Panda Antivirus Platinum 6.0

Virus je zlověstný globální pojem, který neustále vyvolává nepříjemné pocity u většiny uživatelů na celém světě. V roce 1995 se hodně spekulovalo o tom, že po nástupu Windows 95 viry potupně odejdou na smetiště dějin. Dnes je však jasné, že téměř vše zůstalo při starém a nové typy virů opět zákeřně útočí na naše počítače.

Sympatický medvěd ničí viry

Panda Antivirus Platinum verze 6.0 (dále jen Panda) je produktem pravděpodobně největšího evropského producenta antivirových programů – španělské firmy **Panda Software**. Dodává se ve velmi pěkné krabici, která obsahuje jeden CD disk, záchrannou disketu (Emergency Disk), uživatelskou příručku v angličtině (68 stran), přehled poskytovaných služeb (20 stran), licenční certifikát a pěknou barevnou samolepku.

Na CD-ROM je krátká multimediální prezentace a vlastní antivirový systém pro šest různých operačních prostředí – DOS, Windows 3.x, OS/2 Warp, Windows 9x, Windows NT 3.51 a Windows NT 4.0.

V rámci testování musel program čelit šesti vybraným referenčním virům:

One Half.3544 (MS-DOS), One Half.3577 (MS-DOS), J&M.A (MS-DOS), WM/Concept.A (MS Word), WM/CAP.A (MS Word) a XM97M/Laroux.A (MS Excel). Ani jeden z nich neunikl jeho pozornosti a všechny potkal stejný truchlivý osud. Nelze se proto divit, že Panda je držitelem certifikátu prestižní americké asociace **ICSA** (International Computer Security Association). Každý držitel tohoto certifikátu musí identifikovat 100 procent virů ze skupiny *In the Wild* (nejčastější aktivní viry) a více než 90 procent virů ze skupiny *Zoo Collection* (kolekce několika tisíc známých virů).

V rámci testování jsem nejvíce pozornosti věnoval operačním systémům DOS, OS/2 a Windows 9x. V těchto třech prostředích najdete víceméně identický textový antivirus *PAVCL.EXE*, který funguje na příkazové řádce. Při jeho využívání musí uživatel vždy zadat příslušné parametry (např. PAVCL C: D: /CLV).

Panda využívá v systémech Windows 9x, OS/2 i DOS obsahově prakticky shodnou databázi virových vzorků (aktualizace testované verze 23. 4. 1999). S touto databází dokáže spolehlivě identifikovat až 23 240 zákeřných virů.

Panda pro DOS

V rámci instalace produktu, který zabere v systému DOS asi 6 MB prostoru, si můžeme vybrat jednu jazykovou verzi ze sedmi podporovaných – anglickou, francouzskou, německou, italskou, portugalskou, katalánskou nebo španělskou. Po spuštění programu *PAV.EXE* se objeví příjemné

textové či grafické prostředí (podle volby uživatele) s pěti menu v horní části (Files, Scan, Investigate, Vaccinate a Configure) a s dvojicí adresářových oken. Kontextově citlivá nápověda je samozřejmostí. Hlavní výhodou neobvyklého prostředí (vůči ostatním zde popisovaným verzím) je vysoká míra konfigurovatelnosti.

Panda pro Windows 95/98

V této verzi si můžeme vybrat jednu jazykovou verzi z jedenácti (!) podporovaných – anglickou, finskou, francouzskou, německou, italskou, portugalskou, ruskou, slovenskou, španělskou, katalánskou nebo švédskou. Aplikace zde nabízí dvě rozdílná grafická prostředí. Pokud si vyberete slovenskou verzi (osobně doporučuji), budete potřebovat asi 6,5 MB prostoru. Pokud si však vyberete verzi anglickou, musíte obětovat asi 21 MB prostoru.

Plně slovenská verze (včetně nápovědy) je reprezentována aplikačním oknem, které se dost podobá anglické verzi pro OS/2. V horní třetině aplikačního okna najde uživatel čtyři menu (Súbory, Test, Vyhľadávanie a Konfigurácia) prakticky se všemi funkcemi programu. Pod menu je umístěna nástrojová lišta s pěti velkými ikonami.

Klasické vyhledávání virů je založeno na vyhledávání známých řetězců v těle konkrétních virů bez podpory heuristické analýzy. Aby nedošlo k falešným poplachům, je tato metoda zabezpečena sledováním pozice bajtů a sledováním většího množství řetězců. Kontrola komprimovaných souborů (ARJ, ZIP apod.) a makrovirů je samozřejmostí.

Pokud je někde nalezen podlý virus, uživatel může zobrazené hlášení ignorovat (pokračovat v testu), vyléčit soubor, změnit jeho jméno, nebo ho rovnou vymazat. Zároveň se může podívat do seznamu virů, kde jsou informace o všech virech, které program zná. Tyto informace jsou však velmi stručné – jméno, původ, velikost, datum vypuštění, charakteristické vlastnosti, systémové oblasti a typy souborů, které virus napadá (v tomto bodě je třeba český systém AVG vybaven mnohem lépe). Po dokončení testu se zobrazí detailní výsledky všech vykonaných operací. Standardně je tento soubor uložen na disku, takže jej lze snadno vytisknout. Nedostatkem je ale absence možnosti archivovat jakékoliv starší výsledky.

Jestliže máte rádi grafické prostředí Windows 98, můžete používat anglickou verzi, která nabízí nové uživatelské rozhraní. Téměř všechny operace v novém rozhraní jsou doprovázeny příjemným hlasovým komentářem, takže je velmi dobré mít 16bitovou zvukovou kartu.

V každém případě ovšem oceníte rezidentní antivirovou ochranu, která je reprezentována virtuálním 32bitovým ovladačem *Sentinel VxD.* Proces jeho kontroly začíná při otevření souboru a probíhá nepřetržitě. Když je detekován virus, proces se automaticky pozastaví a uživatel dostane informace o viru. Sentinel VxD neustále kontroluje podezřelé operace se soubory a je schopen v reálném čase zjistit a zastavit hrozící riziko virové infekce.

Panda nabízí velmi pružné filtrování virů přicházejících z internetu. Subsystém *Internet Protection Module* prohledává příchozí data na úrovni ovladače Winsock, a proto může zachycovat soubory stahované z FTP archivů, WWW stránek a elektronické pošty. Tento sybsystém se rovněž může zaměřit na konkrétní stránky podle jména, portu nebo IP adresy. Mateřská firma navíc nabízí denní aktualizace a jednotlačítkovou aktualizační funkci *Intelligent Update*, která umožňuje update virové databáze (Virus Signature Database) i vlastního programu buď ručním zásahem uživatele, nebo automaticky na pozadí s použitím plánovače.

Panda pro OS/2 Warp

Při instalaci produktu, který zabere v operačním systému OS/2 asi 2,5 MB prostoru, si můžeme vybrat jednu ze tří jazykovou verzi – anglickou, německou nebo španělskou. Produkt funguje naprosto bezchybně v systému OS/2 Merlin 4.0 i v úplně novém OS/2 Aurora 4.5 (OS/2 Warp Server for E-business).

Po aktivaci programu PAV se v prostředí WPS objeví aplikační okno. V horní třetině najde uživatel tři menu (Files, Scan a Configure) prakticky se všemi funkcemi programu. Pod menu je umístěna nástrojová lišta s pěti velkými ikonami. Velkou část celého okna pod lištou zabírá grafické logo programu.

V pravém dolním rohu je umístěna jedna ikona, která umožňuje okamžité ukončení aplikace. Kontextová hypertextová nápověda je samozřejmostí.

Program nabízí všechny standardní antivirové služby včetně heuristické analýzy na logickém disku HPFS i FAT. Díky speciálnímu 32bitovému ovladači, který lze zdarma získat na internetu, jsem mohl kompletně zkontrolovat také logický disk EXT2 (RedHat Linux 6.0). Rezidentní antivirová ochrana bohužel není součástí této verze produktu. Pokud program zjistí v normálním nebo komprimovaném souboru (ARJ, ZIP apod.) virus, objeví se výstražné okno se čtyřmi funkcemi (viz verze pro Windows).

Hodnocení

Panda Antivirus Platinum verze 6.0 představuje komplexní balík antivirových programů, jenž zajistí ochranu počítače s použitím moderních technologií před všemi typy virů. Aktuální Panda tedy rozhodně představuje novátorský produkt, který je vhodné v příštích letech velmi pečlivě sledovat.

Michal Pohořelský