MONDD, TE KIT VÁLASZTANÁL?
VÍRUSVÉDELMI RENDSZEREK MINŐSÍTÉSE ÉS TESZTELÉSE

Dr. Leitold Ferenc, Veszprémi Egyetem, Veszprog Kft., fleitold@veszprog.hu
Kárpáti Nikoletta, Veszprog Kft., niki@veszprog.hu

BEVEZETÉS

A minőség tágabb értelemben az emberiség történelmével egyidős, azonban korszerű értelmezése a múlt század elején jelent meg, az ipari termelés elterjedésével. Napjainkban egyre nagyobb hangsúly fordítódik a minőségbiztosításra, azaz a termelés és a fogyasztás magas színvonalú minőségére, amely a fogyasztóvédelem, és a fogyasztói igények kielégítése mellett a termelő nyereségét is eredményezi, ami a nemcsak a vállalkozás gazdasági felemelkedését jelenti, hanem hasznos és biztonságos a társadalom számára is. A szoftver is egy termelőfolyamat végterméke, ezért a minőségbiztosítás ezen esetben is elengedhetetlen feltétel. A szoftvertesztelők, a minőségbiztosítással foglalkozó szakemberek a programjaikat a lehetőségekhez képest a legváltozatosabb környezetekben, nagyon sok bemeneti paraméter mellett tesztelik. Antivírus termékek esetén ez még nehezebb és bonyolultabb feladat, hiszen a termék állandóan változik, a fejlesztők újabb és újabb eljárásokat építenek bele. Az antivírus szoftverek általában néhány ezer vírusfelismerő és vírusmentesítő algoritmust tartalmaznak, melyeket sok vírusmintával és természetesen vírusmentes file-okkal is kell tesztelni.

A CHECKVIR PROJECT

A CheckVir projekt alapvető célja, hogy antivírus fejlesztőktől függetlenül teszteljen antivírus szoftvereket és megoldásokat, segítve a felhasználókat és az antivírus fejlesztő cégeket egyaránt. A projekt elindítását az Oktatási Minisztérium Kutatás-fejlesztési Helyettes Államtitkársága (IKTA-00033/2000), valamint az Informatikai és Hírközlési Minisztérium (SZT-IS-5/2001/10/321, SZT-IS-14/27) támogatta. A projekt során 2002 áprilisától kezdődően havonta végezzük el a vírusvédelmi szoftverek tesztelését változó platformon, folyamatosan megújuló vírusmintákkal.

MINŐSÍTÉS

A CheckVir antivírus tesztelési projekt keretében 2004. januártól kezdődően végezzük a vírusvédelmi rendszerek minősítését. A meghatározott feltételeknek megfelelő antivírus rendszerek havonta részesülnek a címben, mely azt bizonyítja, hogy az antivírus rendszerek a legelterjedtebb vírusok ellen sikeresen képesek felvenni a harcot. A minősítési eljáráson minden, a CheckVir projekt keretében tesztelt antivírus termék részt vesz. Lehetőség van arra is, hogy egy fejlesztő több termékből álló termékcsoportja vegyen részt a minősítési eljáráson. Ilyenkor a minősítést a több termék együttesen kapja meg.

MINŐSÍTÉSI SZINTEK

A minősítés során két szintet különböztetünk meg:

1. **Standard Level:** csak a vírusok keresésére vonatkozó információkat vizsgáljuk. A vírusvédelmi rendszernek valamennyi teszteléshez használt vírus minden példányát azonosítani kell.
2. **Advanced Level:** a vírusok keresését és irtását is vizsgáljuk. A vírusvédelmi rendszernek a Standard Level feltételén túlmenően az alábbi feltételeknek kell megfelelnie:
   - A vírus kódját a fertőzött objektumból el kell távolítani, minden olyan vírus esetén, amelyiknél ez elvileg megtehető.
   - A visszaállított objektumnak továbbra is teljes értékűnek kell lennie a használhatóság szempontjából.
   - Bármilyen információvesztés megengedett, amennyiben a vírusvédelmi program erről a felhasználót tájékoztatja. Ide értendő például az az eset is, ha az antivírus egy makróvírus eltávolítása során törli a dokumentum többi makróját, és erről a felhasználót informálja.

VÍRUSKERESÉSI ELJÁRÁSOK

A tesztelés során vizsgáljuk az antivírus rendszerek manuális indítású **(on-demand)**, valamint a folyamatosan figyelő védelem **(on-access)** víruskeresési képességét.

A teszteléshez a legelterjedtebb vírusok fertőzőképes példányait használjuk. A teszteléshez használt víruscsomag összeállításának alapja a tesztelés tárgyhónapját megelőző hónap 1. napjáig közzétett Wildlist (www.wildlist.org) víruslisták összessége. A tesztcsomagban legalább 80%-ban olyan vírusok szerepelnek, melyek megtalálhatók az utolsó 3 víruslista valamelyikében, a maradék 20%-a olyan vírusokat is tartalmazhat, melyek csak régebbi víruslistákban jelentek meg. A tesztcsomagban lévő vírusok listáját minden hónap 1-éig a www.checkvir.hu, illetve a www.checkvir.com oldalon nyilvánosságra hozzuk.

A minősítési eljárásról, az antivírusok futtatásáról szöveges összefoglaló, az eredményekről statisztikai összefoglaló készül, melyet a www.checkvir.hu és a www.checkvir.com weboldalon a tárgyhónapot követő hónap 10-éig közzéteszünk.

TESZTEREDMÉNYEK

2004. februárjában végeztük először az antivírus rendszerek minősítését mind a keresés, mind pedig az irtás szempontjából.

Termék	AVG Anti-Virus	BitDefender Professional Edition	Dr. Web for Windows	eTrust Antivirus v7	F-Secure Anti-Virus for Windows NT Server
Verziószám	7.0 Build 211	v7.2	v4.31a	7.0.139	5.42
Fejlesztő	Grisoft s.r.o.	Softwin SRL.	ID Anti-Virus Lab.	Computer Associates	F-Secure Ltd.
Forgalmazó	FOOLY Stúdió	VirFilter.Hu Bt.	VirFilter.Hu Bt.	Computer Associates Mo.	2F 2000 Kft.

Web	www.avg.hu	www.virfilter.hu	www.virfilter.hu	www.ca.com	www.2f.hu
Keresési eredmények					
Minden példány ismert	189	189	189	189	189
Néhány példány ismert	0	0	0	0	0
Irtási eredmények (nem makró vírusok, összesen 144)					
Minden példányt irtott	132	142	143	144	142
Nem tudott minden példányt irtani	12	2	1	0	2
Néhány speciális eset					
VBS/Haptime.A	nem irtott	irtott	irtott	irtott	nem irtott
VBS/Redlof.A	törölt	törölt, irtott	részben irtott	irtott	részben irtott
Junkie.1027.A	irtott	nem irtott	irtott	irtott	irtott
One_Half.3544.A	irtott	nem irtott	irtott	irtott	irtott
W32/Elkern.A	nem irtott	irtott	irtott	irtott	irtott
W32/Hantaner	nem irtott	irtott	irtott	irtott	irtott
W32/Kriz.4050	nem irtott	irtott	irtott	irtott	irtott
Irtási eredmények (makró vírusok, összesen 45)					
Makrók törölve	6	10	10	45	15
Makrók meghagyva	39	35	35	0	30
Minősítés	**Standard**	**Standard**	**Standard**	**Advanced**	**Standard**

Termék	**Kaspersky Anti-Virus**	**McAfee VirusScan Enterprise**	**Norman Virus Control**	**NOD32**	**Panda BusinesSecure Antivirus**
Verziószám	4.5.0.94	7.1.0	5.70	1.633	3.01.01
Fejlesztő	Kaspersky Lab.	Network Associates	Norman ASA	ESET Software	Panda Software
Forgalmazó	2F 2000 Kft.	Network Associates Magyarországi Képviselete	ANT Kft.	SICONTACT Kft.	Panda Software Hungary
Web	www.2f.hu	www.nai.com	www.ant.hu	www.sicontact.hu	www.pav.hu
Keresési eredmények					

Minden példány ismert	189	189	188	189	189
Néhány példány ismert	0	0	1	0	0
Irtási eredmények (nem makró vírusok, összesen 144)					
Minden példányt irtott	144	144	142	143	143
Nem tudott minden példányt irtani	0	0	2	1	1
Néhány speciális eset					
VBS/Haptime.A	törölt	irtott	részben irtott	irtott	törölt
VBS/Redlof.A	törölt, irtott	törölt, irtott	részben irtott	törölt	törölt, irtott
Junkie.1027.A	irtott	irtott	irtott	irtott	irtott
One_Half.3544.A	irtott	irtott	irtott	irtott	irtott
W32/Elkern.A	irtott	irtott	irtott	nem irtott	irtott
W32/Hantaner	irtott	irtott	irtott	irtott	nem irtott
W32/Kriz.4050	irtott	irtott	irtott	irtott	irtott
Irtási eredmények (makró vírusok, összesen 45)					
Makrók törölve	10	10	34	45	45
Makrók meghagyva	35	35	11	0	0
Minősítés	**Standard**	**Standard**	**-**	**Standard**	**Standard**

Termék	**Trend Micro ServerProtect**	**VirusBuster for Windows**
Verziószám	5.5	4.5 Build 14
Fejlesztő	Trend Micro	VirusBuster
Forgalmazó	2F 2000 Kft.	VirusBuster Kft.
Web	www.2f.hu	www.vbuster.hu
Keresési eredmények		
Minden példány ismert	189	189
Néhány példány ismert	0	0
Irtási eredmények (nem makró		

vírusok, összesen 144)		
Minden példányt irtott	144	143
Nem tudott minden példányt irtani	0	1
Néhány speciális eset		
VBS/Haptime.A	irtott	irtott
VBS/Redlof.A	törölt, irtott	irtott
Junkie.1027.A	irtott	irtott
One_Half.3544.A	irtott	irtott
W32/Elkern.A	irtott	irtott
W32/Hantaner	irtott	nem irtott
W32/Kriz.4050	irtott	irtott
Irtási eredmények (makró vírusok, összesen 45)		
Makrók törölve	45	45
Makrók meghagyva	0	0
Minősítés	**Advanced**	**Standard**

ÖSSZEGZÉS

Számos olyan féregvírus létezik (például az e-mail üzenetekben terjedő vírusok ilyenek), amelyek nem kapcsolódnak más (hasznos) programkódhoz. Ilyen esetben a vírus irtása egyenértékű annak törlésével. Nem ilyen egyértelmű a vírusok irtása olyan vírus esetén (például a W32/MyDoom.A is ilyen), ahol a vírus tömörített és tömörítetlen állapotban is működik, terjedésre képes. Ilyenkor nem dönthető el, hogy egy ZIP állományba tömörített egyetlen fertőzött, futtatható program felhasználói beavatkozásra, vagy pedig a vírus hatására jött létre. Ilyen esetben a vírus irtása történhet úgy, hogy a ZIP állományból töröljük a fertőzött programot és marad egy üres ZIP állomány, de megoldás az is, hogy az egész ZIP állományt töröljük. Mind a kettő elfogadható megoldás. Hasonló problémával találkozhatunk a VB szkripteket fertőző vírusoknál, amelyek akár HTML kódba ágyazva is terjedhetnek.

Az eredmények kiértékelése során megvizsgáltunk néhány speciális esetet (lásd táblázat). A felsorolt vírusok közül a VBS/Haptime.A és a VBS/Redlof.A, olyan tulajdonságú, hogy

bizonyos fertőzései, megjelenési formája esetén a vírus irtása történhet a “fertőzött” állomány törlésével is.
Az antivírusok eredményeit kiértékelve 2 antivírus kapott február hónapban CheckVir ADVANCED minősítést, 9 antivírus ChekcVir Standard minősítést és 1 antivírus pedig nem kapott minősítést.

FELHASZNÁLT IRODALOM

1. Leitold, F.: Független anti-vírus tesztelés
   Networkshop 2002, Eger, 2002

2. Gordon, S.; Howard F. (2000). Antivirus Software Testing for the New Millenium.
   Proceedings of the 23rd National Information Security Conference, Baltimore USA, 2000.

3. Leitold, F. (1995). Automatic Virus Analyser System. Proceedings of the 5th International Virus Bulletin Conference, Boston USA, 1995, pp. 99-107.

4. Leitold, F. (2002). Independent AV testing. Proceedings of the 11th International EICAR Conference, Berlin Germany, 2002.

5. Marx, A. (2000). A Guideline to Anti-Malware-Software testing. Proceedings of the 9th International EICAR Conference Brussels Belgium, 2000.