Adatbiztonság, Vírusvédelem

2F Kft.

- **1994. – Data Fellows F-Prot képviselet**
- **1997. – F-Secure és AVP képviselet**
  - **Nokia és Checkpoint tűzfal megoldások**
  - **Biztonságtechnika, tanácsadás**
- **2002. – Vírus Híradó általános vírusismereti webportál**

Kaspersky Labs

- **1989. – fejlesztések kezdete**
- **1994. – kereskedelmi forgalmazás kezdete**
- **1997. - Az F-Secure licenszeli az AVP víruskereső motort**
- **1999. – KL nemzetközi cégé vált, 50-nél több országban van képviselete**

Három szintű védelem

- MUNKAÁLLOMÁS
  - Valós idejű védelem
  - Kézzel indított keresés
  - Automatikus frissítés
- SZERVER
  - + Hálózatos management
  - + Megosztott könyvtárak védelme
- GATEWAY (Mailserver)
  - + Kimenő és bejövő levélforgalom ellenőrzése

Termékcsalád – teljes körű platform lefedettség

Platformok

- DOS
- Windows 9x/NT/ME/2K/XP munkaállomás, NT és 2K szerver
- Exchange 5.5/2000
- Unix: Sun Solaris, FreeBSD, BSDi, OpenBSD
- Linux: Mandrake, Red Hat, SuSE, Debian, Black Cat
- Lotus Domino for Linux/Windows
- Novell Netware
- Palm OS
- OS/2
- CVP kompatíbilis tűzfal (pl. Checkpoint)

- Anti-vírus program fejlesztő cégből komplett biztonsági megoldásokat fejlesztő céggé kíván válni pl. az idén jelenik meg Anti-Hacker személyi tűzfal

Vírusismeret

- Minden jelenleg ismert vírustípusra
  - Polimorf, önkódoló;
  - Lopakodó, láthatatlan vírusok
  - Java applet;
  - Makróvírusok (Word, Excel, PowerPoint, Help file-ok, stb.)
  - Férgek
  - Trójaiak
- Órákon belül reagálnak az új vírusokra
- 24 órás víruslaboratórium
- Leggyakoribb vírusok ellen egyedi irtó segédprogram (pl. Klez, SirCam)
- Ingyenes, online vírusinformációt szolgáltatnak: www.viruslist.com

Fő modulok

- **Monitor** - Valós idejű keresés (OAS)
- **Scanner** – Kézzel indított alkalmi keresés (ODS)
- **Updater** – Adatállomány frissítő (automatizálható)
- **Control Centre** - Központi beállító felület
- **Office Monitor** – Makró ellenőrző (adatbázisból)
- **Mail Checker** - Levelezés ellenőrző (adatbázisból)
- **KAV Plugin** - Levelezés ellenőrző (adatbázisból)
- **Scanner DOS32** - DOS parancssori scanner (adatbázisból)
- **Script checker** - Valósidejű script ellenőrző heurisztikus tulajdonság vizsgálat
- **Report Viewer** - Jelentésnapló megjelenítő (Monitor, Scanner, Updater külön)
- **Rescue Disk** - Linuxos (Noname)mentesítő lemezkészlet készítő

További modulok a Personal Pro változatban

- **Office Guard - Makróellenőrző**

  Office 2000-be beépülő makrófigyelő, viselkedés figyelő monitor

- **Inspector – Fájl és állományrendszer változásfigyelő**

  Mentesíthető az aktuális állományrendszer, elmenthetőek a megadott állományok CRC ellenőrző összegei, a windows regisztrációs adatbázis másolata és az ini file-ok. A modul minden számunkra észrevétlen változást naplóz, és az így elmentett adatokból helyre tudja állítani az eredeti állapotot. Az eszköz saját meghajtó programot használ (device driver) és az ezzel beolvasott adatokat összehasonlítja az operációs rendszer driver által szolgáltatott adatokkal, ezáltal használatával igen nagy biztonsági szintet érhetünk el.

  - Filerendszer integritásának ellenőrzése
  - CRC ellenőrzőösszeg segítségével a file-ok strukturális és méretbeli változása nyomon követhető
  - Elmentett adatokból az eredeti állomány visszaállítható
  - Változások naplózása

Monitor - Valós idejű keresés

- Ez a legfontosabb modul
- Minden file hozzáférést nyomon követ
- Meghatározható file kiterjesztésekre
- Bármely levelező kliensnél a fertőzött levélre riaszt
- Levéladatbázisok, plain mail file-ok ellenőrizhetőek
- Többszörösen egymásba ágyazott tömörített állományok vizsgálata
- Heurisztikus keresés (Code Analyzer)
- Beágyazott objektumok vizsgálata (Embedded Objects)
- Vizsgálandó összetett állományok maximális mérete megadható
- Tetszőleges file, könyvtár, meghajtó kizárható a keresésből

  Pl. ha egy szerveren a KAV fileserver és exchange verziója egyaránt telepítve van, akkor a monitorból ki kell zárni az Exchange working directory-t
- Gyanús file-ok karanténba zárhatóak.

Monitor – Levelek és levéladatbázisok

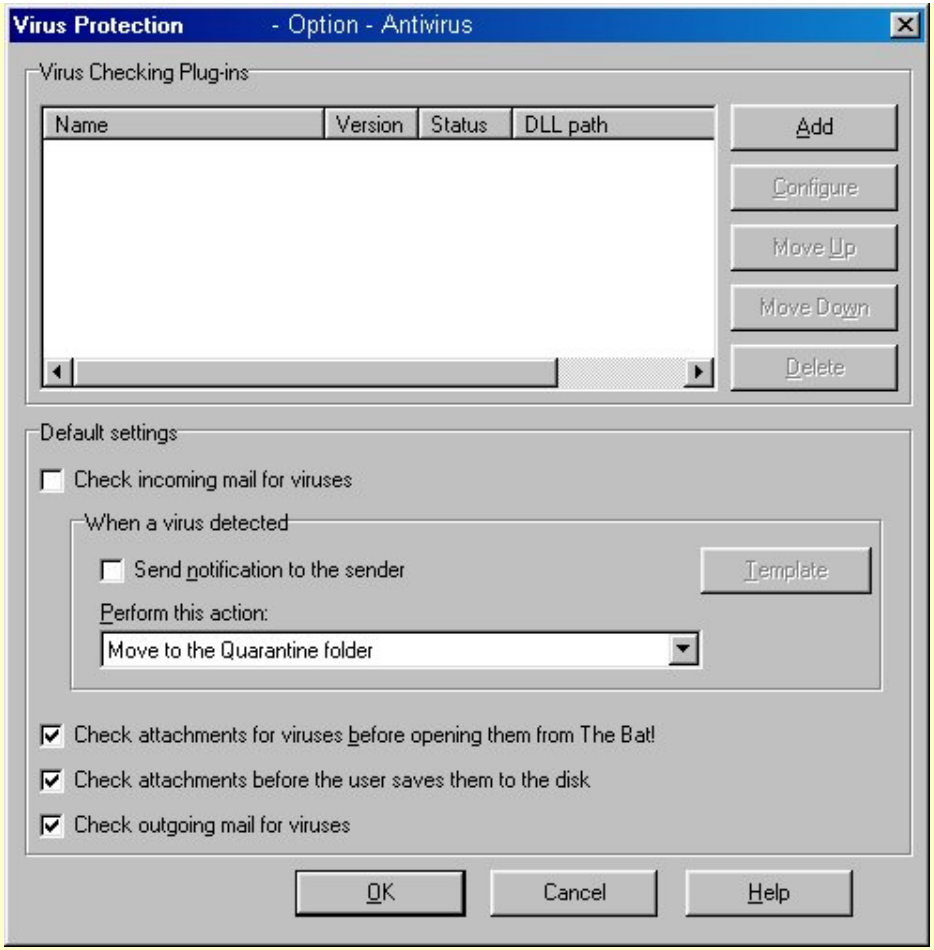
- Tetszőleges levelező programmal valósidőben ellenőrzi a levelekben és a levelezőmappákban a vírusos állományokat
  - MS Outlook
  - MS Outlook Express
  - MS Exchange
  - Eudora Pro, Eudora Light
  - TheBat!, TheBat! Pro
  - Pegasus Mail
  - Netscape Navigator Mail
  - JSMail

Monitor – MS Outlook

- MS Outlook (az Office-ból)
- Be tud épülni, és a fertőzött leveleket már akár le sem tölti
- Valós időben ellenőrzi a ki- és bejövő leveleket
- Értesítési lehetőség a feladónak
- Értesítési lehetőség tetszőleges email címnek (reroute) pl. adminisztrátornak
- Fertőzött levél esetén
  - Try to cure message text
  - Try to cure message attachments
  - Delete non cureable attachments
  - Delete the infected mails
  - Reroute-Send infected messages (változatlanul újraküld, hogy meg legyen eredeti állapot) pl. Quarantine Mailbox

Monitor – TheBat! (Personal Pro, Workstation)

- TheBat! Levelezőkliens
- Be tud épülni, és a fertőzött leveleket már akár le sem tölti
- Valós időben ellenőrzi a ki- és bejövő leveleket
- Értesítési lehetőség a feladónak
- Fertőzött levél esetén
  - To cure the infection
  - To remove infected parts
  - To re-send the message (változatlanul újraküld, hogy meg legyen eredeti állapot)
  - To Delete the message
  - To transfer the infected message to Quarantine



Scanner - Kézzel indított, alkalmi keresés

- Előre létrehozott profile-ok alapján
- Parancssori kapcsolókkal is
- Meghatározható file kiterjesztésekre
- Többszörösen egymásba ágyazott tömörített állományok vizsgálata
- Heurisztikus keresés (Code Analyzer)
- Beágyazott objektumok vizsgálata (Embedded Objects)
- Tetszőleges file, könyvtár, meghajtó kizárható a keresésből
- Gyanús file-ok karanténba zárhatóak
- Levéladatbázisok, plain mail file-ok ellenőrizhetőek
- Időzíthető futtatás
- Megadható a task futásának prioritása (High, Normal, Low)

Scanner - Outlook Express mentesítés

- Outlook Express levéladatbázisok utólag mentesíthetőek
- Compress All Folders – Összes mappa tömörítése
- Kikapcsolt Monitor modul
  - Ha féreg a melléklet, az eredeti levél megmarad melléklet nélkül
  - Ha fertőzött a melléklet, az eredeti levél megmarad mentesített melléklettel

Updater - Vírusdefiníciós adatbázis frissítése

- Kumulatív update: napi, heti, 2 havi
- Le sem tölti a vírusadatbázist, ha az egyező a jelenlegivel vagy régebbit akarnánk letölteni
- Automatikusan időzíthető mód, kézzel indított mód, eseményvezérelt mód: pl. Monitor modul betöltődése után fusson
- Adatállomány listázási lehetőség: Viruslist Generator
- Vírusdefiníciós címlista megadható (Ha nem elérhető, vagy túlterhelt az adott cím, akkor a listában sorrendben halad, vagy véletlenszerűen választ)
- Letöltés HTTP vagy FTP protokoll segítségével
- Aktiválni tudja az Internet-kapcsolatot, és utána ha kell, bontja
- Vírusdefiníciós adatbázis automatikus használatba vétele (Reload)

Control Centre

- A modulok összes beállítási lehetősége erről a központi grafikus felületről érhető el
- Időzített feladatok (frissítés, víruskeresés) létrehozása megadott időben
- Vírusdefiníciós adatbázis frissítés módja (FTP, HTTP), helye (Internet, Local Folder), gyakorisága
- Karantén beállítások
- Komponens lista

Beállítási lehetőségek gyanú esetén

- Külön a fertőzött, és külön a gyanús fájlok esetén
  - No Action
  - Disinfect
  - Save a copy to Backup before disinfect – sima másolat
  - Save a copy to Quarantine before disinfect – kódolt másolat
  - Delete
  - Move to Quarantine
  - Rename
- Ha a mentesítés sikertelen
  - Report Only
  - Rename
  - Delete

Admin Kit - Távmenedzselés Windows alatt 1

- Windows munkaállomások és szerverek vírusvédelméhez
- Távtelepítés
  - 1. Computer Based (2K/NT-ről 2K/NT-re hidden share-rel c$)
  - 2. Login Script Based
- Központi adminisztráció
- Központi frissítés
- Központi karbantartás
- Korlátozások a felhasználók felé jelszavas védelemmel
  - Task leállítása, beállítások változtatása, program leállítása

Admin Kit - Távmenedzselés Windows alatt 2

- Karantén (helyi gép, KAV Server)
- Alert forwarding (MAPI, SMTP)
  - Critical: Infected object found, Object deleted
  - High: Infected object cured, Supicious object found
  - Informal: Warning, I/O error, Monitor internal error
- Virus Outbreak (járvány figyelés)
  - Number of infection, Time period -> email riasztás

Kulcs alapú működés

- **Egyáltalán nincsen kulcs - Demo mód**
  - Nem működik: heurisztikus keresés, mentesítés, archív állományok ellenőrzése, mailbox állományok ellenőrzése
- **Van érvényes éles kulcs - Normál mód**
  - Teljes értékű működés - általában egy éves időszakra
  - Támogatott a több kulcs párhuzamos használata (kombinált licensz)
- **Lejárt az érvényes kulcs - Lejárt mód**
  - Nem működik az update, a detektálás és a mentesítés továbbra is használható
  - A lejárt kulcs a lejárat után nem támogatja a hálózatós működést (management)
  - Ha kézzel próbálják a frissítést, akkor Demo üzemmódba kerül
- **Van érvényes próba (30 napos) kulcs - Trial mód**
  - Teljes értékű működés a próbaidő lejártáig, kulcs lejárása után a program Demo üzemmódba kerül
  - A próba időszak csak egyszer vehető igénybe, próba kulcsot próba kulccsal nem lehet hosszabbítani, azt kizárólag éles kulccsal tudjuk felváltani

KAV for Linux-Unix Mailserver

- Levelezőrendszerek SMTP forgalmának szűrése
- Sendmail, Qmail, Postfix, Exim
- A levelező szerver eredeti beállításait nem kell megváltoztatni
- Értesítés küldése (Sender, Recip, Admin) vírusfertőzésről
- Címcsoportok szerinti szűrés.
- Csatolt állományok kiterjesztés és méret szerinti szűrése.
- Többszörösen egymásba ágyazott tömörített állományok vizsgálata
- Egyszerűen kezelhető webtuner interface
- A konfigurációs állományok parancssorból is szerkeszthetőek
- KAV soha nem változtatja meg a levelek message header részét

Beszerezhetőség, szolgáltatások

- Vásárlás a 2F 2000 cégtől vagy viszonteladóinktól

- E-mailes és telefonos support
- Feliratkozási lehetőség a felhasználói fórumokra
- Tájékoztatás a legújabb program verziókról és új vírusokról weblapunkon: www.2f.hu

- A termékek legfrissebb változata 30 napos próbaváltozatban mindig letölthető
- Az összes termék PDF dokumentációja hozzáférhető

Vége

Köszönöm a figyelmet.

Várom a kérdéseket…