FÜGGETLEN ANTI-VÍRUS TESZTELÉS

Dr. Leitold Ferenc
Veszprog Kft., Veszprémi Egyetem Információs Rendszerek Tsz.
fleitold@veszprog.hu

A szoftver tesztelőknek és minőségbiztosítási szakembereknek a szoftverüket a lehetséges legnagyobb variációjú környezetben kell tesztelniük. Az anti-vírus termékek esetén ez sokkal bonyolultabb, hiszen a termékek folyamatosan változnak, újabb és újabb eljárásokat tartalmaznak. Az anti-vírus rendszerek több tízezer keresési és eltávolítási algoritmust használnak, melyeket egyrészt nagy számú víruspéldányon, másrészt vírusmentes állományokon kell tesztelni. A tesztelési eljárás célja nem az anti-vírus szoftverek rangsorolása, a teszteredmények nem jelentik azt, hogy az egyik anti-vírus szoftver jobb, mint a másik. A teszteredmények csupán azt mutatják, hogy az anti-vírus rendszerek bizonyos esetekben hibásan működnek. Fő célunk, hogy a teszteredményekkel segítsük a számítógép-felhasználókat az anti-vírus szoftver választásában, illetve segítsük az anti-vírus fejlesztőket, hogy a terméküket jobbá és hibamentessé tegyék.

Bevezetés

Napjainkban egyre többen kerülünk a kérdés elé, hogyan oldjuk meg adataink és számítógépes rendszerünk vírusok elleni védelmét. Sok lehetőség adott, számos vírusirtó különböző tudással, támogatással és árfekvéssel áll rendelkezésre. Mind a felhasználók, mind pedig a fejlesztő cégek szempontjából elengedhetetlenül fontos feladat, hogy az egyes vírusvédelmi programok, rendszerek tudása korrekt módon megismerhető legyen. Sajnos a feladat nem egyszerű, a vírusvédelmi programok, rendszerek több tízezer vírust azonosító és eltávolító eljárásait nem könnyű tesztelni. Az előadás egy olyan automatikus, illetve fél-automatikus rendszert mutat be, mely képes arra, hogy vírusadatbázisában lévő vírusokat ellenőrzött körülmények között szaporítsa, majd a tenyésztett vírusokon tesztelje a vírusvédelmi programokat, rendszereket, mind keresési, mind pedig irtási szempontból különböző platformok alatt. Az ezt követő kiértékelés során összesített eredmények mutatják a vírusvédelmi programok, rendszerek gyenge pontjait.

Az OMFB IKTA támogatásával létrejött projekt során egy speciális többfunkciós cluster kiépítése történt meg PC-s hardverarchitektúrából, alapvetően vírustenyésztési, ill. víruskereső tesztelési feladatokra. Alapvető célunk volt, hogy a rendszerrel minél több vírus tudjunk letenyészteni, illetve egy olyan rendszert kidolgozni, amely automatizáltan a tenyésztés mellett megoldja a víruskereső szoftverek tesztelését a tenyészett a vírusokon, majd kimutatást készít az egyes víruskeresők találati, irtási eredményeiből. Ily módon a többfunkciós állomások (kliensek) feladatkiosztása a vezérgépen (szerver) keresztül egy prioritási szintrendszer alapján történik. A kliensek köre dinamikusan változhat, kliensek kapcsolódhatnak a szerverre, illetve kapcsolódhatnak le onnan.

A projekt eredményeként egy olyan minőségbiztosítási szolgáltatást sikerült kifejlesztenünk, mely mind a felhasználókat segítheti vírusvédelmi rendszerük kialakításában, mind pedig az anti-vírus fejlesztőket rendszerük tökéletesítésében.

1. Vírustenyésztő rendszer

A vírusok típusától függően a tenyésztő rendszer

- linux script (shell, perl, stb...),
- VMware vagy Win4Lin és
- esetleg valamilyen automatizáló program (Macro Express, AutoMate vagy Wintask)

együttese.
A tenyésztő rendszer az egyes vírusok tenyésztését a vírus típusától függő algoritmus szerint és eszközök felhasználásával végzi. A tenyésztés szempontjából az alábbi vírustípusokat különböztetjük meg:

1.1. DOS file-vírusok

DOS file-vírusok esetén a tenyésztés DOSemu vagy VMware alatt történik, mivel így a rendszer kívülről könnyen ellenőrizhető. Adott egy DOSemu/VMware image, amely egy lementett, mount-olható (8832-es offszettől) file. Ebbe generál a rendszer egy autoexec.bat-ot, mely felváltva, ciklikusan lefuttatja a goat file-okat és a vírushordozó programot. Az autoexec mindenféle műveletet tartalmazhat, másolást, futtatást, stb. A DOSemu futását kívülről egy program figyeli, és amennyiben az megadott idő (2 perc) múlva sem áll le, automatikusan leállítja. A tenyésztés végén a rendszer megvizsgálja, hogy mely file-ok változtak és melyek nem. Amennyiben valamelyik goat file megváltozott, úgy a rendszer elmenti a változott file-okat. Megvizsgálja továbbá, hogy más programrészeket tartalmazó programterületek változtak-e. Ha igen, akkor azok is mentésre kerülnek.

1.2. Win32 file-vírusok (NE/PE)

A tenyésztés lényegében ugyanúgy zajlik, mint a DOS-os file-vírusoknál, néhány szükségszerű különbséggel:

- Nem DOSemu alatt fut a tenyésztés, hanem VMWare és Win4Lin alatt. A DOSemu ugyanis nem alkalmas a Windows 9x/2000/Me operációs rendszerek futtatására.
- A rendszer nem autoexec.bat-ot generál, hanem valamilyen automatizáló-programmal indít el egy batch file-t, mely lefuttatja a vírusokat, valamint a goatokat.

A tenyésztési környezet függ a használt programtól, mivel VMWare esetén speciális image-re van szükség, míg Win4Lin esetén elég egy könyvtárat kijelölni a natív file-rendszeren. Minden esetben a program másolja ki a (remélhetőleg) fertőzött file-okat egy megadott helyre, ahol ugyanúgy egy előzetes összehasonlító eljárás alapján történik a mentés, mint a DOS vírusok esetén.

1.3. Boot vírusok

A boot-vírusok tenyésztése a DOS vírusok tenyésztéséhez hasonlóan DOSemu vagy VMWare alatt történik. A boot vírusok tenyésztése során azonban nem file-okat, hanem a fertőzött lemez image-eit kell elmenteni. A különböző lemezformátumokhoz különböző emulátorfuttatások tartoznak. A tenyésztés nehézsége abban áll a file-vírusok tenyésztéséhez

képest, hogy itt futásonként csak egy boot szektor, illetve MBR lesz fertőzött. Ez azt jelenti, hogy újabb fertőzések eléréséhez többször kell indítani az emulátort. Külön problémát jelent, ha olyan floppy-n vagy floppy image-en található olyan boot-vírusról van szó, amely a lefutása után nem képes az eredeti operációs rendszert elindítani. Ilyen esetben először a merevlemez (HD) image fertőzését végezzük el, majd ezt követően kerül sor a fertőzött HD image használatával floppy image-ek fertőzésére.

1.4. Makró vírusok

A makróvírusok tenyésztése a *Win32 file-vírusok (NE/PE)* tenyésztéséhez hasonlóan szintén Windows emuláló programmal történik. A tenyésztés végrehajtását ezen belül egy automatizáló program vezérli. A tenyésztés lényegében abból áll, hogy a megfelelő makrózási lehetőséget biztosító program (Word, Excel...) elindítása után beolvassa a fertőzött file-t, majd új file-okat nyit, elmenti őket, létező file-okat olvas be, és elmenti más helyre. A makrózási lehetőséget biztosító programból történő kilépést követően a rendszer összehasonlítást végez, azonban a korábbi esetektől eltérően itt a dokumentumok makróit vizsgálja meg. A dokumentum makróinak száma, elnevezései és tartalma alapján dönti el, hogy mely dokumentumok lettek fertőzöttek.

1.5. Script vírusok

A script vírusok tenyésztése VMware alatt futó Windows operációs rendszer alatt történik. A vírusos állomány lefuttatása / betöltése után várakozunk arra, hogy a vírus maga küldözgessen e-mail-eket, benne újabb víruspéldányokkal. A sikeres tenyésztés szempontjából alapvető fontosságú, hogy a vírusok számára megfelelő táptalajt biztosítsunk. A Script vírusok tenyésztéséhez a konkrét vírus működésétől függően szükséges a megfelelő levelezést biztosító alkalmazás (Outlook, Outlook Express), illetve a script végrehajtásához szükséges Microsoft Host Scripting. A megfelelő levelezést biztosító alkalmazásnál szükséges a vírus működéséhez szükséges paraméterek beállítása (pl. címlista). A tenyésztett vírusokat egyszerűen elmenthetjük a címlista által megadott címre érkező levelek mentésével.

2. Anti-vírus tesztelő és kiértékelő rendszer

Az anti-vírus programok tesztelése két fő részből áll: Az anti-vírus programok futtatása során elkészül a víruskeresésről és/vagy vírusirtásról szóló, a program tevékenységeit rögzítő naplófile. A vírusirtás során a futtatás további “eredménye” azok az állományok, amelyek esetén megtörtént a vírusirtás. A naplófile és a vírustalanított file-ok vizsgálatát végzi az eredmények kiértékelését végző rendszer.

2.1. Anti-vírusok futtatása

Az anti-vírus programok futtatása történhet egyrészt “native” környezetben” és emulált környezetben egyaránt. Az automatikus végrehajtást azon anti-vírus programok esetén, melyek parancssorban nem paraméterezhetők, a WinTask és a MacroExpress makrózási lehetőséget biztosító segédprogramokkal oldjuk meg. Az egyes anti-vírusokat külön-külön kell futtatnunk különböző operációs rendszerek alatt és a keresést befolyásoló különböző beállítások mellett (pl. heurisztika bekapcsolása).

2.2. Eredmények kiértékelése

Az eredmények kiértékelése fertőzött file-onként a mellékelt algoritmus szerint történik. A kiértékelés során különös figyelmet érdemel a vírustalanított állomány és az eredeti goat állomány összehasonlítása. Itt "azonos"-nak fogadunk el olyan, egyébként néhány byte-ban különböző állományokat is, melyek esetén a működőképesség nem változott. Tesszük ezt azért, mert léteznek olyan vírusok, melyek esetén nem létezik olyan algoritmus, melynek segítségével az eredeti állomány visszaállítható (pl. a vírus nem tárolt el elegendő információt a visszaállításhoz). Egy vírus valamennyi példányának ellenőrzését követően egy összesítés történik, mely statisztikailag tartalmazza a helyes felismerés és irtás arányát.

3. Előzetes eredmények

3.1. Tenyésztési eredmények

A vírusok tenyésztését három fázisban végeztük (2001. december 31-ig). Az egyes fázisok között értékeltük a tenyésztési eredményeket és ezek alapján módosítottunk a tenyésztési eljáráson a hatékonyság növelése érdekében. Az egyes tenyésztési fázisok tenyésztési eredményei az alábbiak:

	Tenyésztésre került vírusok száma	**Tenyésztett vírusminták száma**	**Tenyésztés ideje**
1. fázis	10911	1766781	1 hét
2. fázis	2196	651350	2 hét
3. fázis	11642	12359729	29 hét
Összesen	26749	14777860	32 hét

Az állományok nagy száma miatt a tenyésztett vírusokat DAT archiváló egységen rögzítettük.

Az elkészült vírusminta-adatbázis kiváló alapot jelent az anti-vírus programok tesztelésére, melyet a tenyésztéssel párhuzamosan kezdtünk el.

3.2. Hardware és szoftver környezet

A teszteléshez az alábbi rendszereket használtuk:

Intel celeron processor 333-433MHz , 64-128Mb SDRAM
Operációs rendszerek: Windows 95,98,Me,NT4,2000; DOS; Debian GNU/Linux 2.2

3.3. Tesztelt vírusok

A teszteléshez a 3.1. fejezet táblázatában meghatározott vírusokat használtuk

3.4. Tesztelt anti-vírus programok

Az alábbi anti-vírus programokat teszteltük:

- Panda Platinum
- Panda Titanium
- Sophos Anti-Virus

- Kaspersky Anti-Virus Personal Pro
- F-Secure Anti-Virus
- ViRobot Professional
- Norton AntiVirus 2001 Free Trialware
- Norton AntiVirus 2002 Free Trialware
- VirusBuster
- Norman Virus Control
- McAfee VirusScan for Unix Linux
- McAfee VirusScan Command Line for DOS
- McAfee VirusScan Multiplatform
- Frisk's F-PROT Antivirus

3.5. Keresési/találati eredmények

Az egyes anti-vírusokat a tesztelendő vírusok kisebb (kb. 700000 – 1000000 fertőzött állomány) csoportjára futtattuk. Az alábbi táblázatok a naplófile-t korrektül létrehozó anti-vírusok összesített információit tartalmazza a létrehozott naplófile alapján.

F-Secure	Scanned	Infected	Disinfected
Win95	14777860 (100%)	12003735 (81,23%)	9494197 (64,25%)
Win98	14777860 (100%)	12003735 (81,23%)	22923 (0,16%)
WinMe	14777860 (100%)	12003735 (81,23%)	9494197 (64,25%)
WinNT	14777860 (100%)	12003735 (81,23%)	9494197 (64,25%)
Win2000	14777860 (100%)	12003735 (81,23%)	9494197 (64,25%)

A F-Secure tesztelését Windows 98 alatt, az alacsony eltávolítási arányt igazolandó, kétszer végeztük el, különböző számítógépen.

Sophos Sweep	Scanned	Infected	Disinfected
Win95	14777860 (100%)	11897279 (80,51%)	0 (0%)
Win98	14777860 (100%)	11897279 (80,51%)	0 (0%)
WinMe	14777860 (100%)	11897279 (80,51%)	0 (0%)
WinNT	14777860 (100%)	11901163 (80,51%)	0 (0%)
Win2000	14777860 (100%)	11901163 (80,51%)	0 (0%)
DOS	14777860 (100%)	11901163 (80,51%)	0 (0%)
Linux	14777860 (100%)	11901163 (80,51%)	0 (0%)

A Sophos termékek nem képesek a vírust eltávolítani a programállományokból.

VirusScan	Scanned	Infected	Suspicious	Disinfected
Win95	N/A	N/A	N/A	N/A
Win98	N/A	N/A	N/A	N/A
WinMe	N/A	N/A	N/A	N/A
WinNT	14777860 (100%)	11952446 (80,88%)	N/A	9680696 (65,51%)
Win2000	14777860 (100%)	11952446 (80,88%)	N/A	9680696 (65,51%)
DOS	14777860 (100%)	11901163 (80,51%)	22033717 (14,91%)	9626297 (65,14%)
Linux	14777860 (100%)	11901163 (80,51%)	22033717 (14,91%)	9626297 (65,14%)

A VirusScan tesztelése során Windows 95,98 és Me alatt olyan probléma merült fel, mely megakadályozta a naplófile készítését. Ilyen esetben a tesztelést megismételtük, melynek során a probléma ugyanúgy jelentkezett.

VirusBuster	Scanned	Infected	Suspicious	Disinfected
Win95	14777860 (100%)	8363238 (56,59%)	1598856 (10,82%)	3555510 (2,41%)
Win98	14777860 (100%)	8363238 (56,59%)	1598856 (10,82%)	3555510 (2,41%)
WinMe	14777860 (100%)	8363238 (56,59%)	1598856 (10,82%)	3555510 (2,41%)
WinNT	14777860 (100%)	8372534 (56,66%)	1594178 (10,79%)	3593915 (2,43%)
Win2000	14777860 (100%)	8372534 (56,66%)	1594178 (10,79%)	3593915 (2,43%)
DOS	14777860 (100%)	9157338 (61,97%)	1409603 (9,54%)	3555510 (2,41%)
Linux	14777860 (100%)	9157338 (61,97%)	1608144 (10,88%)	3555510 (2,41%)

Frisk's F-PROT	Scanned	Infected	Disinfected
Win95	14777860 (100%)	11802879 (79,87%)	9850145 (66,65%)
Win98	14777860 (100%)	11802879 (79,87%)	9850145 (66,65%)
WinMe	14777860 (100%)	11802879 (79,87%)	9850145 (66,65%)
Win2000	14777860 (100%)	11802879 (79,87%)	9850145 (66,65%)
WinNT	14777860 (100%)	11802879 (79,87%)	9850145 (66,65%)
DOS	14777860 (100%)	11802879 (79,87%)	9850145 (66,65%)

Norton Antivirus	Scanned	Infected	Disinfected
Win95	14777860 (100%)	11589225 (78,42%)	2323098 (15,72%)
Win98	14777860 (100%)	11589225 (78,42%)	2323098 (15,72%)
WinMe	14777860 (100%)	11589225 (78,42%)	2323098 (15,72%)
WinNT	14777860 (100%)	11264025 (76,22%)	2065096 (13,97%)
Win2000	14777860 (100%)	11264025 (76,22%)	2065096 (13,97%)

A többi anti-vírus esetén (Panda, Kaspersky, Virobot, Norman) a tesztelési eljárás során olyan probléma merült fel, mely megakadályozta a naplófile készítését. Ilyen esetben a tesztelést megismételtük, melynek során a probléma ugyanúgy jelentkezett.

A keresésre vonatkozó tesztelési eredmények alapján megállapíthatjuk, hogy a tesztelési eljárást korrektül végrehajtó és a naplófile-t elkészítő anti-vírusok közül egyedül a Frisk cég F-PROT termékére igaz az, hogy platformtól függetlenül pontosan ugyanazt a szolgáltatást képes nyújtani.

3.6. Irtási eredmények

Az egyes anti-vírusokat a tesztelendő vírusok kisebb (kb. 700000 – 1000000 fertőzött állomány) csoportjára futtattuk. Az alábbi táblázatok az irtott állományok vizsgálata során készültek. Az összehasonlíthatóság kedvéért minden anti-vírus esetén az általa irtott (irtani próbált) állományok számának arányában adjuk meg az irtási eredményeket.

F-Secure

	Win95	Win98	WinMe	WinNT	Win2000
A tisztított file kisebb	1,40%	N/A	1,40%	1,40%	1,40%
0 érték változott a file-ban	3,63%	N/A	3,63%	3,63%	3,63%
A tisztított file több, mint 16 byte-tal hosszabb	1,61%	N/A	1,61%	1,61%	1,61%
0 byte változott a programkódban	2,14%	N/A	2,14%	2,14%	2,14%
EXE file kezdete megváltozott	0,16%	N/A	0,16%	0,16%	0,16%
CS:IP/SS:SP változott	1,01%	N/A	1,01%	1,01%	1,01%
EXE header mérete változott	0,81%	N/A	0,81%	0,81%	0,81%

Windows 98 alatt az F-Secure minimális mennyiségű vírust irtott, mely így nem képezheti az analízálás alapját.

Frisk's F-PROT

	Win95	Win98	WinMe	WinNT	Win2000	DOS
A tisztított file kisebb	1,64%	1,64%	1,64%	1,64%	1,64%	1,63%
0 érték változott a file-ban	4,38%	4,38%	4,38%	4,38%	4,38%	4,40%
A tisztított file több, mint 16 byte-tal hosszabb	1,30%	1,30%	1,30%	1,30%	1,30%	1,48%
0 byte változott a programkódban	3,86%	3,86%	3,86%	3,86%	3,86%	3,91%
EXE file kezdete megváltozott	0,44%	0,44%	0,44%	0,44%	0,44%	0,44%
CS:IP/SS:SP változott	1,35%	1,35%	1,35%	1,35%	1,35%	1,49%
EXE header mérete változott	0,81%	0,81%	0,81%	0,81%	0,81%	0,95%

Az egyes operációs rendszerek alatt minimális különbség mutatkozott az irtási tulajdonságokat tekintve.

Kaspersky Anti-Virus Personal Pro

	Win95	Win98	WinMe	WinNT	Win2000
A tisztított file kisebb	1,40%	1,40%	1,39%	1,40%	1,40%
0 érték változott a file-ban	3,57%	3,57%	3,56%	3,57%	3,57%
A tisztított file több, mint 16 byte-tal hosszabb	1,61%	1,61%	1,43%	1,61%	1,61%
0 byte változott a programkódban	2,07%	2,07%	2,02%	2,07%	2,07%
EXE file kezdete megváltozott	0,11%	0,11%	0,11%	0,11%	0,11%
CS:IP/SS:SP változott	0,97%	0,97%	0,97%	0,97%	0,97%
EXE header mérete változott	0,77%	0,77%	0,70%	0,77%	0,77%

Az egyes operációs rendszerek alatt minimális különbség mutatkozott az irtási tulajdonságokat tekintve.

Norman Virus Control

	Win95	Win98	WinMe
A tisztított file kisebb	3,35%	3,35%	3,35%
0 érték változott a file-ban	5,73%	5,73%	5,73%
A tisztított file több, mint 16 byte-tal hosszabb	3,69%	3,69%	3,69%
0 byte változott a programkódban	34,66%	34,68%	34,68%
EXE file kezdete megváltozott	0,04%	0,00%	0,00%
CS:IP/SS:SP változott	36,91%	36,88%	36,88%
EXE header mérete változott	3,35%	3,31%	3,31%

A Norman Virus Control-nak csak az említett operációs rendszereken futó változatát teszteltük, WinNT és Win2000 alatti változat nem volt elérhető. Az egyes operációs rendszerek alatt minimális különbség mutatkozott az irtási tulajdonságokat tekintve.

Panda Platinum

A Panda Platinum a tesztelt operációs rendszerek alatt nem volt képes irtani.

Panda Titanium

	Win95	Win98	WinMe	WinNT	Win2000
A tisztított file kisebb	2,47%	2,47%	2,47%	2,63%	2,63%
0 érték változott a file-ban	2,97%	2,97%	2,97%	3,98%	3,98%
A tisztított file több, mint 16 byte-tal hosszabb	3,73%	3,73%	3,73%	3,63%	3,63%
0 byte változott a programkódban	13,91%	13,91%	13,91%	11,15%	11,15%
EXE file kezdete megváltozott	0,11%	0,11%	0,11%	0,40%	0,40%
CS:IP/SS:SP változott	5,20%	5,20%	5,20%	4,60%	4,60%
EXE header mérete változott	2,04%	2,04%	2,04%	2,27%	2,27%

Az egyes operációs rendszerek alatt minimális különbség mutatkozott az irtási tulajdonságokat tekintve, attól függően, hogy az adott operációs rendszer NT-alapú vagy sem.

Sophos Anti-Virus

A Sophos Anti-Virus a tesztelt operációs rendszerek alatt nem volt képes irtani.

VirusBuster

	Win95	Win98	WinMe	WinNT	Win2000	DOS	Linux
A tisztított file kisebb	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%
0 érték változott a file-ban	2,33%	2,33%	2,33%	2,30%	2,30%	2,32%	2,32%
A tisztított file több, mint 16 byte-tal hosszabb	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%
0 byte változott a programkódban	19,60%	19,60%	19,60%	19,39%	19,39%	19,58%	19,58%
EXE file kezdete megváltozott	0,44%	0,44%	0,44%	0,44%	0,44%	0,55%	0,55%
CS:IP/SS:SP változott	0,33%	0,33%	0,33%	0,33%	0,33%	0,44%	0,44%
EXE header mérete változott	0,00%	0,00%	0,00%	0,00%	0,00%	0,11%	0,11%

Az egyes operációs rendszerek alatt minimális különbség mutatkozott az irtási tulajdonságokat tekintve, attól függően, hogy az adott operációs rendszer Windows alatt fut vagy sem. A VirusBuster volt az egyetlen anti-vírus, amely nem “csökkentette” egyetlen esetben sem az irtott file eredeti méretét és nem is növelte meg feleslegesen azt.

ViRobot Professional

	Win95	Win98	WinMe	WinNT	Win2000
A tisztított file kisebb	3,81%	3,81%	3,81%	3,94%	3,94%
0 érték változott a file-ban	2,34%	2,34%	2,34%	2,39%	2,39%
A tisztított file több, mint 16 byte-tal hosszabb	0,72%	0,72%	0,72%	0,77%	0,77%
0 byte változott a programkódban	6,05%	6,05%	6,05%	6,11%	6,11%
EXE file kezdete megváltozott	1,29%	1,29%	1,29%	1,30%	1,30%
CS:IP/SS:SP változott	1,64%	1,64%	1,64%	1,65%	1,65%
EXE header mérete változott	0,92%	0,92%	0,92%	0,92%	0,92%

Az egyes operációs rendszerek alatt minimális különbség mutatkozott az irtási tulajdonságokat tekintve, attól függően, hogy az adott operációs rendszer NT-alapú vagy sem.

McAfee VirusScan

	Win95	Win98	WinMe	WinNT	Win2000	DOS	Linux
A tisztított file kisebb	1,57%	1,57%	1,57%	1,52%	1,52%	1,55%	1,55%
0 érték változott a file-ban	3,83%	3,83%	3,83%	3,65%	3,65%	3,87%	3,87%
A tisztított file több, mint 16 byte-tal hosszabb	1,16%	1,16%	1,16%	1,27%	1,27%	1,00%	1,00%
0 byte változott a programkódban	2,79%	2,79%	2,79%	2,76%	2,76%	2,67%	2,67%
EXE file kezdete megváltozott	0,17%	0,17%	0,17%	0,20%	0,20%	0,11%	0,11%
CS:IP/SS:SP változott	1,69%	1,69%	1,69%	1,75%	1,75%	1,40%	1,40%
EXE header mérete változott	0,53%	0,53%	0,53%	0,65%	0,65%	0,42%	0,42%

Az egyes operációs rendszerek alatt minimális különbség mutatkozott az irtási tulajdonságokat tekintve, attól függően, hogy az adott operációs rendszer Windows alatt fut vagy sem, illetve, hogy a Windows NT-alapú vagy sem.

Norton AntiVirus

	Win95	Win98	WinMe	WinNT	Win2000
A tisztított file kisebb	2,18%	2,18%	2,18%	1,72%	1,72%
0 érték változott a file-ban	6,68%	6,68%	6,68%	5,65%	5,65%
A tisztított file több, mint 16 byte-tal hosszabb	3,19%	3,19%	3,19%	1,69%	1,69%
0 byte változott a programkódban	4,98%	4,98%	4,98%	3,62%	3,62%
EXE file kezdete megváltozott	1,01%	1,01%	1,01%	0,96%	0,96%
CS:IP/SS:SP változott	1,67%	1,67%	1,67%	1,53%	1,53%
EXE header mérete változott	2,07%	2,07%	2,07%	1,90%	1,90%

Az egyes operációs rendszerek alatt minimális különbség mutatkozott az irtási tulajdonságokat tekintve, attól függően, hogy az adott operációs rendszer NT-alapú vagy sem.

4. Szolgáltatások

Az OMFB IKTA támogatásával létrejött projekt lezárását követően az anti-vírus tesztelésre vonatkozó információkat tovább bővítjük, mind mennyiségileg, mind pedig a felmerülő igényeknek megfelelően minőségileg is. A statisztikai összefoglaló eredményeket pedig az Interneten folyamatosan közzé tesszük a *http://www.checkvir.com* illetve a *http://www.checkvir.hu* címen.

Anti-vírus minőségbiztosító szolgáltatásainkkal az alábbi csoportokat célozzuk meg:

- **Felhasználók**, akik szeretnék a számítógépeiket minél biztonságosabb körülmények között használni. Az anti-vírus tesztelési eredményeinket, melyeket weboldalunkon közzéteszünk mindenki szabadon felhasználhatja saját vírusvédelmi rendszerének tökéletesítéséhez. Egyedi igények alapján természetesen szükség lehet az eddigi vírustapasztalatokból eredő részletes vizsgálatra, vírusvédelmi szabályzat készítésére is.
- **Anti-vírus fejlesztők**, akik szeretnék termékeiket minél megbízhatóbbá tenni. Számukra megfelelő szerződés esetén rendelkezésre bocsátjuk a problémák

reprodukálásához szükséges eszközöket. Ezen túlmenően szükség lehet speciális, egyedi tesztelési eljárások elvégzésére is.

- **Szakújságírók**, akik szeretnék az anti-vírus trendekről informálni az olvasókat. Természetesen lehetőség van komplett, összehasonlító tesztelési eljárások lefuttatására.

5. Összegzés

Az előzetes eredmények során a vírusok felismerésének és így az irtási lehetőségeknek az alacsony értéke abból is adódhatott, hogy néhány esetben demo változatot használtunk a teszteléshez. Az eredmények azonban azt mutatják, hogy az anti-vírus programok nagy része bizonyos esetekben hibásan működik, nemcsak a felhasználók elvárásaihoz, hanem a más platformon futó verzióikhoz képest is. Ez megmutatkozott egyrészt a keresési eredmények, másrészt pedig az irtási tulajdonságok területén is.

Az anti-vírus fejlesztőknek tehát van még feladatuk, hogy termékeiket a lehetőségekhez képest hibamentessé tegyék és ebben hatékony segítséget tudnak nyújtani a projekt keretében kifejlesztett szolgáltatások.

Irodalomjegyzék

[1] Leitold, F.: A számítógépes vírusok felismerésének elmélete és gyakorlata
Kandidátusi értekezés, Budapest, 1994

[2] Leitold, F.: Automatic Virus Analyser System
Proceeding of the 5th International Virus Bulletin Conference, Boston USA, 1995, pp. 99-107.

[3] Leitold, F.: Automatikus vírusanalizáló rendszer
Proceeding of the HISEC'96 Confrence, Budapest, 1996, pp. 112-119.