VírusHíradó

Egy igazi különlegesség az Outlook Express használóinak

Sokféle víruskereső érhető el napjainkban, melyek közül a Kaspersky Anti-Virus Personal, Personal Pro és Windows Workstation termékek igazi érdekességgel szolgálnak. Lehetőséget nyújtanak arra, hogy az Outlook Express adatbázisaiban közvetlenül mentesítsük a fertőzött leveleinket. Ezt a szolgáltatást egyedülállóan csak a Kaspersky Lab víruskereső nyújtják.

Először is érdemes tisztázni, hogy az Outlook Express és a Microsoft Outlook nem azonos termék, csak a nevük hasonló. Lássuk, mi közöttük a különbség. A Microsoft Outlook a külön megvásárolható MS Office csomag része, míg az Outlook Express a Windows 98 óta az operációs rendszerrel együtt kapott "ingyenes" levelező program.

Mit is jelent a közvetlen mentesítés gyakorlatban?

Amennyiben levelezésünk nem egy saját, bejövő és kimenő leveleket vírus ellen szűrő rendszeren megy keresztül, úgy esélyünk van vírusos leveleket kapni. Ha használunk valamilyen víruskereső programot (ezt teszi a felhasználók többsége), úgy a háttérben futó kereső értesít minket a fertőzött levél megnyitásakor, azonban a levél vagy levelek fertőzötten az adatbázisban maradnak, és kitörlésükig magukban hordozzák a vírust. Ha a levél szövege érdekes számunkra, megtehetjük, hogy azt melléklete nélkül saját magunknak elküldjük, így legalább megőrződik a levél szöveges része. Ellenkező esetben az email üzenet törlése az egyetlen megoldás.

Az Outlook Express adatbázisok mentesítése mostantól megkímél bennünket ettől. Ha a levél melléklet fertőzött volt (például egy makróvírusos Word dokumentum), úgy mentesíti azt. Ha a levél egy Internet-férget tartalmaz (például egy I-Worm.Hybris-t), ekkor a mellékletben levő állomány semmilyen hasznos információt nem tartalmaz, ezért a víruskereső törölni fogja. Természetesen az eredeti levél szövege és a levél maga megmarad, csak a melléklet tűnik el.

Mitől újszerű ez a lehetőség?

A tömörített állományokban - és a mi esetünkben a levelezőprogram adatállományai ennek számítanak -

alapesetben kizárólag keresni tudjuk a vírusokat, mentesítést eddig nem tudtunk végezni. A Kaspersky említett programjaiban azonban helyet kapott ez az új opció, melynek működéséhez legalább 5.0 Outlook Express program verzió szükséges, de a vírusmentesítés együttműködik az 5.5 és 6.0 változatokkal is.

Hogyan végezzük el a mentesítést?

A mentesítés idejére kapcsoljuk ki a Monitor modult vagy pedig a Monitor beállításainál kapcsoljuk ki az e-mail üzenetek ellenőrzését. A Scanner modulban válasszuk a keresés helyének a Sajátgép-et, és jelöljük ki a "Scan MS Outlook Express databases" opciót. A sikeres mentesítés előtt mindenképpen szükséges a levelező mappák tömörítése az "Összes mappa tömörítése/Compress all folders" parancs segítségével. Természetesen az ellenőrzés, illetve mentesítés végeztével vissza kell majd kapcsolni a Monitort.

Az aktuális havi kártevők: I-Worm.Aliz és I-Worm.Badtrans II.

Mindkét féreg vírus az Internet segítségével terjed fertőzött email üzenetek mellékleteként. Kódjuk tömörített Win32 platformra írt PE EXE fájl.
Olyan fertőzött email üzenetben érkezhetnek, melynek Subject mezőjébe különböző, véletlenszerűen kiválasztott szövegeket találunk.

A férgek automatikus lefuttatásukhoz egy biztonsági rést használnak ki (IFRAME, hasonló ahhoz, amit a Nimda féreg is használt). Így már akkor aktiválódni tudnak, ha csak olvassuk vagy a preview ablakban megjelenítjük a fertőzött üzenetet (ehhez hasonló volt a KAK.worm féreg, amely szintén a fertőzött melléklet megnyitása nélkül tudott aktiválódni).

Meglepő, hogy ezek a vírusok milyen komoly fertőzést tudtak okozni igen rövid idő alatt. Az ok nagy valószínűség szerint az lehet, hogy azok a felhasználók, akik a figyelmeztetések ellenére sem tartják be az alapvető számítógép biztonsági elveket, újra ugyanabba a hibába estek bele. Nyilvánvaló, hogy a legtöbb vírusfertőzésnek az az oka, hogy nem tanúsítanak kellő óvatosságot az email üzenetekkel kapcsolatban és nem telepítik a megfelelő javító patch állományokat a biztonsági lyukak befoltozására.

A teljes védelemhez (levelezés) feltétlenül szükséges, hogy a megfelelő MS javító állományok is le legyenek futtatva. A védelem Outlook Express / IE böngészőhöz az alábbi helyen található, a "Patch Availability" bekezdés alatt, böngésző-verziónként:

- http://www.microsoft.com/technet/security/bulletin

/MS01-027.mspx

Ha a fentiek nem futnak, mert régebbi verziókról van szó, akkor ugyanez az alábbi helyről tölthető le:

- http://www.microsoft.com/technet/security/bulletin/MS01-020.mspx

Csizmazia István