesebb van belőlük — legalábbis Magyarországon —, mint a megtoldó (appendelő) vírusokból. 1990 januárjáig a következő kettő tette nemkívánatos és nem baráti látogatását a magyar számítógépekben:

Bouncing Ball	/ Olasz pingpongozó boot-vírus
Ogre/Disk Killer	/ Disk Killer

A lemezegység partíciós tábláját megtámadó vírusok a legújabb vírusgeneráció tagjai. Floppyn ezek általában boot- vagy file-vírusokként viselkednek. Közülük csak egy jelent meg Magyarországon — a Stoned/Marijuana —, de átiratainak (sajnos hazai forrásból is!) egyre nő a száma. Szerencsére legtöbbször csak a szövegét írják át, így hagyományos eszközökkel kitakarítható. Eredeti magyar fejlesztés viszont a Töltőgető vírus.

Kis víruslélektan

A következőkben igyekszünk felvillantani néhány sajátosságot a hazai vírusok működéséből, a bevezetőben említett csoportosítás megtartásával. Egyre újabb változatok keletkeznek erkölcsstelen emberek jóvoltából. Vírus ugyanis önmagától nem keletkezik, a számítógép merevlemezére csak floppyról futtatott fertőzött program indításával vagy a program felmásolásával és indításával kerülhet.

A legrégebbi vendég: 1701 / Cascade / Potyogós vírus

Az önmagukat állományba befűző — append — vírusokhoz tartozik. Ez a vírus onnan kapta a nevét, hogy aktivizálódása után a képernyő betűit lepotyogtatja. Először csak egy betű, majd az idő múlásával egyre több betű esik le a képernyő alsó sorába.

A vírus megfejtése során arra a következtetésre jutottunk, hogy azt jól képzett, igen jó DOS programozói ismerettel és leírással rendelkező (DOS Programmer's Reference Guide) szoftveresek készítették. Ezt az állítást arra alapozzuk, hogy a vírusban olyan DOS funkcióhívásokkal találkoztunk, amelyek a forgalomban lévő dokumentációkban nem szerepelnek (Undocumented function call — Reserved).

A Potyogós vírus csak .COM állományokat fertőz meg. A fertőzés hossza 1701 bájttal. A vírus keresési szekvenciája:

```
01 FA 8B EC E8 00 00 5B 81 EB
```

A vírusfej a következő képet mutatja:

:0104	01	DB	01	; Virus dekódolva ?
:0105	FA	CLI		; IT tiltása
:0106	8BEC	MOV	BP, SP	; Stack cím mentése
:0108	E80000	CALL	010B	; Megtudja önmaga
:010B	5B	POP	BX	; helyét
:010C	81EB3101	SUB	BX, 0131	

Ez a vírus a .COM program végére épül be, 1701 bájtal megnövelve a program hosszát. A vírus csak az elindított (futtatott) programot fertőzi meg. Írásvédett lemezre nem tud írni, és ezt ki sem tudja küszöbölni, ezért a DOS a következő hibát jelzi:

```
Write protect error writing drive X
Abort, Retry, Ignore, Fail:
```

Ez a vírus csak egy példányban épül be a programba, ami azt jelenti, hogy ha a program már fertőzött és a Potyogós vírus az utolsó a programkódban — első a végrehajtásban —, akkor abba a programba többször nem mászik bele. Többszörös fertőzés csak más vírussal keveredve lehetséges. Ez utóbbi esetet nevezzük tik-tak fertőzésnek, amikor többféle vírus rétegesen telepszik rá a programra.

Ha először futtatjuk a Poty vírussal fertőzött programot, akkor a vírus rezidens programrészt hoz létre a számítógép memóriájában. Ezt a memóriaterületet a memória map (memóriafoglaltsági térkép) programok (például: MAP.COM) 100-400 bájt hosszú N/A (not available), azaz nem elérhető területként jelzik. Ennek ellenére a vírus teljes egészében a memóriában marad. A rezidens vírusprogramnak itt az a feladata, hogy az összes elindított .COM kiterjesztésű programot megfertőzze. A rezidens program kiveszi a .COM program elején található ugrócímet (JMP X1 X2 — HEX E9 X1 X2 a program elején — a címképzésnek megfelelően HEX X2 X1) és erre a címre ugrik. Ezt követően megvizsgálja, hogy az adott címen 0 van-e. Ha igen, akkor elindítja a futtatandó programot, ha nem, akkor megfertőzi az állományt, és csak utána indítja el a programot. Mindez olyan gyorsan történik, hogy a felhasználó észre sem veszi.

A vírusellenőrzők és vírusölők (killerek) kiveszik a .COM program elejéről az ott lévő címet, és a cím+2-nél megnézik, hogy van-e ott vírus. Ha igen, akkor jelzik azt, illetve kiölik onnan. A programok vírustalanítása a következő lépésekből áll:

— Az adott címen a vírus felismerése.

— A program eredeti ugrócímének megkeresése. (Eredeti ugrócím alatt mindig a fertőzés előtt a program elején található címet értjük, ami több vírus

fertőzése esetén nem egyezik meg a .COM program tényleges ugrócímével.)

— A program eredeti ugrócímének helyreállítása (3 bájtt).

— A felesleges többlethossz (a vírus) levágása (1701 bájtt).

Ezeknek a vírusoknak mindegyike a fertőzés során megnöveli az állomány méretét. A .COM kiterjesztésű programok 64 kb-ánál tovább nem növelhetők. Ha a fertőzés során a vírus túl akarja lépni a 64 kb-átos korlátot, akkor memóriaallokációs hibával az operációs rendszer lefagy.

Milyen is a Potyogós vírus?

A vírus első 35 bájta minden fertőzés során megegyezik. Ez a programrészlet kódolja a vírus további részét (1666 bájtt):

A Poty vírus megvizsgálja, hogy eredeti IBM számítógépen dolgozik-e. Ezt az ellenőrzést úgy végzi el, hogy belenéz a ROM BIOS F000:E008 HEX fizikai címbe, és amennyiben ott megtalálja a „COPR.IBM” stringet, akkor nem fertőz.

A Poty vírus nem tárolja a fertőzés előtti fájl méretet. A vírus a HEX 10-es és 21-es megszakítások kezelését átveszi a DOS-tól. A 10-esre a videómegszakítás (karakterpotyogtatás) miatt, a 21-esre pedig a fertőzés miatt van szüksége. Az INT 21 megszakításnak csak a 4Bh opcióját (a program betöltése és indítása) használja. A többi opcióhívást továbbadja a DOS-nak. A 10-es megszakítás (Int) eredeti címe a vírus elejétől 315, 317 eltolással, a 21-es megszakítás (Int) pedig 311, 313 eltolással található meg a hagyományos módon, azaz Seg Word, Offset word. Az eredeti program első 3 bájta a vírus elejétől 331 bájttal eltolással található meg. Az első 35 bájttal rejtelvei:

:0104	01	DB	01	; Vírus dekódolva?
:0105	FA	CLI		; IT tiltása
:0106	8BEC	MOV	BP,SP	; Stack cím mentése
:0108	E80000	CALL	010B	; Megtudja önmaga
:010B	5B	POP	BX	; helyét
:010C	81EB3101	SUB	BX,0131	
:0110	2EF6872A0101	TEST	CS:[BX:012A],01	; Vírus dekódolva?
:0116	740F	JZ	0127	; IGEN
:0118	8DB74D01	LEA	SI,[BX:014D]	; SI=vírus első 2

```

; bájtja
:011C BC8206      MOV     SP,0682      ; HEX:682 = DEC:1666
:011F 3134        XOR     [SI],SI      ; Dekódolás
:0121 3124        XOR     [SI],SP
:0123 46          INC     SI
:0124 4C          DEC     SP
:0125 75F8        JNZ     011F
:0127 xx          ; Vírus első bájtja

```

A vírus további része kódolt, és minden fertőzött programban más. Ez abból adódik, hogy a kódolásba az eredeti program első három bájtja is belekerül.

A memóriában rezidenssé vált vírus hasonlóképpen tartalmazza az eredeti megszakítási (Int) vektorokat. Azt, hogy van-e vagy nincs a memóriában Poty vírus, a következőképpen lehet megtudni:

```

Chk_Mem:  Push  es
          Push  ds
          Mov   ax,3521h      ;ES:BX – az INT 21h jelenlegi címe
          Int   21h          ;ES=Segment BX=Offset
          Cmp   bx,031Ch      ;Ha van vírus Offset=31Ch
          Jne   Ugrorj_1      ;Poty nem cserélte le
          Mov   ax,WordPtr ES:0139h
          Mov   ds,ax
          Mov   ax,WordPtr ES:0137h
          Mov   ax,2521h      ;DS:DX eredeti Int 21h vektor
          Int   21h          ;Int 21 beállítása az eredeti címre
          Mov   ax,3510h      ;ES:BX Int 10h vektor jelenleg
          Int   21h
          Cmp   bx,0199h
          Jne   Ugorj_2      ; Poty nem cserélte le
          Mov   ax,WordPtr Es:013Dh
          Mov   ds,ax
          Mov   dx,WordPtr ES:013Bh

```

```

Mov    ax,2521h
Int     21h
Ugorj_2: Pop    ds
        Pop     es

```

Variációk egy Poty témájára:

1704/Cascade, a Potyogós első nemzetközi átírat.

A 1704/Cascade vírus a közismert karakterpotyogató vírus átírt változata. A vírus működési mechanizmusa, hatása, terjedési formája teljesen megegyezik a 1701/Cascade vírussal. A két vírus közötti különbség abban van, hogy a dekódolandó vírus hossza 3 bájtal több (HEX=682 — 1666 bájt helyett HEX=685 — 1669 bájt).

A 1704/Cascade vírus első bájtjai:

```

01 FA 8B EC E8 00 00 5B 81 EB 31 01 2E F6 87 2A 01 01 74 0F 8D B7
4D 01 BC 85 06 31 34 31 24 46 4C

```

```

:0104 01          DB      01          ; Virus dekódolva?
:0105 FA          CLI          ; IT tiltása
:0106 8BEC        MOV     BP,SP      ; Stack cím mentése
:0108 E80000      CALL    010B      ; Megtudja önmaga
:010B 5B          POP      BX        ; helyét
:010C 81EB3101    SUB     BX,0131
:0110 2EF6872A0101 TEST    CS:[BX:012A],01 ; Virus dekódolva?
:0116 740F        JZ      0127      ; IGEN
:0118 8DB74D01    LEA     SI,[BX:014D] ; SI=vírus első 2
                                           ; bájtja
:411C BC8546      MOV     SP,4682    ; <HEX&685 &
                                           ; DEC>1669

```

A dekódolandó vírus hossza 3 bájtal több, mint a 1701/Cascade vírusé.

```

:011F 3134        XOR     [SI],SI    ; Dekódolás
:0121 3124        XOR     [SI],SP

```

```

:0123 46          INC     SI
:0124 4C          DEC     SP
:0125 75F8        JNZ     011F
:0127 xx                      ; Vírus első bájtja

```

A vírus detektálása, dekódolása, kiölése a továbbiakban megegyezik az eredeti „törzspéldányú” 1701/Cascade vírusével.

Vendég Bécsből, állandó kvártéllyal: Vienna / Reboot vírus.

Ez a vírus kétféle módon fertőz. Az egyik fertőzési módja az, amikor csak bemásolja magát a .COM program végére, a másik fertőzési módjában pedig felülírja a program első 5 bájtját. A vírus a felülírás során olyan kódot épít be a programba, amely a program indítása után rendszerhívást (Reboot Computer) eredményez. A vírus ezen szekvencia neve alapján kapta a Reboot vírus nevet. A Reboot vírus csak .COM állományokat fertőz meg. A fertőzés hossza 648 bájt. A vírus keresési szekvenciája a következő:

```

FC 8B F2 81 C6 0A 00 BF 00 01 B9 03 00 F3 A4 8B F2 B4 30 CD 21 3C
00 75 03 E9 C7 01 06 B4 2F CD 21 89 9C

```

```

:0104 FC          CLD
:0105 8BF2        MOV     SI,DX
:0107 81C60A00    ADD     SI,000A
:010B BF0001      MOV     DI,0100
:010E B90300      MOV     CX,0003
:0111 F3A4        REP     MOVSB
:0113 8BF2        MOV     SI,DX
:0115 B430        MOV     AH,30 ;DOS verzió
:0117 CD21        INT     21
:0119 3C00        CMP     AL,00
:011B 7503        JNZ     0120
:011D E9C701      JMP     02E7
:0120 06          PUSH    ES
:0121 B42F        MOV     AH,2F ; DTA helye ES:BX

```

:0123 CD21	INT	21
:0125 899C0000	MOV	[SI:0000],BX
:0129 8C840200	MOV	[SI:0002],ES

Az RVK (Resident Virus Killer, Buruzs Tamás programja, Kandó Kálmán Villamos Műszaki Főiskola) is ezt a teljes szekvenciát keresi, a CHKVIR2 (Leitold Ferenc és Tábor Csaba programja, BME) vírusdetektor ennek a szekvenciának az első 5 bájta alapján azonosítja (FC 8B F2 81 C6) a Reboot vírust.

Ez a vírus a .COM program végére épül be 648 bájtal megnövelve a program hosszát. Nem az elindított vírusos programot, hanem a katalógusban valamelyik .COM programot fertőzi meg. Írásvédett lemezre nem tud írni, és ezt a hibát ki sem tudja küszöbölni, ami azt jelenti, hogy a DOS a következő hibát jelzi:

```
Write protect error writing drive X
Abort, Retry, Ignore, Fail:
```

Ez a vírus több példányban beépülhet egy programba. A Reboot vírus a program végére másolódik be. A vírus lemezegységet is képes váltani, ami azt jelenti, hogy ha például az „A” floppyegységről indítottuk a Reboot vírusos programot, elképzelhető, hogy a „C” egységen, merevlemezen fertőz meg valamilyen állományt. A Reboot vírusnak memóriarezidens része nincs!

A Reboot vírussal fertőzött program indítását követően először a vírus aktivizálódik, a vírus pedig aktivizálódása után azonnal fertőz. Az első fertőzés valószínűleg abban a könyvtárban lesz, ahonnan a vírusos programot indították, de fertőzhet más könyvtárakban is. A fertőzést kétféleképpen végezheti el:

1.) Megfertőz egy .COM programot és beköltözik a program végére, lecserélve a .COM ugrócímét önmagára. Ez a fertőzési módszer a szerencsésebb eset. A vírusellenőrző programok kiveszik a .COM program elején található ugrócímét, és cím+7-nél megnézik, hogy van-e ott Reboot vírus. Ha igen, akkor jelzik azt, illetve kiölik onnan.

2.) Tönkreteszi a .COM állományt. Felülírja a .COM program első 5 báját,

elpusztítva az eredeti ugrócímet. A fertőzött program első 5 bájtja a következő lesz: EA F0 FF 00 F0. Ez a szekvencia közvetlen ugrást jelent a ROM-BIOS végére. Ha valamelyik .COM program első 5 bájtja ezt a szekvenciát tartalmazza, akkor a program indítása után a RAM teszt következik (Reboot Computer).

Ezt a fertőzési módszert övön aluli ütésnek lehet nevezni. A Reboot vírus kérdezés és a program információinak elmentése nélkül, egyszerűen felülírja a .COM állomány első öt bájtját. Ezt az információvesztést gyakorlatilag nem lehet visszaállítani. A vírusellenőrzők és vírusölők az ilyen típusú fertőzésnél az állomány törlését javasolják. Ez az eset egy kicsit hosszabb analízist igényel. Szerencsés(!!!) esetben a törlés előtt egy másfajta vírus már megfertőzte az állományt, és az a vírus tartalmazza a .COM program helyreállításához szükséges információkat. A vírusölők erre a fertőzési típusra mondják, hogy halott (ang. dead) állomány.

A fertőzés során minden vírus megnöveli az állomány méretét. A .COM kiterjesztésű programok 64 kbájtnál tovább nem növelhetők. Először az aktuális könyvtárban fertőzi meg a kisebb állományokat. Ha az aktuális könyvtárban elég fertőzés van, akkor könyvtárat vagy diszket vált (például: floppyról harddiszkre).

A Reboot vírus anatómiája:

A Reboot (Boot, Reset) vírus az állomány végére épül be. A Reboot vírus hossza 648 bájt. A Reboot vírus kezdete a .COM program elején található cím+7-nél található meg. A vírus vége, a fertőzött program vége is reboot-szekvenciával kezdődik. EA FF F0 00 F0.

A program ugrócíme fertőzés előtt (belépéskor a program első három bájtja): vírus eleje+511 bájt. A fertőzött program elején jelenleg található ugrócím: vírus eleje+514 bájt. A program hossza fertőzés előtt: vírus eleje+622 bájt (két bájt).

Ennyi információ elegendő a vírus kiöléséhez és a fertőzés előtti állapot visszaállításához.

Már vírust is „koppintanak”: Vienna-B/Reboot vírus

A Vienna-B vírus az eredeti osztrák „Reboot” vírus átfertőztetett változata. Az átfertőztetett

vírus hossza, hatása, beépülési formája teljesen megegyezik az eredeti vírussal. A két vírus közötti különbség a 22. és a 23. bájton van. Ha a vírus azonosítására az első 21 bájtot használjuk (ennél többet szoktak), akkor ugyanazzal a módszerrel mindkét vírust hatástalanítani lehet.

Reboot #1 vírus — Vienna (az eredeti):

```
FC 8B F2 81 C6 0A 00 BF 00 01 B9 03 00 F3 A4 8B F2 B4 30 CD 21 3C
00 75 03 E9 C7 01 06 B4 2F CD 21 89 9C
```

Reboot #2 vírus — Vienna-B (ez pedig az átírat!):

```
FC 8B F2 81 C6 0A 00 BF 00 01 B9 03 00 F3 A4 8B F2 B4 30 CD 21 3A
C0 75 03 E9 C7 01 06 B4 2F CD 21 89 9C
```

A két kulcsszekvenciában látható az eltérés, az, hogy mit írt át a plagizátor az eredeti Reboot vírushoz képest.

Fekete macska helyett péntek 13-ára javasolt programunk:

a Jerusalemb / Péntek 13 vírus kitakarítása

A víruscsalád egyik „legnépszerűbb” tagja, .COM és .EXE állományokat egyaránt fertőz. A Péntek 13 vírus nevét onnan kapta, hogy csak akkor aktivizálja magát, ha 13-a péntekre esik. Más napokon csak fertőz (lappang). Ha viszont a dátum szerint 13-a péntekre esik, akkor minden elindított programot kitöröl a lemezről. A program indítása után „Bad command or file name” (Hibás parancs vagy fájlnev) DOS üzenet jelenik meg a képernyőn. A program még le sem futott, de a vírus már kitörölte a katalógusból. A következő „Dir” parancsnál már nincs is az adott fájl a könyvtárban. A fertőzés hossza 1808—1822 bájt között változó lehet. A vírus keresési szekvenciája:

```
E9 92 00 73 55 4D 73 44 6F 73
      S U M S D O S
```


A vírus csak az elindított .COM és .EXE állományokat fertőzi meg. A vírus az EXE állományokba „tetszőleges számban” beépülhet, a .COM állományokba pedig, ha ő van egyedül, egyszer épül be. A Péntek 13 vírus írásvédett lemezre nem tud írni, de nem lép ki DOS-hibával, tehát nem szól. Ezt az ügyet úgy kezeli, hogy nem sikerült a fertőzés. (Tud felemelt fejjel veszíteni!) Az első vírusos program indításánál 1792 bájt hosszú rezidens vírusprogramot hoz létre, lecserélve a 08 (timer) és a 21 (DOS function call) megszakításokat (interrupts, hooked vector 08 21). A Péntek 13 képes a memóriában a Poty vírussal együtt lenni, ami azt jelenti, hogy .EXE állományok esetén csak a Péntek 13 fertőz a saját hosszával, de a .COM állományok esetén mind a két vírus fertőz. A két vírus hossza $1813+1701=3514$ bájt. Ideális tik-tak páros!

A .COM fertőzések módszertana és a tik-tak fertőzés a Péntek 13-nál:

A vírus a program elejére épül be, maga előtt tolvaa a program további részét. A vezérlést (a .COM állományok elején lévő ugrócímet) magára állítja be. A .COM állományok esetén a fertőzés hossza 1813 bájt, feltételezve, hogy a memóriában nem volt Poty vírus.

Ha a memóriában Poty vírus is volt, akkor a Péntek 13 azt is le fogja futtatni, és ezentúl együtt fognak fertőzni, mint két jó barát. Ha a .COM program eléri a számára maximált 64 kbájtot és a vírusok tovább akarnak fertőzni, akkor a DOS operációs rendszer a következő hibaüzenettel lefagy:

```
Program too big to fit in memory
Memory allocation error
Cannot load COMMAND.COM
```

(A program túl hosszú. Nem fér el a memóriában. Memóriaallokációs hiba. Nem tudom betölteni a COMMAND.COM-ot.)

Ha a Poty és a Péntek 13 is bent van a memóriában, akkor a következő esetek lehetségesek:

- Ha először a Poty vírus költözött a memóriába, akkor ő fog utoljára fertőzni és a vezérlést ő fogja másodikként megkapni.
- Ha először a Péntek 13 volt a memóriában, akkor ő fog utoljára fertőzni. A fertőzés hossza megegyezik, csak a végrehajtási (fertőzési) sorrend más.

A Péntek 13 vírus anatómiája, ha a gazda egy .COM fájl:

A Péntek 13 vírus fertőzési hossza 1813 bájtt. A fertőzés előtti fájl méret a vírusos fájl elejétől a 17.-18. bájton van. A fertőzés előtti program kezdete a vírusos fájl elejétől 1808 bájtra van. Ennyi információ elég a vírusnak a .COM fájlból történő kiöléséhez.

A Péntek 13 vírus anatómiája, ha a gazda .EXE fájl:

A vírus a program végére épül be, ráállítva az .EXE állomány címét önmagára. Az .EXE állományokat a vírus tetszőleges számban megfertőzheti. Ha a program mérete 640 kbájtnál hosszabbra „megdagad”, akkor a következő programindításkor az alábbi DOS hibáüzenet fog megjelenni.

Program too big to fit in memory.

A program túl hosszú. Nem fér be a memóriába.

A Péntek 13 első fertőzésének hossza 1808—1822 bájtt között lehet, mivel „paragrafus” elejére állítja magát. Minden további fertőzés mérete 1808 bájtt.

Program vége 1F 07 5D 5F 5E 5A 59 5B 58 9D E9 1D FD 00 00 00

Vírus eleje E9 92 00 73 55 4D 73 44 6F 73 00 01 DF 1C 00 00
s U M s D o s

A fenti példában látható, hogy a vírus paragrafushatárra teszi magát. A program vége után még 3 bájtt szabad terület (00 00 00) marad. Ez azt jelenti, hogy ebben az esetben a vírus fertőzési hossza 1808+3 bájtt és a vírustalanított program 3 bájttal hosszabb lesz, mint eredeti korában. Ennek a fájl méret-növekedésnek gyakorlati jelentősége nincs.

A Péntek 13 vírus felépítése .EXE állomány fertőzése esetén:

A Péntek 13 vírus fertőzési hossza 1808-1822 bájtt között lehet. Az .EXE program 20.-21. bájttjának értéke HEX „00-C5”. Ennek a bájttnak a megvizsgálása után kell a fájlban tovább keresni a vírust. A vírus helyét a fájlban a hexa 8.-9. és a hexa 16.-17. bájtt mutatja. A számolási módszer a következő:

(8 word + 16 word)*16. Ez a cím mutat a vírus elejére, tehát a fájlt innen kell levágni. Az eredeti program fejlécét (EXE header) ki kell számolni.

A Péntek 13 vírus szerkezete,

ha archivált — önkipakoló — .EXE állományt fertőz és tesz tönkre:

Archív állományokat lemezterület felszabadítására, a tárolt állományok méretének csökkentésére hozunk létre. Az állományok archiválását speciális archiváló programokkal (pl. ARC, PKARC, PKPACK) hozzuk létre. Az .ARC fájlnev-kiterjesztésű állományok az adatokat tömörített formában tartalmazzák. A vírusok ezeket az állományokat nem támadják meg. A PKARC programcsomag tartalmaz egy önkicsomagoló rutint, amelyet az archivált állomány elé kell másolni. Ennek az az előnye, hogy az archív állomány kicsomagolásához nincs szükség kicsomagoló programra (ARC, PKXARC, PKUNPAK, NARC). A PKSFX önkicsomagoló program segítségével azonban archivált .EXE állományt hozunk létre, amit a vírus már meg tud támadni. Hazánkban a jelenlegi „népszerű” vírusok közül a Péntek 13 beépül az archív állományba.

A PKSFX program fejlécében az .EXE állomány mérete akkorának van megadva, mint a PKSFX program mérete, tehát az archív állomány mérete sehol nincs definiálva. Az önkicsomagoló program az első tömörített állományra ugrik és onnan kezdi a kicsomagolást. A Péntek 13 vírus is a PKSFX fejlécből veszi ki az .EXE program méretét, így az első archivált állomány elejét 1808 bájtal felülírja. A fertőzés során a fertőzött állomány mérete nem változik meg, mert a vírus az állomány közepébe írja be magát. A vírusölők ezt a típusú fertőzést információvesztés nélkül nem tudják helyreállítani. Egy helyreállítási mód van: a fertőzött állomány kivágása és a „lyuk” befoltozása. Ezzel a módszerrel legalább a további, nem fertőzött archív állományokat meg lehet menteni.

Tömörítésre újabban a PKZIP/PKUNZIP programrendszer különböző verzióit használják. Itt a helyzet hasonló az előbbihez, de most már van értelme az állomány helyreállításának. Ugyanis a programcsomag része a PKZIPFIX program, amellyel a lyuk befoltozható. A pointer továbbra is az EXE fej végére mutat a PKZIP-es állományoknál. Ráadásul a 1.10-es amerikai verzió és az attól kezdődő újabb programok esetében ennek az .EXE fejnek a mérete

is változik, attól függően, hogy rövid vagy pedig teljes szolgáltatást nyújtó programfejet kértünk e a ZIP2EXE-től a program elé.

Jerusalem Mutant / Kedd 1 — magyar átirat

A Jerusalem mutánsvírus a Jerusalem-B vírus Magyarországon átirat változata. Az eredeti vírus átirására az motiválta a hazai programozót, hogy a szabadszoftverként terjesztett vírusölő programok ne tudják felismerni és hatástalanítani az átirat változatot. Megjelenése után alig pár hónappal az egyik leggyakoribb amerikai vírussá vált, az ottani killerek sem irtották.

Természetesen a Jerusalem-B vírus úgy került átirásra, hogy a Prgdoki v.2.11E nem tudta hatástalanítani, és önmaga is megfertőződött a vírus hatására. A vírusnak két fő része került átirásra. Az egyik a vírusazonosító kód, amely a Jerusalem-B esetében:

```
E9 92 00 73 55 4D 73 44 6F 73
      s U M s D o s
```

míg a Jerusalem mutáns esetében:

```
E9 92 00 73 55 4D 73 44 6E 73
      s U M s D n s
```

A másik az aktivizálódási dátumnak péntek 13-ról kedd 1-re változtatása. A Jerusalem-B vírus dátumellenőrző rutinja:

```
B4 2A      mov  ah,2Ah                ;Dátum lekérdezése
CD 21      int  21h                  ;DOS - ah=function 2Ah
06 000E 00  mov  bájt ptr cs:data-20e,0 ; (8FA3:000E=0)
81 F9 07C3  cmp  cx,7C3h             ;1987 utáni dátum
74 30      je   Ugorj-tovább-1        ;Ha nem tovább
3C 05      cmp  al,5                  ;A hét 5. napja - péntek?
75 0D      jne  Ugorj-tovább-2        ;Ha nem tovább
80 FA 0D    cmp  dl,0Dh               ;HEX=0D = 13.van
75 08      jne  Ugorj-tovább-3        ;Ha nem tovább
```

A fenti vírusrészletből látszik, hogy az eredeti vírusrutin csak 1987 utáni péntek 13-án fejt ki hatását. Az átírt vírus dátumellenőrző rutinja:

```

B4 2A      mov  ah,2Ah                ;Dátum lekérdezése
CD 21      int  21h                  ;DOS - ah=function 2Ah
06 000E 00  mov  bájtt ptr cs:data-20e,0 ; (8FA3:000E=0)
81 F9 07C3  cmp  cx,7BCh             ;1980 utáni dátum
74 30      je   Ugorj-tovább-1        ;Ha nem tovább
3C 05      cmp  al,2                  ;A hét 5. napja - Kedd ?
75 0D      jne  Ugorj-tovább-2        ;Ha nem tovább
80 FA 0D    cmp  dl,1                 ;HEX=0D = 1.van
75 08      jne  Ugorj-tovább-3        ;Ha nem tovább

```

Az átírt Jerusalemb-B vírus az 1980. évtől kezdődő kedd elsejei napokon töröl. Jogos a kérdés, hogy mi értelme van az 1987-es dátumot 1980-ra megváltoztatni. Ennek oka a következő: az IBM-kompatibilis XT típusú gépeket 1980-ban kezdte forgalmazni az IBM cég. Ezek a számítógépek nem voltak ellátva úgynevezett valós idejű órakártyával (real time clock card), így a valós dátumot és időt minden bekapcsolásnál a felhasználónak kellett beállítania. Ha a felhasználó nem akarta, vagy elfelejtette a valós idejű dátum- és időpont-beállítást elvégezni, akkor az automatikusan 1980 01 01-re állt be. A fenti átírással tehát a vírus gyakorlatilag minden számítógépen dátum-beállítástól függetlenül ki tudja fejteni pusztító hatását. A későbbiek során az IBM PC/AT kategóriájú számítógépeket már ellátták úgynevezett valós idejű órával.

A Jerusalemb mutáns — Kedd 1. vírus beépülése, terjedése, pusztító hatása megegyezik az eredeti víruséval, csak az aktivizálódás dátumában tér el. A vírus pontos felismerése érdekében a dátum környékéről vettem mintát (Sz. I.), így a vírus könnyen és nagy biztonsággal felismerhetővé vált.

Egy nemkívánatos barát Szófiából: Dark Avenger / Eddie

A vírusok közül Eddie „barátomat” tartom a legügyesebben megírt, állományhoz hozzáépülő vírusnak, és máig sem értem, hogy ha valaki programozástechnikában ennyire zseniális, az miért adja vírusírássra a fejét. Min-

denesetre szép intellektuális kaland volt a visszafejtése, csak ne tette volna tönkre annyiszor a merevlemezt! (Szegedi Imre).

A vírus elnevezéseit a fájlhoz hozzáépülő vírusban található szöveg alapján kapta:

Eddie lives...somewhere in time!

DIANA P.

This program was written in the city of Sofia.

(C) 1988-89 Dark Avenger

A nyugati szakirodalom a vírust Dark Avenger-nek — Sötét Bosszúállónak nevezte, a magyar szakirodalomban Eddie néven terjedt el. („Keresztapja” a CWI-ben megjelent cikkében Kis János volt.) A vírus hossza 1800 bájt, de .EXE állományba történő beépülése esetén +15 bájttal hosszabb lehet. A vírus a COMMAND.COM, .COM, .EXE, .OVL (overlay=átfedő) állományokba épül be. Memóriarezidens része van. A vírus keresési szekvenciája a vírusban található szöveg lehet: „Eddie” vagy „Dark Avenger”.

A Dark Avenger vírust az USA-ban izolálták először, az U. C. DAVIS támaszponton. Valószínű származási forrása Bulgária. Magyarországon 1989 augusztusában bukkant fel. (Én 1989 októberében találkoztam először vele. — Sz.I.)

Ha egy vírussal fertőzött programot elindítunk, a vírus aktivizálódik, de nem rögtön, hanem csak a programból való kilépéskor, bár a vezérlés először a víruskódra kerül rá. A vírus elsőként a COMMAND.COM parancsprocesszort támadja meg, majd gyakorlatilag elveszi a DOS-tól a teljes vezérlést! Ez nem túl ravasz megoldás, mert manapság már minden valamirevaló vírusfigyelő szoftver rajtatartja a szemét az operációs rendszer állományain (pl.: IBMIO.SYS, IBMDOS.COM, COMMAND.COM).

Íme az „ellopott” megszakítások listája. Látható, hogy a DOS-nak alig jut valami, amit Eddie ne ellenőrizne... „valahol az időben”.

08 - Timer

Megszakítás a rendszerórától

09 - Keyboard

Klaviatúramegszakítás

10 - Video Services

Képernyő kezelése

13 - Disk I/O	Lemezműveletek
16 - Keyboard I/O	Klaviatúraműveletek
1C - User Timer	Felhasználói óra
21 - DOS Service Call	DOS-hívások
25 - Absolute Disk Sector Read	Abszolút lemezszektor-olvasás
26 - Absolute Disk Sector Write	Abszolút lemezszektor-írás
27 - Terminate and Stay Resident	Programfutás után rezidens marad
28 - DOS Timeslice	DOS időosztás

Ha a vírus rezidenssé vált, akkor minden lemezműveletnél fertőz. Mivel a vírus abszolút szektorírást végez, nem aktualizálódik a fájllehelyezési tábla (FAT), így az állományokat nem fogjuk megtalálni a lemezen („sector not found”). A vírus a klaviatúrakezelő megszakítást is „magába szívja”, így a billentyűzettel is gondok lehetnek (például DOSEDIT). Az Eddie vírus nem az elindított állományokat fertőzi meg, hanem minden lemezműveletnél fertőz, és nagyon gyorsan terjed. Gyakorlati tapasztalatok szerint 5-20 perc alatt képes a merevlemez összes állományát megfertőzni, ezért ellene eddig csak a vírusmegelőző programok bizonyultak hatásosnak, melyek kifejlesztését az ilyen vírusok különösen indokoltá tették.

Eddie szállást csinál magának az .EXE állományokban:

Ha vírusos programot indítunk, akkor a vezérlés először a vírusra kerül rá, a víruskód egy része lefut, és a rezidens víruskód aktivizálódik. Ezt követően a vezérlés az eredeti kódra ugrik vissza. A programból történő kilépés esetén megfertőződik a COMMAND.COM parancsprocesszor. Ezt követően gyakorlatilag egy-két percen belül minden állományunk fertőzött lesz.

A vírus fertőzési hossza .EXE állomány esetén 1800 bájt, de +15 bájtig terjedő eltérés lehet, mert a vírus a paragrafushatárra teszi magát. Amíg nem fertőzött meg minden állományt, addig az állományok végéhez épül hozzá. Ha pedig már minden állományt megfertőzött, akkor a víruskód egy részét véletlenszerűen bemásolja a lemez bármelyik részére. A fertőzési állapotot a boot-szektorban DOS névnek fenntartott helyen jelzi egy bájton. Az állományhoz hozzáépülő víruskód nincs kódolva. A megfertőzött program eredeti információi (amelyek a visszaállításhoz szükségesek) a program utolsó

bájtjain, a vírus végén találhatók, fordított sorrendben. A fejrész azonosítója .EXE programok esetén „MZ”, míg a .COM programoknál valamilyen ugró (jump) utasítás, például az „E9”.

A víruskód viszonylag rövid, ahhoz képest, hogy a vírusprogram mire képes. Ezt a vírusíró úgy érte el, hogy közvetlen BIOS (Basic Input Output System) hívásokat és BIOS kódvégrehajtást használ. Ha a vírus aktív, akkor rezidens programok indítása nem mindig lehetséges.

A vírus írásvédett floppylemezt nem tud megfertőzni, de a hibát kezeli, kritikus hibakezelő rutint tartalmaz.

A Dark Avenger nem szokványos módon válik rezidenssé, vagyis nem a TSR (terminate and stay resident) rutinon keresztül, hanem közvetlenül az úgynevezett megszakítási táblába (interrupt table) írja be a címét. Így a vírus a DOS operációs rendszer hívásaival a memóriában nem fedezhető fel. Ha lekérdezzük a DOS 21 megszakítás címét a 35-ös funkcióval, akkor a visszaadott DOS 21 cím és a megszakítási táblába írt cím között különbséget találunk. A vírus a memória végébe épül be, mivel a DOS 21-es megszakítás címét oda helyezi át: 9F1A:02EE.

A vírus aktivizálódásának feltétele, hogy a lemezen már minden fertőzhető állomány fertőzött legyen. Amikor ez bekövetkezik, akkor önmagából részleteket és szövegeket másol át véletlenszerűen az állományok közepébe. Később a főkönyvtárt tartalmazó rész kivételével a merevlemez egyes cilindereit alacsony szintű formázással tönkreteszi. Ez a rossz, illetve íráshibás szektorok felszaporodását idézi elő, végül a rendszer leáll, lefagy, összeomlik.

A Flushot vírusfigyelő rendszer „őrizete mellett” elindítottam egy Eddie vírussal fertőzött állományt, így aktivizáltam a vírust, majd elkezdtem dolgozni (SZ.I.). Először egy Clipper programot fordítottam. A vírus felfüggesztette a fordító munkáját, megfertőzött egy állományt, és visszaadta a vezérlést a fordítóprogramnak. Mindez olyan gyorsan történt, hogy gyakorlatilag észre sem lehetett venni a fertőzés műveletét. Egy másik esetben, amikor a Dark Avenger vírus szintén aktív volt, Turbo Pascal fejlesztői környezetben dolgoztam. Az integrált fejlesztői környezetben a megírt programnak ugyanott átalakíthatókv égrehajtható (.EXE) állománnyá. S mire a forráskódú programot végrehajthatóvá fordítottam, a vírus már bele is mászott a programba.

Dark Avenger fertőzést észlelve új rendszert kell hívni egy írásvédővel leragasztott vírusmentes rendszerlemezről, majd el kell indítani a megfelelő mentesítő programot. Máskülönbén éppen a mentesítő programok lehetnek a fertőzés továbbhurcolói vagy az integritásvédelemmel ellátottak nem is működnek.

Egy kis muzsika: Yankee Doodle / Music / 5 órai tea

Az eredeti Yankee Doodle vírus azonkívül, hogy aktív rezidens állapotban délután 5 órakor nagy hangerővel eljátssza az amerikaiak kedvenc nótáját, a mai napig semmi pusztítást nem végzett. Hacsak azt nem tekintjük ilyesminek, hogy a veszélyesebb Ping Pong vírussal találkozva azt egy kicsit átalakítja, melynek eredményeként a Ping Pong 100 fertőzést végrehajtva végül önmagát pusztítja el. Ezzel szemben a Yankee Doodle átiratai között igazán kártékonyak is vannak. Az egyik magyar változat például törli vagy legalábbis részlegesen használhatatlanná teszi azt az állományt, amelybe beépült.

A Yankee Doodle az állományok végére épül be, hossza 2885 bájt, legfeljebb +15 bájt eltéréssel a paragrafushatár miatt. A vírus .EXE és .COM állomány esetén egyaránt a paragrafushatárra teszi magát. („Megszokott” esetben a vírusok csak .EXE állományoknál teszik magukat paragrafushatárra, míg .COM állományok esetén ez nem szükséges.) A vírus nem a szokványos módon, nem a DOS megszakításait kihasználva válik rezidenssé, hanem a memória-ellenőrző blokkon keresztül (MCB — Memory Controll Block), ezért a memóriatérképet vizsgáló programok nem is látják.

A fertőzött program először a vírus elejére ugrik (F4 7A 2C), és a víruskód lefutása után a vezérlés visszakerül oda, ahová eredetileg kerülnie kellett volna. A vírus első bájtjai, keresési szekvenciája:

F4 7A 2C 00 00 00 07 0A BE 0A 4D 5A 07 00 06 00

A vírus elejétől (a program elején lévő ugrócímtől) számított 7-8-9-10. bájt tartalmazza a program fertőzés előtti hosszát. A fenti példában 2567 bájt hosszú — hexa 0A07 — állományt fertőzött meg a vírus.

M Z

F4 7A 2C 00 00 00 07 0A BE 0A 4D 5A 07 00 06 00

A vírus az eredeti program első 32 bájtyát a víruskód elejétől számított 11. bájttól tartalmazza. Az .EXE program azonosítója, az „MZ” könnyen felismerhető. A fenti információk alapján az eredeti program hossza, fejrészenek információtartalma helyreállítható.

A vezérlés .COM állományok esetén nem ugyanoda kerül, mint .EXE állományok esetén, hanem a vírus elejétől számított 1998. bájtra, vagyis a vírus végére. A program eredeti információi a vírusos program elején levő ugrócímtől visszaszámolva 1998. bájton vannak. Ha megtaláltuk a vírus elejét, akkor a program eredeti információi a vírusban ugyanúgy vannak elhelyezve.

A vírus elején lévő ugrócím — 1998. bájtt.

F4 7A 2C 00 00 00 44 10 BE 0A E9 E1 00 0D 0A 4D

Az eredeti program hossza 4164 bájtt — hexa 1044 — volt a fertőzés előtt. A .COM állomány elején lévő ugróutasítás (jump).

F4 7A 2C 00 00 00 44 10 BE 0A E9 E1 00 0D 0A 4D

A program elején levő eredeti ugrócím. A vírus a .COM programból is 32 bájtnyi információt tárol el magába. A fenti információk alapján az eredeti .COM program helyreállítható.

Iván a rettentő talán Bulgáriából jött? Iván/Victor V.1.0 / Iván

Az Iván vírust Magyarországon először a Kandó Kálmán Villamosipari Műszaki Főiskolán fedezték fel, 1990 januárjában. Ezt követően terjedt el az ország minden területén. A víruskódban elhelyezett szöveg alapján kapta a nevét („Thanks to Ivan.”). És bár szövege szerint szovjet import („This program was imported from USSR.”), nem tartjuk valószínűnek, hogy a vírust a Szovjetunióban írták. A nyugati szakmai körök a kelet-európai országokat úgy tartják nyilván, hogy ott megy a nagy szoftvercserebere, a

meglévő vírusok átírása és új vírusok kifejlesztése. Az amerikai BBS külön állományban részletezi a kelet-európai vírushatárak felbukkanásait és Daniel Karchev bolgár vírusgyártó „kisiparost”. Sajnos a vírusíráshoz szükséges szakmai tudás is megvan.

Az Iván vírus hossza 2442 bájt. A .COM és .EXE állományokat egyaránt megfertőzi. A vírusnak van rezidens része is, amit a normál memóriatérképet (memory map) vizsgáló programok nem mutatnak ki. Ez a vírus nem az elindított állományokat fertőzi meg, hanem az aktuális könyvtár egyes állományain meggy végig sorra. Ha már kellőképpen elterjedt, akkor az egyes programokat „megeszi”, tönkretesz. A vírus fertőzésének ebben a stádiumában az egyes programokat már nem lehet helyreállítani, mert a vírus nem tárolja el az ehhez szükséges információkat. Jelentős károkozásra képes. 1990 tavaszán egyetlen délután sikerült szinte teljesen tönkretennie a Mikro-számítógép Magazin 80 Mbájtos winchesterének tartalmát, amikor a diák-szerkesztőség tagjai a Shotokan játékprogrammal szakközépiskolájukból behurcolták a fertőzést.

A zárt operációs rendszerek a vírusok ellen nagyobb védelmet nyújtanak, mint az egyszerű DOS. Ha a vírus mégis bejut egy zárt rendszerbe, akkor viszont nagyobb pusztítást végez. Így történt akkor is, amikor a miskolci ÉMÁSZ-nál a Novell hálózat alatt működő rendszerük teljesen leült. Két hálózati vezérlőgép (server) esett az Iván vírus áldozatául. Az egyik gépen annyira előrehaladott volt a fertőzés, hogy már nem lehetett a programokat megmenteni.

A vírusprogram nincs kódolva. Nem az elindított programokat fertőzi meg és nem minden program indításánál fertőz. A vírus rezidensen installálja magát a memóriában. A vírus beépülését .EXE program esetén mutatom be. A vírus hozzámásolja magát az állomány végéhez, és a vezérlést önmagára irányítja rá. A vírus első bájtjai a következők:

E8 B1 00 E9 3D 64 40 86 50 11 2A 2E 2A 00 43 4F

A vírus az eredeti programhosszat a vírus elejétől számított 47-48. bájton tárolja:

```

E8 B1 00 E9 3D 64 40 86 50 11 2A 2E 2A 00 43 4F
4D 45 58 45 01 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F
E3 02 00 00 00 00 00 00 00 20 40 86 50 11 3C 23

```

Ebben a példában az eredeti program hossza 9020 bájtt — hexa 233C — volt. A program helyreállításához szükséges további információkat a vírus elejétől számított 64. bájttól találjuk meg:

```

E8 B1 00 E9 3D 64 40 86 50 11 2A 2E 2A 00 43 4F
4D 45 58 45 01 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F
E3 02 00 00 00 00 00 00 00 20 40 86 50 11 3C 23
00 00 46 46 2E 45 58 45 00 20 45 00 58 45 00 18
02 E0 2E 29 BC 47 00 00 00 00 00 00 00 09 23 00

```

Az eredeti .EXE program első 32 bájta:

```

4D 5A 3C 01 12 00 02 00 20 00 F3 02 FF FF 18 02
E0 2E 29 BC 47 00 00 00 1E 00 00 00 01 00 5F 00

```

A program teljes helyreállításához szükséges további információkat a meglévők alapján kiszámíthatjuk.

Egy másik család: a boot-szektor megtámadó vírusok

Magyarországon egyre szélesebb körben terjednek az olyan típusú vírusok, amelyek a DOS számára fenntartott boot-szektor fertőzik meg. Ezzel a módszerrel a vírus a DOS operációs rendszer betöltése előtt rezidenssé válik és az operációs rendszert már a vírus tölti be, ezért a vírusok jelenléte csak akkor észlelhető, ha aktivizálják magukat. A boot-vírusok általában pusztító jellegűek és aktivizálódásuk — jelenlétük észrevétele — során rombolnak is. Hazánkban két ilyen típusú vírus terjedt el 1990 közepéig, az olasz ping-pongozó boot-vírus (Bouncing Ball) és a Disk Killer (Ogre/Disk Killer V.1.00).

A boot-vírusok működési mechanizmusának megértéséhez először vizsgáljuk meg a DOS operációs rendszer működését. A számítógép operációs

rendszerének betöltési folyamata a következőképpen zajlik le:

A gép bekapcsolása után először a BIOS (Basic Input Output System) lefuttatja a számítógép tesztjét (POST — Power On Self Test) majd az „A” floppylemez meghajtójához fordul. Ha ott nem talál lemezt, akkor a merevlemez első, „C” jelölésű partíciós táblájához fordul (angolul — master boot sector) és megnézi, hogy van-e a lemezen operációs rendszer. Ha van, akkor betölti a boot-szektor, majd az operációs rendszert. (A DOS operációs rendszer verziójától függően IO.SYS, MSDOS.SYS).

Ha a betölthető („bootolható”) egységen nincs operációs rendszer, akkor a DOS a boot-szektorból a következő üzenetet jeleníti meg:

Non-system disk or disk error.

Replace and press any key when ready.

(Nem rendszerlemez vagy lemezhiba. Cserélje ki, és nyomjon le egy billentyűt ha készen van.)

A boot-vírust írók az operációs rendszer működését, betöltési folyamatát tökéletesen ismerték. A boot-vírusok azon az elven működnek, hogy megszakítva az operációs rendszer betöltésének folyamatát, önmaguk épülnek be abba. Így a vírusok jelenlétét a felhasználók gyakorlatilag nem veszik észre. Ez az elv olyannyira igaz, hogy amikor egy boot-vírussal fertőzött lemezzől akarjuk az operációs rendszert betölteni, akkor a vírus aktivizálódik és a rendes rendszerüzenetet írja ki. A DOS rendszerüzeneteinek kiírása viszont csak akkor lehetséges, ha a vírus tárolja magába az általa lecserélt információkat, vagy bejegyzi magába, hogy hová helyezte át az eredeti rendszer adatait.

A boot-szektor a DOS 25-ös megszakításával — abszolút szektorolvasás — lehet beolvasni. Ilyenkor a boot-szektor a 0. szektor (vagyis az első elérhető). Ez azonban merevlemez esetén nem így van. (Lásd később a Stoned vírusról.) A boot-szektor beolvasását az úgynevezett 13-as BIOS megszakítással — lemezírás/olvasás — szintén meg lehet tenni. Mivel pedig a BIOS megszakítások egy szinttel közelebbiek a számítógéphez, ezért ezzel a megszakítással a teljes lemeztartalom elérhető. A későbbiek során ennek jelentősége lesz.

A talján ördög: Bouncing Ball / Olasz pingpongozó boot-vírus

A vírus Olaszországból származik. Külföldön először Londonban jelent meg. Írója azonos lehet a Potyogós vírus szerzőjével. Ez a boot-vírus csak az IBM PC/XT számítógépek merevlemezét fertőzi meg, ami arra enged következtetni, hogy egy korábbi generációhoz tartozik, és közvetlen processzorkódot használ. A vírus fertőzése során 1024 bájt hibás szektort jegyez be a FAT-táblába floppylemez és merevlemez esetén is. A boot-vírusok a lemezek egyes szektoraiba épülnek be. Helyüket a lecserélt boot-szektorban tárolják, így az általuk lefoglalt szektorokat hibásan jegyzik be a FAT-táblába. Ezzel a módszerrel nem fordulhat elő olyan eset, hogy a felhasználó más kóddal, más programmal felülírja a víruskódot, ami különben rendszerösszeomlást okozhatna. A vírus az első szabad területre épül be, nem felülírva a lemezegységen található információkat. A fent leírtak alapján láthatjuk, hogy a vírus nem a megszokott módon, nem az állományokhoz épül be, hanem a boot-szektorhoz viszonyítva helyezi el magát. A vírust a floppyn lehet a leghamarabb észrevenni. A floppylemezek formázásakor általában nincsenek hibás szektorok bejelölve. Ha tehát a DOS CHKDSK parancsával ellenőrizzük lemezünket és 1024 bájtot vagy annak többszörösét találjuk hibás szektornak, akkor érdemes a lemezt alaposabban is megvizsgálni. Ha több lemezen találunk egyformán azonos méretűnek jelölt hibás szektort, akkor már majdnem biztosak lehetünk benne, hogy boot-vírusunk van. (Meglepetések ugyanis adódhatnak. Lásd később a Stoned/Marijuana vírusnál.)

A vírus aktivizálódásának megnyilvánulásait leírtuk a vírushatározó fejezetben. Ha a vírus aktív (a memóriában van) és a DOS operációs rendszerből kiadjuk a következő parancsot: „PROMPT \$N”, akkor a lemezen „\$N” nevű 0 bájt hosszú állományt találunk. Ha a „PROMPT \$P” parancsot adjuk ki, majd ezt követően „Time 0” vagy „Time 30” következik, akkor a vírus működésbe lép.

A vírus elhelyezkedése a memóriában a hexa 77C0:7EDF.

A vírusazonosító bájtsorozata:

```
8E D8 A1 13 04 2D 02 00 A3 13 04 B1 06 D3 E0 2D C0
07 8E C0 BE 00 7C 8B FE B9 00 01
```

Ez a vírus volt az első elterjedtebb boot-vírus. A későbbi boot-vírusok működési elve hasonló, azzal a különbséggel, hogy a vírusok már nem a DOS-területre teszik a kódjukat és az eredeti boot-szektor, hanem a DOS által részben kihasználatlan (a Novell által viszont teljesen kihasznált), úgynevezett rejtett területre, sávra (hidden sectors). A Ping Pong vírus az eredeti boot-szektor lecseréli a vírus egy részére, a víruskód további részét és az eredeti boot-szektor hibás (bad) szektorként bejelölt lemezterületen helyezi el. Ezeket az információkat a lecserélt boot-szektorban tárolja. A Ping Pong vírus a hibás szektor információit a lecserélt boot-szektor 506-507. bájtnál tárolja. Ennek megfelelően az eredeti boot-szektor a következőképpen található meg.

$$\text{Virus_további_része} = (506[\dots] + 507[\dots] * 256) + 1$$

A vírus kiírtása az eredeti boot-szektor visszaállításán és a hibásnak bejelölt szektorok felszabadításán múlik.

Gyári szoftverrel érkezett, s majdnem leállt tőle a hazai bankrendszer:Ogre/Disk Killer

Ez a boot-vírus Magyarországon 1989 októberében jelent meg. Egy banki szoftvert gyártó kft. vezetője felkérésére hatástalanítottam és írtam rá az első vírusölő programot (DISKKILL.EXE). Ez a vírus sajnos sok kárt okozott. Szokás szerint nem gyanakodtak arra, hogy a számítógép rendellenességeit vírus okozhatja, és engem (SZ.I.) akkor kerestek meg, amikor egyik nagy bankunknál a hitelkártya kibocsátása előtt ez a vírus már tönkretette adatállományait. A bank is a kft.-t kötelezte a vírus kiírtására. A Disk Killer az NSZK-ból, egy Seagate winchester-szállítmányhoz adott eredeti Disk Manager lemezein érkezett. Valószínűleg a külföldi sokszorosító üzemből történt szabotázs eredményeként került a vírus a lemezre.

A Disk Killer vírus fertőzése során a floppylemezen 3072 bájtnál hibás szektort jelöl be és ide teszi magát. Miután rejtőzködési helyét hibás szektornak álcázza, annak felülírása nem lehetséges. (A vírus működését és üzeneteit részletesen ismertetjük a vírushatározóban, ezért itt nem ismételjük meg.)

A Disk Killer valóban gyilkos program. Ha aktivizálódott, akkor már újra kell formázni a merevlemezt. Remélhetőleg minden fontos programról és adatállományról volt floppyra elmentett biztonsági másolatunk. A vírus aktivizálódása után — az üzenet megjelenésekor — azonnal kapcsoljuk ki számítógépünket! Speciális segédprogramokkal így esetleg megmenthetünk néhány adatállományt. A vírus először a boot-szektor, FAT-táblát és a katalógust (directory) teszi tönkre, írja felül.

Természetesen a vírus eltávolítása során a számítógépet mindig egy nem fertőzött — leragasztott — lemezen lévő operációs rendszerrel kell újraindítani. Jó tudni, hogy a Disk Killer vírus jelenlétét a floppylemezeken a DOS CHKDSK parancsával is egyszerűen ki lehet mutatni. Például: „CHKDSK A:”. Ha a vírus rezidens volt, akkor a parancs lefutása után a floppylemez vírusos lesz, és a CHKDSK program 3072 hibás bájtot vagy ennek többszörösét jeleníti meg. A vírus az 5 1/4"-os, 1,2 Mbájtos floppylemezt rosszul kezeli le, ezért a CHKDSK csak 2560 bájt hibás szektort mutat ki.

A Disk Killer az operációs rendszernek fertőzött floppylemezzel történő betöltésével vagy betöltési kísérletével kerül rá a merevlemezre. A vírus a merevlemezeken nem jelöl be hibás szektorokat, hanem a DOS által fenntartott rejtett sávon (hidden track) búj meg. Az eredeti boot-szektor lecseréli, a vírus további részét és az eredeti boot-szektor a merevlemez 0. fejének 0. sávjának utolsó 6 szektorára teszi. Az eredeti boot-szektor a 0. fej 0. sáv utolsó szektorán van.

A 360 kbájtos, 5 1/4"-os floppylemez fertőzése esetén a vírus az eredeti boot-szektor lecseréli, a további víruskódot és az eredeti boot-szektor 3072 bájt terjedelmű hibás szektorban tárolja. A hibás szektorra történő ugrás miatt ennek értékét a lecserélt boot-szektorban feljegyzi. Az eredeti boot-szektor így a következőképpen található meg:

```
Virus_további_rése=25[...]+26[...]*256
```

Az 1,2 Mbájtos, 5 1/4"-os floppylemezt a vírus hibásan kezeli, ezért az eredeti boot-szektor nem tárolja. Ebben az esetben a hibásnak bejelölt szektorok száma 5 vagyis 2560 bájt. Erről a lemezzel nem lehet a vírust a hagyományos módon kiirtani, mivel nem tárolja az eredeti boot-szektor.

Új vírusgeneráció: támadás a partíciós tábla ellen

Magyarországon 1990 január-februárjától egyre szélesebb körben terjedt el egy akkor még ismeretlen elven működő vírus. Ez a DOS számára fenntartott partíciós táblát fertőzi meg. Ezzel a módszerrel a vírus már a DOS operációs rendszer betöltése előtt (BIOS szinten) rezidenssé válik, és az operációs rendszert maga a vírus tölti be. Ebben az esetben a vírusok jelenléte már csak akkor észlelhető, ha aktivizálják magukat. A boot- és a partíciós tábla vírusok ilyenkor általában már rombolnak is. Hazánkban egy ilyen típusú vírus terjedt el 1990 elején, a Stoned/Marijuana.

A partíciós táblát megtámadó vírusok működési mechanizmusának megértéséhez először vizsgáljuk meg a DOS operációs rendszer működését és betöltési folyamatát.

A számítógép bekapcsolása után az EPROM-ba égetett mikroprogram lefutásával indul a számítógép működése. A BIOS-ban lévő mikroprogram először a partíciós táblát olvassa be. Ekkor még a DOS operációs rendszer betöltéséről szó sincs. Mivel a partíciós tábla az első „bootolható” szektor, ezért ezt „master boot” (fő betöltő) szektornak nevezik. A BIOS ebből a szektorból olvassa ki, hogy melyik partíció az aktív, amelyikről a DOS operációs rendszert be kell tölteni. Ha a partíciós tábla hibás információkat vagy nem megfelelő operációs rendszert talál, akkor a következő üzenetet jeleníti meg:

Invalid partition table.

Error loading operating system.

Missing operating system.

(Érvénytelen partíciós tábla. Az operációs rendszer betöltési hibája. Hiányzó operációs rendszer.)

A partíciós tábla vírusok azon az elven működnek, hogy megszakítva az operációs rendszer betöltési folyamatát — amit a BIOS végez —, beépülnek abba. Így a vírusok jelenlétét a felhasználók gyakorlatilag nem veszik észre. Sőt az aktív vírus a normális rendszerüzenetet írta ki. Ezt úgy tudja megtenni, hogy tárolja magában a lecserélt információkat, vagy bejegyzí önmagába azt, hogy hová helyezte át az eredeti rendszer adatait.

A Stoned/Marijuana vírus 1990 január-februárjában Magyarországon igen gyorsan elterjedt, ami jellemző minden új elven működő vírusra. (Leírását lásd a vírushatározó fejezetben.) Magyarországi átirói főleg az üzenetek szellemeskedő aktualizálásával foglalkoztak. Például:

„Your computer is now stoned. Legalize MSZMP”

A Magyarországon elterjedt Stoned vírus egyaránt fertőz floppylemezt és merevlemezt is. Csak az „A” meghajtóba helyezett floppylemezt fertőzi meg, függetlenül annak típusától és kapacitásától. A vírus lecseréli az eredeti boot-szektorát önmagára, és az eredeti boot-szektorát a katalógusba — az 1. fej 0. sáv 3. szektorára — helyezi át. Ha a vírus által áthelyezett terület foglalt volt, akkor az ott lévő adatok elérhetetlenek lesznek, ha pedig később töltjük fel a lemezt, akkor az használhatatlanná válik. Merevlemez fertőzése esetén a vírus a partíciós táblát cseréli le és az eredetinek a szektorát a 0. fej 0. sáv 7. szektorára helyezi át. Önállóan működő (nem hálózati) merevlemezű PC-k esetén a fenti szektor kihasználatlan, tehát a vírus nem okoz kárt.

Nem különvonalas (non-dedicated) Novell üzemmódban történő használata esetén a Stoned vírus meg tudja fertőzni az adagoló (server) gép merevlemezét. Ez a fertőzés a Novell rendszerállományának felülírásával jár, ami a Novell-rendszer megsérülését eredményezi. Ha a Stoned vírust nem távolítjuk el a merevlemezről, akkor a Novell hálózati szoftver nem telepíthető újra. A Novell-rendszer adatvesztés nélküli helyreállítása csak pontos vírusismeretek birtokában történő rendszerprogramozói beavatkozással lehetséges.

Egyik honvédségi intézményünkénél a Stoned vírus Novell-rendszert tett tönkre, amit egy hardveres kollégának folyamatos konzultációs segítséggel sikerült megszüntetnie, és a rendszert újraélesztette. A dolognak az a szépséghibája, hogy azóta több helyen is tartottak tanfolyamokat, és tudtukon kívül tovább terjesztették a vírust. El lehet képzelni, mi történt volna akkor, ha a vírus nem jelezte volna jelenlétét minden 8. rendszerindításra. A vírusok kiengedésük után kontrollálatlanok lesznek. Ezért oktatáskor más gépen soha semmilyen körülmények között nem használunk még bemutatásra sem vírust. Az ilyen bemutatókat mindig jelszóval többszörösen védett, hordozható

laptop géppel végezzük. Oktatási munkánk megkönnyítésére készítettük el vírusdemó lemezünket. Az ezen található programok az ismert vírusok viselkedését szimulálják, de bármiféle károkozás és szaporodás nélkül!

És futottak még...

Minden nagy hardver- és szoftvergyártó „lyukasra” tervezi termékeit. A széles körhöz eljutó publikációkban nem jelennek meg részletes és pontos dokumentációk. (Lásd DOS.) De nemcsak az „egyszerű” szoftvereket készítik el „lyukakkal”, hanem a fejlesztés megkönnyítésére a nagyobb rendszereket is. Ilyen a Novell hálózati rendszer is. S éppen egy ilyen „lyukon” keresztül lehet visszanyerni a Műszertechnika egyik segédprogramjával a megrongálódott server gép merevlemez-állományainak jó részét.

Hasonlóak az egyes szintekhez való hozzáférést engedélyező, gyárilag beépített jelszavak is (password). Most folyik a hajtóvadászat a Novell egyik ilyen rejtett utasításának megfejtésére. Néhány programozó már rájött, de gondosan titkolja, hogy milyen — természetesen illogikus — billentyűkombináció lenyomásával lehet minden bejelentkezési procedura nélkül supervisorsként bejutni a rendszerbe. Ezek az utasítások nemcsak a programozó életét könnyítik meg, hanem „vészkijáratot” hagyva a munka biztonságát is növelik — egészen addig, amíg ezzel a lehetőséggel nem élnek vissza.

A Novell sincs védve a programvírus-fertőzésekkel szemben — bár maga az egyik leginkább immunis szoftver. A hazánkban közismert „Poty” vírusnak létezik egy kifejezetten Novell környezetre írt változata, amely nyilvánvalóan magyar fejlesztés. Ebben a víruskód eredeti, amit a „tréfacsináló” megfejtelt néhány rutinnal. Nemcsak a COMMAND.COM-ot fertőzi meg, hanem a Novell közösen használt és minden programmal érintkezésbe kerülő billentyűzetvezérlő rutinját is. Így a Novell azon védelme, hogy a programokhoz fizikailag is csak a jogos felhasználót engedi hozzáférni, nem védi meg a vírustól a többi felhasználó programjait. Szerencsére a kód jelentős hasonlósága miatt a fertőzés leküzdhető.

Más vírusok is be tudnak jutni a Novell rendszerébe. Elegendő megfertőzni a mindenki által használt Login programot, s a vírus bármely felhasználó bejelentkezésénél aktivizálódhat. Ha a vírus a memóriában van, akkor már könnyű a dolga. A másik fertőzési mód, ha a vírust a Novell generáló

programcsomagjába teszik, és ezzel minden generált Novell vírusos lesz.

Végül néhány szót egy egészen speciális magyar vírusról. A Haltguard vírus egyes magyar szoftverek terméke egyes magyar szoftverek ellen. A harc Robin Hood-i módszerekkel folyik. Ha a vírus felismeri a célba vett copyright jelzést vagy az annak szerzője által alkalmazott standard eljárást — például másolás elleni védelmet —, akkor igen egyszerű trükkel teszi tönkre az eredeti szoftvert, hogy az ne működjön. Vagy csak egy ugróutasítást ír be, ami a program végére mutat, vagy pedig megcseréli az első két bájtot. Így a gép a program indításakor lefagy, a program CRC ellenőrző algoritmus (cyclic redundancy check) viszont megmarad. Más programokra a vírus ártalmatlan. Főleg Győr környékén fordult elő. Ha bizonyos ideig nem találkozik áldozatával, akkor kiiktatja önmagát. Várható, hogy éppen ezért esetleg teljesen eltűnik. A vírus az egyik magyarázat szerint onnan kapta nevét, hogy ha a szoftver előzőleg „ÉLT”, akkor a vírussal történő találkozása után „megHALT”. Bár ilyen logikával a nevet sok más vírus is joggal viselhetné.

```
file: PELDA1.COM DANGER !!! Virus v2.0 found ! Strike any key !
```

```
file: PELDA2.COM DANGER !!! Virus v2.0 destroyed this file !  
Do you want to delete this file ? y/n
```

```
A Virus v2.0 Reboot tönkretette ezt a file-t.  
Törli ezt a file-t ? y/n
```

Ha a CHKVir nem tudja helyreállítani az állományt,
akkor rákérdezés után törli azt

A VÍRUSOK ÖSSZEFOGLALÓ TÁBLÁZATA

A MCAFEE ASSOCIATES 1989. MÁJUSI LISTÁJA ALAPJÁN

A vírusok felsorolása a McAfee-féle egységes referencianevekkel történt. A táblázatban betűjelzések mutatják, hogy a vírusok a gép és a programok mely részére veszélyesek. A gömbölyű zárójelben található, hogy a külföldi szakirodalom — főleg a nyugat-európai és az amerikai előfordulás alapján — hány olyan vírusváltozatot ismer, amely ugyanazzal az eljárással ismerhető fel, de nem mindig írtható ugyanazzal a módszerrel. A szögletes zárójelben található rövidítés a McAfee által javasolt rövidített kód, amely a számítógépes nyilvántartásra, illetve a vírusirtó programokban való azonosításra szolgál. További jelmagyarázat:

A vírus fertőzési módjára és viselkedésére utaló jelölések:

x = Igen

. = Nem

A károkozás oszlopába írt betűk jelentése:

B = Károsítja vagy felülírja a boot-rekordot

O = Az operációs rendszer működését befolyásolja

P = Program- vagy overlay-állományokat károsít vagy felülír

D = Adatállományokat károsít vagy felülír

F = A merevlemezt, a floppyt vagy azok egyes részeit formázza

L = Közvetlenül vagy közvetve rossz állománykapcsolatokat okoz

Egyéb jelölések:

N/A = nincs adott hossz vagy nem jellemző

* = A rejtett, másképpen „stealth” technikát használó vírusok az utóbbi időben jelentek meg. Nem a hagyományos módon válnak rezidenssé, illetve a DOS számára az állomány eredeti állapotát mutatják meg

** = Névváltozás

*** = Eredeti magyar vírus

Fertőzi a merevlemez partíciós tábláját-----+
 Fertőzi a merevlemez boot-szektorát-----+ |
 Fertőzi a floppy boot-rekordját-----+ | |
 Overlay-állományokat fertőz-----+ | | |
 .EXE állományokat fertőz-----+ | | | |
 .COM állományokat fertőz-----+ | | | | |
 A COMMAND.COM-ot fertőzi-----+ | | | | | |
 Rezidens része marad a tárban-.--+ | | | | | | |
 A víruskódot „titkosítja” ----+ | | | | | | | |
 Hagyományosan rejtett * ----+ | | | | | | | | |

										Mennyivel
										növeli
										a fertőzött
										program
										méretét

Vírusnév	V	V	V	V	V	V	V	V	V	V	V	Károkozás
----------	---	---	---	---	---	---	---	---	---	---	---	-----------

AIDS (3) [Aids] x	Felülír!		
AirCop [AirCop]	. . x x . .	N/A	B,O	
Alabama (2) [Alabama]	. . x . . x	1560	O,P,L	
Alameda (2) [Alameda]	. . x x . .	N/A	B	
Amstrad (5) [Amst] x	847	P	
Anthrax - Boot [Atx]	. . x x	N/A	O,P,D	
Anthrax - File [Atx]	. . x x x x	1206	O,P,D	
Armagedon [Arma]	. . x x x	1079	O,P	
Ashar [Brain]	. . x x . .	N/A	B	
Brain (3) [Brain]	. . x x . .	N/A	B	
Cascade-B (9) [170x]	. x x . x	1704	O,P	
Chaos [Chaos]	. . x x x .	N/A	B,O,D,F	
Dark Avenger (2) [Dav]	. . x x x x x . . .	1800	O,P,L	
Datacrime (2) [Crime]	. x . . x	1280	P,F	
Datacrime-B [Crime-B]	. x . . x	1168	P,F	

A VÍRUSOK ÖSSZEFOGLALÓ TÁBLÁZATA

Datacrime II [Crime-2]	. x . . x x	1514	P, F
Datacrime II-B [Crime-2]	. x . x x x	1917	P, F
Dbase [Dbase]	. . x . x	1864	D, O, P
Den Zuk (3) [Zuk]	. . x x . .	N/A	O, B
Devil's Dance [Dance]	. . x . x	941	D, O, P, L
Disk Killer (2) [Killer]	. . x x x .	N/A	B, O, P, D, F
Do-Nothing [Nothing]	. . x . x	608	P
Doom2 [Dm2]	. . x . x x	2504	O, P, D, L
EDV (2) [EDV]	x . x x x x	N/A	B, O
Fellowship [Fellow]	. . x . . x	1022	O, P, D, L
Fish-6 [Fish]	x x x x x x x . . .	3584	O, P, L
Flash [Flash]	. . x x x x	688	O, P, D, L
Flip [Flip]	. x x x x x x . . .	2343	O, P, D, L
Form [Form]	. . x x x .	N/A	B, O, D
Frere Jacques [Frere]	. . x . x x x . . .	1811	O, P
Friday 13th COM [Fri13] x	512	P
Fu Manchu (2) [Fu]	. . x . x x x . . .	2086	O, P
Ghost Boot [Ghost]	. . x x x .	N/A	B, O
Ghost COM [Ghost] x	2351	B, P
Icelandic (2) [Ice]	. . x . . x	642	O, P
Icelandic II [Ice-2]	. . x . . x	661	O, P
Icelandic-3 [Ice-3]	. . x . . x	853	O, P
ItaVir [Ita] x	3880	O, P, L, B
Jerusalem (9) [Jeru]	. . x . x x x . . .	1808	O, P
Jerusalem-B [Jeru]	. . x . x x x . . .	1808	O, P
JoJo [JoJo]	. . x . x	1701	O, P
Joker [Joke]	. . x x x		O, P
Joshi [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
Kennedy [Kennedy]	. . x . x	308	O, P
Korea (2) [Korea] x x . . .	N/A	B, O
Kukac ***	. . . x x	448	O
Lehigh [Lehigh]	. . x x	Felülir!	P, F

Leprosy	. . x x x x x . . .	Felülír!	
Liberty [Liberty]	. . x x x x x . . .	2862	O,P
Lisbon (2) [Lisb] x	648	P
Mardi Bros. [Mardi]	. . x x x .	N/A	B,O
Microbes [Micro]	. . x x x .	N/A	B,O,D
MIX1 [Ice]	. . x . . x	1618	O,P
Murphy [Murphy]	. . x x x x x . . .	1277	O,P
New Jerusalem [Jeru]	. . x . x x x . . .	1808	O,P
Ohio [Ohio]	. . x x . .	N/A	B
Ontario [Ont]	. x x x x x	Változik	O,P,D
Oropax (3) [Oro]	. . x . x	2773	P,O
Pakistani Brain **	. . x x . .	N/A	B
Payday [Payday]	. . x . x x x . . .	1808	P
Perfume (2) [Fume] x	765	P
Pentagon [Pentagon] x . . .	N/A	B
Ping Pong-B (2) [Ping]	. . x x x .	N/A	O,B
Ping Pong (3) [Ping]	. . x x . .	N/A	O,B
Plastique (3) [Plq]	. . x x x x x . . .	3012	O,P,D
Polimer ***	. . . x x	512	O,ú
Print Screen [Prtscr]	. . x x x .	N/A	B,O,D
P1 (3) [Plr]	. x x . x	Változik	O,P,D,L
RedX [Redx]	. . . x x	796	O,P
Saratoga [Ice]	. . x . . x	632	O,P
Saturday 14th [Sat14]	. . x . x x x . . .	685	F,O,P,L
Shake [Shake]	. . x . x	476	O,P
Slow [Slow]	. x x . x x x . . .	1721	O,P,L
Solano (2) [Solano]	. . x . x	2000	O,P,L
Sorry [Sorry]	. . x x x	731	O,P
Stoned/Marijuana (2) [Stoned]	. . x x . x	N/A	O,B,L
Stoned-II [Stoned]	. . x x . x	N/A	O,B,L
Subliminal [Sub]	. . x x x	1496	O,P
Sunday (2) [Sunday]	. . x . x x x . . .	1636	O,P
Surv01 [SurvA]	. . x . x	897	O,P
Surv02 [SurvA]	. x . . x	1488	O,P

A VÍRUSOK ÖSSZEFOGLALÓ TÁBLÁZATA

Suriv03 [SurivB]	. . x . x x x . . .		O, P
Sylvia/Holland [Holland] x	1332	P
Swap Boot [Swap]	. . x x . .	N/A	B
Taiwan (2) [Taiwan] x	708	P
Taiwan3 [T3]	. . x x x x x . . .	2905	O, P, D, L
TCC [TCC]	. . . x x x x . . .	4909	O, P, D, L
Tiny (7) [Tiny]	. . . x x	163	O, P
Töltőgető/Fill *** x x x	N/A	B, P
Turbo Kukac ***	. . . x x	512	O
Typo/Fumble [Typo]	. . x . x	867	O, P
Typo Boot [Typo]	. . x x x .	N/A	O, B
Traceback (2) [3066]	. . x . x x	3066	P
Vacsina (2) [Vacs]	. . x . x x x . . .	1206	O, P
Vacsina V05	. . x . x x x . . .	1217	O, P
Vacsina V16	. . x . x x x . . .	1530	O, P
Vacsina V24 [Vacs]	. . x . x x x . . .	1760	O, P
Vcomm (3) [Vcomm] x	1074	O, P, L
Victor [Victor]	. . x x x x x . . .	2458	P, D, L
Vienna-B [Vienna] x	648	P
Vienna/648 (14) [Vienna] x	648	P
Virus-90 [90]	. . x . x	857	P
Virus-101 [101]	. x x x x x x x . .	2560	P
V800 [V800]	x x x . x	None	O, P, L
V2000 (3) [2000]	. . x x x x x . . .	2000	O, P, L
V2100 [2100]	. . x . x x	2100	O, P, D, L
Wolfman [Wolf]	. . x x x x	2064	O, P
W-13 (2) [W13] x	532	O, P
XA1 [XA1]	. x . . x	1539	F, O, P, L
Yankee Doodle (3) [Doodle]	. . x . x x	2885	O, P
Yankee Doodle v1	. . x . x x	2890	O, P
Yankee Doodle v2	. . x . x x	2940	O, P
Yankee Doodle v3	. . x . x x	2772	O, P
Yankee - 2 [Doodle2] x x	1961	O, P
Yankee - H 3 ** x x	2932	O, P

Yankee - H 4 ** x x	2941	O,P
400 (5) [400]	. . x . x	Változik	O,P,D
405 [405] x	Felülír!	
512 (4) [512]	x . x x x	None	O,P,L
651 [651]	. . x . x	651	O,P,D
1008 [1008]	. x x x x	1008	O,P,D,L
1024 [1024]	. . x x x	1024	O,P
1210 [1210]	. . x . x	1210	O,P,L
1226 (3) [1226]	. x x x x x x . . .	1226	O,P,D
1253 - Boot [1253]	. . x x x x	N/A	O,P,D,L
1253 - COM [1253]	. . x x x	1253	O,P,D,L
1260 [1260]	. x . . x	1260	P
1381 [1381] x x . . .	1381	O,P
1392 [1392]	. . x x x x	1392	O,P,L
1536/Zero Bug [Zero]	. . x . x	1536	O,P
1559 [1559]	. . x x x x	1554	O,P,L
1701/Cascade [170x]	. x x . x	1701	O,P
1704/Cascade [170x]	. x x . x	1704	O,P
1704 Format [170x]	. x x . x	1704	O,P,F
1720 [1720]	. . x . x x x . . .	1720	F,O,P,L
1971/8 Tunes [1971]	. . x . x x x . . .	1971	O,P
2930 [2930]	. . x . x x	2930	P
3551/Syslock [Syslock]	. x . . x x	3551	P,D
4096 (2) [4096]	x . x x x x x . . .	4096	D,O,P,L
5120 (2) [5120]	. . . x x x x . . .	5120	O,P,D,L

Összeállította és átdolgozta az Ázsió-Viki vírusellenes csoportja.

Vírus-szaktanácsadás:

Ázsió-Viki, 1065 Budapest, VI., Bajcsy-Zsilinszky út 3. IV. em.

Tel.: 142-0176, 122-3025, 122-9061, 122-2619. Fax.: 142-3765.

KERESZTREFERENCIA-TÁBLÁZAT

A táblázatot részben szakirodalmi azonosításra tudjuk felhasználni, részben gyakorlati eligazodásra, amikor szeretnénk megtudni, hogy a kereskedelemben és a szoftverkommuna csatornáiban fellelhető programcsomagok valójában milyen vírusok ellen hatásosak. Az első, betűrendes oszlop elnevezései mellett a második oszlopban az a főcím szerepel, amely alatt az adott vírus a részletes leírásban megtalálható. Ha e táblázat alapján azonosítani tudjuk a vírusnevet, akkor a határozótáblából kikereshetjük a vírus főbb ismérveit, a részletes leíró részben pedig megnézhetjük, hogy mire számíthatunk...

Összeállításunkban nem törekedhattünk teljességre. Elsősorban azokat a neveket vettük fel, amelyek a vírusleíró szakmunkákban, újságcikkekben vagy egyéb közleményekben a leggyakrabban előfordulnak. A tábla remélhetőleg segít majd eligazodni a vírusnevek kavalkádjában.

Vírusnév	McAfee-féle egységes referencianév
----------	---------------------------------------

A

AIDS	AIDS
AIDS Trojan Inf.	AIDS Trojan Information
AirCop	AirCop
Alabama	Alabama
Alameda	Alameda
Amstrad	Amstrad
Anthrax-Boot	Anthrax-Boot
Anthrax-File	Anthrax-File
April 1st	Surv 1.01
April 1st-B	Surv 2.01
Armagedon	Armagedon

Ashar	Ashar
Austrian	Vienna
Austrian #2	Cascade

B

Barcelona	Barcelona
Black Avenger	Dark Avenger
Black Friday	Jerusalem
Blackjack	Cascade-B
Boot	Ping Pong-B
Bootkiller	Disk Killer
Bouncing Ball	Ping Pong
Bouncing Dot	Ping Pong

C

(C) Brain	Brain
Cascade	Cascade
Cascade-B	Cascade-B
Century	4096 virus
Chaos	Chaos
Christmas virus	Christmas
Columbus Day	Datacrime, Datacrime II, Datacrime IIB, Datacrime-B
COM	Friday The 13th COM
Computer Ogre	Disk Killer

D

Dark Avenger	Dark Avenger
Datacrime	Datacrime
Datacrime II	Datacrime II
Datacrime IIB	Datacrime IIB
Datacrime-B	Datacrime-B
DBase	DBase
December 24th	Icelandic-III

Den Zuk	Den Zuk
Devil's Dance	Devil's Dance
Disk Crunching	Icelandic, Saratoga
Disk Killer	Disk Killer
Disk Ogre	Disk Killer
Do-Nothing	Do-Nothing
Doom2	Doom2
DOS-62	Vienna
DOS-68	Vienna

E

Eddie	Dark Avenger
EDV	EDV

F

Fall	Cascade
Falling Letters	Cascade, Ping Pong-B
Falling-Letters Boot	Swap Boot
Felllowship	Felllowship
Filler	Töltögető
Fish-6	Fish-6
Flash	Flash
Flip	Flip
Form	Form
Frere Jaques	Frere Jaques
Friday 13th	Jerusalem
Friday 13th COM	Friday The 13th COM
Fu Manchu	Fu Manchu
Fumble	Typo COM
Frodo	4096

G

Ghost Boot	Ghost Boot
Ghost COM	Ghost COM

Ghostballs	Ghost Boot, Ghost COM
Golden Gate	Golden Gate

H

Hahaha	AIDS
Halloeichen	Halloeichen
Hawaii	Stoned
Herbst	Cascade
Hiding	4096
Holland Girl	Holland Girl

I

Ice	Mix1
Icelandic	Icelandic
Icelandic-II	Icelandic-II
Icelandic-III	Icelandic-III
Israeli	Jerusalem, Surv 1.01, 2.01, 3.00
Israeli Boot	Swap
Italian	Ping Pong
ItaVir	ItaVir
Ivan	Victor

J

Jerusalem	Jerusalem
Jerusalem-A	Jerusalem
Jerusalem-B	Jerusalem
Jerusalem-C	Jerusalem
Jerusalem-D	Jerusalem
Jerusalem-E	Jerusalem
JoJo	JoJo
Joker	Joker
Joshi	Joshi
July 13th	July 13th
June 16th virus	Pretoria

K

Kennedy	Kennedy
Korea	Korea
Kukac	Kukac

L

Lehigh	Lehigh
Leprosy	Leprosy
Liberty	Liberty
Lisbon	Lisbon

M

Machosoft	Machosoft
Mardi Bros.	Mardi Bros.
Marijuana	Stoned
Mazatlan	Golden Gate
Merritt	Alameda
Mexican	Devil's Dance
Miami	Friday The 13th
Microbes	Microbes
MisSpeller	Typo Boot
Mistake	Typo Boot
MIX1	MIX1
MIX/1	MIX1
Munich	Friday The 13th COM Virus
Murphy	Murphy
Music	Yankee Doodle-B
Music Virus	Oropax
Musician	Oropax

N

Netherlands Girl	Holland Girl
New Jerusalem	New Jerusalem

New Zealand

Stoned

O

Ogre

Disk Killer

Ohio

Ohio

One In Eight

Vienna

One In Ten

Icelandic, Icelandic-II

One In Two

Saratoga

Ontario

Ontario

Oropax

Oropax

Ö

Ötörai tea

Yankee Doodle

P

Pakistani

Brain

Pakistani Brain

Brain

Palette

Zero Bug

Payday

Payday

Peking

Alameda

Pentagon

Pentagon

Perfume

Perfume

Ping Pong

Ping Pong

Ping Pong-B

Ping Pong-B

Plastique

Plastique

PLO

Jerusalem

Polimer

Polimer

Poty #1

Cascade

Poty #2

Cascade-B

Potyogós Command.com

Cascade

Pretoria

Pretoria

Print Screen

Prtscr

R

Reboot vírus	Vienna-B
RedX	RedX
Rendszerhívó vírus	Vienna-B
Russian	Jerusalem

S

San Diego	Stoned
Saratoga	Saratoga
Saturday 14th	Saturday 14 th
Search	Den Zuk
Seoul	Alameda
SF	SF
Shake	Shake
Shoe_Virus	Ashar
Shoe_Virus-B	Ashar-B
Slow	Slow
Smithsonian	Stoned
Solano	Solano
Sorry	Sorry
South Africa	Pretoria
South African	Friday Thé 13th COM Virus
Spanish	2930 virus
Spanish II	1720 virus
Stoned	Stoned
Stoned II	Stoned II
Stupid	Do-Nothing
Subliminal	Subliminal
Sunday	Sunday
Sunny	Taiwan
Sylvia	Holland Girl
System	Icelandic-II
Syslock	3551

Surv 1.01	Surv 1.01
Surv 2.01	Surv 2.01
Surv 3.00	Surv 3.00
Surv01	Surv 1.01
Surv02	Surv 2.01
Surv03	Surv 3.00
Swap	Swap
SysLock	Syslock

T

Taiwan	Taiwan
Taiwan3	Taiwan3
Taunt	AIDS
TCC	TCC
Tiny	Tiny
Töltögető	Töltögető
Tuesday 1st	Tuesday 1st virus
Turbo Kukac	Turbo Kukac
Traceback	Traceback
Traceback II	Traceback II
Typo Boot	Typo Boot
Typo COM	Typo COM

U

UIUC Virus	Ashar
UIUC Virus-B	Ashar
Unesco	Vienna

X

XAl virus	Christmas
-----------	-----------

Y

Yale	Alameda
Yankee Doodle	Yankee Doodle

KERESZTREFERENCIA-TÁBLÁZAT

Yankee Doodle-B

Yankee Doodle-B

V

Vacsina

Vacsina

Vacsina-B

Vacsina-B

Vcomm

Vcomm

Venezuelan

Den Zuk

Vera Cruz

Ping Pong

VGA2CGA

AIDS

Victor

Ivan

Vienna

Vienna

Vienna-B

Vienna-B

Virus-90

Virus-90

Virus101

Virus101

V800

V800

V2000

V2000

V2100

V2100

Victor

Victor

W

Wolf

Wolfman

Wolfman

Wolfman

W13

W13

Z

Zenélő vírus

Vacsina-B

Zero Bug

Zero Bug

Kódnevűek

4K

4096

5 Pm tee

Yankee Doodle

62-B

Vienna-B

100 Years virus

4096 virus

400

400

405	405
500	Golden Gate
512	Friday The 13th COM
632	Saratoga
640K COM virus	Do-Nothing
642	Icelandic
648	Vienna
651	651
765	Perfume
867	Typo COM
1008	1008
1024	1024
1168	Datacrime-B
1210	1210
1226	1226
1253-Boot	1253-Boot
1253-Com	1253-Com
1260	1260
1280	Datacrime
1381	1381
1392	1392
1514	Datacrime II
1536	Zero Bug
1636	Sunday
1701	Cascade
1704	Cascade, Cascade-B
1704 Format	1704 Format
1704-B	Cascade-B
17Y4	17Y4
1720	1720
1808	Jerusalem
1813	Jerusalem
1917	Datacrime IIB
1971/8	Tunes

KERESZTREFERENCIA-TÁBLÁZAT

2080	Fu Manchu
2086	Fu Manchu
2351	Ghost COM
2930	Traceback II
3066	Traceback
3551	SysLock
4096	4096
4711	Perfume
5120	5120

VÍRUSHOSSZ

REFERENCIATÁBLÁZAT

Egyéb eszközök hiányában a régebbi családokba tartozó vírusoknál sok esetben meg tudjuk állapítani, hogy a fertőzött állományok milyen hosszal nőttek meg. A diagnosztizálásban ilyenkor segít a vírushossz referenciatáblázata, amely azt mutatja meg, hogy az ismert fájlvírusokkal történő egyszeri fertőzés esetén mennyivel nő meg az állomány hossza. Ez a táblázat az összefoglaló adatokkal és a könyv leíró részeiben foglaltakkal együtt segít meghatározni a fertőzést okozó programvírust.

Hossz:	Név:	Azonosító jel:
163	Tiny (7)	[Tiny]
308	Kennedy	[Kennedy]
400	400 (5)	[400]
405	405	[405]
448	Kukac	
476	Shake	[Shake]
512	Polimer	
512	Turbo Kukac v9.9	
512	512 (4)	[512]
512	Friday 13th COM	[Fri13]
532	W-13 (2)	[W13]
608	Do-Nothing	[Nothing]
632	Saratoga	[Ice]
642	Icelandic (2)	[Ice]
648	Lisbon (2)	[Lisb]
648	Vienna/648 (14)	[Vienna]
648	Vienna-B	[Vienna]
651	651	[651]
661	Icelandic II	[Ice-2]
685	Saturday 14th	[Sat14]

688	Flash	[Flash]
708	Taiwan (2)	[Taiwan]
731	Sorry	[Sorry]
765	Perfume (2)	[Fume]
796	RedX	[Red]
800	V800	[V800]
847	Amstrad (5)	[Amst]
853	Icelandic-3	[Ice-3]
857	Virus-90	[90]
867	Typo/Fumble	[Typo]
897	Surviv01	[SurvivA]
941	Devil's Dance	[Dance]
1008	1008	[1008]
1022	Fellowship	[Fellow]
1024	1024	[1024]
1074	Vcomm (3)	[Vcomm]
1079	Armagedon	[Arma]
1168	Datacrime-B	[Crime-B]
1201	July 13th	[J13]
1206	Anthrax - File	[Atx]
1206	Vaccina (2)	[Vacs]
1210	1210	[1210]
1217	Vaccina V05	
1226	1226 (3)	[1226]
1253	1253 - Boot	[1253]
1253	1253 - COM	[1253]
1260	1260	[1260]
1277	Murphy	[Murphy]
1280	Datacrime (2)	[Crime]
1332	Sylvia/Holland	[Holland]
1381	1381	[1381]
1392	1392	[1392]
1488	Surviv02	[SurvivA]
1496	Subliminal	[Sub]

1514	Datacrime II	[Crime-2]
1530	Vaccina V16	
1536	1536/Zero Bug	[Zero]
1539	XA1	[XA1]
1554	1559	[1559]
1560	Alabama (2)	[Alabama]
1618	MIX1	[Ice]
1636	Sunday (2)	[Sunday]
1961	Yankee - 2	[Doodle2]
1701	1701/Cascade	[170x]
1701	JoJo	[JoJo]
1704	1704/Cascade	[170x]
1704	Cascade-B (9)	[170x]
1704	1704 Format	[170x]
1720	1720	[1720]
1721	Slow	[Slow]
1726	June 16th	[June16]
1760	Vaccina V24	[Vacs]
1800	Dark Avenger (2)	[Dav]
1808	Jerusalem (9)	[Jeru]
1808	Jerusalem-B	[Jeru]
1808	New Jerusalem	[Jeru]
1808	Payday	[Payday]
1811	Frere Jacques	[Frere]
1864	Dbase	[Dbase]
1917	Datacrime II-B	[Crime-2]
1971	1971/8 Tunes	[1971]
2000	Solano (2)	[Solano]
2000	V2000 (3)	[2000]
2064	Wolfman	[Wolf]
2086	Fu Manchu (2)	[Fu]
2100	V2100	[2100]
2343	Flip	[Flip]
2351	Ghost COM	[Ghost]

2458	Victor	[Victor]
2504	Doom2	[Dm2]
2560	Virus-101	[101]
2772	Yankee Doodle v3	
2773	Oropax (3)	[Oro]
2862	Liberty	[Liberty]
2885	Yankee Doodle (3)	[Doodle]
2890	Yankee Doodle v1	
2905	Taiwan3	[T3]
2930	2930	[2930]
2932	Yankee - H 3	
2940	Yankee Doodle v2	
2941	Yankee - H 4	
3012	Plastique (3)	[Plq]
3066	Traceback (2)	[3066]
3551	3551/Syslock	[Syslock]
3584	Fish-6	[Fish]
3880	ItaVir	[Ita]
4909	TCC [TCC]	
4096	4096 (2)	[4096]
5120	5120 (2)	[5120]

VÍRUSSZIGNATÚRÁK

Az alábbiakban a vírusok felismeréséhez használt alapvető azonosító sztringeket, az úgynevezett vírusszignatúrákat adjuk meg a HTScan szabad-szoftver és a hasonló elven működő többi program által használt formában. A vírusnév előtti pontosvesszőt elhagytuk. (Megjegyzendő, hogy néhány itthon nem ismert vírusnak csak az azonosító szekvenciáját ismerjük. Más ismérvek azonosításához használja többi táblázatunkat is!) A víruspánik bekövetkeztekor az IBM cég terjesztett az USA-ban, Mexikóban és Venezuelában egy SCAN.EXE (illetve VIRSCAN.EXE) nevű szekvenciális víruskereső programot. Hasonló módon az is egy .LST kiterjesztésű ASCII állományban tárolta a keresési szekvenciákat. A megszokottól eltérő szekvenciákat IBM-SCAN megjegyzéssel közöljük, s mivel e szekvenciák kiválasztása sok bizonytalanságot tükröz, csak tájékozódásra ajánljuk.

Három sor tartozik egy vírushoz. Az első egy legfeljebb 30 karakter hosszú elnevezés, a második sor mutatja, hogy hol kell keresni a harmadik sorban megadott, maximálisan 80 karakter hosszú hexadecimális sorozatot.

Alabama

COM, EXE

C606F900013CD375062EC606F90000BB40008EDB33DB8A4717240C3C0C7541

Anarkia

COM, EXE

5C02B82125CD218E063100268E062C0033FFB9FF7F

Anti-Pascal

COM

BF0C018B360C0103F7B95D021E07EA00

April 1st COM

COM

89263401B419CD2104412EA265

April 1st COM (IBM-SCAN)

COM

89263401B419CD2104412EA265032EA2B103BF6703578BF2807C013A750D8A04
2EA265032EA2B103

April 1st EXE

EXE

2EA31700BB17000E1FB4DECD21

April 1st EXE (IBM-SCAN)

EXE

2EA31700BB17000E1FB4DECD21B42ACD2181FA0104742281F9BC077506E8C504

Ashar boot (IBM-SCAN)

BOOT

8CC88ED88ED0BC00F0FBA0067CA2097C8B0E077C890E0A7CE85900

Birthday (IBM-SCAN)

COM, EXE

2E8B360101FCBF00015703F72E8936F000B90300F3A4B430CD213C037303E9F8

01B44ABB75032E031EF000B90400D3EB43CD21BB0800B448CD21

Brain, Shoe or Ashar

BOOT

F4A113042D0700A31304B106D3E08EC0BE007C

Brain(C) boot (IBM-SCAN)

BOOT

8CC88ED88ED0BC00F0FBA0067CA2097C8B0E077C890E0A7CE85700

Companion (AIDSII, 8064)

COM, EXE

5589E581EC0202BFCA050E57BF3E011E57

Dark Avenger

COM, EXE

49CD21BBFFFFB448CD2181EBE700727B8CC1F913CB

Dark Avenger/Eddie (IBM-SCAN)

COM, EXE

E800005E81EE6B00FC2E81BC05074D5A740EFA8BE681C40808FB3B26060073CD

5006561E8BFE33

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

dBase

COM

FB750A86E09DCFE9CE06E9810381FF0AFB742E3D004B

December 24th

EXE

6803A32400A16A03051000A31C0090

Den Zuk

BOOT

FA8CC88ED88ED0BC00F0FBB8787C50C3

Devil's Dance

COM

AD03F3A426C706000003015E1E068CC048

Disk Killer (Ogre)

BOOT

02F7361A0088163F01A34101C3A14101

Do Nothing

COM

C21ECD707219A36F02B442B0028B1E6F02B90000

Durban (SAT14)

COM, EXE

9D02A4E2FD06B82135CD211F891E5302

EDV

BOOT

DB8ED8C7078118813F8118740D2D00103D00B875ECB800A8

Falling Letters/Potyogós boot

BOOT

31C0CD13B80202B90627BA0001BB00208EC3BB0001CD139A00010020

Fish(6)

COM, EXE

8F06DB0E2E8326DB0EFE2E803EDA0E0075112EFF36DB0E

Form

BOOT

B9FF00FCF3A506B89A0050BBFE01B80102

Friday the 13th

COM, EXE

1E8BECC746100001E80000582DD700B104D3E88CCB03C32D100050

Fu Manchu A

COM, EXE

72454D484F72

Fu Manchu (2086) B

COM, EXE

8ED0BC200950B8230250CBFC06

Ghost - boot átíró verziója

BOOT

7D83EA247211800EF77D0156579090905F5E8026F77DFE

Ghost - COM verziója

COM

F281C60A00BF0001B90300F3A48BF2B430CD213C007503E9C601

Golden Gate - version C

BOOT

A717800FADBDAD5507173384

Golden Gate - version C2

BOOT

A717DDAFF001233907173385

VÍRUSLÉLEKTAN

HAHAHA

COM

2A546869732046696C6520486173204265656E20496E66656374656420427920

Hallöeichen

COM, EXE

4B00C7065B005555BA4900C706FB003000E8A1FEFF064A01

Icelandic/Saratoga

COM, EXE

A3030003D8438EC333F633FF0E1FB9D007

Icelandic (IBM-SCAN)

COM, EXE

8CDB4B8EDBB04DA20000A103002D8000A3030003D8438EC333F633FF0E1FB9D0
07

Icelandic/Saratoga II

COM, EXE

26C6067F03FFB452CD212E8C066D02268B47FE8EC026030603004040

Itavir

COM, EXE

9B00908A16D70B80FA02741B1E52B41CCD218A075A

Jerusalem (PLO/sUMsDos)

COM, EXE

FC062E8C0631002E8C0639002E8C063D002E8C0641008CC0

Khetapunk (1392)

COM, EXE

2F01C3E80700E83A00E86600C3BF0001A1030180000905E5051B82135CD218C

LDV

BOOT

A406B8330150CBBB4C008B0F8B5702

Lehigh

COM,

605380FC4B740880FC4E7403E977018BDA807F013A75058A07EB07

Liberty

COM, EXE

03E8CD0072C2BB13012E813F4D5A7505

VÍRUSSZIGNATÚRÁK

Lisbon 648

COM

2FCD21895C00908C44029007BA5F009001F2B41A

Mix 1

COM, EXE

2933C08EC02680261704

Mix 1B

COM, EXE

2733C08EC02680261704

Nichols

BOOT

DD0DDF0FDD0FFF0A000ABA00

Ohio

BOOT

B106D3E08EC0BE007C33FFB90410FCF3A406B8000450CBB90400

Oropax

COM

8200C7069C007D098C0E9E00C7068400EE088C0E8600FB2E803E070100

Ping Pong or Typo Boot

BOOT

8ED8A113042D0200A31304B106D3E02DC0078EC0BE007C8BFEB90001

Ping Pong/286

BOOT

7D807426BEBE81B90400807C0401740C807C04047406

Polimer

COM

E90C01B000B40ECD21BAC000B41ACD21

Pretoria (June14)

COM

C933D2E85BFFE81200B440BA0001

Prudent

EXE

2F040175D00E0E1F07BED3042BC92E8A0446410AC0

PSQR
COM, EXE
A526C606FE03CB580510008EC00E1FB9B306D1E9
PtrSc
BOOT
DBB801038A365F01B90100CD6DE824005A595F5E5B
Shake
COM
5E50E800005EB80342CD213D34217503
Solano
COM
175858BF00012E893E2101582EA32301
Stoned (Marijuana)
BOOT
1E5080FC02721780FC0473120AD2750E33C08ED8A03F04A8017503E80700
Sunday
COM, EXE
C80510008ED0BC5D0650B8C40050CBFC062E8C063100
Surv 1.01
COM
81F9C407721B81FA0104
Surv 2.01
EXE
81F9C407722881FA0104
Surv3
COM, EXE
4F0026A0FE032EA2510026C706FC03F3A526C606FE03CB58
Sylvia
COM, EXE
8D36030133C933C0AC3C1A7404
Syslock
COM, EXE
D1E98AE18AC13306140031044646E2F25E5958C3

VÍRUSZIGNATÚRÁK

Taiwan

COM

B90800BEBC03BF00F8FCF3A4B9C4028B364801

Turbo @ (Kukac)

COM

CD20E80000905E5051B021B435CD21

Twelve Tricks Trojan Dropper

COM, EXE

BE640231944201D1C24E79F7

Twelve Tricks Trojan

BOOT

8CC88ED0BC007C8BF48EC08ED850

Vacsina

COM, EXE

DA012E890E0800B8014380E1FECD2173

Vacsina EXE2COM conversion

COM

03C8894FFB8B0E160103C8894FF78B0E1001894FF98B0E1401894FF58B3E1801

Vcomm

EXE

7D02B440CD21E83E00A19B02A33602A19D02A334021E

Vienna "A" (DOS 62)

COM, EXE

8BFE81C71F008BDE81C61F00

Vienna "B" (DOS 62)

COM, EXE

8BFE83C71F908BDE83C61F90

Virdem

COM

B200B40ECD21B43B8D16DF03CD21EB4C90B43B8D16DF03

VP

COM

290332E43A062A037503E94902403D

Virus-90

COM

C5030133C033DBB909008D561289D6030043

W13 family

COM

D681C60000FCB90300BF0001F3A48BFAB430CD213C007503

XA1 (Tannenbaum)

COM

FA8BEC5832C08946028146002800

(XA1) Boot record zapped by XA1

BOOT

5B83C30D8CC88ED8E81500EBFE

Yale

BOOT

BB40008EDBA11300F7E32DE0078EC00E1F81FF56347504FF0EF87D

Yankee Doodle 2772

COM, EXE

9F83C4049E7303E9F002B8004233C933

Yankee Doodle 2885

COM, EXE

9F83C4049E7303E97A0233C933

Yankee Doodle/Music (IBM-SCAN)

COM, EXE

E800005B81EBD4072EC6875C00FFFC2E80BF5B00007418BE0A0003F3BF0001B9

2000F3A40E2EFFB76400061E50EB138CDA83C2102E03162000522EFF361E0006

1E5053BB2C00F8B803C6CD215B7307581F07E898FFCB

Zero-Bug (Palette)

COM

5A45CD602EC606250601902E803E2606

4th Bulgarian (V512)

COM, EXE

B830CD21BE04008EDE80FC1EC5440872

333

COM

9452028BFAB90300CD21803DE97405E87E00F8

405

COM, EXE

B8000026A2490226A24B0226A28B0250B419CD2126A24902B4470401

648

COM

FC8BF281C60A00BF0001B90300F3A48BF2B430CD213C007503E9C701

765

COM

EF408EC70E1FB90004FCBF0000F3A481EC0004

847

COM

4FBA5F02CD217202EBA0BA8000B41A

867

COM

D681C2050033C9B44FCD2173EF

17XX

COM

F6872A0101740F8DB74D01BC

1704(B) vagy 17Y4

COM

FA8BECE800005B81EB31012EF6

1704-B (IBM-SCAN)

COM

FA8BE-

E800005B81EB31012EF6872A0101740F8DB74D01BC850631343124464C75F8

17Y4 (IBM-SCAN)

COM

FA8BCDE800005B81EB31012EF6872A0101740F8DB74D01BC850631343124464C75F8

1704-C/1704-Format

COM

F6872A0101740F8DB74D01BC850631343124464C77F8.

1971
 COM, EXE
 B7003B445B7219B8907EE8C800B80835CD21895C5D
 1813 (IBM-SCAN)
 COM, EXE
 8ED0BC000750B8C50050CBFC062E8C0631002E8C0639002E8C063D002E8C0641
 008CC0
 V2000 (EDDIE 2)
 COM, EXE
 B413CD2F5A1F2E8994A7072E8C9CA9072E
 2086 Virus (IBM-SCAN)
 COM, EXE
 8ED0BC200950B8230250CBFC062E8C062C002E8C0634002E8C0638002E8C063C
 008CC0
 2730
 COM, EXE
 9177917AA4B7570056000000
 2930
 COM, EXE
 2906E8E005B419CD218884E300E8CE048A95E2000E1F7509
 2930 (IBM-SCAN)
 COM, EXE
 E82906E8E005B419CD218884E300E8CE048A95E2000E1F7509
 3066
 COM, EXE
 7106E82806B419CD2189B451018184510184088C8C5301
 4096
 COM, EXE
 875EECFCC383C30381FBCC0272E95BE8890AE421
 The 9800:0000 (1554)
 COM, EXE
 9B00FFFF7203A39B00A19B003DFFFF741FB000

IRODALOMJEGYZÉK

A számítógépes vírusok kutatásának szakterületén nagyon kevés a valóban forrásértékű publikáció. Az információk megszerzésében sokszor a nem közölhető forrásokra és személyes kapcsolatokra kell támaszkodni. A legjobban használható, bár igen nehezen elérhető kiadványok ebben a témakörben a számítógépes betörők és programfeltörők (a „hackerek”) kiadványai. Hasonlóan jól használhatóak, de még ennél is nehezebben beszerezhetőek egyes országok adatbűnözéssel, illetve adatbiztonsági ajánlásokkal kapcsolatos belső anyagai. Az USA-ban az FBI, az NSZK-ban az Alkotmányvédő Hivatal végez bizonyos adatbűnözést megelőző és ezzel kapcsolatos tájékoztató tevékenységet, bár ez sok esetben a kommunikáció ellenőrzésével, az emberek zaklatásával vagy betarthatatlan szabályok előírásával jár együtt. E szervezetek nyugati szakkönyvtárakban és vállalatoknál fellelhető tanulmányai mégis értékes információforrások.

Szegedi Imre 1990 szeptemberében védte meg doktori disszertációját a számítógépes vírusok témakörében. Ehhez olyan irodalomjegyzéket is készített, amelyből alábbi összeállításunk jelentős hányadát merítettük. Az anyagok egy része nincs meg a hazai szakkönyvtárakban. Azok a Hamburgi Egyetemi Központi Könyvtárból, a bécsi Technische Hochschule könyvtárából és más nyugat-európai könyvtárakból kerültek könyvtárközi kölcsönzéssel vagy személyes látogatások alkalmával a szerzők kezébe.

1. Az Alaplap mikroszámítógép magazin „Vírusőrző” rovata rendszeres információkat ad a vírusokról. Publ.: Cédus Informatikai Rt., Budapest. (Továbbiakban: Alaplap.)

2. Auf der Knie. In: Der Spiegel, 1988, 11. 7. 294. p.

3. Bayerische Hackerpost. München. (A bajor számítógépbetörők szakmai fóruma.)

4. Brunnstein, Klaus: Blindes Vertrauen in den Computer. Unterschätztes Risiko. In: Bild der Wissenschaft, 2/1988. 96. p.

5. Brunnstein, Klaus: Mythen und Fakten über Computer-Viren. In: Chip, 3/1980,

50-56. pp.

6. Brunnstein, Klaus: Über Viren, Würmer und andere seltsame Geister in Computersystemen — ein kleines Informatik-Bestiarium. In: Angewandte Informatik, 10/1987, 397. p.

7. Brunnstein, Klaus: Viren-Telex mit Virus-Katalog. Ein monatlicher Informationsbrief für Datensicherheit, 1989-1990. Ed.: Vogel Verlag, Würzburg.

8. Burger, Ralph: Das große Computer-Viren Buch. Ed.: Data Becker GmbH, Düsseldorf-Wien, 1987. (Későbbi kiadásait részben átfírták, aktualizálták.)

9. Burger, Ralph: Das große PC Viren Schutzpaket. Ed.: Data Becker GmbH, Düsseldorf-Wien, 1989.

10. Cohen, Fred: Computer Viruses: Theory and Experiments. Ed.: University of Southern California, 8/1984. Reprint in Computer & Security, 6/1984.

11. Cohen, Fred: „Computer Viruses”. Dissertation. University of Southern California. Ed.: USC, 1985.

12. Cohen, Fred: Models of Practical Defenses against Computer-Viruses. In: Computer & Security, 2/1989.

13. A Computerworld-Számítástechnika rendszeresen közölt a vírusokra vonatkozó információkat és előrejelzéseket. Publ.: Computerworld Informatika Kft., Budapest.(Továbbiakban: CWI.)

14. Datenschleuder. Hamburg. (A Chaos hackerscsoport folyóirata.) Ed.: Chaos, Hamburg.

15. Die Hackerbibel. Vol. 1.-2. (Német hacker-kiadvány.) Ed.: Chaos, Hamburg.

16. Dierstein, R.: Das Israel Virus. In: KES, 2/1988.

17. Dierstein, R.: Die neue Gefahr: Computer-Viren. In: KES, Zeitschrift für Kommunikations- und EDV-Sicherheit. (Továbbiakban: KES) 3/1985, 4/1985. Peter Hohl Verlag, Ingelheim.

18. Ducan, R. (compiled): The Ms-Dos Encyclopedia. Ed: Microsoft Press, Redmond, Washington, 1988.

19. Elmer-DeWin, P.: Invasion of the Data Snatchers! In: Time, 26/9/1988. 62. p.

20. Experimente mit Computer-Viren. A KES 2/87. száma idézi a Die Datenschleuder underground lapot. (No.18. 2/1987.)

21. Fites, P.; Johnston, P.; Kratz, M.: The Computer Virus Crisis. Ed.: Van Nostrand Reinhold, N.Y. 1989.

22. Flu_Shot+ ver.1.5 User manual. Ed.: Software Concepts Design, N.Y. 1989.

23. Frost, David: The Complete Computer Virus Handbook. Ed.: Price Waterhouse, 1988.

24. Greenberg, R.M.: Know the Viral Enemy. In: Byte, 6/1989. 275. p.

25. Günter, Frhr. von Gravenreuth: Computer Viren, Datenspione, Crasher und Cracker. In: Neue Zeitschrift für Strafrecht, Heft. 5. 1989. 201-248. p.
26. 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. pp.
27. Hirst, Joe: List of known PC viruses. Publ.: British Computer Virus Research Center, Brighton/Essex; 1989.
28. Hoppenrath, D.: Computerviren: Problem oder Psychose. In: Computer Persönlich, 3/1989. 45. p.
29. Hoppenrath, D.: Impfung via Software. In: Computer Persönlich, 3/1989. 48. p.
30. Hoppenrath, D.: Kranke Programme. In: PC-Magazin, 35/1988. 20. p.
31. Hozzászólás vírusügyben. In: CWI, 1988. 25. szám.
32. Goodwin, Jim: Virus Information Summary List. In: VSUM9003.ZIP 1990-02-18 from Homebase/CVIA Bulletin Board BBS, USA.
33. 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.
34. Kastenmüller, S.: Erkennen von Computer-Viren. In: KES 4/1988.
35. Kis János: A tiltott gyümölcs mindig kíváncsú. In: Alaplap, 1990. 9. szám, 38. p.
36. Kis János: Egy veszélylehetőség realitássá vált. Virtank.doc, a Prgdoki 2.11...2.13 verzióihoz adott összefoglaló dokumentációs állomány. Szamizdatként Budapest, Kecskemét. 1988-1989.
37. Kis János: Hogyan kell vírust írni? In: Delta-Impulzus, 1989. 9. szám, (V. 6.), 40. p.
38. Kis János: Modern trójai háború. In: Delta-Impulzus, 1989. 8. szám, (IV. 22.), 24. p.
39. Labor, Zeitschrift für Word processing. (Víruscikkek, adatátvitel.) Technikai szamizdat. Ed.: Labor c/o Glaser, D-2000 Hamburg 50, Hospital-strasse 61.
40. McAfee, John: Scanxx.DOC, Cleanxx.DOC, Netscan.DOC, Vshieldxx.DOC, Virlist.txt szoftver-dokumentációs állományok. 1988-1990.
41. McAfee, John: The virus cure. In: Datamation, 1989. 02. 15. 29-40. pp.
42. Ms-Dos-Viren erkennen und bekämpfen. Chip Special, No. 82005/90003 1. Aufl. Ed.: Vogel Verlag, Würzburg, 1990.
43. Mußtopf, Günther: Drei Schritte zur Heilung. In: Chip, 11/1989. Ed.: Vogel Verlag, Würzburg, 1989.

44. Mußtopf, Günther (comp.): Trojanische Pferde, Viren und Würmer. Eine ernstzunehmende Gefahr für Pc-Anwender. Ed.: PerComp Verlag GmbH, Hamburg, 1989.
45. Mußtopf, 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.
46. Péntek 13-a! Vírusölő program. In: CWI, 1989. 36. szám.
47. Rablók és pandúrok. In: CWI, 1989. 6. szám.
48. Roberts, R.: Computer Viruses. Ed.: Compute! Books, Greensboro, NC, 1988.
49. Rubenking, N.J.: Infection Protection. In: PC Magazine, 4/1989. 193. p.
50. Schöneburg, E.: Computer Centre Risk Analysis by Expert Systems. In: Dornier Post eng. ed. 1/1987. Dornier GmbH, Friedrichshafen.
51. Schöneburg, E.: Computer-Viren — Eine aktuelle Bedrohung für Computer-Systeme. In: Dornier Post, deutsch. ed. 1/1987. Dornier GmbH, Friedrichshafen.
52. Schöneburg, E.: Computer-Viren und Trojanische Pferde. Gefährliche Softwareangriffe an Computersysteme. In: Neue Zürcher Zeitung, 1987. 9. 29.
53. Schöneburg, Eberhard — Heinzmann, Frank — Namyslik, Frank: Computer-Viren. Gefahren und Schutzmöglichkeiten. Ed.: Markt und Technik Verlag, Haar bei München, 1989.
54. Schöneburg, Eberhard — Heinzmann, Frank — Namyslik, Frank: Virus Power Pack (Programm und Buch). Ed.: Markt und Technik Verlag, Haar bei München, 1989.
55. Shapira, Eli — Sherman, Yuval: Turbo Anti Virus Toolkit *Tntvirus* ver. 6.80A dokumentációs állománya és felhasználói kézikönyve. Ed.: Carmel Software, Haifa, 1990.
56. Shapira, Eli — Sherman, Yuval: Turbo Anti Virus Toolkit *Tntvirus* ver. 6.71B demó verzió dokumentációs állomány. Ed.: Carmel Software, Haifa, 1990.
57. Sperber, J.: Virusfieber. In: Microcomputer Zeitschrift, 7/1988. 74. p.
58. Számítógépvírusok avagy ki fél a cyberpunkoktól? In: CWI, 1989. 31. szám.
59. Szegedi Imre: Harc az adatgyilkosok ellen. In: Alaplap. 1990. 8. szám, 32. p.
60. Szegedi Imre: Megindult a hazai vírustenyésztés? In: Alaplap, 1990. 10. szám, 36. p.
61. 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.)
62. Szegedi Imre: Szisztematikus doktorálás. In: Alaplap, 1990. 9. szám 36. p.
63. Technical Notes on AIDS DISK Trojan Mail Information. In: AIDSTECH.ZIP,

1989-12-23. From: Homepage/CVIA Bulletin Board BBS, USA.

64. Terjed a vírusjárvány az Egyesült Államokban. In: CWI, 1989. 22. szám.

65. Tűzre, vízre, adatokra vigyázzatok. In: CWI, 1989. 34. szám.

66. Újabb gyógyszer a Péntek 13-a ellen. In: CWI, 1989. 40. szám.

67. Verborgener Befehl — Bericht Cohens Arbeit. In: Der Spiegel, 4/1987.

68. Védőoltás vírus ellen. In: CWI, 1989. 22. szám.

69. Vírusok. In: CWI, 1988. 13. szám.

70. Wochlebie, H.: Der Weihnachtsbaum, der um die Welt ging. In: KES, 1/1988.

Tartalom

ELÖLJÁRÓBAN	5
JÓTÉKONY KÖD	9
EGY KIS TIPOLOGIA	19
EGY PÁNIK TÖRTÉNETE: PÉNTEK 13	28
GYAKORLATI VIROLÓGIA	31
SZÁMHÁBORÚ ÉS VAKLÁRMA	40
AIDS TÁJÉKOZTATÓ LEMEZ	53
NEM CSODASZEREK	71
VÍRUSHATÁROZÓ	91
VÍRUSVILÁG MAGYARORSZÁGON	170
A VÍRUSOK ÖSSZEFOGLALÓ TÁBLÁZATA	202
KERESZTREFERENCIA-TÁBLÁZAT	208
VÍRUSHOSSZ	219
VÍRUSSZIGNATÚRÁK	223
IRODALOMJEGYZÉK	234