**ELŐADÁSOK NYOMDAKÉSZ ANYAGA**

# SPAMBIZNISZ – A KÉRETLEN LEVELEK ÚTJA A TÁMADÓTÓL AZ ÁLDOZATIG

***Krasznay Csaba, krasznay.csaba@kancellar.hu***
*kancellár.hu Kft.*

## Bevezetés

Napjaink legnagyobb kihívásai közé tartozik a kéretlen elektronikus levelek kezelése. Az iparági statisztikák alapján elmondható, hogy az összes elküldött e-mail kb. 40%-a tartozik ebbe a körbe, ami naponta több mint 10 milliárd kéretlen levelet jelent. Eszerint egy felhasználó egy évben 2200 spamet kap. Ennek megfelelően a védelmi megoldások száma és minősége is sokat fejlődött az elmúlt időkben. De ezek csak tüneti kezelések. A megfelelő védekezéshez tudni kell a kór okát is. Előadásomban megvizsgálom a kéretlen levelek útját a megrendelőktől, azaz a hirdetőktől az áldozatokig, az internetet használó milliókig. Részletesen kitérek az ilyen küldemények típusaira, a gyanítható bűnszövetkezetek működésére, akik a postázást intézik, és azokra a műszaki megoldásokra, melyekkel milliószámra lehet e-mail címeket szerezni, valamint ezekre a leveleket eljuttatni. Végül bemutatom a kéretlen levelek célpontjait is.

A vizsgált területen sok esetben nehéz hiteles információkat szerezni, ezért sokszor iparági szakértőkre vagy bírósági ítéletekre kell hagyatkoznunk. Azonban azok az informatikai támadások, melyek minden nap érik még a legkisebb szervezet infrastruktúráját is, közvetett bizonyítékot jelentenek arra, hogy a háttérben hatalmas üzletet jelentő szervezett bűnözés folyik. Szun Ce mondása szerint „Ismerd meg az ellenséget, és ismerd meg önmagadat, így akár száz csatát is megvívhatsz vereség nélkül”. A statisztikák szerint a spamek ellen az információs társadalom már sok csatát elveszített. Talán éppen azért, mert nem ismerjük kellően az ellenségünket. Előadásom célja tehát az, hogy az érdeklődők betekintést kaphassanak ebbe a sötét háttérbe is, illetve megismerjék azokat az egyébként roppant innovatív technológiákat, melyeket a támadók bevetnek.

## A kéretlen levelek típusai

Az informatikai biztonság több területén is igaz, hogy nehéz egzakt kategóriákat felállítani az adott támadás típusairól, éppen ezért ahány tanulmány, annyiféle csoportosítás használatos. Igaz ez a kéretlen levelekre is, nem utolsósorban ezek állandó változása miatt. Ráadásul az altípusok arányai is minden hónapban, minden kimutatásban mások. Az alábbiakban a Symantec 2007. februári Spam Monthly Report [1] kiadványának kategóriáit ismertetem. Ez többnyire megfelel az iparági szóhasználatnak, és jól szemlélteti a különböző típusok arányait is, melyek a tanulmány írásakor voltak érvényesek.

- Termékekkel kapcsolatos levelek: általános termékeket és szolgáltatásokat kínáló üzenetek. Például órák, ékszerek, befektetési szolgáltatások. A vizsgált időszakban ez a típus az összes kéretlen levél 23%-át tette ki.

- Felnőtteknek szóló levelek: olyan termékek vagy szolgáltatások, melyek felnőtt személyeknek szólnak, pornográf jellegük miatt különösen zavaróak. Például pornográf oldalak hirdetései, személyes hirdetések, társkereső szolgáltatások hirdetései. A vizsgált időszakban ez a típus az összes kéretlen levél 4%-t jelentette.
- Üzleti levelek: olyan kéretlen levelek, melyek pénzzel, tipikusan tőzsdei, vagy más üzleti befektetéssel kapcsolatosak. Például tőzsdei levelek, kölcsönök, jelzálogok hirdetései. A vizsgált időszakban ez a típus az összes kéretlen levél 25%-át tette ki.
- Csalások: olyan levelek, melyek valamilyen széleskörű csalásba próbálják bevonni az áldozatot. Például ilyenek a nigériai levelek, a piramisjátékok hirdetései, a lánclevelek. Ez a típus az összes kéretlen levél 4%-át jelentette.
- Egészséggel kapcsolatos levelek: gyógyászati termékek és szolgáltatások hirdetései. Például ide sorolhatjuk az impotencia elleni szerek, nyugtatók, gyógynövények reklámozását. A kéretlen levelek 23%-a volt ilyen típusú 2007. első hónapjában.
- Megtévesztő levelek: a levél látszólag egy jól ismert vállalattól érkezik. Ismert még phishing, azaz adathalász támadásként is, melynek során az áldozat e-mail címét, felhasználónevét, és mindenekelőtt a jelszavát próbálják megtudni. Például online banki és árverési oldalak figyelmeztetései. A felmérés szerint ez a típus 3%-ot jelentett az összes spamforgalomban.
- Szabadidővel kapcsolatos levelek: díjakkal, nyereményekkel, nyerési lehetőségekkel csábító üzenetek. Például online kaszinók hirdetései, nyaralási ajánlatok. 5%-ot jelentett ez a típus a teljes forgalomban.
- Internettel kapcsolatos levelek: internetes vagy más számítógéppel kapcsolatos termékek és szolgáltatások hirdetései. Például webhostolás, web design, szoftverek. Ez a teljes kéretlen levél forgalom 13%-át tette ki.
- Politikai levelek: ilyenek egy jelölt vagy párt hirdetése kampányidőszakban. Például szavazatszerző, anyagi támogatást kérő levelek. A vizsgált időszakban az ilyen típusú levelek nem jelentkeztek kimutatható számban.
- Spirituális levelek: egyházi, spirituális közösségek kéretlen hirdetései. Például tagtoborzás, asztrológiai hirdetések. A vizsgált időszakban az ilyen típusú levelek nem jelentkeztek kimutatható számban.

# A kéretlen levelek megrendelői

A Symantec felmérése alapján 2007. első hónapjában a kéretlen levelek háromnegyedét az üzleti, a termékekkel kapcsolatos és az egészséggel kapcsolatos üzenetek tették ki. De vajon kik állnak az üzenetek mögött?

## *Tőzsdei csalások*

A legtöbb kéretlen levél jelenleg tőzsdei befektetési ajánlatokkal kapcsolatos. Valószínűleg ezek hozzák a legnagyobb jövedelmet is. Robert Lemos Securityfocuson publikált tanulmányának [2] forgatókönyve jól mutatja, hogy a szervezett bűnözés milyen módon használja ki az internetes technológiákat. Mit látnak az internetezők? Adott egy alacsony áron megszerezhető részvény, aminek az árfolyama hirtelen elkezd emelkedni, majd tömeges e-mailek kerülnek kiküldésre arról, hogy a vállalkozás valamilyen jelentős eredménnyel készül megjelenni. Ettől természetesen még magasabbra kúsznak a részvényárfolyamok.

A kívülálló azt hihetné, hogy az ilyen támadások mögött az a cég áll, amelynek a részvénye felfelé kúszik. Ez tévedés, ugyanis amikor kiderül, hogy csalás áll a részvények emelkedése mögött, az árfolyamok hirtelen zuhanásba kezdenek, és általában alacsonyabb szinten állnak meg, mint ahonnan indultak.

Valójában a következő történik. A támadók valamilyen „hagyományos” informatikai támadás során hozzáférést szereznek olyan alkalmazásokhoz, melyeken keresztül részvényeket lehet venni. Ez általában azonosítók és jelszavak megszerzését jelenti phishing támadás vagy trójai fertőzés során. A vállalat kiad egy közleményt, amiben valamilyen céggel kapcsolatos hírt közöl. A támadó ebben a pillanatban elkezd részvényeket vásárolni a megszerzett azonosítókon keresztül – természetesen nem a saját pénzén. Csak egyetlen azonosító az övé, így az el tud tűnni a sok másik legálisnak látszó vevő között. Ezután különböző spam küldési technikákon keresztül olyan leveleket küld ki, melyekben az eredetileg ártatlan hírt kicsit átalakítva vonzó befektetés látszatát kelti. A naiv áldozat meglátja a csábító hírt, az emelkedő részvényárfolyamot, és ő is elkezd vásárolni. Ezzel még jobban emelkedik az árfolyam, és eljön az a pillanat, amikor a támadó elad. Hamarosan kiderül, hogy csalás volt az árfelhajtás, az árfolyam zuhanni kezd, mindenki rosszul jár – az áldozat, a cég – egyedül a támadó szerzett hasznot. Jelenleg ennél jövedelmezőbb támadást nem találtak ki ebben a műfajban.

## *Termékhamisítások*

Idézet az Európai Bizottság 2005. október 11-én kelt sajtóközleményéből [3]:
„2005. október 10-én az Európai Bizottság újabb konkrét lépéseket hirdetett meg a termékhamisítás leküzdésére. A hamisított termékek egyre fenyegetőbb veszélyt jelentenek az európai fogyasztók egészségére - hangsúlyozta sajtótájékoztatóján Kovács László, adó és vámügyi biztos, az Európai Bizottság magyar tagja. Elmondta, bár a sikeres felderítések száma évről évre nő, az Európai Uniónak fokoznia kell a küzdelmet a termékhamisítás ellen. 2004-ben ugyanis a lefoglalt hamisított áruk mennyisége soha nem látott méreteket öltött: 103 millió hamisított terméket foglaltak le, 12%-kal többet, mint az előző évben, és 1000% többet, mint 1998-ban.”

Ebben az emelkedésben jelentős szerepet játszott az, hogy a kéretlen levelek útján sokkal hatékonyabban lehet hirdetni a hamisított termékeket, mintha arra várnánk, hogy a vevő betéved a boltunkba. És ha már milliószámra mennek ki az üzenetek, érdemes a legnagyobb bevételt generáló termékeket reklámozni. Ezek pedig a luxuscikkek. Jellemző például a következő, ún. replica store honlap FAQ-jából származó gondolkodás:

- Miért vegyek másolt órát az eredeti helyett?
- Azért, mert anélkül keltheted a jólét látszatát, hogy több ezer dollárt kéne kifizetned. Ezek az órák pontosan úgy néznek ki, mint azok, amik a hivatalos kereskedőknél kaphatók, és amiket nem engedhetsz meg magadnak. Semmi magyarázat nincs arra, hogy ezek az órák miért csak a gazdagok kiváltságai, ezért vegyél te is magadnak egyet!

A vásárlót ilyen, és ehhez hasonló módon beszélik le az eredeti termékekről. Arról természetesen egy szót sem szól a honlap, hogy az ilyen másolás bűncselekmény. Talán ezért nem szállít az online kereskedő Németországba és Svájcba.

- Hogyan léphetek kapcsolatba az áruházzal?
- Kattints ide, és küldj nekünk e-mailt!

Bár a honlap végig arról győzködi a vásárlót, hogy amit vesz, az tökéletes minőségű, a boltnak nincs fizikai megjelenése, így természetesen a garanciát sem lehet érvényesíteni. Pedig ezek a másolatok eléggé silány minőségűek.

### *Gyógyszerreklámok*

Az eddigi típusok „csak” az áldozatok pénztárcájára voltak veszélyesek. A hamis gyógyszerek azonban már emberéletekbe kerülhetnek. Éppen ezért az Európai Bizottság ebben a témában is adott ki sajtóközleményt [4], melyben az interneten eladásra kerülő gyógyszerek veszélyeire hívta fel a figyelmet.

A trendek azt mutatják, hogy leginkább a potencianövelő és a nyugtatószerek illegális kereskedelme mutatkozik meg a kéretlen levelekben. Ezek a népszerű gyógyszerek ugyanis eredeti kiadásban drágák és nehezen (értsd orvosi vizsgálat után) hozzáférhetők. Illegális kereskedelemben azonban nagyon kelendőek. Igaz, a „hatóanyaguk” sokszor nemhogy elősegítené a páciens gyógyulását, de meg is öli az áldozatot. A USA Today 2007. február 14-én adott hírt egy kínai gyógyszerhamisító gyár leleplezéséről. A gyárban 2000 kék pirulát foglaltak le 320.000 $ értékben. [5] A híradás arról nem szól, hogy ennek a gyárnak hány áldozata volt.

## A kéretlen levelek postásai

A SpamHouse.org szervezet folyamatosan aktualizált listát vezet a világ 10 legtöbb kéretlen levelet kiküldő személyéről és szervezetéről. [6] Ezek többsége Oroszországból vagy Ukrajnából származik. Néhány példa:

- Alex Poljakov: az ukrán „úriembert” tartják napjaink legtöbb spamet generáló támadójának. Az interneten terjedő, nehezen ellenőrizhető információk szerint ő a felelős szinte minden jelzáloggal, gyógyszerrel, pénisznövesztővel és befektetési ajánlattal kapcsolatos kéretlen levélért.
- Leo Kuvajev: orosz származású, amerikai spammer. 2005-ben 37 millió dolláros büntetést szabott ki rá egy amerikai bíróság, azóta szökésben van.
- Amichai Inbar: az izraeli származású spammer szoros kapcsolatban áll orosz kollégáival. Több milliárd pornográf és egészségügyi spam elküldéséért felelős.
- Ruszlan Ibragimov: az orosz programozó nevéhez fűződik a legnépszerűbb spamküldő szoftverek megírása, gyaníthatóan több férget is ő írt.
- Michael Lindsay: a SpamHouse állítása szerint cége teljes körű domainszolgáltatást nyújt a spammereknek.

A sort még lehetne folytatni, az azonban látszik, hogy ezek az emberek főállásban a kéretlen levelek továbbításával foglalkoznak, és ami a legszomorúbb, hogy a hatóságok többnyire tehetetlenek, nem tudják őket megfékezni. Feltételezések szerint a rangsor első 10 helyezettje felelős a világ összes spamtermésének 80%-áért.

## Spamküldési technikák

A sikeres spamküldéshez két dolog kell: sok számítógép, és még több e-mail cím. Az előző bekezdésben említett személyek legnagyobb értéke az, hogy hatalmas mennyiségű számítógép áll rendelkezésükre a kéretlen levelek elküldésére. Ezek az ún. botnetek. A Wikipedia definíciója [7] szerint a botnet olyan kompromittált számítógépekből álló hálózat, amelyeket rosszindulatú szoftverek segítségével egy helyről tudnak irányítani.

A botnet kialakításához tehát kell egy féreg vagy egy trójai, ami az áldozat számítógépét megfertőzi. Ezek egy hátsókaput (backdoor) nyitnak az áldozat számítógépén, amihez a spammer hozzá tud férni, irányítani tudja őket. Friss e-mail adatbázisokat tud feltölteni, és a megrendelő igényeinek megfelelő tartalmú szövegeket tud elhelyezni a levelekben.

A legismertebb ilyen szoftver talán a Send-Safe, melyet a már említett Ibragimov fejlesztett. A napvilágra került információk szerint a szoftverből egyszerűen, látványos kezelőfelületen keresztül lehet a spameket beállítani és kiküldeni. A Send-Safe szolgáltatásai interneten keresztül rendelhetők meg, hasonlóan egy legális, banner alapú online hirdetéshez. A másik népszerű eszköz a Dark Mailer, mely kevésbé látványos, de hasonlóan hatékony GUI-n keresztül képes kéretlen levelek milliárdjait előállítani és szétküldeni.

Szükség van még rengeteg élő e-mail címre. Ezeket számos formában lehet megszerezni. A legegyszerűbb megvenni egy ilyen listát. Nem is olyan régen magyar levelezőlistákon sok tízezer élő e-mail címet tartalmazó listát árult valaki (spamben). Koreában január végén vettek őrizetbe egy férfit, aki Dél-Korea szinte teljes lakosságának e-mail címével rendelkezett.

De az ilyen listákat össze kell gyűjteni, ami komoly feladatot jelent. A teljesség igénye nélkül néhány technika:

- Vírusok, férgek útján: régóta ismert a károkozóknak az a funkciója, hogy a megfertőzött gépen e-mail címek után kutatnak. Ezeket a címeket spammelésre is fel lehet használni.
- Nyilvános forrásokból: az interneten számtalan helyen találhatók e-mail címek. Weboldalakon, Usenet oldalakon, fórumokban. Egy jól megírt, e-mail címekre optimalizált keresőrobot rövid idő alatt több millió e-mail címet tud összegyűjteni.
- Találgatással: az e-mail címek gyűjtése hasonlóan tud működni a jelszavak brute-force jellegű feltöréséhez. Generáljunk véletlenszerűen felhasználóneveket, adjunk hozzá egy domain nevet, és próbáljuk meg elküldeni. Ha nem kapunk vissza hibajelzést, akkor az az e-mail cím érvényes. Ezt a támadást hívják Directory Harvest Attacknak (DHA).
- Emberi ráhatással: az információbiztonság leghatékonyabb támadása az emberi ráhatással (social engineering) történő támadás. Ha sok e-mail címet akarunk, akkor kérjük el. Lesz olyan, aki odaadja.

## A spamek áldozatai (?)

Bizonyára sokakban felmerül a kérdés: ki az, aki spameket elolvassa, és utána vásárol? Ha valamire nincs kereslet, akkor előbb-utóbb a kínálat is megszűnik. Az átlag internetező nem különbözik az átlagembertől. Sokan inkább olcsón akarnak vásárolni, és nem veszik figyelembe az ezzel okozott károkat. A károkat, melyeket saját maguknak és embertársaiknak okoznak.

Ahogy a hétköznapokban is láthatjuk, mennyien vesznek hamisított terméket, ez ugyanúgy tetten érhető ez az interneten is. Jól mutatja a tendenciát a Business Software Alliance 2004 végén publikált felmérése [8], melyben 6 ország 6000 internetezőjét kérdezték meg a spamekkel kapcsolatos véleményükről. A felmérésben Brazília, Kanada, Franciaország, Németország, Nagy-Britannia és az USA vett részt. Az eredmények azt mutatják, hogy minden országban, minden típusú spam legalább 20%-át a címzettek elolvassák. De ami még megdöbbentőbb, a legkevesebbet vásárló kanadaiak közül is 32% már költött pénzt olyan termékre, amit spamben hirdettek. A braziloknál ez az arány 66%.

## Összefoglalás

Kéretlen levelet küldeni érdemes. Érdemes a termék előállítójának, érdemes a spam terítőinek, első látásra érdemes a vásárlóknak is. Az internet egyik legnagyobb átka mégis a kéretlen levelek tömege. Vajon vesztésre állunk? Véleményem szerint pillanatnyilag igen. A

gyenge jogi szabályozás miatt, a határokon átnyúló cselekmények miatt, és főleg a célpontok vásárlási aktivitása miatt a kéretlen levélküldés sokáig része lesz az életünknek. Hiába tartóztatnak le spammereket, jönnek helyettük újak. A spamszűrő szoftverekkel csak tüneti kezelést lehet adni, az igazán hatékony védekezést a vásárlói tudatosság fejlődése jelenthetné. Ez azonban már nem informatikai probléma.

## Irodalomjegyzék


[1] The State of Spam – A Monthly Report, Symantec, http://www.symantec.com/avcenter/reference/Symantec_Spam_Report_-_February_2007.pdf

[2] Robert Lemos: Spammers get bullish on stocks, SecurityFocus, http://www.securityfocus.com/news/11435

[3] A Bizottság újabb intézkedéseket szorgalmaz a termékhamisítás ellen, Európai Bizottság, http://ec.europa.eu/commission_barroso/kovacs/speeches/counterfeit_IP.pdf

[4] Commission warns about fake drugs on the internet, European Comission, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/06/375&format=HTML&aged=1&language=EN&guiLanguage=en

[5] Report: Chinese police bust fake Viagra factory, USA Today, http://www.usatoday.com/news/world/2007-02-14-china-viagra_x.htm

[6] Spamhaus Statistics : The Top 10, The SpamHouse Project, http://www.spamhaus.org/statistics/spammers.lasso

[7] Botnet, Wikipedia, http://en.wikipedia.org/wiki/Botnet

[8] Consumer Attitudes Toward Spam in Six Countries, Business Software Alliance, http://cauce.ca/system/files/BSAConsumerAttitudes.pdf