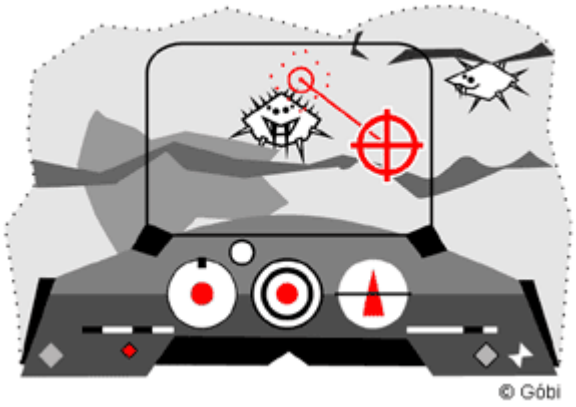
VírusHíradó

## Az anti-vírus programok tesztje

A vírusvédelmi programok legrangosabb és legfontosabb megmérettetése a Virus Bulletin rendszeres tesztelése.




Itt az összes magára valamit adó vírusvédelmi terméket fejlesztő cég igyekszik elindulni és céljuk: minél több "100%"-os helyezés elérése az idők folyamán. Ha egy fejlesztő gárda meg akarja győzni a felhasználókat termékük kiválóságáról, ahhoz az itt rendszeresen elért jó helyezés és persze minél több begyűjtött "100% Award" trófea a legjobb ajánlólevél és bizonyíték.

A teszteknél más és más operációs rendszeren kell bizonyítaniuk a különböző termékeknek, hogy ők a legjobbak a mezőnyben.
A platformok között szerepel a DOS, a Windows 95, 98, NT, ME és 2000, de természetesen megtalálható itt a Novell Netware is. Ezek közül mindig egyet választanak ki az aktuális megmérettetéshez.

A tesztekben az alábbi módon vizsgálják a különböző programok tulajdonságait:

A teszteket elsősorban valódi, az előző hónapban leggyakrabban előforduló vírusokkal végzik.

Ezeken a valós környezetben is előforduló ( In The Wild ) vírusokon kívül szerepelnek még olyan, csak laboratóriumi körülmények között előforduló vírusállományok is, amelyeket a tesztelés céljára hoztak létre (például több, különböző vírus által többszörösen fertőzött fájlok).

Ezenkívül természetesen egy minden eddigi vírust tartalmazó vírusgyűjteményen is bizonyítaniuk kell. Ebben a gyűjteményben mindenféle kártékony kód megtalálható: boot-vírusok, file-vírusok, makro-vírusok, polimorfikus (alakváltoztató) vírusok, stb.

Minden anti-virus terméket a telepítés után jelentkező alapbeállításokkal használnak (deafult settings). Ezek a beállítások rendelkeznek arról, milyen elemek és milyen kiterjesztésű állományok kerüljenek vizsgálatra és hogyan használják a heurisztikus keresést (a vírusszerű tulajdonságokat a konkrét vírus ismerete nélkül is felismerő analizálást). Az alapbeállítások mindenkor egy ésszerű kompromisszumot képviselnek a hatékonyság és a teljesítmény egyidejű figyelembe vételével. Valós idejű kereséskor csak az előre meghatározott kiterjesztéssel rendelkező állományok kerülnek vizsgálatra, mert ha minden file ki lenne választva, azt még a legerősebb gép sem tudná jelentős lassulás nélkül kezelni.

Ha egy program a vadon élő vírusok (In The Wild, ITW) felderítésénél teljesíti a 100%-ot, az egy igen kiváló és fontos részeredmény, még akkor is, ha a végső összesítéskor csak kisebb mutató jön ki.

A hatékony működést mind a valósidejű (On Access Scan), mind pedig a kézzel indított (On Demand Scan, ODS) keresésnél bizonyítani kell.

A kézzel indított keresésnél először elemzik a "Csak jelentés" (report only) üzemmódban indított vírus detektálás napló állományát (log file).
A hálózati állományok és CD ROM lemezek ellenőrzésekor előfordulhatnak olyan szórványos, telepítésből eredő hibák, amik befolyásolnák a teszt eredményeit, ezért a teszt állományok vizsgálata mindig a helyi gép merevlemezén történik.

Néhány terméknél az is előfordul, hogy a keletkezett naplóállomány használhatatlan a teszt szempontjából, vagy egy bizonyos fájl méretet elérve, összeomlik maga a víruskereső program. Ezekben az esetekben az a kedvelt megoldás, hogy lefuttatnak egy keresést fertőzés esetén törlést választva, egy következőt vírus esetén karanténba helyezéssel és egy harmadikat, ami ezek után elvileg már nem találhat(na) fertőzést. Ami vírust a program ebben az utolsó menetben jelez, azt úgy tekintik, mint kihagyott és elhibázott tételt.

A valósidejű védelem tesztjéhez (On Access Scan, OAS) olyan eszközt választanak, amely ismétlődően végigmegy az összes tesztállományon, szép sorjában megnyitva azokat. A vírusvédelmi programoknak meg kell akadályozni a fertőzött állományokhoz való hozzáférést. A tesztelő eszköz naplóállománya egyértelműen jelezni fogja, mely fájlokat nem sikerült megnyitnia a víruskereső miatt.

Megfelelő eszköz lehet egy ilyen teszthez például az XCOPY

utasítás is, amely teljes könyvtárstruktúrákat másol át egyik helyről a másikra.

Ezeknél az eljárásoknál néhány vírusvédelmi terméknél előfordulnak később reprodukálhatatlan tévesztések, amikor a rengeteg fertőzött állomány nagyvalószínűséggel túlterheli a felismerő motort (scanning engine).

Az a termék, amelyik meg akar felelni a 100% elvárásainak, nem hibázhat a felismerések során. Ez nem csak azt jelenti, hogy összes vírust észlelnie kell, de azt is, hogy tiszta állományokra nem adhat riasztást.

A vakriasztások teszteléséhez beágyazott objektumokat tartalmazó állományokat (OLE = Object Linking and Embedding ) és garantáltan tiszta teszt fájlokat használnak. Sok termék olyan riasztást is generál, ahol nem egy konkrét vírust jelez, hanem csak ismeretlen gyanút (suspicious file) állapít meg. Ezt ugyan nem tekintik hibának, de a termék eredményei közé zárójelben feljegyzik.

A tömörített állományok vizsgálatánál (azoknál a termékeknél, ahol ez a funkció nem alapértelmezett, ott a teszt idejére kézzel bekapcsolják) a tökéletes felismerési képesség mellett mérni szokták a keresés sebességet is.

Az F-Secure Anti-Virus és a Kaspersky Anti-Virus is rendszeresen részt vesz ezeken a rangot adó teszteken, és eddig már sokszorosan prezentálták a 100%-os teljesítményt. Az elmúlt néhány évben az F-Secure víruskeresői hétszer, a Kaspersky termékek pedig tizennégy alkalommal feleltek meg ennek a szigorú minősítésnek.
Bár az F-Secure egy olyan több víruskereső magot tartalmazó program, amely a Kaspersky cég motorját is magában foglalja, a különbség oka az alapbeállítások különbözőségével magyarázható.

Az angol illetőségű Virus Bulletin cég honlapja a www.virusbtn.com címen érhető el.

Csizmazia István