VírusHíradó

Adatállományok frissítése - a kisujjunk mozdítása nélkül

A víruskereső programok forgalmazói nem győzik hangsúlyozni, hogy az eredményes használat egyik legfontosabb kritériuma, hogy az adatállományok mindig naprakészek legyenek. Felvetődik a kérdés, hogy egy ilyen lényeges folyamatot nem lehetne-e és nem kellene-e kivonni napi - esetleg elfelejthető - tevékenységeinkből és azt teljes mértékben "gépesíteni". Az élvonalbeli víruskeresők igyekeznek ezt a gondot levenni a vállunkról és e téren is hatékony, teljesen automatikus megoldásokkal szolgálnak.

Az F-Secure víruskereső programban a kézi frissítésen felül egy minden igényt kielégítő megoldással találkozhatunk. A BackWeb nevű frissítő programot mind az egyedi felhasználók, mind pedig a hálózatos környezetben üzemelő cégek eredményesen tudják használni. A frissítés az anyacég finnországi nagyteljesítményű BackWeb szerveréről történik Internet kapcsolaton keresztül. A letöltés minimális adatforgalomra optimalizált módon történik, ami azt jelenti, hogy csak a szükséges különbözetek töltődnek le. Lehetőségünk van még arra is, hogy percrekész biztonsági híreket és információkat is kaphassunk elsőkézből. A beállításokat egyszer, a telepítéskor kell jól megadnunk, ezután ezzel a résszel többet nem lesz gondunk.

A következő képen láthatók a BackWeb beállítási lehetőségei:

*** kép!!! ***

A Kaspersky Anti-Virus program szintén igyekszik hatékonyan gondoskodni a magától működő frissítésekről. Az alapértelmezett beállítások szerint naponta egyszer elvégzi az Interneten keresztüli frissítést.

Ennek tulajdonságai részletesen is beállíthatóak a programban. Lehetőség van kézzel indítható, vagy megadott esemény bekövetkeztekor (pl. Monitor modul betöltődése után) aktivizálódó frissítésre, de a folyamat indítása akár egy hónappal előre automatikusan ütemezhető. Megadható, hogy a beírt HTTP, illetve FTP címeket a beírás sorrendjében használja (foglaltság esetén automatikusan a következő címen próbálja), vagy ezek közül véletlenszerűen válasszon. Beállítható az is, hogy a frissítéshez aktiválja az Internet

kapcsolatot, majd a letöltés végeztével bontsa is azt. A teljes folyamat eredménye naplózható is, így később is ellenőrizhető, mikor és hogyan történtek a frissítések. A hálózatos környezetben működő Kaspersky Anti-Virus for Windows Workstation hálózati menedzsment eszköze, az Admin Kittel képes Alert Routingra is. Ez a funkció a rendkívüli eseményekről szóló értesítések az adminisztrátoroknak való továbbítást jelenti. Ez a frissítés szemszögéből nézve azt jelenti, hogy a nem csak a futási problémákról és vírusfertőzésekről, hanem vírusismereti adatállományok frissítési eseményekről is kaphat egy, vagy több tetszőleges cím email üzenetet. Ez a lehetőség természetesen az F-Secure menedzsment programjában, a Policy Manager Console-ban is megtalálható.

Az aktuális havi kártevők

Fájlcserés támadás: Worm.Kazaa.Benjamin
Névváltozatok: Benjamin, Kazaa worm

Úgy tűnik, az összes új vírus indulni szeretne a "világon leggyorsabban terjedő fertőzés" kétes címéért. Az elmúlt hónapban meglepőnek gondoltuk a hazánkban is rekordot döntő Klez vírus elterjedtségét, most azonban meg kell állapítsuk, újabb "rekorder" jelent meg a színen.
A féreg a terjedéséhez a Kazaa fájlátvitelét használja P2P (Peer to Peer) hálózaton. A Kazaa hálózata lehetővé teszi, hogy felhasználói fájlokat vigyenek át egymáshoz a Kazaa kliens szoftvert használva. A Benjamin nevű férget Borland Delphi nyelven írták, mérete körülbelül 216 kB és az AsPack eszközzel tömörítették. A féreg minden fájl végére szemetet ír az álcázás miatt, így a fájl mérete nagyban változhat.

Először a féreg egy hamis hibaüzenetet jelenít meg, majd bemásolja magát a %WinDir%SYSTEM könyvtárba a következő néven: EXPLORER.SCR. Ezután létrehoz két kulcsot a Registry-ben, majd a rendszer újraindítása után aktivizálódik.

A féreg terjedése csak akkor valósulhat meg, ha a KaZaa P2P kliens szoftver telepítve van. A program információk után kutat a Registry-ben a Kazaa kliensről és létrehozza a "%WinDir%TempSys32" könyvtárat, melyet hozzáférhetőnek regisztrál az összes KaZaa hálózat használója számára. Ezt a könyvtárat a program a saját másolataival tölti meg, melynek különböző neveit a féreg törzsében található lista alapján választja. A terjedés a következőképpen zajlik. Az „áldozat” egy fájl után kutat a Kazaa hálózaton, amit a már megfertőzött gép hozzáférhető fájlok listáján talál meg. Nem sejtve a problémát, a felhasználó letölti a keresett fájlt és megnyitja, így megfertőzi a saját gépét.

Hatások
A féreg megnyitja a "www.benjamin.de" Web oldalt, melyen egy hirdetés látható.

Az F-Secure és Kaspersky Anti-Virus programok a 2002. május 20. adatállományokkal már képesek detektálni.

Csizmazia István