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-

rért vásárolta meg és azóta is szakadatlanul fejleszti az élenjáró kommunikációs diszpécserközpontot.

Az elektronikus levelezéssel kétes világkarriert befutott, káros jelenség a kéretlen tömeglevél, a „spam". A való világban csupán kellemetlen bosszúság a postai úton jövő reklámújság-áradat (angolul junk-mail), e-világbeli megfelelője viszont szinte már a normális kommunikációt fojtogatja. Az e-mail 33 éves történetében az első alkalommal tavaly, 2003-ban történt meg, hogy a spamek száma megelőzte a normális e-mailek számát. Valószínűleg ez a tény mozdította meg az amerikai kongresszust, hiszen hat éven át tartó hezitálás után 2003 decemberében végre elfogadta az első, „Can-Spam Act" nevű – C(ontrolling the) A(ssault of) N(on-)S(olicited) P(ornography) A(nd) M(arketing) Act – szövetségi törvényt a spam megregulázására.

A spam körül egész iparág sarjadt ki az évek során: spamellenes szervezetek, spamkereső szoftverek, feketelisták, szűrőprogramok, hírlevelek stb. Az AOL (America On-Line) tipizálja a spameket a Subject (tartalom) szerint. Természetesen mindenki számára túlságosan is ismerős a Viagra online, a nigériai „könyörgés", az on-line nyeremény, az adósságkezelés, a legalacsonyabb jelzálográta, és persze a pornográf oldalak özöne.

A spam elleni harcban a tudósok visszanyúltak egy angol matematikus, Thomas Bayes 1763-ban (halála után két évvel) publikált munkájához, címe: Essay towards Solving the Problem in the Doctrine of Chances. Bayes valószínűség-számítási írásában a jövő eseményeinek eshetőségét vizsgálja. A Hotmail.com által is alkalmazott Bayes-féle spam-szűrő úgy működik, hogy „tanul" a használó törlési szokásaiból, és bizonyos jellemzők alapján már maga dob ki e-maileket, vagy jelzéssel látja el azokat. Ráadásul ez a tanulás egyre finomabb szűrést eredményez!

A spam szó eredetét érdemes felidézni – elnézést, hogy idézek pár mondatot a három évvel ezelőtti Katalist-levelemből. „A SPAM a Spiced Pork And haM rövidítése, ami a HORMEL élelmiszeripari vállalat 1936-ban piacra került márkája volt. Olcsó húskonzerv, szakasztott olyan, mint a Magyarországon a 60-as években »sztár alkalmazásnak« számító kínai löncshús."

A húskészítmény ma is töretlen népszerűségnek örvend, haspók zarándokok számára még SPAM-múzeum is van a HORMEL Foods vállalat székhelyén, Austinban (Minnesota): http://www.spam.com

„A Monthy Python Flying Circus színházi társulata adta elő azt a jelenetet, amikor az étteremben a viking harcosok egyre hangosabban skandálják, hogy spam-spam-spam-spam, végül fülsiketítő lesz az egész, és minden egyéb beszélgetést elnyom ez a lárma. Rendkívül leleményes volt az az ismeretlen – valószínűleg a Usenet köreiből –, aki a spam szót a tömeges, mindent elborító levélözönre alkalmazta." A gyártó már megbékélt azzal, hogy terméke ilyen negatív értelmet is fölvett, ám megkülönböztetik a csupa nagybetűs SPAM-et – amely az ehetőnek mondott termék márkaneve – és a csupa kisbetűset, ami a baljós értelmű fogalmat jelöli.

Mint ismeretes, mind a spamek, mind a vírusok terjesztésének közkedvelt módszere a hamisítás, közelebbről a levél feladójának (From:) meghamisítása. A mostani, „Végzetem" nevű vírusnál elhűlve tapasztaltam, hogy mennyire felkészületlenek a rendszerek „világszerte". A mailerdémonok és gépi postamesterek százával-ezrével dobták vissza a leveleket – a hamisított címekre! Pedig az e-mail fejlécében pompásan lehet látni, valójában honnan érkezett egy levél, nslookuppal vissza lehet fejteni a feladót legalábbis a szerver szintjéig. Oda kellene visszaküldeni a levelet, és nem a robotok által találomra beírt, a küldeménnyel semmiféle kapcsolatban nem álló címekre... (Zimányi Magda a 2003. szeptember 18-ai levelében utal a KFKI honlapján elérhető kalauzra, ahol a különböző levelező-kliensek beállításai megtalálhatók: http://listserv.iif.hu/SCRIPTS/WA.EXE?A2=ind0309&L=katalist&P= R27718&D=0&H=0&I=-3&O=A&T=1.) 2003 decemberében egy amerikai spamellenes honlap részére készítettem egy összeállítást az e-mailek fejlécének természetrajzáról. Címe: Olvassunk e-mail-fejléceket. Ez az anyag – magyar nyelvű! – elérhető a következő honlapon: http://www.stopspam.org. (A fejlécen a dátum 1993. szeptember 3744-et mutat. Ironikus számlálás, 1993 szeptemberében állt meg ugyanis az idő egyes szakértők számára, amikor az AOL kapcsolódott az internethez és dilettánsok tömege lepte el a hálózatot...)

Közvetlenül a magyar szöveghez ezen a címen juthatunk: http://www.stopspam.org/email/headers/headers_hu.html

Bánhegyi Zsc