V.S.K. Víruskeresést Segítő Környezet 1991-1995. V:4.21 1995.05.08.

Tartalomjegyzék

V.S.K. Víruskeresést Segítő Környezet 1991-1995. V:4.21 1995.05.08.

A program megírásának előzményei
(SCAN NECESSE EST)

A vírusok - ezek az intelligencia magas fokán álló, de azt rossz célok érdekében mozgósító programok - ellen védekezni kell, mint azt az alcím is sugalmazza. A védekezés nagyjából hasonló hatásfokú, mint a forgalmas úttesten való átkelésre fordított figyelem:

- megtehetjük, hogy körülpillantás nélkül egyszerűen átszaladunk a kocsik között; ilyenkor, ha megússzuk baj nélkül, azt inkább a szerencsénknek köszönhetjük és nem a jó stratégiai érzékünknek;

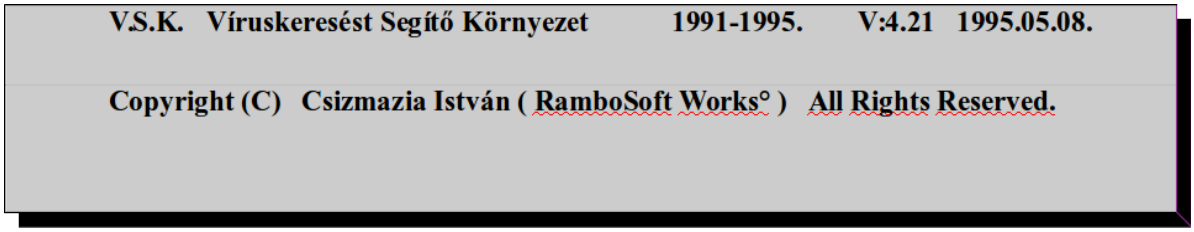
- lehet aztán álló nap siránkozni, hogy milyen sanyarú az élet, az ember már át sem mehet a túloldalra a sok robogó autó miatt; és

- csinálhatjuk a hagyományos módon: először balra majd jobbra nézve (ezt a metódust Angliában vagy Ausztráliában ne kövessük) a megfelelő időben, a megfelelő sebességgel óvatosan átkelünk az úttesten, még az is megtörténhet, hogy várni is kell valamennyit, viszont vélhetően baj nélkül átjutunk.

Az első példa a vírussal egyáltalán nem törődőket példázza, ők a problémát félvállról veszik (talán csak az első fertőzésig lesznek ilyen bátrak).

A második csoport túl nagy és hamis jelentőséget tulajdonít az egésznek (ilyeneket hallani tőlük, hogy a vírusnapokon egyáltalán ne kapcsoljuk be a gépet, stb. Ez igencsak érdekes lehet egy könyvelés vagy számlázó program esetén, arról már nem is beszélve, hogy a HETI CHIP vírusnaptárába bepillantva meggyőződhetünk róla, hogy minden nap többszörös vírusnap van.)

A többség által járt harmadik út látszik a helyesnek: óvatosság, körültekintés és akkor nagy valószínűséggel sok mindent meg lehet előzni, ha nem is mindent: a figyelmes gyalogost is elütheti egy őrült vagy részeg autós, de ez nem ok arra, hogy az átkelésnél ne nézzünk szét! A rendszeres ellenőrzés (a winchester esetenkénti és a floppy-k rendszeres ellenőrzése, jól megválasztott keresőkkel) legalább 95%-os védelmet jelent. A detektorok kiválasztása akkor helyes, ha legalább kétfélét használunk: kell egy standard, nagy tudású nemzetközileg is ismert és elismert program és kell egy hazai, a helyi átiratokat is ismerő, esetleg könnyen bővíthető vagy a nagyközönség számára is rendelkezésre álló, hazai fejlesztő szoftvertermék. Sajnos, egyenlőre jól működő, ingyenes hazai



program nem áll rendelkezésre. Itt még érdemes megjegyezni, hogy aki a termékére 100% biztonságot hirdet az vagy csaló vagy jobb esetben csak sarlatán, esetleg csaló és sarlatán egyszerre.

Újdonságok a VSK régi (3.xx) verziójához képest

Hasznosnak bizonyulhatnak azok az eszközök, amelyek nyilvántartott szekvenciák nélkül is, a sűrűn használt állományok méret és egyéb változásait is figyelik vagy pedig heurisztikus keresésre is képesek és így konkrét vírus ismerete nélkül is gyanakodhatnak vírusszerű kódrészletekre. Az ismertetendő keretrendszer és természetesen maguk a kiválasztott detektorok is rendelkeznek ezen jó tulajdonságokkal.

Ez a VSK 4.xx rendszert most annyiban érinti, hogy igazából az F-PROT program lett a víruskeresés gerince. A legaktuálisabb vírusokat ez fogja figyelni, Friderik Skularsonéktól érkezik a rendszeres, legalább kéthavonta frissített verzió. Sajnos ez a rendszeresség már a múlté a régi SCAN verzióit illetően. Az utolsó hagyományos V117 SCAN és CLEAN páros 1994. július 15-én jelent meg. Ez év elejétől lehettünk tanúi, hogy a McAfee csapat párhuzamosan kétféle víruskeresőt is fejlesztett. Ez a megszokott SCAN-CLEAN mellett egy jó ötletnek látszó, egy programba összefogott SCAN2.x lett, amely például a CLEAN funkciót is végre tudja hajtani a megfelelő paraméter hatására. A megjelent új program rögtön a 2.00 verzióval indult, mára már a 2.13E változatnál tartanak és úgy tűnik, csak ezt a vonalat fogják fejleszteni. A kezdeti változatok sokáig különböző gyermekbetegségekben szenvedtek.

Éles vírusokkal az alábbi tapasztalataim voltak:

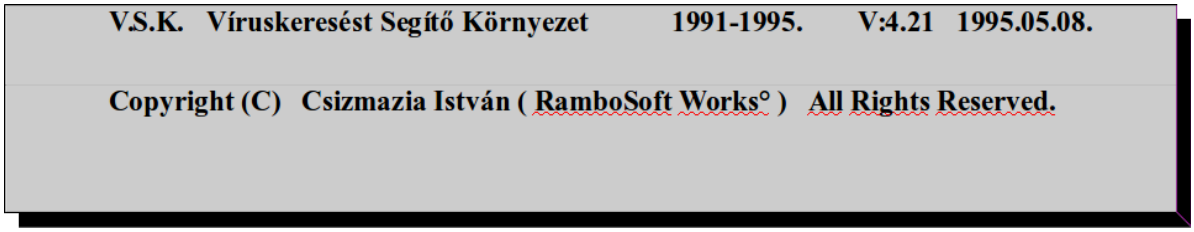
- NEM mentesített a CLEAN paraméterrel olyan vírusokat, amiket dokumentáció szerint le tud szedni és amit már az olyan ősverzió, mint CLEAN113 is jól felismert és irtott pl. Michelangelo.

- NEM ismert fel egyéb régebbi vírusokat, amiket a másik elől program pedig hibátlanul kezelt.

- NEM kompatibilis a paraméterezése és a szignatúra megnevezése a hagyományos SCAN, CLEAN programokkal.

- NEM volt létrehozható tetszőleges útvonalon a naplófile, csak az indító helyen.

- Sebessége valóban gyorsult, de eleinte úgy tűnt, ez a minőség rovására tett engedménynek volt



köszönhető.

- Leragasztott lemezen elindított mentesítés után sikeres leszedést jelzett tévesen.

Ezek miatt a VSK rendszerben mindmáig a 117-es hagyományos verzió dolgozott. A fent említett problémák egy része mostanára megoldódott, ezért a jövőben a 2.13E verziótól kezdődően a SCAN2xx fog futni. A rendszerbe illesztése a vakriadók és memóriafoglalás alapos tesztelése után volt csak lehetséges. A /CLEAN opciója viszont most sem egészen korrekt, ezért érdemes eltenni a CLEAN117-et is.

A HTSCAN felett sajnos eljárt az idő, több gépen is panaszkodtak lefagyásra. Ez részint a program régi, azóta sem frissített (1991-es) .EXE állományának tudható be. A keresési szignatúráit mindig a konvencionális memóriába tette, rendellenes megszakításnál maga után a memóriát nem szabadította fel, a szignatúrákat ott hagyta memóriaszemétként, amit aztán a következő keresés vírusnak látott. Hátrányos tulajdonsága volt még a rendkívüli lassúság is, sokan ezért hanyagolták el az ellenőrzéseket.

Ezen gondok némelyikén a korrekt gép behangolás tudott segíteni pl. ha víruskeresés előtt nem indítunk rezidens programot, szerepel a CONFIG.SYS-ben a HIMEM.SYS és az EMM386.EXE device driverként, a DOS=UMB,HIGH helyes megadása, a CED és a DOSEDIT letiltása, stb. A két kereső, az F-PROT a 2.12-es változattól, a SCAN pedig a 2.XX változattól új keresési algoritmust vezetett be, mellyel a futási idő drasztikus csökkenését érték el. Emiatt, és a HTSCAN elhagyása miatt most kb. fél-egyharmad idő alatt fognak a keresések lezajlani, de változatlanul alapos minőséggel. Az F-PROT kétféleképpen fut: először ismert vírusszignatúrákat keres (ún. SECURE SCAN MODE), másodszor heurisztikus vagyis vírusszerű kódrészletek után kutat (ún. HEURISTIC MODE) - ilyenkor még ismeretlen vírusokat is képes megtalálni.

V.S.K. Víruskeresést Segítő Környezet 1991-1995. V:4.21 1995.05.08.

A program funkciója

A program célja, hogy a vírustesztelést és az eredmény kiértékelését lényegesen leegyszerűsítse és a nyilvántartott vakriadóktól megkíméljen, észlelés esetén pedig egyértelmű jelzésekkel tudassa a felhasználót, hogy mi történt, meggátolva a munka további folytatását az elhárításig.

A program kifejlesztését az indokolta, hogy használatával és kellő odafigyeléssel a vírusfertőzések döntő többségét meg lehet akadályozni, illetve idejében fel lehet ismerni. Jelenlegi ismereteink szerint nincs megfelelő hardver eszköz (vírusvédelmi kártya), amely teljes körűen és megbízhatóan ellátná ezt a feladatot és itt az ár/teljesítmény viszonyokat még meg sem említettem.

A szerző már 1988 óta foglalkozik vírusvédelemmel (boldog békeidők, akkoriban egy kézen fel lehetett sorolni őket: potyogós, resetelő, Péntek 13) és személyes tapasztalatból tudja, hogy egy nagyobb vállalatnál micsoda kavalkádot okozhat nem csak maga a vírus, hanem már az is, ha egy víruskereső állandóan trükkös kérdéseket szegez szerencsétlen felhasználónak, hogy mit tegyen ("Valamelyik program állományt akar létrehozni, engedélyezi ?" szól például egy PE2-s szöveg editálásnál, mikor egy új állományt akarunk szerkeszteni. Ennél már csak az lenne érdekesebb, ha minden billentyűnyomás után rákérdezne: Biztos, hogy le akarta nyomni ezt a billentyűt?...). Egyszerűbb esetekben a keretprogramnak önállóan kell tudnia szelektálnia az eseményeket, segíteni a laikus felhasználót és ez a VSK rendszer előnye.

A program által használt detektorok

A vizsgálat az F-PROT és a SCAN programok segítségével történik. A detektálás itt a következőket jelenti: az F-PROT program a kelet-európai vírusokra is jól kihegyezett, de vírusszerű kódrészleteket is felismer. A SCAN program a nemzetközileg is elismert McAfee Associates Egyesült Államokbeli vírusellenes cég legfrissebb, hozzáférhető, szabadszoftverként terjesztett standard vírusdetektálója.

Mai tudásunk szerint e két program együttes használata nagymértékben biztosítja az ismert vírusok kimutatását. Ezt hazai és külföldi elektronikus levelezési rendszereket
(BBS) üzemeltető szakemberek is megerősítik.

Többlet a két detektorhoz képest

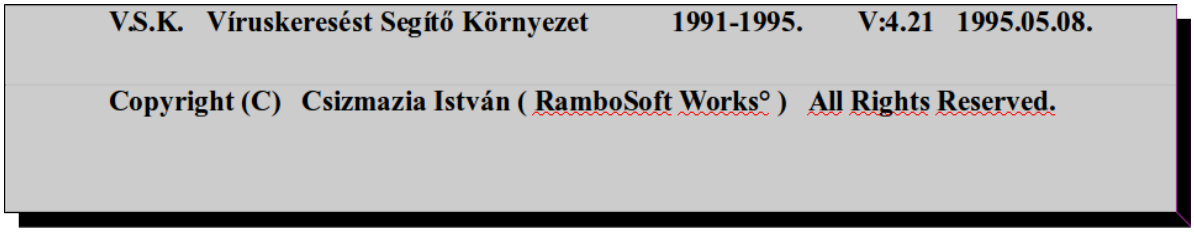
Ezen kívül még nem ismert vírusokat is észlelhet a rendszer: a TESZTCOM és TESZTEXE állományok csali, üres kódot tartalmazó .COM illetve .EXE file-ok, és a VSK detektálás előtt ellenőrzi ezen két file sértetlenségét. Ha ezek közül bármelyik sérült, hosszabb, más dátumú, más attribútumú - ez fertőzésre utalhat - a gép működését a VSK megfelelő hibaüzenet kíséretében leállítja. Ha minden rendben volt, futtatja őket és ezután következik a kívánt meghajtó vírusellenőrzése. A tesztállományok rendszeres indítása a nem ismert vírusok csalijaként funkcionál, feltételezve, hogy az a sűrűn futó programokat támadja meg elsőként. A mellettük bemásolt .EX és .CO kiterjesztésű állományok a file összehasonlítás megkönnyítésére szolgálnak.

A detektálás eredményeképpen naplóállományok keletkeznek. Mivel a sérült, fertőzött vagy gyanús gép vizsgálatakor el akarjuk kerülni a vizsgálandó lemezre való írást, a naplófile merevlemez vizsgálatkor az A: meghajtó főkönyvtárába, floppy ellenőrzéskor a C: meghajtó főkönyvtárába fog írni pl. VSKF_A.VIR néven. A név negyedik betűje a detektáló program neve, az aláhúzás karakter után a vizsgált meghajtó betűjele és a .VIR kiterjesztés következik.

VSKF_?.VIR	Az F-PROT naplóállománya
VSKS_?.VIR	A SCAN naplóállománya

Ezek szövegállományok, melyeket a detektorok készítenek a keresés naplózásaként. Ebből később is tájékozódhatunk az állományok állapota után (például behívjuk PE2-be, kinyomtathatjuk, stb.). A naplófile-ok mindig a legutolsó futás eredményét tükrözik. Ha a naplózás az A: meghajtóra készül, úgy a napló floppy lemezt előbb az F-PROT program megvizsgálja BOOT vírusokra. Ha a program vírusgyanút talált a naplóállományban - ezt az üzenetet a képernyőről tudjuk meg - úgy ennek részleteit a fent említett file-okban megtalálhatjuk.

A program használatával el tudjuk kerülni, hogy a detektálás alatt végig a képernyőt kelljen figyelemmel kísérnünk és a futás után keletkezett naplófile utólagos böngészését is megspórolhatjuk. A döntés felelősségének átvállalásával még a számítógéphez és vírusokhoz



kevésbé értő munkatársakat sem hozzuk bizonytalan döntési kényszerhelyzetbe, de minden gyanús esetben megakadályozzuk a további fertőzést.

Az ellenőrzés kétféle eredménnyel zárulhat:

- ha minden rendben és nem találtunk vírusgyanút, akkor a következő, zöld alapon fehér felirat tűnik fel:

A program 1 perc 59 másodpercig futott.
Csao Ragazzi!

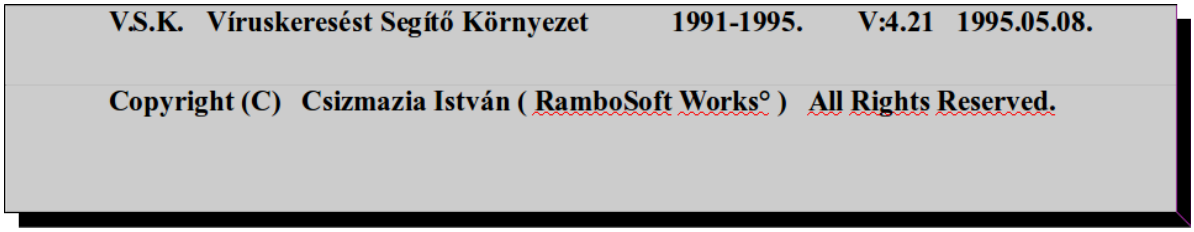
Ez az üzenet 3 másodpercig látható (vagy billentyű nyomásra eltűnik) és utána dolgozhatunk tovább. A kis szünet oka, hogy a több meghajtó vizsgálatánál is legyen időnk elolvasni a program üzenetét.

A VSK 4.xx-ben két új üzenettel bővült a Tiszta környezet típusú kiírás. Ilyenkor nem zöld, hanem cián alapon villogó fehér üzenet jelenik meg. Ha fizikailag sérült, nem indítható file-t talál, akkor az alábbi felirat jelenik meg:

INFO:---> Fizikai (Cannot Execute) hibát talált a secure scan keresés. Ez filesérülést jelent, nézzen utána a VSKF_*.VIR naplóállományban!

Ha a kódrészlet szerinti keresés gyanús szekvenciát talál:

INFO:---> Gyanús, de nem vírusos file-t talált a heurisztikus keresés. Ha ez először történik, nézzen utána a VSKF_*.VIR napló állományban!



¨ ha fertőzésgyanús állomány(oka)t találtunk, figyelmeztető hangeffektus kíséretében az alábbi felirat olvasható:

és ennél az üzenetnél a gép lefagy (processor halt). Ez egy szándékos leállás, mert már előfordult, hogy a detektálás futásának az eredményét figyelmen kívül hagyva tovább dolgoztak a fertőzött gépen, további galibát okozva. A hiba felirat piros alapon sárga betűkkel villogva jelenik meg a riasztás okát is megjelölve. Innen már csak
(szándékosan !) resettel vagy a gép ki-bekapcsolásával lehet kikeveredni. A program probléma esetén hangjelzéssel, vírusgyanú esetén egy kis zenével is megpróbálja felkelteni a figyelmünket

Telepítési és futási alapfeltételek

A telepítéshez szükséges:

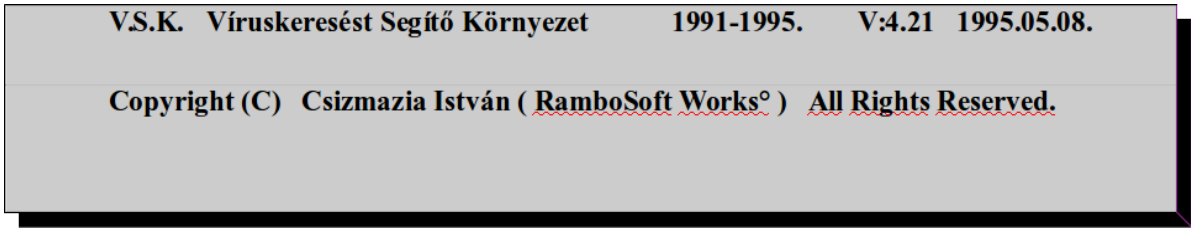
A konfigurációban legyen merevlemez.
A merevlemezen legalább 2.2 MB szabad hely.
A konfigurációban legyen legalább egy floppymeghajtó.

V.S.K. Víruskeresést Segítő Környezet 1991-1995. V:4.21 1995.05.08.

A program bármilyen (MDA, HERCULES, CGA, EGA, VGA) monitoros rendszeren működőképes.

A futtatáshoz szükséges:

A naplólemezegységen (C:\ vagy A:\ ) legalább 100 kB szabad hely.
Sértetlen CHKDSK állapot.
Az VSK rendszer programjai legyenek felinstallálva a C:\SCAN könyvtárba.
Legalább 560 kB szabad memóriakapacitás.



Itt egy kis magyarázattal tartozom, miért is kell a programoknak kötelezően a C:\SCAN alkönyvtárban lennie. Ezt a korlátozást nem a programozói tudás hiányos volta okozta, hanem az a meggondolás, hogy a gépen esetleg lehet máshol is, más útvonalon is vírusdetektor, és ha pl. a PATH listában előbb szerepel a másik, mondjuk régebbi változat, akkor az futna és nem a legfrissebb. Így viszont, ha a C:\SCAN könyvtárban aktualizáltunk, biztos, hogy az a példány lesz megszólítva. További haszna még e megoldásnak, hogy a DOS az indítandó programot, ha azt útvonal nélkül indítjuk, először az aktuális könyvtárban, majd a PATH útvonalain végigkeresi és ez több másodperces várakozást is jelenthet, míg útvonallal indítva azonnal tud futni; sőt az is egy lehetséges eset, hogy az éppen aktuális könyvtárban egy ősrégi, esetleg vírusfertőzött SCAN változat van és egy floppy ellenőrzésekor ez indulna a friss C:\SCAN-ben lévő helyett. Tehát az a jó, ha a VSK hívásai mindig a C:\SCAN könyvtárból történnek.

Az install lemez tartalma és a VSK rendszer állományai

Ezek a z állományok vannak az INSTALL floppy lemezen:

INSTALL.EXE	57979	1992-09-15	12.00
INSTALL.DAT	2046	1994-12-08	7.11
$$$$$$$1.EXE	1046407	1994-12-07	11.02
$$$$$$$2 EXE	15135	1994-05-11	6.27

Az installálás az INSTALL.EXE elindításával automatikusan történik. Az install megszakad, ha nincs elég hely a célmeghajtón (minimum 2.2 MB szükséges). A cél meghajtót és könyvtárat mindig C:\SCAN-nek válasszuk. A SCAN könyvtárnak nem szükséges az AUTOEXEC.BAT PATH listájában szerepelnie, az indításokról a C:\ könyvtárban lévő A, B és REGGEL.BAT gondoskodik. Ha minden rendben zajlik, úgy az alábbi állományok kerülnek a winchesterre:

VSK.EXE	35113	1994-12-07	11.00

V.S.K. Víruskeresést Segítő Környezet 1991-1995. V:4.21 1995.05.08.

VSK.INF	116	1994-12-07	11.01
TESZTCOM.CO	2060	1993-12-02	10.00
TESZTCOM.COM	2060	1993-12-02	10.00
TESZTCOM.INF	121	1994-12-01	10.32
TESZTEXE.EX	2572	1993-12-02	10.00
TESZTEXE.EXE	2572	1993-12-02	10.00
TESZTEXE.INF	121	1994-12-01	10.32
TM.EXE	7504	1988-10-16	16.50
LABTEST.EXE	18417	1991-06-06	0.00

F-PROT.EXE	1011641	1994-11-10	2.15
ENGLISH.TX0	32870	1994-11-11	2.15
VIRLIST.LIS	265347	1994-11-23	15.55
VIR-HELP ENG	213184	1994-11-09	14.12
SIGN.DEF	229966	1994-11-09	2.15
VIRUS.TXT	11761	1994-11-23	15.24
NEW215.TXT	6111	1994-11-23	14.21

SCAN.EXE	174554	1994-11-16	2.13
SCAN.DOC	2308	1994-12-01	10.31

CLEAN.DAT	54027	1994-11-16	2.13
NAMES.DAT	143682	1994-11-16	2.13
SCAN.DAT	137677	1994-11-16	2.13
VIRLIST.TXT	358549	1994-11-29	11.00
VALIDATE.EXE	15958	1994-11-16	2.13
VALIDATE.TXT	3560	1994-11-16	2.13
CLEAN.EXE	197445	1994-07-15	6.21
CLEAN117.DOC	20958	1994-07-15	6.27

VSK.EXE ellenőrző adatai:

A VALIDATE ellenőrző programmal készített helyes ellenőrző összegek:

VSK.EXE 35113 12-07-1994 11:00a 2187 4E26

Használati javaslat és időigények

Futtatása a merevlemez(ek)re minden reggel, idegen floppy lemezekre minden behelyezéskor ajánlatos, ez mind az alapmemóriát, mind a 640 kB és 1 MB közötti memóriaterületet, a lemez (partíció) boot-szektorát, a partíciós programot valamint az aktív partíció boot-szektorát és a lemezen (partíción) szereplő összes állományt minden ismert vírus ellen átvizsgálja. Ez különösen olyan gépen érdekes, amit többen is használnak felváltva. Ha ezt nem teszi meg valaki, winchester esetében minimális alapkövetelményként legalább a heti egyszeri alkalommal a VSK minden merevlemezére (partíciójára) való lefuttatása a REGGEL.BAT segítségével azért legyen elvárható.

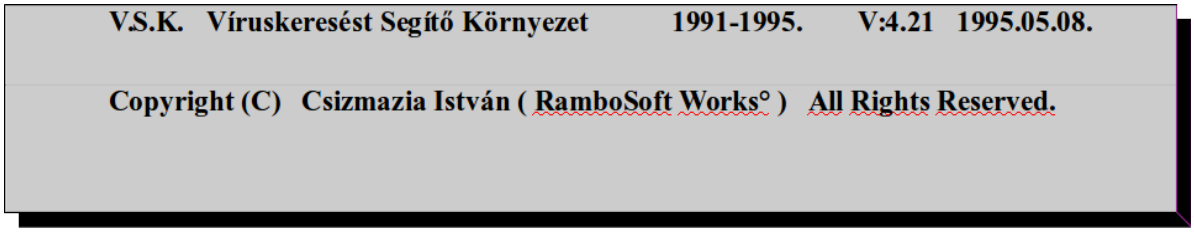
Ez egy átlagos gépen, átlagos winchester telítettséggel a gép teljes vizsgálata 3-15 percet igényel, míg egy floppy lemezé 0.5-1.5 percet. A lemezek vizsgálati ideje a rajta lévő file-ok számával arányosan emelkedik. Ez a vizsgálati idő a keresők frissítése után is emelkedhet egy minimális szinttel, mivel a vírusok száma is emelkedő tendenciát mutat, pl. a SCAN213E verziója már 4480, az F-PROT 3.15 pedig 4846 félét különböztet meg.

Minden hajlékonylemez (főleg az idegen, de saját is) behelyezéskor az VSK A (vagy VSK B) futtatása az A.BAT vagy B.BAT segítségével ellenőrizzünk.

Az ellenőrzés NEM BIZALMATLANSÁG a másik kolléga iránt, hanem indokolt óvatosság. Volt már rá precedens, hogy egy lemez vizsgálatakor a tulajdonos azt mondta: "nem kell megnézni, most vettem ki a gépemből" és a vizsgálat kimutatta, hogy szépen ott csücsül a bootszektorban egy Michelangelo vírus. Volt nagy meglepetés a tulajdonos részéről.

A napi teljes merevlemez átvizsgáláshoz C:\, D:\ és E:\ merevlemezek esetén például az alábbi REGGEL.BAT állományt használhatjuk:

```
tm start
VSK c
VSK d
VSK e
tm stop
```



Itt a tm a TM.EXE Norton időmérő-stopper programot hívja, így több merevlemez partíció átnézése után egy summa időt is láthatunk. Erre a floppy vizsgáló A.BAT esetében nincs szükség, mert egy futás idejét a VSK.EXE is kiírja.

Íme az A.BAT lehetséges tartalma:

VSK a

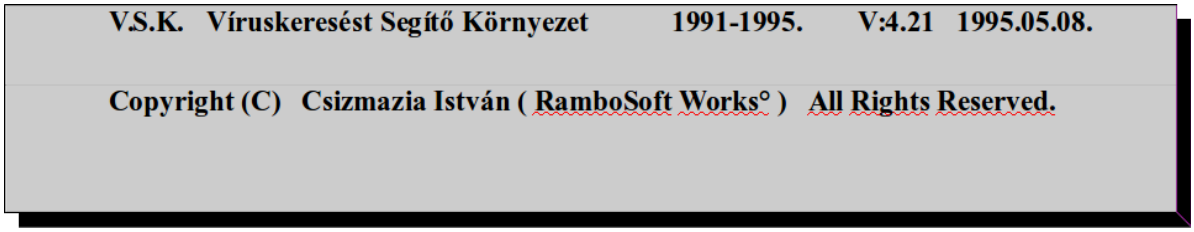
Tömörített futtatható állományok vizsgálata

A futó programok tömörítése annyira bevett gyakorlat, hogy maga a SCAN, a sok helyen használt gyári programok többsége, mint pl. CLIPPER'87 és CLIPPER 5.01 is ezzel készült, a MICROSOFT programok többsége, de a B&GRAPH és az új MS-DOS 6.x esetében valamennyi végrehajtható állomány tömörített.

A víruskeresők tömörítésre utaló felirata csak tájékoztatás, de az újonnan beszerzett szoftvereinknél, ha tehetjük, egyszer próbáljuk a megfelelő kitömörítővel az eredeti .EXE (.COM) file-okat visszaállítani és a saját nyugalmunk érdekében egyszer így is ellenőrizni. Ha ezt a visszaalakítást nem tudjuk elvégezni, csak valószínűségi alapon mondhatjuk, hogy vírusmentes, 100%-ig ezt kizárni nem lehet. A SCAN és
F-PROT programokról még érdemes megemlíteni, hogy az LZEXE-vel és PKLITE-al tömörített .EXE-k “belsejét” is tudják ellenőrizni.

Az új detektor változatok birtokba vétele

Célszerű MODEM-en keresztül beszerezni a friss és garantáltan eredeti detektorokat. A megbízhatóság egy igen fontos kérdés: példaként említem, hogy a SCAN szoftver egymást követő verziószámai között többször előfordult már, hogy hármat is léptek felfelé, mert a köztes verziókat hamisították a vírusírók. Ezért nem mindegy, honnan kerül beszerzésre a víruskereső szoftver. Emiatt csak megbízható változatokat érdemes használni a munka során. Ha mégis kapunk valahonnét egy új kiadást, akkor az alábbiakra érdemes figyelni:



- Az eredeti pl. Fidonet-es tömörített állományok úgynevezett "authorization code"-ot tartalmaznak. Ez egy olyan egyedi kód, amelyet csak egy konkrét ZIP vagy ARJ tulajdonos tud készíteni. Ha ez az AV kód benne van, ez már biztató jel, ugyanakkor hiánya sem jelent okvetlenül rosszat, pusztán csak azt, hogy már újracsomagolt pakkot kaptunk. Ha eredeti a tömörített csomagunk, CSAK így adjuk tovább, ne változtassunk rajta: ezzel segítsünk másoknak is az igazi változat könnyű felismerésében.

- Következő teendő a futtatható állományok ellenőrzése a VALIDATE programmal - először persze magát a VALIDATE-t nézzük meg. A mellékelt .DOC állományokban mindig megtalálható a kétféle CRC ellenőrző összeg értéke. Ha ez egyezik, az egy pozitív momentum; ha nem, akkor inkább NE használjuk!

- Korábbi verziójú víruskeresőkkel ellenőrizzük le az új állományokat.

- Óvatosságból ellenőrizhetjük pl. a VIRNET BBS-en (MODEM telefon: 1154402, 8 adatbit 1 stopbit, paritás nélkül, MNP5), hogy tényleg kijött-e ez a verzió.

- Érdemes először egy szeparált helyi gépen tesztelni és csak néhány napi korrekt futás és az esetleges vakriadók felismerése után frissíteni a többi helyen.

- Az óvatosság kedvéért MINDIG el szoktam tenni az egy változattal régebbi detektort is - biztos, ami biztos. Erre jó példa volt a CLEAN V84, amelyik nem tudta a Michelangelo-t kiirtani, jó hogy kéznél volt a V82 is, azzal működött. A következő verzióban vagy a hibajavított, úgynevezett bugfix változatban természetesen már kijavítják a hibákat, de addig is kell üzemelni valahogy.

A keresők új verziójára való upgrade-je a VSK szempontjából semmilyen nehézséget nem okoz, sőt a friss változatok használata a siker egyik fontos záloga.

A VSK által visszaadott DOS errorlevel értékek

Ha a program sikertelenül fut le, hangjelzés kíséretében hibaüzenetet ír ki és a DOS ERRORLEVEL függvény által lekérdezhető értékkel tér vissza:

0	Minden keresés sikeresen lefutott, nem talált vírust
1	Vírust talált és lefagyott (tehát ezt soha nem kapom vissza!)
2	A VSK sikertelen futása. Nem történt detektálás, mert a VSK-nak Kevés a szabad memória.
	Kevés megadott paraméter.
	A paraméter hosszabb, mint egy betűjel.
	A paraméter nem betűjel.
	Nincs A: meghajtó a naplózáshoz.

	Nincs C: meghajtó a naplózáshoz.
	Kevés a hely a(z) A: meghajtón a naplózáshoz.
	Kevés a hely a(z) C: meghajtón a naplózáshoz.
	Nem létező meghajtó.
	Nem üzemkész a(z) A: floppy meghajtó.
3	Hiányzik a C:\SCAN\F-PROT.EXE állomány
4	Hiányzik a C:\SCAN\SCAN.EXE állomány vagy fizikailag hibás a vizsgálandó lemez
6	Valamelyik file-ba irányított naplóállomány nem tudott elkészülni

8	Help kérés ("?" paraméter beadása) esetén
9	Hiányzik a C:\SCAN\ könyvtárból a TESZTCOM.COM és/vagy TESZTEXE.EXE állomány

V.S.K. Víruskeresést Segítő Környezet 1991-1995. V:4.21 1995.05.08.

Az F-PROT program használt paraméterei:

F-PROT SECURE SCAN mód:

/all	minden file-t vizsgáljon kiterjesztéstől függetlenül
/nobreak	ne lehessen a vizsgálatot megszakítani CTRL-C-vel vagy CTRL-Break-kel
/report=a:\b\c.d	készítsen naplófile-t megadott néven
/old	ne üzenjen, ha 3 hónapnál régebbi a kereső
/command	mindenféleképpen parancssormódban üzemeljen

F-PROT HEURISTIC mód:

/all	minden file-t vizsgáljon kiterjesztéstől függetlenül
/nobreak	ne lehessen a vizsgálatot megszakítani CTRL-C-vel vagy CTRL-Break-kel
/report=a:\b\c.d	készítsen naplófile-t megadott néven
/old	ne üzenjen, ha 3 hónapnál régebbi a kereső
/command	mindenféleképpen parancssormódban üzemeljen
/append	az előző naplóállományhoz hozzáfűződik az új napló
/analyse	a heuristic mód kapcsolója

A SCAN program használt paraméterei:

/nopause	ne várjon billentyűre vírusészlelés esetén
/nobreak	ne lehessen a vizsgálatot megszakítani CTRL-C-vel vagy CTRL-Break-kel
/sub	az útvonalból nyíló könyvtárakat is nézze
/report a:\b\c.d	naplózzon az adott nevű fileba
/rptcor	fizikai hibás (corrupt) állományokat is listázza a naplózás
/rpterr	egyéb futás során észlelt hibákat (error) is listázza a naplózás

Kivételek és vakriadók kezelése

A vakriadók, a keresők által a vírusokból kiragadott kódrészlet véletlen egyezése tiszta kódrészlettel elég ritka esemény, de tisztázása: hogy tényleg nem vírus, nagy körültekintést és többszörös, szakértők általi megerősítést kíván.

Hamis detektálásnál pl. egy a nevezetes kivételt ellenőrzünk, akkor ha csak a DOS errorlevel értéke alapján döntenénk, ez egyértelműen sok vakriasztást okozna. A VSK gondoskodni tud ezen, hamis riadók kiszűréséről.

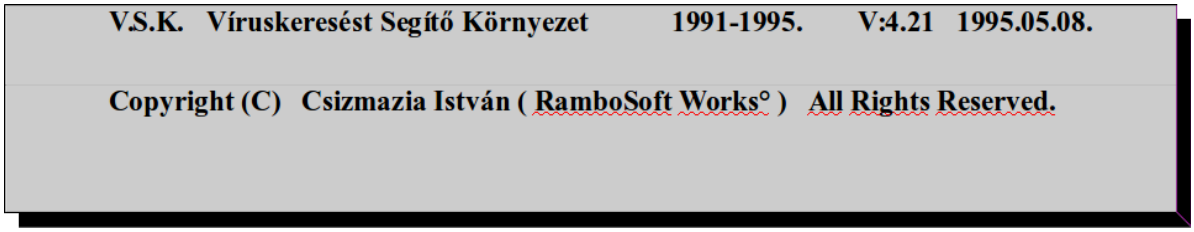
Ez úgy történik, hogy kiszűri a nevezetes kivételeket és csak az ettől különböző, igazi fertőzések okoznak riasztást. Ez a kivételállomány egyszerűen bővíthető.

Gyanús, de nem vírusos állományok

A heurisztikus keresésnél már említettem, hogy gyanús szekvenciát találhat az F-PROT. Ez nagy valószínűséggel nem vírus, csak vírusszerű tulajdonságai vannak vagy lehetnek: pl. furfangos visszafejtés gátlót, DEBUG ellenes védelmet tartalmaz. Eddig 2 ilyen, nem vírusos állományt sikerült felfedezni.

A KVIR.COM a K vírus irtója, melyet a VIRKILL készlethez mellékel Rudnai Tamás. A FYI.COM egy kis segédprogram a CDGRAB nevű direkt CD kezelő programcsomagban.

KVIR.COM	985	1993-03-21	18.28
FYI.COM	1329	1994-01-19	0.16



Vírusellenőrzés WINDOWS rendszer alól

SOHA ne indítsuk a VSK víruskeresést WINDOWS alól! A vizsgálat egyébként is ilyenkor arra és csak arra a DOS ablakra fog vonatkozni, a másikban mindeközben vígan tenyészhet a vírus, nem fogjuk észre venni.

A VSK rendszer batch állományai (A.BAT, B.BAT, REGGEL.BAT) elvileg indíthatók lennének a WINDOWS rendszer File Manager ablakából is: a megfelelő indító .BAT ikonjára kétszer rákattintunk és így indíthatnánk el az ellenőrzést. Mindazonáltal nem érdemes így használni: azon túlmenően, hogy a detektorok amúgy is lassú futása tovább lassul, mivel csak maghatározott időszeletet kap, a vírusészlelés processzor HALT utasítása több, mint drámai hatást okoz mondjuk a SMARTDRV cache-ében tanyázó adatainkra nézve, magyarul ez Windowsos adatvesztést eredményezne. Tehát indítása lehetséges, de nem ajánlatos. Vagy kiszállunk a Windowsból vagy csak egy sima keresőt pl. SCAN-t, WINSCAN-t használjunk ilyenkor, de a kivételeket akkor nekünk kell figyelni menet közben. Valamit valamiért.

Egyéb jó tanácsok

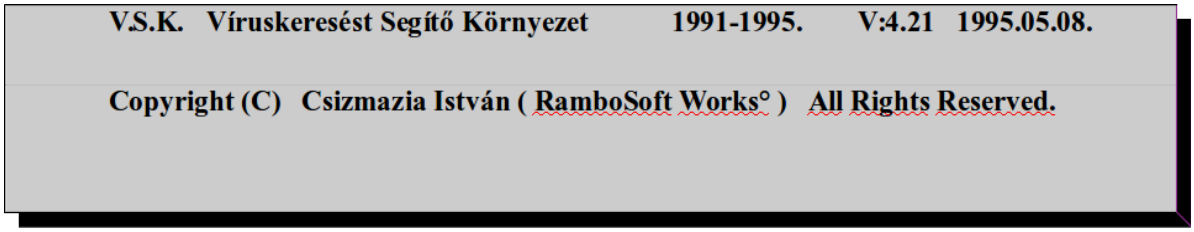
- Sose hagyjunk floppylemezt a meghajtóban, ha elmegyünk a géptől. Áramszünet esetén előfordulhat, hogy a gép a floppy-ról boot-ol és ha az boot-vírussal fertőzött, az máris a memóriába illetve a winchesterünkre kerülhet át.

- Ismeretlen eredetű lemezt mindig ellenőrizzük le.

- Ismeretlen eredetű programokat mindig ellenőrizzük le, csak ezek után futtassuk őket.

- Minden saját vagy pótolhatatlan munkát mentsünk napi rendszerességgel két különböző floppy lemezre. Egy PCTOOLS-t még megszerezhetünk valahogyan, de a saját elveszett munkánkat senki nem adhatja vissza nekünk.

- Mindig legyen egy tiszta, leragasztott rendszerlemezünk a közelben, kritikus esetekre félretéve.



- Rendszeresen vizsgáljuk a merevlemez állapotát a SCANDISK programmal. Lefagyáskor, áramszünet után a megszakított lemezműveleteknél (Windows alatt különösen) előfordulhat, hogy az adatok lemezre írása és a lemezterület adminisztrációja nincs szinkronban és ezzel bizonytalanná válik a merevlemez, adatvesztés fordulhat elő. Esetleges áramszünetet, WINDOWS lefagyását követően indítsuk újra a gépet. Adjuk ki a SCANDISK parancsot. Ez ellenőrzi, vannak-e logikailag szétesett láncolatok (CHKDSK hibák) a lemezen. Ha vannak, először is mentsük el újabb keletű, elmentetlen állományainkat, majd próbáljuk meg a Norton Disk Doctorral helyreállítani, amit lehet. Csak ezután adjuk ki a CHKDSK/F parancsot. Ez a szétesett láncolatokat helyreállítja a winchesteren, de sokszor előfordul, hogy az éppen utoljára használt állományok megsérülnek illetve új javításunk eredménye elveszik. Szétesett láncolatú gép tartós használata tömeges, akár az egész merevlemez tartalmát érintő adatroncsolódáshoz is vezethet. Tehát első a mentés, és csak utána az NDD, majd CHKDSK/F parancs. Clipper programok használata esetén ilyenkor inkább töröljük le az index file-okat és generáltassuk ezeket újra. A dBASE file-okhoz tartozó sérült indexállományok használata a TELJES adatbázis megsemmisülését is okozhatja.

- Kellő tapasztalat híján ne próbáljuk barkácsolni, mentesíteni: inkább kérjünk segítséget egy hozzáértő kollégától. Erre is tudok egy példát mondani: ha a Michelangelo egy speciális átiratával van dolgunk, előfordulhat, hogy a CLEAN azt eredeti változatként ismeri fel és a mentesítés után (az eredetileg megjelölt X.-ik szektorhelyet próbálja visszaállítani, de ez a mutáns egy MÁSIK, Z.-ik területre mentette el az eredeti merevlemez adatokat, és így a MENTESÍTÉSTŐL) omlik össze végleges adatvesztést okozva a gép (természetesen az aljas vírusátvakaró ilyetén szándéka szerint).

- Ha megtörtént a baj, és biztos a vírusfertőzöttség, haladéktalanul értesítsük a velünk kapcsolatban lévő cégeket: ez erkölcsi kötelesség, ilyen esetekben a hallgatás felér egy tudatos bűncselekménnyel. Nem szégyen, ha önhibánkon kívül vírust találunk.

- A magyar fejlesztésű vírusdetektorokat vagy a szövegállományban olvashatóan tárolt szekvenciájú keresőket lehetőleg NE engedjünk külföldre kerülni.

```
V.S.K.  Víruskeresést Segítő Környezet        1991-1995.      V:4.21  1995.05.08.

Copyright (C)  Csizmazia István ( RamboSoft Works° )  All Rights Reserved.
```

- Ha egy teljes partíciót használunk lemeztömörítés céljára (pl. STACKER, DOUBLESPACE, SPEEDSTORE, stb.), akkor ne a fizikai helyén keressünk vírust, hanem a keletkező új logikai drive-ot vegyük csak fel a REGGEL.BAT soraiba. Ezzel jelentős futásidőt takaríthatunk meg és nem dolgozunk feleslegesen.

Copyright-ok

F-PROT	is a trademark of Frisk Software International
SCAN	is a trademark of McAfee Associates

Vírusmentes környezetet kíván a szerző:

.....

Csizmazia István

Budapest, 1995. május 8.