CheckVir
Független anti-vírus tesztelés

VESZPROG Kft.

Dr. Leitold Ferenc
fleitold@veszprog.hu

AV szoftverek

- nagy mennyiségű vírus kezelése
  -> nagy mennyiségű keresési és irtási algoritmus
- naponta megjelenő újabb verziók
- kibocsátás előtt tökéletesen tesztelhető?
- további problémák:
  – operációs rendszerek biztonsági problémái
  – hibás vírusok

Célkitűzések

- Vírusismeret tesztelése
  - keresés és irtás szempontjából
  - nagy mennyiségű víruspéldány használata
- 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 futtatása
- 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 analizálása

- **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

Publikációk

- **Számítástechnika**
  - 2003. januártól havonta jelentkező beszámoló cikk
- **PC World**
  - 2003. januártól minden számban
- **Előadások nemzetközi és hazai fórumokon**
  - EICAR 2002, 2003
  - Networkshop

Minősítés

- 2004. januártól
- Havonta ismétlődő
- Változó platformok
- Két kategória
  - csak keresés vizsgálata
  - keresés és irtás vizsgálata
- A legelterjedtebb vírusok alapján

VESZPROG

CHECKVIR®
STANDARD
WWW.CHECKVIR.COM

CHECKVIR®
ADVANCED
WWW.CHECKVIR.COM