Spamekről, spamelőkről

A *Sophos* ma az egyik legmarkánsabb *brand*, bevezetett és hírnévre jutott cégnév: hallatán a vírusok és férgek nyüszítve eltakarodnak, a trójai falovak recsegve-ropogva pozdorjává hullnak. Az Egyesült Királyságban, az Oxford melletti Abingdonban székelő, 1985-ben alakult vállalat biztonsági termékeit százötven országban több tízmillió számítógépen futtatják naponta, a Sophos a vírusvédelem óriása a *Norton,* a *McAffee* és az *F-Secure* mellett.

A legfrissebb veszélyekről, a védekezés módjairól rendkívül gazdag anyag található a cég honlapján (http://www.sophos.com) – onnan kiindulva ismerkedjünk meg új szakkifejezésekkel, olyanokkal, amelyek a rendszeresen aktualizált on-line szótárba, a Merriam-Websterbe sem kerültek még be. Szemezgessünk, milyen eszközökkel él a megújulásban eminens spamelők hada, és villantsunk fel jelzésszerűen egy-kettőt a világhálón navigálókra leselkedő veszélyekből. Egyáltalán nem csökkent a hálóra küldött *malware-ek,* azaz rosszindulatú programok mennyisége, amelyek egyik altípusa a gépünkről jelentést küldő *spyware*, kémeszköz. Ebbe a családba tartozik például a népszerű *keylogger,* billentyűleütés-követő, amely a bejelentkező jelszavainkat naplózza és 'hazaküldi' a gyártó hackernek, akit akár már magyar helyesírással hekkernek is írhatunk. A macska-egér harc a spamelők, víruskészítők és a védekező harcosok között folytatódik. Ne felejtsük el, hogy egyedül 2004-ben 10 724 új vírust azonosítottak, és 2005. január 1-jén a létező vírusok száma 97 535 volt.

Az e-mail ma is kitüntetett hordozórakétája a hamis és káros küldeményeknek. A *BubbleBoy*, a neve ellenére egyáltalán nem vicces 'Buborékfiú' 1999-es megjelenése óta már nemcsak a mellékletek kibontása lehet veszélyes, hanem a levél olvasása is kiválthatja a vírusos kód aktiválódását. Egyébként a BubbleBoy nemcsak kártékony természete miatt nem vicces, a szó eredete szerint sem: az 1990-es években futó amerikai szappanopera, a *Seinfeld* egyik epizódjában Jerry, a címszereplő meglátogat egy beteg gyereket, aki műanyagbuborékban él... (Erről a maga nemében úttörő vírusról annyi technikai részletet áruljunk el, hogy a Microsoft Outlookon át az Internet Explorerben két, potenciálisan károssá tehető ActiveX vezérlőt – scriptlet.typelib, Eyedog – tud futtatni.

Az aktivizált vírus az indító állományban létrehoz egy UPDATE.HTA nevű fájlt, amely aztán a PC bootolásakor rendszerelemeket módosít, és elküldi önmagát az Outlook címjegyzékében található címekre. Még szerencse, hogy a vírus megjelenése után a Microsoft sietve javítócsomagot, ún. *patch*ot bocsátott ki, amellett a Win98-nál frissebb verziónál már nem is fut a BubbleBoy.)

A junk-mail, a spam változatlan virágzása miatt nézzük meg, milyen kimeríthetetlenül rafináltak a spam-küldők a levelek célbajuttatásában. Leleményes magatartásuk lényege az elkenés, ködösítés, elkendőzés – angol műszóval: *obfuscation* –, ami egyfajta védekezés és reakció a spamszűrő (antispam) programok új nemzedékére. Ezek a mailszerverekbe, levelezőkliensekbe telepített szoftverek professzionális felismerő módszerrel komplex szótári ellenőrzést végeznek, amelynek során a spamek által leggyakrabban használt szavak alapján különítik el és teszik karanténba a gyanús leveleket. A spam egyéb elfogadott terminusa például az UBE (Unsolicited Bulk Email) = kéretlen tömeges e-mail, illetve az UCE (Unsolicited Commercial Email) = kéretlen kereskedelmi e-mail.

A spamelők felkutatására és sarokba szorítására ma már vannak módszerek: *honeypot*-nak (mézescsupor) hívják a spammerek befogására felállított csapdarendszereket. Egyes biztonsági cégek pedig a *tarpit* (szurokgödör) eljárással úgy büntetik a spamküldőt, hogy gépére lassító programokat küldenek. Látni való, hogy az egy évvel ezelőtt az USA-ban elfogadott CAN-SPAM törvény nem javított a helyzeten, bár van példa arra is, hogy spamelőt börtönbe csuktak. Az egyik lebukott nagybani játékos nyomán azért napvilágra került, hogy nem rossz üzlet a spam. A North Carolina államban élő *J. Jaynes* naponta húszmillió spam-levelet küldött szét. Ebből a

hatalmas mennyiségből mindössze pár száz eladást tudott realizálni, ami nagyon rossz arány, mégis, havonta 750 ezer dolláros jövedelemre tett szert! (http://www.f-secure.com/2004)

Persze magában a spam még ártatlan is lehetne, de a levelek kezelésével, a törléssel eltöltött egyre hosszabb idő miatt oda az ártatlanság. A nagyobb baj az, hogy a spamek hátán az élősködők tömege terjed a világhálón – a vírusok, hátsó ajtón érkező trójaiak egyik fő szállítóeszköze a spam. Rutinszerű eljárás például a s*poofing*-nak (kész átverésnek) nevezett trükk, amely a levél küldőjének (From:) a címét hamisítja meg. A *maildrop* olyan átmeneti postafiók, amit a spamküldő ad meg a válaszlevelek számára, és még a lelepleződés előtt felszámol.

Alább néhány, a tömeglevelek küldői körében köz(?)kedvelt fogást idézünk. A spamelők a webalapú mailkliensek sajátosságait használják ki. Ezek a levelező-szoftverek az internet anyanyelvén – HTML-ben – és modorában – CSS-en (Cascading Style Sheet) – társalognak: a spamszűrő szoftver látja a HTML/CSS-kódolást, a kliensben a címzett pedig a kódolás megjelenített formájával, a webes megjelenítéssel találkozik.

Mintának vegyük a világháló e-kereskedőinek vagy tán e-kufárjainak egyik állandó propagandatételét, a rendkívüli életerőt felmutató Viagra-reklámot.

Elveszve az űrben

A viagra szót még az egyszerű, cseppet sem vizuális spamfilter is messziről felismeri és karanténba dugja. Kamuflázs céljából, tehát hogy a szűrő ne ismerje föl a szótári ellenőrzés alapján ezt a szót például a levél tárgyában, a Subjectben, valamilyen módon eltorzítják, spáciumot (szóközt) tesznek az egyes betűk közé (V I A G R A), vagy ‘a’ helyett @-jelet írnak (vi@gr@).

Fekete lyuk

Ez még ügyesebb: a HTML-kódolást használva a betűk közé spáciumot tesznek be, ugyanakkor a spácium méretét nullára állítják, tehát az üres leütés eltűnik a betűk közül. A spamszűrő szoftver ezt látja:

V
i
a
g
r
a,

a levél címzettje pedig ezt:

Viagra.

Láthatatlan tinta

A spam küldője a szűrő számára egy ártatlan szöveget kínál, közben a valódi üzenet a levél címzettje számára szól. A HTML-kódot használja oly módon, hogy az ártatlan fals szövegben a betűk színe megegyezik a háttér színével, azaz láthatatlan a levélben, csak a HTML-érzékeny spamszűrő olvassa.

<body bgcolor=white>Viagra
Szia édesanyám, finom volt a krumplileves, amit küldtél, szerető fiad</body>

Talán mondani se kell, hogy ebből a szövegből a böngészőben mindössze az jön elő, hogy Viagra.

Vissza a feladónak

A spamelő szándékosan rossz címre küldi az e-mailt, de a From mezőbe egy kiszemelt, mit sem sejtő címzett postacímét írja. Mivel a levél nem kézbesíthető (non-deliverable), a szolgáltató szerver visszaküldi – ám nem oda, ahonnan ténylegesen kapta, hanem a From mezőben szereplő címre.

Játék a számokkal

Itt is a HTML-kódolás a lényeg. A HTML-ben a betűknek is megvan a kódjuk, tehát a spamekre jellemző szavakat kiszűrő programot úgy cselezik ki, hogy a rendes betűk helyett a HTML-kódokat használják (pl. az a betű HTML-kódja: &97;)

Ezt látja a (szegény) spamszűrő program:

V
i
a
g
r
a

És mit lát a levél emberi olvasója? Hát ezt:

Viagra.

Mikropötty

Az angolul *microdot*ként elhíresült fogás úgy működik, hogy a szó közepére egy idegen karaktert írnak be, ám olyan apró, pontszerű, 1-es méretre zsugorítják, hogy a filtráló programot megzavarja a mikrobetű használata és átengedi a spamet. Nézzük a CSS-ben, hogy néz ez ki:

Vziagra

Amelyből a böngészőben ezt látjuk:

V.iagra.

Számos próbálkozás történt a spam-blokkolásra, jelesül például arra, hogy a *spambot*ok, a spamelők számára címeket begyűjtő robotok ne tudják betakarítani az e-mail címeket. Ennek a védekezésnek az angol szakszava: *munging*. Az e-mail cím eltorzítása, mondjuk az @ jel helyett at beírása azonban rontja az internet interaktivitását, a spambotok pedig amúgy is mosolyogva túllépnek ezen a kis akadályon, és megszerzik a címeket.

Szelíd védekezésnek számít, ha úgy küldjük a levelet, hogy a címzett(ek) címét nem a To mezőbe írjuk, hanem ahelyett a *blind carbon copy* (a titkos címzett) mezőjébe (Bcc) írjuk a címzett(ek) címét, amely eltakarja a spamgyűjtők elől a címjegyzéket.

Ahogy szó volt róla, a levélolvasás is lehet veszélyes üzem. A probléma az, hogy a legtöbb helyen például az Outlook Express úgy van beállítva, hogy a letöltött levelek közvetlen rálapozásakor a Preview módban megjelenik a levél. Biztonságosabb, ha a Preview modult kikapcsoljuk és a levéllistában a Subject alapján próbáljuk kiszűrni az ártalmas leveleket.

Bölcs tanács, hogy a spamekre ne válaszoljunk, csak töröljük őket. Nem szabad válaszolni egyebek közt olyan kérdésekre, hogy „ha nem akar feliratkozni a hírlevélre, ide klikkelve (vagy ezen a címen) lemondhatja”. Ha erre válaszolunk, a spammer tudni fogja, hogy az adott e-mail cím él. Nézzünk még mutatóba néhány, a félrevezetésből direkt csalásba torkolló hálós trükköt.

Page-jacking – mouse-trapping – phishing

Page-jacking (weblaprablás): Egy ismert, jó reputációjú cég webhelyéről néhány oldalt lemásolnak, azokat egy új webcímen beindítják és nagyobb keresőmotoroknál regisztrálják. A keresés során a találati link révén odakerülő használót redirect paranccsal átirányítják egy általuk ellenőrzött honlapra. Ezen a lapon aztán előfordulhat a *mouse-trapping* (egérfogás), amelynél a Back (vissza) gomb használatát tiltják le – ilyenkor legjobb újraindítani a gépünket.

Úgy is ki lehet kerülni ezeket, hogy a Kedvencek listájából kattintunk az ismert honlapra, és nem egy ismeretlen webhely linkjéből – vagy pedig a Címsorba közvetlenül írjuk be az ismert webcímet.

Fishing: ez a rendkívül veszélyes, szemléletesen horgászásnak nevezett fogás szintén a weblaprablás folyománya: e-mailben vagy ismeretlen webhelyen szereplő linkre kattintás esetleg ilyen álhonlapra, talán saját bankunk képét bitorló helyre visz, ahol pinkódot, hitelkártya-számot meg ilyesmit kérnek. Az így kicsalt bizalmas információ aztán sokszor a viruló *cyberscam* (kiberbűnözés) eszköztárát bővíti.

Bánhegyi Zsolt

A http://virus.lap.hu/ weboldal részlete: