Figyeljünk a fájlnév-kiterjesztésre!

A vírusok e-mailes (csatolt fájl útján való) terjesztésének egyik bevett formája az attachment fájlnév-kiterjesztésének elkendőzése, illetve meghamisítása.

Ismert dolog, hogy sima szövegfájlok olvasása, sőt a „valódi" jpg, gif kiterjesztésű képek megtekintése általában nem jár ártalmas programindítással. A baj az, hogy sokszor a vírusgyártók hamisítják a fájlnév-kiterjesztést. Ha a Windows egy txt kiterjesztésű fájlt lát, ahhoz a Notepad (Jegyzettömb) programot indítja el, ha a kiterjesztés doc, akkor az MS-Wordöt. A sima JPEG-fájl is csupán a kép megrajzolásához szükséges gépi utasításokat tartalmazza, s a viewer, a nézőprogram a képolvasási standard utasításait várja a bejövő jpg-fájltól.

Számos email-program alapban a fájlok nevét kiterjesztés nélkül mutatja. Pl. ha egy vírus e-mailhez csatolt fájlként mint artatlan_barany. jpg.vbs érkezik, az e-mailt kezelő program az árulkodó kiterjesztést (vbs) elhagyja, és a fájlnév mint jpg-fájl jelenik meg. Mivel a vbs a Visual Basic szkript kiterjesztése, ha az említett csatolt fájlra klikkelünk, a vbs-programkód végrehajtásra kerül, és az elrejtett vírus aktivizálódik.

Hasonlóképpen a fájltípusok jellegzetes ikonját is tudják hamisítani. (Így trükközött a Nimda-vírus.) Említsünk meg még egy furfangot. Íme egy fájlnév: artatlan_baranyka.jpg .vbs. Itt látszik, hogy sok-sok spáciumot írtak be, elválasztva a hamisított kiterjesztést (jpg) a valóditól (vbs). Vannak programok, amelyeknél kisméretű ablak nyílik, és ha a fájlnév nem fér be az ablakkeretbe, akkor a program jobbról csonkolja a fájlnevet, így a valódi kiterjesztés nem lesz látható. Ilyen zseniális ötlettel terjedt annak idején a Shoho-vírus.

A védekezés fokozására érdemes megjeleníteni a fájlnevek teljes képét. A fájlnév kiterjesztése megjeleníthető az Outlook Expressben is: My Computer (Sajátgép) –> View (Nézet) –> Folder Options (Mappa beállításai) –> View (Nézet) –> Hide file extensions for known type files (Ismert fájltípusok kiterjesztéseinek elrejtése) – itt törölni kell a pipát, majd az Apply (Alkalmaz) gombra kattintani, és fel leszünk vértezve sok minden ellen.

Sajnos azonban nem minden ellen. Továbbra sem látható pl. a .shs (Shell Scrap objektum), .mad, mam, .pif kiterjesztés. Ám ezen is lehet segíteni, mégpedig a registry módosításával. Emlékszünk még a DOS-ban a rejtett fájlokra? A Windowsban is van ilyen. Két alapfájl – user.dat, system.dat – hordozza a legfontosabb beállításokat. Ezek rejtett rendszerfájlok, amelyek megváltoztatásához a regedit-szerkesztőt kell használni. (Ez már kényes dolog, és jobb, ha innen a rendszergazdára bízzuk a feladatot... A registry-beállítások módosításánál nincs megerősítés, azonnal életbe lép a változtatás.) Itt a NeverShowExt registry-értéket kell AlwaysShowExt értékre átállítani.

Bánhegyi Zsolt

Az e-mailtől a spamig és tovább...

Az e-mail születési éve 1971, amikor *Ray Tomlinson*, a BBN-cég mérnöke írásba foglalta a programot, 1982-ben pedig Jonathan Postel fogalmazta meg az SMTP-t (Simple Mail Transfer Protocol). Mind a mai napig ez a kváziszabvány (RFC 821) áll minden e-kommunikáció mögött.

Az e-mail 30 éves évfordulóját méltattam a Kataliston egy 2001. október 4-ei levélben:

http://listserv.iif.hu/SCRIPTS/WA.EXE?A2=ind0110&L=katalist&D=0&I=-3&m=8108&P=2421&F=P

(Ha a szöveg kifut az ablakból, akkor a Proportional Font beállítást kell választani a Katalist menüjében.)

Az e-mailt globális világszámmá a hotmail tette. A bangalore-i (India) születésű *Sabeer Bhatia*, a CalTech műszaki egyetem PhD-s hallgatója és *Jack Smith* az Apple cégnél találkozott, ők ketten alapították a hotmailt. Az első ingyenes e-mail-oldal 1996. július 4-én, az USA függetlenségének napján indult, bevételeit a levelekkel továbbított hirdetések alapozták meg. A Microsoft 1997-ben szédületes összegért, 400 millió dollá-