Ismeretlen vírusok felismerése

Vírusvédelmi sorozatunk mostani tesztjében visszatekintünk az elmúlt egy évre. A minősítési eljárás mellett megvizsgáljuk a vírusvédelmi szoftverek heurisztikus képességeit is – közelebbről azt, hogyan reagáltak vagy reagálnak az egy év alatt megjelent új vírusokra.

[írta: Leitold Ferenc]

A korábbi évekhez hasonlóan a 2005. évben is az e-mailekben terjedő férgek és vírusok keltették a legnagyobb járványokat. Ebben a hónapban azt vizsgáltuk, hogy az antivírusszoftverek vajon észlelik-e az ismeretlen vírusokat. Erre a célra a víruskereső szoftverek 2005. februári és júniusi verzióit használtuk, és azt igyekeztünk kideríteni, hogyan azonosítják a később megjelent vírusokat. Olyan víruspéldányokkal tettük őket próbára, amelyeket akkor még egyetlen vírusvédelmi szoftver sem ismerhetett; a mai antivírusszoftverek persze már elbánnak mindegyikkel. Ebből természetesen adódik, hogy a februári és a júniusi szoftvereket más-más víruskészleten ellenőriztük.

A vírusvédelmi szoftverek heurisztikus képességét jellemző mutatók szerint az ismeretlen vírusok azonosítása sajnos nem megy tökéletesen a már meglevő vírusvédelmi szoftverekkel. Csak akkor érhetjük el a lehető legnagyobb biztonságot, ha folyamatosan frissítjük a szoftvereket, bár sok vírust, férget éppen a heurisztikus felismerés akadályoz meg a szélesebb körű elterjedésben.

CheckVir minősítés

Januárban a CheckVir tesztlabor tesztjében a Windows XP Professional operációs rendszeren vizsgáltuk a vírusvédelmi rendszerek keresési és irtási algoritmusait. A teszthez a legelterjedtebb vírusok példányait használtuk. Külön is vizsgáltuk, hogy a vírusvédelmi rendszerek hogyan szűrik ki az e-mailek vírusait a Microsoft Outlook Express levelezőügyfél legújabb változatában. STANDARD szintűnek minősítettük azokat a vírusvédelmi rendszereket, amelyek minden fertőzött példányban felismerték a vírust és megakadályozták, hogy a felhasználó elindítsa a vírus kódját. ADVANCED szintűnek minősítettük közülük azokat, amelyek (lehetőség szerint) az eredeti állapot visszaállításával ki is irtják a vírust. Az *on-access* védelem és az *on-demand* keresésben a vírusvédelemnek ugyanúgy kell működnie. CheckVir MAILSCANNER minősítést kaptak azok a vírusvédelmi szoftverek, amelyek felismerték a legelterjedtebb vírusokat a Microsoft Outlook levelezőrendszerbe érkező, illetve az abból távozó e-mailekben, blokkolták ezeknek a leveleknek a mozgását, és csak akkor engedték tovább őket, ha sikerült eltávolítaniuk belőlük a víruskódot.

A minősítés eredményei alapján 2006 februárjában a CheckVir tesztlaborban a következő termékek kaptak ADVANCED minősítést: eTrust Antivirus; McAfee VirusScan; NOD32 Antivirus System; BullGuard Antivirus.

A következő termékek kaptak STANDARD minősítést: AVG Anti-Virus; F-Secure Anti-Virus; Kaspersky Anti-Virus; Norton Antivirus; Panda Titanium 2005; VirusBuster for Windows.

A következő termékek szerezték MAILSCANNER minősítést: AVG Anti-Virus; BullGuard Antivirus; eTrust Antivirus; F-Secure Anti-Virus; Kaspersky Anti-Virus; McAfee VirusScan; NOD32 Antivirus System; Norton Antivirus; Panda Titanium 2005; VirusBuster for Windows.

A vírusok pontos listája, valamint a minősítés további részletei a www.checkvir.hu weboldalon olvashatók.

Termék	AVG Anti-Virus 7.1	BullGuard Antivirus	eTrust Antivirus	F-Secure Anti-Virus Client Security	Kaspersky Anti-Virus 5.0 for Windows Workstations	McAfee VirusScan Enterprise	NOD32 Antivirus System	Norton AntiVirus 2005	Panda Titanium 2006 Antivirus + Antispyware	VirusBuster Professional 2005
Verziószám	7.1 (Build 371)	6.0	v7.1.192	6.01 build 11441	5.0.225	8.0i	2.50.32	11.0.16.2	5.01.00	5.1 (Build 40)
Fejlesztő	Grisoft s.r.o.	Bullguard	Computer Associates	F-Secure Ltd.	Kaspersky Lab.	McAfee	ESET Software	Symantec Corp.	Panda Software	VirusBuster
Gyanúsított állományok										
2005. februári vírusvédelem* (összesen 4742 állomány)	203	N/A	2	18	8	535	1199	0	87	1
2005. júniusi vírusvédelem* (összesen 2879 állomány)	25	N/A	2	0	10	302	539	17	351	8
Vírusvédelem (420 különböző típusú vírus)										
Hány példányt azonosított?	420	420	420	420	420	420	420	420	420	420
Hány példányt távolított el? (on-demand, on-access)	412	420	420	413	416	420	420	419	419	415
A levelezőügyfél védelme										
Minden példányt blokkolt/irtott	420	420	420	420	420	420	420	420	420	420
Minősítés(ek)	CHECKVIR STANDARD	CHECKVIR ADVANCED	CHECKVIR ADVANCED	CHECKVIR STANDARD	CHECKVIR STANDARD	CHECKVIR ADVANCED	CHECKVIR ADVANCED	CHECKVIR STANDARD	CHECKVIR STANDARD	CHECKVIR STANDARD
	CHECKVIR MAILSCANNER	CHECKVIR MAILSCANNER	CHECKVIR MAILSCANNER	CHECKVIR MAILSCANNER	CHECKVIR MAILSCANNER	CHECKVIR MAILSCANNER	CHECKVIR MAILSCANNER	CHECKVIR MAILSCANNER	CHECKVIR MAILSCANNER	CHECKVIR MAILSCANNER
*A heurisztikus képességek teszteléséhez a gyártók korábbi verziójú termékeit használtuk.										