MIT IS MONDOTT? HOGY IS HÍVJÁK?
ELIGAZODÁS A KÁRTEVŐK VILÁGÁBAN

Dr. Leitold Ferenc, fleitold@veszprog.hu
Veszprémi Egyetem

A világon a legelterjedtebb vírusok legautentikusabb forrása a Wildlist szervezet honlapja, melyen (általában) havonta jelenik meg a legelterjedtebb kártevők listája. Ez a lista a a világ legelismertebb szakértőinek jelentésein alapul és kitűnő információs anyag a szakértőknek. Ők mindig pontosan tudják, hogy melyik vírus melyik. Sajnos az átlagos számítógép felhasználók nem képesek azonosítani a kártevők neveit. A 'description' menüpont alatt némi információ olvasható a vírusokról, azonban ezekkel kapcsolatban néhány probléma adódik:

- Az utolsó elérhető információk már nem aktuálisak.
- Az információk az F-Secure adatbázisán alapulnak, így az elnevezések az F-Secure neveihez kötődnek.
- Néhány esetben nincsen információ egyes elemekhez.
- Néhány esetben azonos információk tartoznak különböző variánsokhoz.

Ebben a szituációban az egyedüli jó megoldás a kártevők egzakt neveinek kereshető publikálása lehet, amelyek így már használtok azonosításra.

A probléma megoldását egy Real-Time antivírus ellenőrző rendszer adhatja. Ez a rendszer alkalmas arra, hogy az elterjedt vírusokkal, illetve a vírusvédelmek verzióival lépést tartva, **naprakész információkkal szolgáljon a vírusvédelmek által használt elnevezésekről, illetve az antivírusok legfontosabb minősített paramétereikről** valamennyi számítógép felhasználó számára. A rendszer képes arra, hogy észlelje az antivírusok újabb verzióinak a megjelenését és automatikusan az előre elkészített vírusgyűjteményen néhány futtatást (keresést és eltávolítást) hajt végre, az eredményeket kiértékeli és az Interneten elérhetővé teszi. Egy újabb vírus, féreg megjelenésekor is végrehajtódik az ellenőrzés, illetve ennek megfelelően frissítésre kerülnek az adatok. Az így létrejövő adatbázisban megfelelő kereséssel az egyes vírusnevek összerendelhetők és bárki lekérdezheti, hogy a saját számítógépén talált kártékony kód pontosan milyen fertőzést takar. A futtatások során ellenőrizhető az eltávolító algoritmus eljárása: hogyan és milyen módon történik az eltávolítás (törlés, irtás, esetleg nem tudja eltávolítani.

A Real-time antivírus ellenőrzések egzakt információkat biztosíthatnak a kártevők azonosításához, ami magában foglalja az antivírus termék nevét, verzióját, build számát, adatbázis verzióját, … Lehetőség van továbbá korábbi információk keresésére is.