

Független anti-vírus tesztelés

IKTA 00033/2000



VESZPROG Kft.

Projektvezető: Dr. Leitold Ferenc
fleitold@veszprog.hu

Célkitűzések



- **Vírusismeret tesztelése**
 - keresés és **irtás** szempontjából
 - anti-vírusok ellenőrzése kb. 15000 víruson
- **Valós munkakörnyezet <-> Automatizálás**
- **Stabilitás, extrém esetek vizsgálata**
 - > anti-vírus választás segítése
 - > AV fejlesztők részére értékes információ

A tesztelés fő lépései



- **Vírusok biztonságos környezetben történő szaporítása**
- **Az anti-vírus szoftver lefuttatása**
- **Eredmények analizálása**
- **A teszt ismételt végrehajtása új vírus megjelenése, ill. új AV verzió kiadása esetén**

Vírusok szaporítása



- **Biztonságos környezetben**
 - Emulált operációs rendszereken
(például: VMWare, DOSemu, Win4Lin)
 - Különálló, szeparált számítógépen
- **Folyamatosan indítva a fertőző file-t és az eredeti “goat” file-t**
- **Programozható makrózást biztosító szoftverekkel (például: makró vírusokhoz)**

Anti-vírus szoftverek futtatása



- **Különböző beállításokkal**
 - on-access keresés
 - on-demand keresés
- **Keresés és/vagy irtás**

Eredmények analízálása



- **A keresési eredmények ellenőrzése**
 - A fertőzött file-ok listájának és a szoftver által azonosított vírusos file-ok listájának összehasonlítása
- **Az irtási eredmények vizsgálata**
 - A megváltozott tartalmú és a szoftver által felismert vírusos file-ok listájának összehasonlítása
 - A goat file-ok és a változott file-ok összehasonlítása

Automatikusan, fél-automatikusan kezelt vírustípusok



- **File vírusok**
 - DOS-os futtatható programok
 - Windows-os futtatható programok
- **Boot vírusok**
- **Makró vírusok (Word, Excel)**
- **Internet segítségével fertőző vírusok**

